# Ανοικτό Πανεπιστήμιο Κύπρου

**Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

**Μεταπτυχιακό Πρόγραμμα Σπουδών *Στην Ασφάλεια Υπολογιστών και Δικτύων***


Μεταπτυχιακή Διατριβή

## Ανίχνευση Ιστότοπων Ηλεκτρονικού Ψαρέματος με Χρήση Εικόνων Οπτικοποίησης και Βαθιάς Μάθησης


**Χρίστος Κουσιουμής**

**Επιβλέπων Καθηγητής**
**Δρ. Σταύρος Σιαηλής**



**Νοέμβριος 2020**

# Ανοικτό Πανεπιστήμιο Κύπρου

**Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

**Μεταπτυχιακό Πρόγραμμα Σπουδών *Στην Ασφάλεια Υπολογιστών και Δικτύων***


# Μεταπτυχιακή Διατριβή

## Ανίχνευση Ισοτόπων Ηλεκτρονικού Ψαρέματος με Χρήση Εικόνων Οπτικοποίησης και Βαθιάς Μάθησης


**Χρίστος Κουσιουμής**

**Επιβλέπων Καθηγητής**
**Δρ. Σταύρος Σιαηλής**


Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.


**Νοέμβριος 2020**

# Περίληψη

Η ανάγκη για χρήση Διαδικτυακών υπηρεσιών, κατέστησαν το Διαδίκτυο αναπόσπαστο κομμάτι της καθημερινότητας μας. Ωστόσο η απλότητα του βοήθησε τους εγκληματίες του κυβερνοχώρου να εξαπατούν χρήστες και οργανισμούς με τη μέθοδο επίθεσης ηλεκτρονικού ψαρέματος, υποκλέπτοντας χρήματα και ευαίσθητα δεδομένα. Για τον λόγο αυτό, η επιστημονική κοινότητα επέδειξε το ενδιαφέρον μελέτης και αποτελεσματικής αντιμετώπισης αυτού του προβλήματος. Πολλές από τις μεθόδους ανίχνευσης ιστότοπων ηλεκτρονικού ψαρέματος που αναπτύσσονται σε πρόσφατες έρευνες κάνουν χρήση Μηχανικής Μάθησης και Τεχνητών Νευρωνικών Δικτύων τα οποία αποτελούν ένα νέο εργαλείο για την αντιμετώπιση του προβλήματος. Σκοπός της παρούσας μεταπτυχιακής διατριβής είναι να διερευνήσει εάν είναι δυνατή η ανίχνευση ιστότοπων ηλεκτρονικού ψαρέματος δια μέσου οπτικοποίησης του πηγαίου κώδικα HTML, στη βάση τριών καμπύλων οπτικοποίησης σε συνάρτηση, τη χρήση CNN δικτύων και CNN-RNN, καθώς και την αξιολόγηση αυτών με βάση το ποσοστό ακριβείας επικύρωσης. Η εργασία απαρτίζεται από πέντε κεφάλαια. Στο πρώτο κεφάλαιο γίνεται περιληπτική παρουσίαση της βιβλιογραφικής ανασκόπησης σε σχέση με το αντικείμενο της έρευνας, γίνεται ένας σύντομος συμπερασματικός σχολιασμός των ερευνών και ακολούθως τονίζεται η συμβολή της παρούσας μεταπτυχιακής διατριβής στο αναφερθέν αντικείμενο της έρευνας. Στο δεύτερο κεφάλαιο παρουσιάζεται σύντομη ιστορική αναδρομή του ηλεκτρονικού ψαρέματος, η γενική μεθοδολογία επίθεσης και η έκταση που έχει πάρει τα τελευταία χρόνια. Στο τρίτο κεφάλαιο περιγράφονται οι τεχνολογίες και τα εργαλεία που χρησιμοποιήθηκαν για την υλοποίηση του έργου. Στο τέταρτο κεφάλαιο περιγράφεται ο πειραματικός σχεδιασμός ο οποίος αποτελείται από έξι στάδια. Το πρώτο στάδιο αφορά τη συλλογή URL συνδέσμων και την εξαγωγή εικόνων(οπτικοποίησης)του πηγαίου κώδικα HTML με τη χρήση κατάλληλου εργαλείου με στόχο τη δημιουργία dataset. Ακολούθως το δεύτερο, τρίτο, τέταρτο και πέμπτο στάδιο αφορά την εκπαίδευση των νευρωνικών δικτύων MobileNet, MobileNet-RNN, Xception-RNN και Custom-CNN, εν συνεχεία τη δοκιμή αυτών για την κατηγοριοποίηση των εικόνων με στόχο την απάντηση του κατά πόσο ο ιστότοπος αποτελεί ιστότοπο ηλεκτρονικού ψαρέματος ή όχι. Στο έκτο στάδιο παρουσιάζονται τα αποτελέσματα εκπαίδευσης και δοκιμών για κάθε είδος καμπύλης και μοντέλου και γίνεται εξαγωγή συμπερασμάτων. Ακολούθως στο έκτο και τελευταίο κεφάλαιο εξάγονται τελικά συμπεράσματα, παρατηρήσεις καθώς γίνονται προτάσεις οι οποίες πιθανόν να βοηθήσουν στη μελλοντική εξελικτική πορεία της έρευνας στο παρόν αντικείμενο.

## Summary

The need to use online services has made the Internet an integral part of our daily life. However, the user-friendly nature of these services has given rise to cybercrime as both users and organizations are deceived through electronic phishing, stealing of money and sensitive data. Due to this rise, the scientific community has invested a lot in research so as to effectively address this issue. A number of methods that detect websites that deal with phishing have been developed in recent research and make use of machine learning and neural networks which become a new tool for the effective dealing of this problem. The purpose of this postgraduate thesis is to investigate whether it is possible to detect phishing sites through the visualization of the HTML source code, on the basis of three visualization curves in function, the use of CNN networks and CNN-RNN, as well as the evaluation of them based on the rate of accurate validation. The first chapter summarizes the bibliographical review in relation to the subject of this research; a short concluding remark on the research is followed by a highlight of the contribution of this postgraduate thesis to the research subject mentioned. The second chapter presents a brief historical retrospection of phishing along with the general attack methodology and its extent in recent years. In the third chapter, the technology and tools that have been used for the realization of this project are described. The fourth chapter deals with the description of the experimental design in six stages. The first stage concerns the collection of URL links and the extraction of images (visualization) of the Custom HTML source code, using an appropriate tool with the goal of creating a dataset. Subsequently, the third, fourth and fifth stages concern the training of the neural networks MobileNet, , MobileNet-RNN, Xception-RNN and Custom-CNN, followed by the testing of these for the categorization of images in order to answer whether the site is a phishing site or not. In the sixth and final chapter, final conclusions are drawn, observations and proposals are made that may help the future evolutionary course of research in this field.

## Ευχαριστίες

Θέλω να ευχαριστήσω τον επιβλέποντα Καθηγητή της παρούσας μεταπτυχιακής διατριβής κ. Σταύρο Σιαηλή που με παρακίνησε να ασχοληθώ με το συγκεκριμένο θέμα, καθώς και για την γενική επίβλεψή του.

Επίσης, θέλω να ευχαριστήσω τη σύζυγό μου Άννα για τη στήριξη και τη συμπαράστασή της καθ' όλη τη διάρκεια του μεταπτυχιακού προγράμματος καθώς και την πολύ αγαπημένη μου κόρη Ρεγγίνα για την υπομονή και τον χρόνο που μου αφιέρωσε.

# Περιεχόμενα

# Πίνακας Εικόνων

# Πίνακες

# Πίνακας Σχημάτων



# Συντομογραφίες

| Συντομογραφίες | Ορισμοί |
|---|---|
| CNN | Convolutional Neural Network |
| RNN | Recurrent Neural Networks |
| LSTM | Long Short Term Memory |
| URL | Uniform Resource Identifier |
| SVM | Support Vector Machines |
| HTML | Hypertext Markup Language |
| HTTPS | Hypertext Transfer Protocol Secure |
| SSL | Secure Sockets Layer |
| ISTR | Internet Security Threat Report |
| RGB | Red Green Blue |
| APWG | Anti-Phishing Working Group |
| AOL | American OnLine |
| CSS | Cascading Style Sheets |
| AROW | Adaptive Regularization of Weights |

# Κεφάλαιο 1
# Βιβλιογραφική Ανασκόπηση

## 1.1 Εισαγωγή

Το ηλεκτρονικό ψάρεμα σύμφωνα με (Marchal, et al. 2014, 458-471) παραβιάζει τους τρεις βασικούς πυλώνες της ασφάλειας την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Με την πάροδο του χρόνου έχουν προταθεί και εφαρμοστεί ποικίλες προσεγγίσεις για την ανίχνευση επιθέσεων ηλεκτρονικού ψαρέματος (phishing) τόσο σε εμπορικούς όσο και σε δημόσιους τομείς. Στόχος της παρούσας βιβλιογραφικής ανασκόπησης είναι η παρουσίαση μερικών ερευνητικών προσεγγίσεων στο εν λόγω αντικείμενο και η περιγραφή των πλεονεκτημάτων, μειονεκτημάτων και ο εντοπισμός προβλημάτων καθώς και οι τρόποι αντιμετώπισής τους. Ο τελικός στόχος είναι να καταδειχθεί πώς μπορεί η παρούσα μεταπτυχιακή έρευνα να βοηθήσει και να συμβάλει στην ερευνητική κοινότητα για την αντιμετώπιση των ιστότοπων ηλεκτρονικού ψαρέματος(phishing).

## 1.2 Μέθοδοι Ανίχνευσης Ιστότοπων Ηλεκτρονικού Ψαρέματος

### 1.2.1. Συστήματα Ανίχνευσης Βάση Λίστας

Τα συστήματα ανίχνευσης ηλεκτρονικού ψαρέματος βασισμένα σε λίστες είναι μια προσέγγιση αρκετά διαδεδομένη. Τα συστήματα αυτά χρησιμοποιούν δύο λίστες, τη μαύρη λίστα και τη λίστα με τις επιτρεπόμενες διευθύνσεις (Blacklist και Whitelist) για την ταξινόμηση των νόμιμων διευθύνσεων και των διευθύνσεων ηλεκτρονικού ψαρέματος. Τα συστήματα ανίχνευσης ηλεκτρονικού ψαρέματος που βασίζονται στη λίστα επιτρεπόμενων(Whitelist) διευθύνσεων δημιουργούν λίστες από ασφαλείς και νόμιμες ηλεκτρονικές διευθύνσεις για την παροχή των απαραίτητων πληροφοριών. Κάθε διεύθυνση που δεν περιλαμβάνεται στη λίστα επιτρεπόμενων (Whitelist) θεωρείται ύποπτη.

Το 2008 οι Cao, Han και Le (Cao, Han and Le 2008) ανέπτυξαν ένα σύστημα που δημιουργεί μια λίστα επιτρεπόμενων διευθύνσεων καταγράφοντας τη διεύθυνση IP κάθε ιστότοπου που έχει επισκεφτεί ο χρήστης. Όταν ο χρήστης επισκέπτεται έναν ιστότοπο, το σύστημα προειδοποιεί εάν υπάρχει ασυμβατότητα στις καταχωρημένες πληροφορίες του ιστότοπου. Ωστόσο, αυτή η μέθοδος δεν είναι ιδιαίτερα αποτελεσματική γιατί θεωρεί ύποπτους τους νόμιμους ιστότοπους που επισκέφτηκε για πρώτη φορά ο χρήστης . Το 2018 οι Jain και Gupta (Jain and Gupta 2018) ανέπτυξαν μια νέα μέθοδο η οποία προειδοποιεί τους χρήστες για τους νόμιμους ιστοτόπους χρησιμοποιώντας λίστα επιτρεπόμενων διευθύνσεων (Whitelist) η οποία ενημερώνεται αυτόματα. Αυτή η μέθοδος αποτελείται από δύο φάσεις, τη φάση αντιστοίχισης της IP διεύθυνσης και τη φάση εξαγωγής χαρακτηριστικών από τον πηγαίο κώδικα των ιστότοπων. Σύμφωνα με τα πειραματικά αποτελέσματα σε αυτή την έρευνα επιτεύχθηκε 86,02% πραγματικό θετικό ποσοστό και 1,48% ψευδώς αρνητικό ποσοστό.

Οι μαύρες λίστες δημιουργούνται από URL διευθύνσεις, οι οποίες είναι γνωστές ως ιστότοποι ηλεκτρονικού ψαρέματος (phishing). Οι καταχωρήσεις στις λίστες προέρχονται από διάφορες πηγές, όπως συστήματα ανίχνευσης ανεπιθύμητων μηνυμάτων, ειδοποιήσεις χρηστών, από οργανισμούς κ.λπ. Η χρήση μαύρων λιστών καθιστά αδύνατο για τους εισβολείς να επιτεθούν ξανά μέσω των ίδιων διευθύνσεων URL ή των IP, οι οποίες είχαν χρησιμοποιηθεί προηγουμένως για επίθεση. Ο μηχανισμός ασφαλείας ενημερώνει τις μαύρες λίστες είτε εντοπίζοντας κακόβουλες διευθύνσεις URL είτε τις IP διευθύνσεις. Οι χρήστες μπορούν να κατεβάσουν τις λίστες από έναν διακομιστή και να προστατεύσουν τα συστήματά τους από τις διευθύνσεις ηλεκτρονικού ψαρέματος που αναφέρονται στη λίστα. Τα συστήματα που βασίζονται στη μαύρη λίστα, ωστόσο, δεν έχουν τη δυνατότητα να εντοπίσουν μια πραγματική επίθεση ή μια επίθεση που εμφανίζεται για πρώτη φορά (zero_day). Αυτοί οι μηχανισμοί ανίχνευσης επιθέσεων έχουν χαμηλότερο ψευδώς θετικό ποσοστό από τα συστήματα που βασίζονται στη μηχανική μάθηση. Η επιτυχία του συστήματος ανίχνευσης επιθέσεων ηλεκτρονικού ψαρέματος με βάση τη μαύρη λίστα είναι περίπου στο 20% με βάση τους (Khonji, Iraqi and Jones 2013, 2091-2121) και (Sheng, Holbrook, et al. 2010) . Επομένως, φαίνεται ότι τα συστήματα που βασίζονται στη μαύρη λίστα δεν είναι αποτελεσματικά και δεν αποτελούν αξιόπιστο μηχανισμό ανίχνευσης επιθέσεων. Ωστόσο, ορισμένες εταιρείες παρέχουν υπηρεσίες ανίχνευσης επιθέσεων ηλεκτρονικού ψαρέματος χρησιμοποιώντας

συστήματα τα οποία είναι βασισμένα σε μαύρες λίστες (blacklist) , όπως για παράδειγμα το Google Safe Browsing API (Google Safe Browsing 2012), PhishNet (Prakash, et al. 2010, 1-5). Αυτά τα συστήματα χρησιμοποιούν έναν κατά προσέγγιση αλγόριθμο αντιστοίχισης για να ελέγξουν αν η ύποπτη διεύθυνση URL υπάρχει στη μαύρη λίστα ή όχι. Οι προσεγγίσεις που βασίζονται στη μαύρη λίστα απαιτούν συχνές ενημερώσεις. Επιπλέον, η ταχεία ανάπτυξη της μαύρης λίστας απαιτεί υπερβολικούς πόρους συστήματος σύμφωνα με τους (Sharifi και Siadati 2008) και (Sheng, Holbrook, et al. 2010, 373-382).

Εκτός από τις στατικές τεχνικές, οι δυναμικές τεχνικές οι οποίες μπορούν να μάθουν από τα προηγούμενα δεδομένα (ειδικά από μεγάλα δεδομένα) μπορούν να παράγουν μια καλύτερη λύση με τη βοήθεια προσεγγίσεων μηχανικής μάθησης .

### 1.2.2 . Συστήματα Ανίχνευσης με Βάση τη Μηχανική Μάθηση

Μια από τις δημοφιλείς μεθόδους εντοπισμού κακόβουλων ιστότοπων είναι η χρήση μεθόδων μηχανικής μάθησης . Προκειμένου να αναπτυχθεί ένα σύστημα εντοπισμού που βασίζεται στη μάθηση, τα δεδομένα εκπαίδευσης πρέπει να περιέχουν πολλά χαρακτηριστικά τα οποία να σχετίζονται με την κλάση τον νόμιμων ιστότοπων και των ιστότοπων ηλεκτρονικού ψαρέματος. Με τη χρήση ενός αλγορίθμου εκμάθησης, μπορεί να είναι εύκολο να εντοπιστούν οι αόρατες ή μη ταξινομημένες διευθύνσεις URL με έναν δυναμικό μηχανισμό.

Μια από τις προσεγγίσεις με τη χρήση μεθόδων μηχανικής μάθησης είναι η ταξινόμηση πολλαπλών επιπέδων για το φιλτράρισμα των URL διευθύνσεων ηλεκτρονικού ψαρέματος. Οι Suryavanshi και Jain (Suryavanshi and Jain 2015, 41-46) σε αύτη την έρευνα , παρουσίασαν μια καινοτόμα μέθοδος για την εξαγωγή χαρακτηριστικών από το περιεχόμενο των URL συνδέσμων ηλεκτρονικού ψαρέματος. Χρησιμοποιούνται αλγόριθμοι πολλαπλής ταξινόμησης όπως SVM, AdaBoost και Naive Bayes. Αυτοί οι αλγόριθμοι χωρίζονται σε τρία επίπεδα χρησιμοποιώντας 21 διαφορετικά χαρακτηριστικά και στη συνέχεια πραγματοποιείται μια διαδικασία δύο βημάτων με τη βοήθεια ενός άλλου αλγορίθμου ταξινόμησης. Σε αυτή την προσέγγιση υπάρχουν

προβλήματα αναφορικά με τον χρόνο που καταναλώνεται, την πολυπλοκότητα καθώς εμπλέκονται και τα ζητήματα απόδοσης, έτσι δεν αποτελεί μια βέλτιστη μέθοδο.

Στο άρθρο (Le, Markopoulou and Faloutsos 2011, 191-195) οι Le, Markopoulou και Faloutsos αναγνώρισαν τους ιστότοπους ηλεκτρονικού ψαρέματος (phishing) ταξινομώντας τους με χαρακτηριστικά από το URL όπως το μήκος, τον αριθμό των ειδικών χαρακτήρων που παρουσιάζονται, τον κατάλογο, το όνομα του τομέα και το όνομα αρχείου. Το σύστημα ταξινομεί ιστότοπους εκτός σύνδεσης χρησιμοποιώντας τον αλγόριθμο Support Vector Machines. Η προσαρμοστική τακτοποίηση των βαρών, η στάθμιση εμπιστοσύνης και το Perceptron νευρωνικό δίκτυο, χρησιμοποιούνται για διαδικτυακή ταξινόμηση. Σύμφωνα με τα αποτελέσματα των πειραμάτων, η χρήση του αλγόριθμου AROW αυξάνει το ποσοστό ακρίβειας ενώ μειώνει τις απαιτήσεις πόρων του συστήματος.

Στο άρθρο των (Bhagyashree and Tanuja 2015, 46-50) , περιγράφεται μια τεχνική βασισμένη σε χαρακτηριστικά που κατηγοριοποιεί τις URL διευθύνσεις σε διευθύνσεις ηλεκτρονικού ψαρέματος ή νόμιμες διευθύνσεις. Οι συγγραφείς χρησιμοποιούν διάφορα χαρακτηριστικά από τις διευθύνσεις λαμβάνοντας υπόψη τη δομή των URL. Για την ταξινόμηση των URL διευθύνσεων, χρησιμοποιείται ο αλγόριθμος μηχανικής μάθησης Random Forest. Κατασκευάζει έναν ταξινομητή ο οποίος αποφασίζει εάν μια δεδομένη URL είναι διεύθυνση ηλεκτρονικού ψαρέματος (phishing) ή όχι. Επιπλέον, έχει προταθεί ένα νέο σχέδιο για τον εντοπισμό URL διευθύνσεων ηλεκτρονικού ψαρέματος (phishing) ασχολείται με την ελεύθερη πρόσβαση και εξόρυξη περιεχομένου των URL διευθύνσεων.

Στο άρθρο τους οι (Basnet and Doleck 2015, 220-223), χρησιμοποιούνται λειτουργίες που βασίζονται στις URL διευθύνσεις με στόχο να εντοπίσουν αν ένα URL αποτελεί διεύθυνση ηλεκτρονικού ψαρέματος (phishing) ή όχι. Εξορύξαν και διαχώρισαν τα χαρακτηριστικά σε 4 γενικές ομάδες, όπως λεξικά, λέξεις-κλειδιά, μηχανή αναζήτησης και φήμη. Οι συγγραφείς έχουν δείξει ότι μια διεύθυνση URL ηλεκτρονικού "ψαρέματος" μπορεί να αναγνωριστεί χρησιμοποιώντας τα δεδομένα μόνο της URL διεύθυνσης, χωρίς να εξεταστεί το περιεχόμενο του νόμιμου ιστότοπου και ανεξάρτητα από το περιεχόμενο ή το μέσο που διανέμεται η URL διεύθυνση. Το άρθρο αξιολογεί επιπλέον εάν το URL που είναι προσβάσιμο στο κοινό είναι ηλεκτρονικό ψάρεμα (phishing) ή όχι.

Στο άρθρο των (Hoon, Kim and Lee 2015, 131-135), οι συγγραφείς προτείνουν μια διαδικασία αναγνώρισης ηλεκτρονικού ψαρέματος που βασίζεται σε ευρετική μέθοδο (indexing) η οποία χρησιμοποιεί χαρακτηριστικά που βασίζονται σε διευθύνσεις URL. Αυτή η μέθοδος χρησιμοποιεί μερικά χαρακτηριστικά από URL διευθύνσεις από προηγούμενες μελέτες και εισάγει νέες δυνατότητες αναλύοντας τις διευθύνσεις ηλεκτρονικού ψαρέματος. Επίσης, χρησιμοποίησαν διάφορους ταξινομητές μηχανικής μάθησης με σκοπό να επιλέξουν τον καλύτερο ταξινομητή. Η προτεινόμενη μέθοδος μπορεί να παρέχει ασφάλεια σε μεμονωμένα δεδομένα και να μειώσει τα προβλήματα που πηγάζουν από επιθέσεις ηλεκτρονικού ψαρέματος, καθώς επίσης παρέχει και τη δυνατότητα εντοπισμού νέων προσωρινών ιστότοπων ηλεκτρονικού ψαρέματος.

Στο άρθρο (Shinde, et al. 2015, 30-33), παρουσιάζεται ένα μοντέλο που ανακαλύπτει τους ιστότοπους ηλεκτρονικού ψαρέματος. Το μοντέλο χρησιμοποιεί χαρακτηριστικά από το URL και τον HTML κώδικα της ιστοσελίδας για να αποφασίσει εάν πρόκειται για ιστότοπο ηλεκτρονικού ψαρέματος ή όχι. Σε αυτό το πλαίσιο, ο συγγραφέας εφάρμοσε το σύμπλεγμα K-Means για τις τεχνικές πρόβλεψης κατά πόσο, ένας ιστότοπος αποτελεί ιστότοπο ηλεκτρονικού ψαρέματος ή όχι. Εάν εξακολουθεί να μην είναι σε θέση και να αδυνατεί να αποφασίσει για τη νομιμότητα του ιστότοπου τότε εφαρμόζεται ο Naive Bayes ταξινομητής για να δώσει το αποτέλεσμα. Επιπλέον, το εκπαιδευτικό μοντέλο εφαρμόζει εξαγωγή χαρακτηριστικών από το HTML tag του ιστότοπου .

Σε ορισμένες έρευνες (Rao and Pais 2018)οι συγγραφείς χρησιμοποιούν μια υβριδική μέθοδο χρησιμοποιώντας όχι μόνο προσεγγίσεις μηχανικής μάθησης αλλά και έλεγχο εικόνας. Μια σημαντική αδυναμία της ανίχνευσης ηλεκτρονικού ψαρέματος με βάση την εικόνα (οπτικά) είναι η ανάγκη μιας αρχικής βάσης δεδομένων εικόνων ή προηγούμενης γνώσης (ιστορικό του ιστότοπου) σχετικά με την ιστοσελίδα. Ωστόσο, η προτεινόμενη προσέγγιση είναι απαλλαγμένη από αυτές τις εξαρτήσεις. Χρησιμοποίησαν τρεις κατηγορίες χαρακτηριστικών: χαρακτηριστικά τα οποία βασίζονται σε υπερσυνδέσμους, χαρακτηριστικά που βασίζονται σε τρίτους και χαρακτηριστικά από ασαφείς URL διευθύνσεις. Αν και η χρήση υπηρεσιών τρίτων αυξάνει τον χρόνο ανίχνευσης, ωστόσο αυξάνει και το ποσοστό ακρίβειας του συστήματος έως και 99,55%.

Στο άρθρο (Jain and Gupta 2018, 687-700)παρουσιάζεται μια προσέγγιση κατά του ηλεκτρονικού ψαρέματος, η οποία χρησιμοποιεί τη μηχανική μάθηση εξάγοντας 19

χαρακτηριστικά για να αναγνωρίσει τους ιστότοπους ηλεκτρονικού ψαρέματος από τους νόμιμους. Χρησιμοποιήθηκαν 2141 σελίδες ηλεκτρονικού ψαρέματος από το PhishTank και το Openfish, καθώς και 1918 νόμιμες ιστοσελίδες από δημοφιλείς ιστότοπους της Alexa καθώς από κάποιες διαδικτυακές πύλες πληρωμών και ιστότοπους τραπεζικών συναλλαγών. Με τη χρήση της μηχανικής μάθησης, η προτεινόμενη προσέγγιση άγγιξε πραγματικό θετικό ποσοστό στο 99,39%.

Στο άρθρο (Feng, et al. 2018)προτείνεται μια νέα μέθοδος ταξινόμησης βασισμένη σε νευρωνικό δίκτυο για την ανίχνευση ιστοσελίδων ηλεκτρονικού ψαρέματος χρησιμοποιώντας τον αλγόριθμο Monte Carlo και την αρχή ελαχιστοποίησης κινδύνου. Χρησιμοποίησαν 30 χαρακτηριστικά τα οποία κατηγοριοποιούνται σε τέσσερις κύριους τομείς και αφορούν τα χαρακτηριστικά που βασίζονται στη γραμμή διευθύνσεων, τα χαρακτηριστικά που βασίζονται στις μη φυσιολογικές γραμμές διευθύνσεων, τα HTML χαρακτηριστικά και τα χαρακτηριστικά από JavaScript και το domain . Το σύστημα ανίχνευσης φτάνει στο 97,71% ποσοστό ακρίβειας και 1,7% ψευδώς θετικό ποσοστό στις πειραματικές μελέτες.

## 1.3 Σύντομος Σχολιασμός Μελετών

Πιο πάνω παρουσιάστηκαν μερικές από μια πληθώρα μελετών , που ασχολούνται με το αντικείμενο ανίχνευσης ιστότοπων ηλεκτρονικού ψαρέματος. Σύμφωνα με αυτές τις μελέτες καταδεικνύεται ότι οι μέθοδοι για ανίχνευση ιστότοπων ηλεκτρονικού ψαρέματος ποικίλουν καθώς βασίζονται σε ένα ευρύ φάσμα τεχνικών. Η μέθοδος ανίχνευσης ιστότοπων ηλεκτρονικού ψαρέματος όπως παρουσιάστηκε πιο πάνω, συνιστά τη χρήση και ανάπτυξη της Τεχνητής Νοημοσύνης με συνάρτηση τη Μηχανική Μάθηση. Η παρούσα μεταπτυχιακή διατριβή επιδιώκει να προσφέρει μια ακόμα εναλλακτική μέθοδο μέσω της οπτικοποίησης του πηγαίου κώδικα, τη χρήση της Τεχνητής Νοημοσύνης και της Βαθιάς Μηχανικής Μάθησης, η οποία θα συμβάλει όσο το δυνατόν στον εμπλουτισμό της υπάρχουσας γνώσης, καθώς και στην ανίχνευση ιστότοπων ηλεκτρονικού ψαρέματος.

## 1.4 Συμβολή Παρούσας Μεταπτυχιακής Διατριβής

Σε αυτή τη μεταπτυχιακή διατριβή, χρησιμοποιήθηκαν και υλοποιήθηκαν μοντέλα εκπαίδευσης CNN καθώς και CNN-RNN μέσω της βιβλιοθήκης Keras TensorFlow της Google κάτω από γλώσσα υψηλού επιπέδου Python. Η χρήση αυτής της μεθόδου επιλέχθηκε με σκοπό την άμεση εξόρυξη δεδομένων και τη σύγκριση της ακρίβειας επικύρωσης των μοντέλων. Τα μοντέλα εκπαιδεύτηκαν με στόχο να αναγνωρίζουν ιστότοπους ηλεκτρονικού ψαρέματος από τις εικόνες που δημιουργήθηκαν από τα δεδομένα του HTML κώδικα. Στην παρούσα μέθοδο δε λήφθηκαν υπόψη χαρακτηριστικά που βασίζονται στη γραμμή διευθύνσεων ή σε χαρακτηριστικά που βασίζονται σε υπερσυνδέσμους. Αντίθετα χρησιμοποιήθηκε η μέθοδος οπτικοποίησης (visualization) του περιεχομένου του HTML κώδικα που σχετίζεται με ιστότοπους ηλεκτρονικού ψαρέματος καθώς και νόμιμους ιστότοπους. Κατά των έλεγχο των εικόνων αυτών με τη χρήση των συνελικτικών νευρωνικών δικτύων καθώς και παράλληλων συνελικτικών δικτύων με δίκτυα ανατροφοδότησης, προέκυψαν τα τελικά συμπεράσματα και απαντήθηκαν σημαντικά ερωτήματα αναφορικά με τη μέθοδο οπτικοποίησης καθώς και με το ποσοστό ακρίβειας επικύρωσης ενός ιστότοπου ως ιστότοπο ηλεκτρονικού ψαρέματος ή όχι.

Η μέθοδος της έρευνας, υλοποιήθηκε για τον εντοπισμό ιστότοπων ηλεκτρονικού ψαρέματος, στη βάση ενός dataset το οποίο συλλέχθηκε από διάφορες βάσεις δεδομένων συνδέσμων ηλεκτρονικού ψαρέματος. Στο dataset απεικονίζονται ιστότοποι με χαρακτηριστικά σύνδεσης (login) από πολύ γνωστές επωνυμίες. Οι παραχθείσες εικόνες χρησιμοποιήθηκαν για την εκπαίδευση των μοντέλων Βαθιάς Μηχανικής Μάθησης. Σκοπός ήταν να αναγνωριστεί αν κατά πόσο ή οπτικοποίηση του HTML κώδικα μπορεί να παρουσιάσει χαρακτηριστικά τα οποία να βοηθήσουν στην αναγνώριση ενός ιστότοπου ηλεκτρονικού ψαρέματος, να εξαχθούν συγκριτικά αποτελέσματα με βάση τρεις τύπους εικόνων οπτικοποίησης με βάση της καμπύλες Hilbert , Zigzag και Zorder, καθώς επίσης και να παρουσιαστούν συγκριτικά αποτελέσματα στη βάση του ποσοστού ακριβείας του κάθε μοντέλου. Τα βήματα που ακολουθήθηκαν για την ολοκλήρωση της έρευνας και την εξαγωγή των συμπερασμάτων είναι τα ακόλουθα:

- Συλλογή συνδέσμων ιστότοπων ηλεκτρονικού ψαρέματος και νόμιμων ιστότοπων.

- Απόξεση του HTML κώδικα και οπτικοποίηση του (δημιουργία εικόνων).
- Διαχωρισμός του συνόλου των δεδομένων σε εικόνες εκπαίδευσης(training), επικύρωσής (validation) και δοκιμής(test).
- Δημιουργία και εκπαίδευση μοντέλων με το πρόγραμμα Keras TensorFlow. Ακολούθως έγινε εξέταση της συμπεριφοράς των εικόνων του σετ δοκιμών(test), την οποία θέσαμε είτε ως (phishing) είτε ως (legitimate) με το ανάλογο ποσοστό ακριβείας.
- Εξαγωγή συμπερασμάτων.

# Κεφάλαιο 2
# Ηλεκτρονικό Ψάρεμα

## 2.1 Εισαγωγή

Στον κόσμο του κυβερνοχώρου, οι περισσότεροι άνθρωποι επικοινωνούν μεταξύ τους είτε μέσω υπολογιστή είτε μέσω ψηφιακών συσκευών που είναι συνδεδεμένες στο Διαδίκτυο. Ο αριθμός των ατόμων που χρησιμοποιούν υπηρεσίες διαδικτυακών τραπεζικών συναλλαγών, ηλεκτρονικές αγορές και άλλες διαδικτυακές υπηρεσίες αυξάνεται λόγω της εύκολης πρόσβασης, της γρήγορης εξυπηρέτησης καθώς και της βοήθειας που υπάρχει. Ένας εισβολέας παίρνει αυτήν την κατάσταση ως ευκαιρία να κερδίσει χρήματα ή φήμη κλέβοντας ευαίσθητες πληροφορίες οι οποίες απαιτούνται για την πρόσβαση σε διαδικτυακούς ιστότοπους παροχής υπηρεσιών. Το ηλεκτρονικό ψάρεμα "phishing" είναι ίσως η πιο δημοφιλής και εύκολη εκτέλεση επίθεσης και αποτελεί απειλή για οργανισμούς, ιδρύματα και απλούς χρήστες.

## 2.2 Σύντομη Ιστορική Αναδρομή

Το ηλεκτρονικό ψάρεμα (phishing), αποτελεί πρακτική απόκτησης διαπιστευτηρίων υπολογιστή από χρήστες μέσω χειραγώγησης ή εξαπάτησης, χρονολογείται τουλάχιστον 25 χρόνια στην AOL, όπου κακόβουλοι χρήστες πλαστοπροσώπησαν τα μέλη του προσωπικού της AOL και έστειλαν άμεσα μηνύματα σε άλλους χρήστες και τους έπεισαν να αποκαλύψουν κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών. Ο ίδιος ο όρος επινοήθηκε από τον Koceilah Rekouche, έναν χάκερ γνωστό στο διαδίκτυο με το ψευδώνυμο Da Chronic, ο οποίος δημιούργησε ένα εργαλείο για την αυτοματοποίηση και την επιτάχυνση αυτής της διαδικασίας το 1995. Η χειροκίνητη διαδικασία ονομάστηκε μερικές φορές ως ψάρεμα (όπως η αναζήτηση κωδικών πρόσβασης) , και ο Rekouche χαρακτήρισε τη μέθοδο κλοπής κωδικού πρόσβασης του λογισμικού του “phishing” - ο όρος και η μέθοδος εδραιώθηκε και στη συνέχεια επεκτάθηκε πολύ πέρα από την AOL τις τελευταίες τρεις δεκαετίες.

## 2.3 Γενική Μεθοδολογία Επιθέσεων Ηλεκτρονικού Ψαρέματος

Οι περισσότερες επιθέσεις ηλεκτρονικού ψαρέματος λειτουργούν δημιουργώντας ψεύτικες εκδόσεις αυθεντικών ή νόμιμων ιστοσελίδων με σκοπό να αποκτήσουν την εμπιστοσύνη του χρήστη και στη συνέχεια να αποστείλουν πλαστά μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία θα περιέχουν ένα ή περισσότερους συνδέσμους URL. Αυτός ο σύνδεσμος όταν πατηθεί, οδηγεί σε μια ψεύτικη ιστοσελίδα. Στις περισσότερες περιπτώσεις αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου μοιάζουν με επαγγελματικά και εξουσιοδοτημένα, ζητώντας από μεμονωμένα άτομα ευαίσθητα δεδομένα. Ένα κλασικό παράδειγμα επίθεσης ηλεκτρονικού ψαρέματος είναι όταν ο επιτιθέμενος (phisher) στέλνει χιλιάδες μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν μια δελεαστική και συνάμα ελκυστική προσφορά λέγοντας ότι «έχετε κερδίσει ένα πακέτο διακοπών ή ότι θα λάβετε δάνειο με πολύ χαμηλό επιτόκιο» κ.τ.λ. και ζητά από τον χρήστη να κάνει κλικ σε έναν σύνδεσμο. Όταν ο χρήστης το πράξει, θα του ζητηθεί να συμπληρώσει ευαίσθητα δεδομένα όπως τον αριθμό της πιστωτικής κάρτας και τον αριθμό λογαριασμού κ.τ.λ. Μόλις συμπληρώσει τα δεδομένα, η εργασία του phisher ολοκληρώνεται. Μπορεί να πουλήσει αυτά τα δεδομένα ή να τα χρησιμοποιήσει για κακόβουλο σκοπό. Αρκετές φορές οι ψεύτικοι ιστότοποι οι οποίοι είναι αντίγραφα νόμιμων ιστότοπων (για παράδειγμα, PayPal, Amazon κ.λπ.) φιλοξενούνται σε δωρεάν ή επί πληρωμής διακομιστές. Αυτούς τους ιστότοπους σε πολλές περιπτώσεις είναι σχεδόν αδύνατο να τους διακρίνει το ανθρώπινο μάτι αν ανήκουν στους νόμιμους ιστότοπους ή στους ιστότοπους ηλεκτρονικού ψαρέματος.

## 2.4 Παραδείγματα Μηνυμάτων Ηλεκτρονικού Ψαρέματος

Ακολουθούν παραδείγματα επιθέσεων ηλεκτρονικού ψαρέματος που υποβάλλονται στο (Reporting n.d.) και APWG ( Anti-Phishing Working Group). Η Εικόνα 1 αποτελεί ένα γενικό μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο στοχεύει σε όποιο παραλήπτη κατέχει PayPal λογαριασμό. Το λεξιλόγιο και οι εκφράσεις που χρησιμοποιούνται έχουν σκοπό να κερδίσουν την εμπιστοσύνη του παραλήπτη. Επίσης χρησιμοποιούνται και

λέξεις-κλειδιά όπως <<περιορισμός λογαριασμού>> ή και το <<τελικό κλείσιμο του λογαριασμού>>. Μέσω των απειλών γίνεται προσπάθεια να πανικοβάλει τον αναγνώστη ο επιτιθέμενος ώστε να προβεί στο άνοιγμα του συνδέσμου URL για να καταχωρήσει τα διαπιστευτήρια του προσωπικού του λογαριασμού ή άλλα σημαντικά δεδομένα.

Οι επιτιθέμενοι συχνά χρησιμοποιούν γνωστά ονόματα εταιρειών ή προσποιούνται ότι είναι κάποιος γνωστός. Στην Εικόνα 2 είναι ένα άλλο μήνυμα ηλεκτρονικού ταχυδρομείου της γνωστής εταιρείας Netflix. Αποτελεί ένα μήνυμα ηλεκτρονικού ψαρέματος που έχει σχεδιαστεί για να υποκλέψει προσωπικά στοιχεία. Το email υποστηρίζει ότι ο λογαριασμός του χρήστη είναι σε αναμονή γιατί το Netflix αντιμετωπίζει κάποια προβλήματα με τα τρέχοντα στοιχεία χρέωσης και καλεί τον χρήστη να κάνει κλικ σε έναν σύνδεσμο για να ενημερώσει τον τρόπο πληρωμής του. Ο σύνδεσμος μπορεί να κατευθύνει τον χρήστη σε ένα παράνομο ιστότοπο ηλεκτρονικού ψαρέματος ο οποίος θα βοηθήσει τον επιτιθέμενο να υποκλέψει τα διαπιστευτήρια του χρήστη ή πιθανόν να εγκατασταθεί κακόβουλο λογισμικό (ransomware) ή αλλά προγράμματα που μπορούν να κλειδώσουν τα δεδομένα του χρήστη.


PayPal

Security Center

Military Grade Encryption is Only the Start

At PayPal, we want to increase your security and comfort level with every transaction. From our Buyer and Seller Protection Policies to our Verification and Reputation systems, we'll help to keep you safe.

PayPal is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

Recently, our Account Review Team identified some unusual activity in your account. In accordance with PayPal's User Agreement access to your account will be limited. This is a fraud prevention measure meant to ensure that your account is not compromised.

In order to secure your account we may require some specific information from you. We encourage you to log in by clicking on the link below and complete the requested form as soon as possible.

https://wwwpaypal.com/cgi-bin/webscr?cmd=_login-run

Ignoring our request, for an extended period of time, may result in account limitations or may result in eventual account closure.

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account
We apologize for any inconvenience.

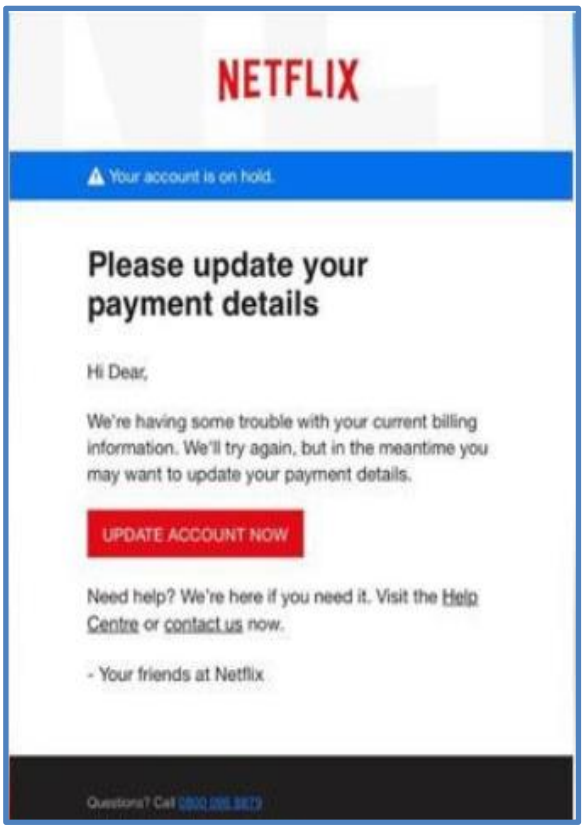
Sincerely,
PayPal Account Review Department

PayPal Email ID PP4392

*Please do not respond to this e-mail as your reply will not be received.

PayPal VERIFIED

**Εικόνα 1.** PayPal phishing Email


NETFLIX

Your account is on hold.

Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

Need help? We're here if you need it. Visit the Help Centre or contact us now.

- Your friends at Netflix

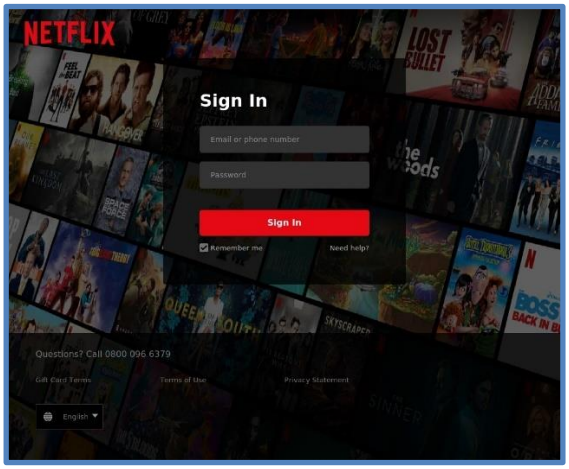
Questions? Call

**Εικόνα 2.** Netflix phishing Email

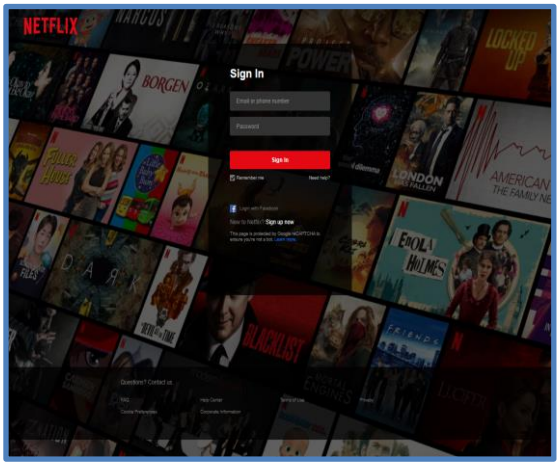
Οι ιστότοποι ηλεκτρονικού ψαρέματος δημιουργούνται όπως προαναφέρθηκε για να εξαπατήσουν ανυποψίαστους χρήστες κάνοντας τους να πιστεύουν ότι βρίσκονται σε νόμιμο ιστότοπο. Για να προσδιορίσει εάν ο ιστότοπος είναι νόμιμος ή αποτελεί έναν καλοσχεδιασμένο ψεύτικο θα πρέπει να ελεγχθούν μερικοί βασικοί δείκτες για να εξακριβωθεί η αυθεντικότητά του.

- Να γίνει έλεγχος της διεύθυνσης URL και SSL.
- Να αξιολογηθεί το περιεχόμενο του ιστότοπου.

Το πρώτο βήμα είναι η μετάβαση στη διεύθυνση URL και ο οπτικός έλεγχος της εγκυρότητάς της. Τα απλά ορθογραφικά λάθη , τα γραμματικά λάθη ή εικόνες χαμηλής ανάλυσης είναι σημεία τα οποία προδίδουν τους ιστότοπους ηλεκτρονικού ψαρέματος. Ωστόσο μερικοί ιστότοποι είναι πολύ καλά κατασκευασμένοι και είναι αρκετά δύσκολο να διακριθούν από το αντίστοιχο ντόμινο ιστότοπο. Όπως βλέπουμε στις πιο κάτω Εικόνες 3 και 4 , είναι πολύ δύσκολο να διακριθεί οπτικά ποια από τις δύο ιστοσελίδες είναι νόμιμη.

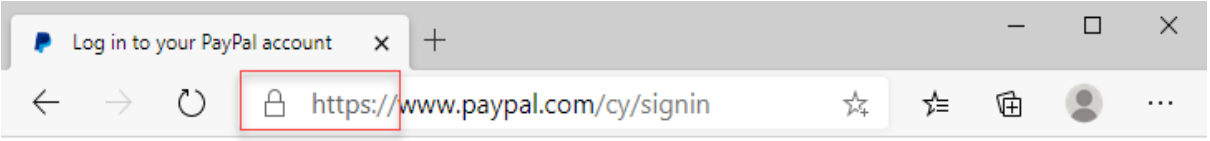



**Εικόνα 3**. Phishing Netflix Login




**Εικόνα 4.** Αυθεντική Netflix Login

Η μετάβαση στο σύνδεσμο URL και ο έλεγχος εγκυρότητάς του βλέποντας αν ξεκινά με κεφαλίδα "https://" ή "shttp://" αποτελεί ένα ακόμα σημείο διερεύνησης, όπως φαίνεται στην Εικόνα 5, το οποίο μπορεί να βοηθήσει στην αναγνώριση του ιστότοπου ως νόμιμου η μη. Το "s" υποδηλώνει ότι η διεύθυνση ιστού έχει κρυπτογραφηθεί και ασφαλιστεί με πιστοποιητικό SSL.




**Εικόνα 5.** Παράδειγμα SSL

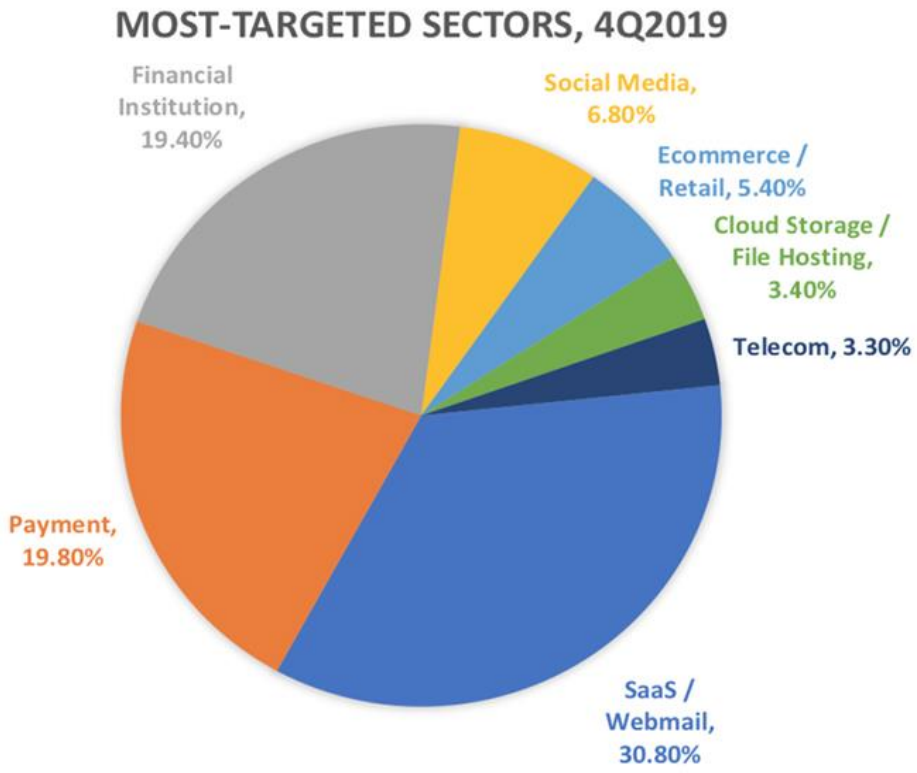
Ωστόσο η ένδειξη HTTPS δε διασφαλίζει απόλυτα την αυθεντικότητα της διεύθυνσης ιστού. Οι επιτιθέμενοι εξέλιξαν τους ιστότοπους ηλεκτρονικού ψαρέματος (phishing) και κατασκεύασαν ιστότοπους που χρησιμοποιούν το HTTPS πρωτόκολλο. Σύμφωνα με την έκθεση (Phishing Activity Trends Report 1st Quarter 2019) από το (ANWG) με τη χρήση αυτής της τακτικής έχουν αυξηθεί οι επιθέσεις ηλεκτρονικού ψαρέματος έως και 58%.

## 2.5. Έκταση Προβλήματος

Αυτός ο τύπος επίθεσης στον κυβερνοχώρο εξακολουθεί να είναι κοινός και διαδεδομένος στη σύγχρονη εποχή. Μέσα από έρευνα στο (Wombat 2019) το 2018 το 83% των ερωτηθέντων δηλώνουν ότι υπέστησαν επιθέσεις ηλεκτρονικού ψαρέματος , οι οποίες ήταν αρκετά αυξημένες σε σχέση με το 2017 που ήταν στο 73% . Οι επιθέσεις ηλεκτρονικού ψαρέματος αυξάνονται κάθε χρόνο λόγω της αύξησης του αριθμού των χρηστών του Διαδικτύου. Σύμφωνα με την έκθεση (Phishing Activity Trends Report 1st Quarter 2018) του APWG, εντοπίστηκαν 263.538 επιθέσεις ηλεκτρονικού ψαρέματος κατά το πρώτο τρίμηνο του 2018 και παρατηρήθηκε ότι το 39,4% των επιθέσεων αυτών είχαν στόχο τον τομέα των πληρωμών. Σε αναφορά της (RSA 2018) Q1 μια παγκόσμια εταιρεία που βασίζεται στην ασφάλεια του κυβερνοχώρου, εκτίμησε ότι η μέση αξία των παράνομων συναλλαγών στην Αμερική ήταν 508 δολάρια, αξία η οποία είναι 144% υψηλότερη από τη μέση αξία των νόμιμων συναλλαγών. Αυτές οι συναλλαγές πραγματοποιούνται κάνοντας χρήση κλεμμένων στοιχείων από πιστωτικές κάρτες ή άλλες ευαίσθητες πληροφορίες όπως για παράδειγμα κωδικούς πρόσβασης, αριθμούς κοινωνικών ασφαλίσεων αριθμούς ταυτότητας κ.τ.λ. Το ηλεκτρονικό ψάρεμα (Phishing) αποτελεί ένα από τα εργαλεία που χρησιμοποιούν οι επιτιθέμενοι για να κλέψουν ευαίσθητες πληροφορίες τις οποίες εκμεταλλεύονται για να προβούν σε παράνομες συναλλαγές.

Σύμφωνα με την έκθεση του APWG ο συνολικός αριθμός ιστότοπων ηλεκτρονικού ψαρέματος (Phishing) που εντοπίστηκε από την ομάδα εργασίας κατά του ηλεκτρονικού ψαρέματος από τον Οκτώβριο μέχρι τον Δεκέμβριο του 2019 ανήλθε στις 162.155. Ακολούθως από τον Ιούλιο μέχρι τον Σεπτέμβριο του 2019 καταγράφηκε ο υψηλότερος αριθμός που ανήλθε στις 266.387.

Οι περισσότεροι ιστότοποι ηλεκτρονικού ψαρέματος στοχεύουν σε χρήστες - οργανισμούς που χρησιμοποιούν συστήματα ηλεκτρονικού ταχυδρομείου τα οποία φιλοξενούνται στον ιστό, σε εταιρικά συστήματα ηλεκτρονικού ταχυδρομείου, σε μέσα κοινωνικής δικτύωσης καθώς και σε ηλεκτρονικά μέσα πληρωμών. Σκοπός τους η αύξηση του αριθμού των πιθανών θυμάτων. Στην Εικόνα 6 παρουσιάζεται το ποσοστό των πιο συχνών στόχων επίθεσης το 2019 με βάση το (Help Net Security n.d.)




**Εικόνα 6.** Ποσοστά πιο συχνών στόχων επίθεσης το 2019

Το ηλεκτρονικό ψάρεμα εξακολουθεί να προκαλεί μεγάλη ανησυχία όχι μόνο λόγω της αύξησης του αριθμού των επιθέσεων ηλεκτρονικού ψαρέματος, αλλά και λόγω των εξελιγμένων μεθόδων που χρησιμοποιούν οι επιτιθέμενοι για την εκτέλεση των επιθέσεων.

## 2.5. Επίλογος

Σύμφωνα με τα προαναφερθέντα στατιστικά στοιχεία οι επιθέσεις ηλεκτρονικού ψαρέματος παρουσιάζουν μια εξελικτική και συνάμα αυξητική τάση η οποία αποτελεί απειλή για οργανισμούς, ιδρύματα και απλούς χρήστες. Αναφορικά με τα πιο πάνω είναι προφανής η ανάγκη για περεταίρω έρευνα και εφαρμογή καινοτόμων μεθόδων για την αντιμετώπιση των επιθέσεων.

# Κεφάλαιο 3
# Τεχνολογίες που Χρησιμοποιήθηκαν

Για την υλοποίηση της μεταπτυχιακής διατριβής χρησιμοποιήθηκαν οι ακόλουθες τεχνολογίες οι οποίες βοήθησαν στη διεξαγωγή της πειραματικής διαδικασίας και την εξαγωγή αποτελεσμάτων.

## 3.1 Python Βιβλιοθήκη Requests

Η βιβλιοθήκη Requests και η μέθοδος get() χρησιμοποιήθηκε για την απόξεση των ιστότοπων. Η βιβλιοθήκη Requests επιτρέπει την αποστολή HTTP αιτήματος χρησιμοποιώντας γλώσσα Python. Υποβάλλοντας ένα HTTP αίτημα για μια ιστοσελίδα χρησιμοποιώντας την get() μέθοδο, ανακτάται ο πηγαίος κώδικας (source code) και αποθηκεύεται το περιεχόμενο τοπικά σε μορφή συμβολοσειράς. Κατά την περίοδο των αρχικών δοκιμών απόξεσης ιστότοπων, παρατηρήθηκαν σημαντικές διαφορές μεταξύ του πηγαίου κώδικα των νόμιμων ιστότοπων και των ιστότοπων ηλεκτρονικού ψαρέματος. Οι νόμιμοι ιστότοποι περιέχουν πολλούς συνδέσμους (script), κώδικα ελέγχου ταυτότητας καθώς αρκετές φορές έχουν περισσότερο όγκο συμβολοσειρών. Σε αντίθεση οι ιστότοποι ηλεκτρονικού ψαρέματος περιέχουν συνδέσμους εικόνων καθώς και βασικές φόρμες εισαγωγής δεδομένων. Οι αρχικές δοκιμές έδωσαν θετικά αποτελέσματα καθώς κατά τη φάση της διαμόρφωσης των συμβολοσειρών σε εικόνα είναι αναμενόμενο να προκύπτουν ορατές διαφορές οι οποίες θα βοηθήσουν στη φάση της εκπαίδευσης των μοντέλων βαθιάς μηχανικής μάθησης.

## 3.2 BinVis.IO

Το BinVis.io αποτελεί ένα διαδικτυακό εργαλείο που επιτρέπει οπτική ανάλυση και εξερεύνηση δυαδικών αρχείων. Ο δημιουργός του Binvis.io, Aldo Cortesi (Cortesi 2015), για μεγάλο χρονικό διάστημα πειραματίζεται με την οπτικοποίηση δεδομένων και έχει χρησιμοποιήσει το εργαλείο για οπτικοποίηση της εντροπίας σε δυαδικά αρχεία, καθώς επίσης και σε εφαρμογές κατηγοριοποίησης κακόβουλων λογισμικών malwares. Το Binvis.io παρέχει τη δυνατότητα εξαγωγής δυαδικής οπτικοποίησης και χαρτογράφησης αρχείων κάνοντας χρήση των καμπύλων Hilbert Curve, Z-order Curve και Zigzag Curve. Το εργαλείο λαμβάνει μεμονωμένους χαρακτήρες και με μια πληθώρα χρωμάτων κωδικοποίησης, καταχωρεί κατάλληλο (RGB- Red Green Blue) χρώμα στον κάθε χαρακτήρα και εξάγει την εικόνα με τα ανάλογα χαρακτηριστικά της κάθε καμπύλης. Στις πιο κάτω Εικόνες 7,8 και 9 παρουσιάζεται ένα παράδειγμα χρωματικής κωδικοποίησης της λέξης "password" με τη χρήση πηγαίου κώδικα του (Cortesi 2015) κάτω από γλώσσα προγραμματισμού python .

- **Καμπύλη Hilbert**

"password" σε hex '' 70 61 73 73 77 6f 72 64 0a ''

**Εικόνα 7.** Δημιουργία εικόνας Hilbert

- **Καμπύλη Zigzag**

"password" σε hex '' 70 61 73 73 77 6f 72 64 0a ''

**Εικόνα 8.** Δημιουργία εικόνας Zigzag

- **Καμπύλη Z-order**

“password” σε hex ’’ 70 61 73 73 77 6f 72 64 0a ’’

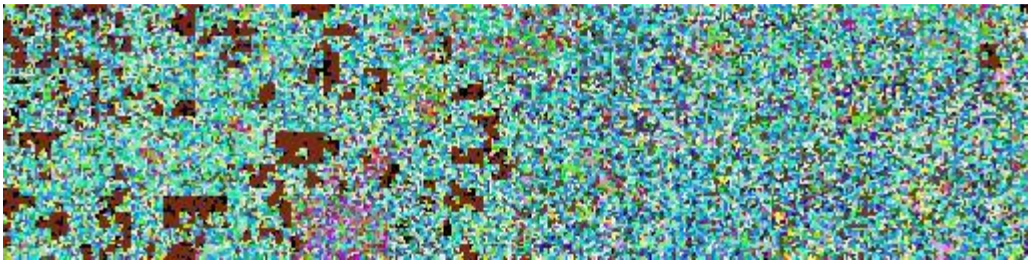
**Εικόνα 9.** Δημιουργία εικόνας Z-order

Σύμφωνα με τις πιο πάνω Εικόνες 6, 7 και 8, διαφαίνεται η κωδικοποίηση κάθε χαρακτήρα της λέξης “password” σε δεκαεξαδική τιμή καθώς και η μετατροπή του σε ένα χρώμα (RGB).

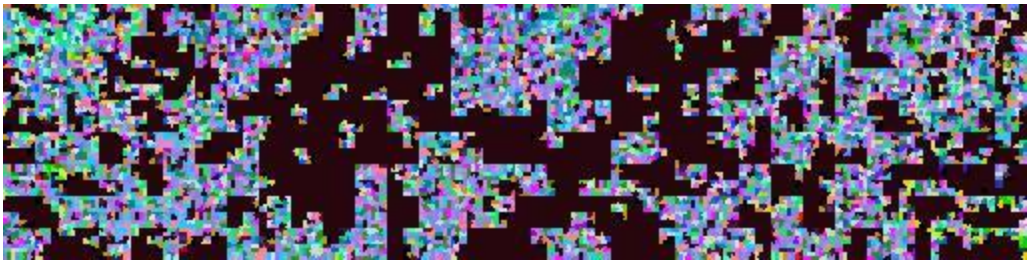
Χρησιμοποιώντας τον πηγαίο κώδικα του εργαλείου Binvis.io, ορίζονται ως δεδομένα εισόδου η απόξεσή (scarping) του HTML ιστότοπου . Ο μεγάλος όγκος συμβολοσειρών του πηγαίου κώδικα ενός ιστότοπου επιφέρει στην έξοδο του Binvis μια δυσνόητη εικόνα. Ο κάθε χαρακτήρας – συμβολοσειρά η οποία περιέχεται στον πηγαίο κώδικα HTML, κωδικοποιείται και μετατρέπεται σε μια καθορισμένη RGB τιμή. Τα χρώματα αντιστοιχούν στην κάθε συμβολοσειρά και λαμβάνουν την ανάλογη διάσταση σε σχέση με την καμπύλη χρήσης όπως προαναφέρθηκε. Το μέγεθος της παραγόμενης εικόνας είναι σταθερό και καθορισμένο εξαρχής στα 128 εικονοστοιχεία. Σε αναλογία του όγκου των δεδομένων εισόδου που λαμβάνει το εργαλείο, δημιουργείται μια εικόνα σταθερού μεγέθους αλλά διαφορετικής πυκνότητας. Η κάθε εικόνα που δημιουργείται, αποθηκεύεται με ένα μοναδικό όνομα το οποίο παράγεται από συνδυασμό δεδομένων, χαρακτηριστικό όνομα του URL τη διεύθυνση URL και την τρέχουσα χρονική στιγμή.

Οι πιο κάτω Εικόνες 10 και 11, αποτελούν εικόνες εξόδου καμπύλης Hilbert ενός νόμιμου ιστότοπου και ενός ιστότοπου ηλεκτρονικού ψαρέματος, του ιστότοπου σύνδεσης της Amazon. Διακρίνονται σαφείς και εμφανείς διαφορές ανάμεσα στις δύο εικόνες. Η Εικόνα 10 του νόμιμου ιστότοπου περιέχει περισσότερη πληροφορία λόγω συνήθως του αυξημένου αριθμού υπερσυνδέσεων, του αριθμού των φορμών εισαγωγής στοιχείων καθώς και των αδειών χρήσης. Σε αντίθεση με την Εικόνα 11 του παράνομου ιστότοπου ηλεκτρονικού ψαρέματος, διακρίνεται λιγότερη πληροφορία λόγω πιθανής έλλειψης

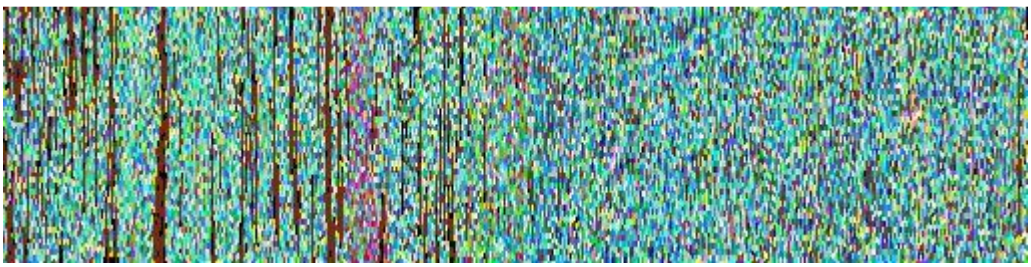
αριθμού υπερσυνδέσεων, μη χρήσης (CSS), χρήσης μόνο μιας φόρμας εισαγωγής στοιχείων καθώς επίσης και έλλειψη σεναρίων ασφαλείας (Security Scripts). Οι διαφορές μεταξύ των εικόνων είναι προφανείς, όπως προφανείς είναι και οι διαφορές που διαφαίνονται μεταξύ των Εικόνων 12 και 13 της καμπύλής Zigzag και αντίστοιχα των Εικόνων 14 και 15 της καμπύλης Zorder, γεγονός το οποίο επιφέρει θετικό αποτελέσματα κατά την εκπαίδευση και δοκιμή των μοντέλων μας.



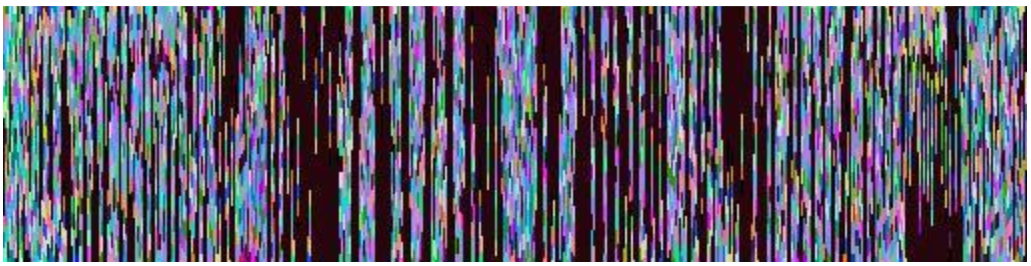
**Εικόνα 10.** Hilbert Νόμιμος Ιστότοπος Σύνδεσης Amazon



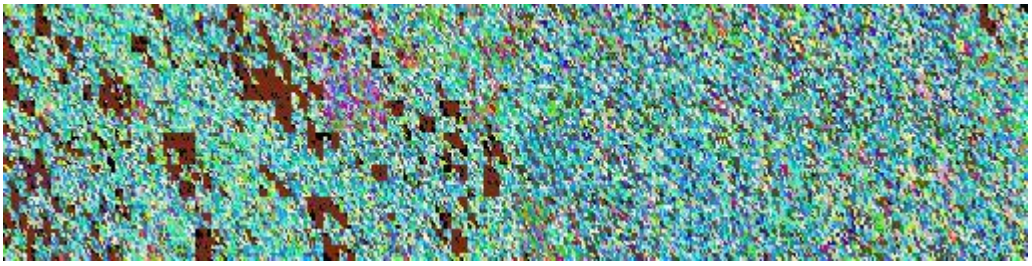
**Εικόνα 11.** Hilbert Ιστότοπος Σύνδεσης Ηλεκτρονικού Ψαρέματος Amazon



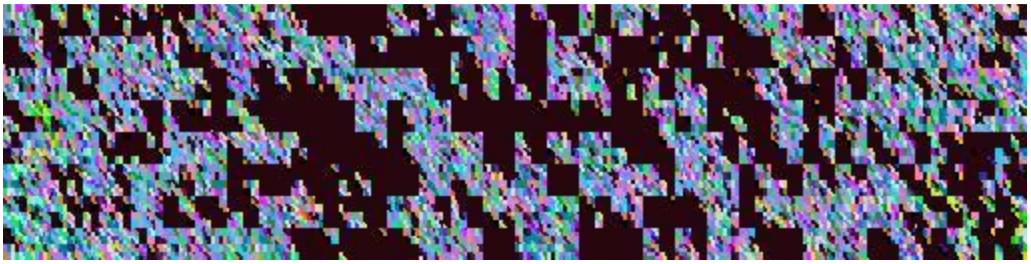
**Εικόνα 12.** Zigzag Νόμιμος Ιστότοπος Σύνδεσης Amazon



**Εικόνα 13.** Zigzag Ιστότοπος Σύνδεση Ηλεκτρονικού Ψαρέματος Amazon



**Εικόνα 14.** Z-order Νόμιμος Ιστότοπος Σύνδεσης Amazon



**Εικόνα 15.** Z-order Ιστότοπος Σύνδεσης Ηλεκτρονικού Ψαρέματος Amazon

## 3.3 Keras-TensorFlow

Το Keras είναι ένα API βαθιάς Μηχανικής Μάθησης ή μια βιβλιοθήκη νευρωνικών δικτύων υψηλού επιπέδου που λειτουργεί πάνω από την πλατφόρμα μηχανικής μάθησης TensorFlow της Google και είναι γραμμένο σε γλώσσα προγραμματισμού Python. Στη βαθιά Μηχανική Μάθηση η χρήση του Keras επιτρέπει την εύκολη και γρήγορη δημιουργία πρωτοτύπων καθώς και την απρόσκοπτη λειτουργία σε CPU και GPU. Στη μεταπτυχιακή διατριβή το Keras χρησιμοποιήθηκε ως εργαλείο για τη δημιουργία και εκπαίδευση των μοντέλων. Τα μοντέλα από βαθιά συνελικτικά νευρωνικά δίκτυα χρειάζονται αρκετό χρόνο εκπαίδευσης σε πολύ μεγάλα σύνολα δεδομένων. Μια μέθοδος συντόμευσης αυτής της διαδικασίας είναι η χρήση των βαρών από προ-εκπαιδευόμενα

μοντέλα τα οποία δημιουργήθηκαν από μεγάλα σύνολα δεδομένων για σκοπούς αναγνώρισης εικόνων όπως για παράδειγμα το ImageNet. Το ImageNet παρέχει ένα μεγάλο σύνολο δεδομένων με περισσότερα από δεκαπέντε εκατομμύρια εικόνες υψηλής ανάλυσης που ανήκουν σε περίπου είκοσι δύο χιλιάδες διαφορετικές κατηγορίες. Το Keras παρέχει εύκολη πρόσβαση σε πολλά μοντέλα αναγνώρισης εικόνας, με υψηλές αποδόσεις στη βάση του ImageNet όπως το Interception, ResNet , VGG και πολλά άλλα. Για την ανάπτυξη της έρευνας λήφθηκαν τα βάρη του ImageNet και ενσωματώθηκαν στα μοντέλα με σκοπό τη διάκριση και των προσαρμοσμένων δεδομένων .

## 3.4 MySQL Workbench

Το MySQL Workbench είναι ένα εργαλείο με γραφικό περιβάλλον, που διαχειρίζεται MySQL διακομιστές και βάσεις δεδομένων. Παρέχει μοντελοποίηση δεδομένων, ανάπτυξη σε SQL καθώς και ολοκληρωμένα εργαλεία διαχείρισης για τη διαμόρφωση εξυπηρετητών, εργαλεία δημιουργίας αντιγράφων ασφαλείας και πολλά άλλα. Το MySQL Workbench χρησιμοποιήθηκε για την κάλυψη των απαιτήσεων κατά τη φάση συλλογής νόμιμων σελίδων και σελίδων ηλεκτρονικού ψαρέματος. Το MySQL Workbench είναι ένα δωρεάν εργαλείο ανοιχτού κώδικα, αρκετά ελαφρύ και εύχρηστο. Έτσι θεωρήθηκε ως ιδανική λύση για την ταχύτερη προσέγγιση για την υλοποίηση μιας απλής βάσης δεδομένων.

# Κεφάλαιο 4
# Πειραματικός Σχεδιασμός και Αποτελέσματα

## 4.1 Μέθοδος Υλοποίησης

Η μέθοδος που χρησιμοποιήθηκε για την ανίχνευση τυχόν ιστότοπων ηλεκτρονικού ψαρέματος (phishing) απαιτεί τη δημιουργία εικόνων (οπτικοποίηση) του πηγαίου κώδικα των ιστότοπων ηλεκτρονικού ψαρέματος καθώς και νόμιμων ιστότοπων. Στις εικόνες απεικονίζεται η δομή, το περιεχόμενο και ο όγκος του πηγαίου κώδικα κάθε ιστότοπου. Οι εικόνες που δημιουργήθηκαν, χρησιμοποιήθηκαν για την εκπαίδευση τεσσάρων μοντέλων, δύο (CNN-RNN) και δύο CNN μοντέλων μέσω της βιβλιοθήκη νευρωνικών δικτύων υψηλού επιπέδου Keras-TensorFlow, με στόχο την αναγνώριση των ιστότοπων ηλεκτρονικού ψαρέματος (phishing). Για την ολοκλήρωση του πειραματικού σχεδιασμού και την εξαγωγή αποτελεσμάτων και συμπερασμάτων ακολουθήθηκαν ( 6 ) στάδια.

1. Συλλογή και δημιουργία εικόνων(οπτικοποίηση) ιστότοπων.
2. Εκπαίδευση πρώτου MobileNet μοντέλου και δοκιμή αυτού.
3. Εκπαίδευση δεύτερου MobileNet-RNN μοντέλου και δοκιμή αυτού.
4. Εκπαίδευση τρίτου Xception-RNN μοντέλου και δοκιμή αυτού.
5. Εκπαίδευση τέταρτου Custom-CNN μοντέλου και δοκιμή αυτού.
6. Εξαγωγή αποτελεσμάτων και συμπερασμάτων.

## 4.2 Συλλογή Δεδομένων

Η διαδικασία συλλογής δεδομένων ήταν μια δύσκολη και χρονοβόρα διαδικασία κατά την ανάπτυξη της παρούσας μεταπτυχιακής διατριβής. Η συλλογή πηγαίου κώδικα (source code) από μοναδικούς ιστότοπους ηλεκτρονικού ψαρέματος αποτελούσε τον αρχικό τύπο δεδομένων και ήταν μια δύσκολη εργασία , καθώς ήταν δύσκολο να βρεθούν πηγές διευθύνσεων ηλεκτρονικού ψαρέματος που να παρέχουν ακριβείς διευθύνσεις. Αρχικά μια γρήγορη προσέγγιση ήταν η συλλογή διευθύνσεων ηλεκτρονικού ψαρέματος από τη βάση δεδομένων του ιστότοπου (PhishTank n.d.) σε μορφή αρχείου CSV. Στο αρχείο καταγράφεται μεγάλος όγκος από ιστοτόπους ηλεκτρονικού ψαρέματος οι οποίοι ωστόσο κατά τη φάση απόξεσης του πηγαίου κώδικα άρχισαν να εμφανίζουν προβλήματα. Μερικά από τα προβλήματα οφείλονταν στην απόσυρση των ιστότοπων λαμβάνοντας σφάλματα σελίδας 404 και προβλήματα προσβασιμότητας λαμβάνοντας σφάλματα σελίδας 403.
Για την επίλυση αυτού του προβλήματος χρησιμοποιήθηκαν URL διευθύνσεις ιστότοπων ηλεκτρονικού ψαρέματος από το (PhishTank n.d.) οι οποίες καθορίζονταν ως ενεργές. Ωστόσο πολλές από αυτές παρουσίαζαν προβλήματα προσβασιμότητας και διαθεσιμότητας. Κατά τη συλλογή πηγαίου κώδικα από ιστότοπους εντοπίστηκαν σελίδες που δεν περιείχαν φόρμες σύνδεσης, καθώς αρκετές διευθύνσεις εκτελούσαν ransomware επιθέσεις κατά την εκτέλεσή τους.

Ακολούθως έγινε προσπάθεια συλλογής δεδομένων από άλλες βάσεις ιστότοπων ηλεκτρονικού ψαρέματος, (OpenPhish n.d.) και (Isitphishing n.d.). Σε αυτές τις βάσεις είχαν περιοριστεί τα πιο πάνω προαναφερθέντα προβλήματα αλλά μόνο στις περιπτώσεις που οι ιστοσελίδες ηλεκτρονικού ψαρέματος ήταν πρόσφατες. Οι περισσότεροι ιστότοποι ηλεκτρονικού ψαρέματος είχαν μέγιστη ενεργή διάρκεια 24 ώρες. Επίσης ένα άλλο πρόβλημα που εμφανίστηκε ήταν η επισύναψη σελίδων με λανθασμένη ετικέτα. Οι σελίδες ηλεκτρονικού ψαρέματος αναφέρονταν σε άλλες επωνυμίες από αυτές που καταγράφονταν στην ετικέτα. Τα πιο πάνω προβλήματα προκάλεσαν αύξηση στον χρόνο συλλογής δεδομένων καθώς και καθυστέρηση στη διεκπεραίωση της πειραματικής διαδικασία.

Για την αντιμετώπιση μερικών προβλημάτων κατά τη συλλογή κατάλληλων δεδομένων για εκπαίδευση των μοντέλων, εισάχθηκε στον κώδικα η βιβλιοθήκη imgkit η οποία παρέχει μια ζωντανή εικόνα ενός στιγμιότυπου οθόνης κάθε ιστότοπου. Αυτό βοήθησε στη συλλογή ιδανικών εικόνων για την εκπαίδευση των μοντέλων βαθιάς μηχανικής μάθησης.

Ένα άλλο σημαντικό ζήτημα που προέκυψε ήταν η ανάγκη χρήσης εικονικού δικτυού VPN για την πρόσβαση και απόξεση ιστότοπων ηλεκτρονικού ψαρέματος. Ο πάροχος υπηρεσιών διαδικτύου αναγνωρίζει ως κακόβουλους μεγάλο αριθμό ιστότοπων ηλεκτρονικού ψαρέματος και δεν επιτρέπει την πρόσβαση. Μέσω των εικονικών δικτύων είναι δυνατή η παράκαμψη των υπηρεσιών ασφαλείας του παρόχου υπηρεσιών διαδικτύου και η πρόσβαση στους ιστότοπους. Η χρήση εικονικού δικτυού αρχικά βοήθησε και στη συγκέντρωση ιστότοπων ηλεκτρονικού ψαρέματος που είχαν διαφορετική γλώσσα πέραν της Αγγλικής. Μερικοί ιστότοποι προσάρμοζαν τη γλώσσα παρουσίασής τους ανάλογα με τον τόπο που βρισκόταν ο VPN διακομιστής. Η αλλαγή γλώσσας αλλάζει και τη μορφή του πηγαίου κώδικα, ως αποτέλεσμα κατά τη μετατροπή των συμβολοσειρών του πηγαίου κώδικα σε εικόνα να προκύπτουν διαφορετικές εικόνες για τον ίδιο ιστότοπο όπως φαίνεται στην Εικόνα 16 και 17 .

Αγγλικά “password” σε hex΄΄70 61 73 73 77 6f 72 64 0a‘‘

**Εικόνα 16.** Δημιουργία εικόνας Hilbert της Αγγλικής λέξης “password”

Ελληνικά ‘’κωδικός’’ σε hex “ 3ba 3c9 3b4 3b9 3ba 3cc 3c2”

**Εικόνα 17.** Δημιουργία εικόνας Hilbert της Ελληνικής λέξης “ κωδικός”

Ο αρχικός στόχος της εργασίας ήταν η συλλογή δεδομένων από ιστοτόπους που παρουσιάζονται σε διάφορα πρότυπα γλώσσας. Ωστόσο δεν κατέστη δυνατό λόγω του περιορισμένου αριθμού ιστότοπων ηλεκτρονικού ψαρέματος οι οποίοι έχουν τη δυνατότητα να παρουσιάζονται σε ανάλογη γλώσσα σε σχέση με τον τόπο που βρίσκεται ο VPN διακοσμητής. Επίσης δεν εντοπίστηκε αρκετά ικανοποιητικός αριθμός ιστότοπων ηλεκτρονικού ψαρέματος που να παρουσιάζεται η αρχική του μορφή σε διαφορετική γλώσσα πέραν της Αγγλικής. Έτσι εγκαταλείφθηκε ο στόχος αυτός και επικεντρώθηκε η συλλογή δεδομένων από ιστότοπους ηλεκτρονικού ψαρέματος που παρουσιάζονται στην Αγγλική γλώσσα.

### 4.2.1 Εφαρμογή Συλλογής Δεδομένων

Κατά τη φάση συλλογής δεδομένων δημιουργήθηκε μια εφαρμογή σε γλώσσα Python η οποία παρέχει τη δυνατότητα απόξεσης και αποθήκευσης του HTML κώδικα σε μία μεταβλητή από ένα δοθέν νόμιμο ιστότοπο ή ιστότοπο ηλεκτρονικού ψαρέματος. Για την εισαγωγή URL διευθύνσεων στην εφαρμογή χρησιμοποιήθηκε η βιβλιοθήκη python CSV. Ανάλογα με το είδος της URL διεύθυνσης καταχωρείται σε κατάλληλο csv αρχείο το οποίο περιέχει τρία (3) πεδία τα οποία είναι το name, url και language. Ακολούθως εισάγεται η URL διεύθυνση σε μια μέθοδο και παράγει μια ζωντανή εικόνα ενός στιγμιότυπου οθόνης του ιστότοπου. Στη συνέχεια τα δεδομένα που λήφθηκαν κατά την απόξεση του HTML κώδικα καταχωρούνται στην είσοδο του κώδικα BinVis (Cortesi,nd) για την παραγωγή των επιθυμητών εικόνων. Για τη δημιουργία επιθυμητών εικόνων καλείται ο κώδικας BibVis (Cortesi 2015)τρεις (3) διαδοχικές φορές έτσι ώστε να δημιουργήσει την αντίστοιχη εικόνα για την καθεμιά από τις καμπύλες Hilbert, Zigzag και Zorder αντίστοιχα. Ο κώδικας της εφαρμογής για τη συλλογή δεδομένων και παραγωγή εικόνων παρουσιάζεται στο Παράρτημα Z-1.1 και Z-1.2 .

### 4.2.2 Διεπαφή Εφαρμογής Συλλογής Δεδομένων

Η εισαγωγή URL διευθύνσεων οι οποίες καταχωρούνται στο ανάλογο csv αρχείο, γίνεται μέσω της διεπαφής γραμμής εντολών και καθίσταται μια απλή διαδικασία. Όπως φαίνεται στην ακόλουθη Εικόνα 16, μέσω της γραμμής εντολών εκτελείται μια εντολή με όρισμα"-S" και επιλογή "bad" ή "good". Η επιλογή "bad" η "good" υποδηλώνει αν το csv αρχείο περιέχει URL διεύθυνσης ηλεκτρονικού ψαρέματος ή νόμιμες διευθύνσεις

αντίστοιχα. Όπως διαφαίνεται παράγεται αρχικά όπως προαναφέρθηκε μια ζωντανή εικόνα ενός στιγμιότυπου οθόνης της δοθείσας διεύθυνσης και ακολούθως οι τρεις (3) εικόνες με παρουσίαση αντίστροφης μέτρησης.


**Εικόνα 18.** Διεπαφή Εφαρμογής

### 4.2.3 Βάση Δεδομένων

Για την καταγραφή και αποθήκευση των δεδομένων όπως φαίνεται και στην Εικόνα 18 θεωρήθηκε σημαντική η χρήση μιας βάσης δεδομένων. Η βάση δεδομένων κάλυψε βασικές ανάγκες κατά τη φάση συλλογής δεδομένων. Αρχικά υπήρξε ανάγκη για έλεγχο διπλών εγγραφών καθώς επίσης παρείχε και ευελιξία κατά τη φάση επιλογής εικόνων για την εκπαίδευση των μοντέλων. Η MySQL θεωρήθηκε ως βέλτιστη λύση λόγω της γρήγορης προσθήκης, μέσω της python στην εφαρμογή συλλογής δεδομένων καθώς και στις μειωμένες απαιτήσεις υπολογιστικών πόρων. Στη βάση δεδομένων έχουν δημιουργηθεί δύο πίνακες “Legitimate” και “Phishing”. Στον κάθε ένα αντίστοιχα έχουν αποθηκευτεί οι URL διευθύνσεις, το όνομα επωνυμίας τους, η γλώσσα εμφάνισης, οι εικόνες στιγμιότυπων των ιστότοπων , οι εικόνες παραγωγής των τριών καμπύλων, το μονοπάτι αποθήκευσης όλων των εικόνων καθώς επίσης η ημερομηνία συλλογής και πηγαίος κώδικας. Ο πίνακας “Phishing” μπορεί σε μελλοντική εργασία να ενεργεί και ως μαύρη λίστα με σκοπό την αύξηση απόκρισης ενός συστήματος.

### 4.2.4 Ποσότητα Δεδομένων

Για τη δημιουργία του (dataset) συλλέχθηκαν και δημιουργήθηκαν εικόνες (οπτικοποίηση) από τον πηγαίο κώδικα ιστότοπων ηλεκτρονικού ψαρέματος για δεκαπέντε (15) επωνυμίες όπως φαίνεται στον ακόλουθο Πίνακα 1. Οι ιστότοποι αυτοί περιείχαν χαρακτηριστικά σύνδεσης χρήστη (Login).

| **Α/Α** | **Επωνυμίες** | **Εκπαίδευση** | **Επικύρωση** | **Δοκιμή** | **Σύνολο** |
|---|---|---|---|---|---|
| 1. | Adobe | 50 | 10 | 5 | 65 |
| 2. | Alibaba | 50 | 10 | 5 | 65 |
| 3. | Amazon | 50 | 10 | 5 | 65 |
| 4. | AT&T | 43 | 8 | 5 | 56 |
| 5. | Bank of American | 50 | 10 | 5 | 65 |
| 6. | Chase Bank | 50 | 10 | 5 | 65 |
| 7. | DHL | 50 | 10 | 5 | 65 |
| 8. | eBay | 40 | 8 | 5 | 53 |
| 9. | Facebook | 50 | 10 | 5 | 65 |
| 10. | Google | 50 | 10 | 5 | 65 |
| 11. | LinkedIn | 50 | 10 | 5 | 65 |
| 12. | Microsoft | 85 | 10 | 5 | 100 |
| 13. | Netflix | 50 | 10 | 5 | 65 |
| 14. | PayPal | 50 | 10 | 5 | 65 |
| 15. | Yahoo | 50 | 10 | 5 | 65 |
| | | **768** | **146** | **75** | **989** |

**Πίνακας 1.** Συνολικός Όγκος Δεδομένων (Dataset)

Για την εκπαίδευση, επικύρωση και δοκιμή επιλέχθηκαν οι πιο πάνω ποσότητες όπως φαίνονται στον Πίνακα 1. Αν και σε νευρωνικά δίκτυα, συνιστάται να χρησιμοποιούνται όσο το δυνατό μεγάλοι αριθμοί εικόνων εκπαίδευσης για τη λήψη υψηλότερης ακριβείας επικύρωσης, κατά την αρχική δοκιμή που έγινε μόνο με τριάντα (30) εικόνες της PayPal επωνυμίας, αντλήθηκαν θετικά αποτελέσματα όσον αφορά την ταξινόμηση μεταξύ του

νόμιμου ιστότοπου και των ιστότοπων ηλεκτρονικού ψαρέματος. Ωστόσο θα ήταν δυνατή η συλλογή περισσότερων δεδομένων από αυτά που παρουσιάζονται στον Πίνακα 1, αλλά λόγω περιορισμένου χρόνου δεν κατέστη δυνατό. Μετά από αρκετό χρόνο και καθότι έγινε μια γενική εκτίμηση του συνόλου των εικόνων που συλλέχθηκαν, αποφασίστηκαν τα ακόλουθα:

- Δεδομένα εκπαίδευσης (Training Data) : Χρησιμοποιήθηκε το 77% του συνόλου των εικόνων της κάθε επωνυμίας για εκπαίδευση.
- Δεδομένα επικύρωσης (Validation Data) : Χρησιμοποιήθηκε το 15,4% του συνόλου των εικόνων της κάθε επωνυμίας για επικύρωση.
- Δεδομένα δοκιμών (Testing Data) : Χρησιμοποιήθηκε το 7,6% του συνόλου των εικόνων κάθε επωνυμίας για δοκιμές των μοντέλων και εξαγωγή συμπερασμάτων των προβλέψεών τους.

Η εκπαίδευση των μοντέλων αποσκοπεί στην εκμάθηση των κατάλληλων τιμών των βαρών του κάθε νευρώνα ώστε συλλογικά να επιφέρει το βέλτιστο επιθυμητό αποτέλεσμα κατά την ταξινόμηση ενός υπόπτου ιστότοπου σε ιστότοπο ηλεκτρονικού ψαρέματος ή νόμιμο ιστότοπο.

## 4.3 Πρώτο Στάδιο Πειράματος

Για την ανάπτυξη του πρώτου μέρους της πειραματικής διαδικασίας χρησιμοποιήθηκε το μοντέλο MobileNet που ανήκει στην κατηγορία των συνελικτικών νευρωνικών δικτύων (CNN) και παρέχεται από τη βιβλιοθήκη του Keras.

### 4.3.1 MobileNet Μοντέλο

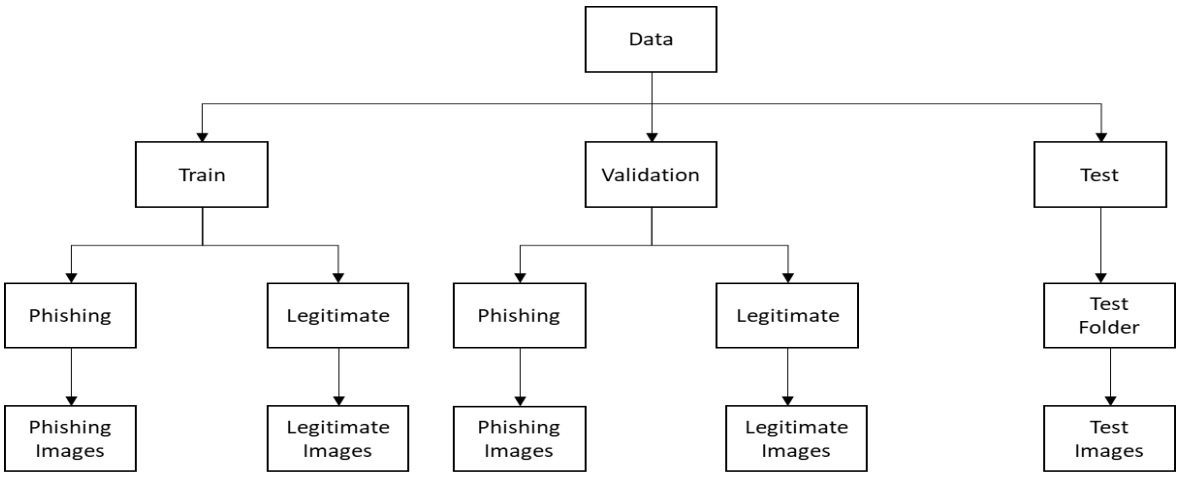
Το MobileNet είναι ένα μοντέλο βαθιάς μηχανικής μάθησης, με (CNN) αρχιτεκτονική για ταξινόμηση εικόνας και Mobile Vision. Κατασκευάστηκε από την Google τον Απρίλιο του 2017. Αποτελεί ένα μικρό και αποτελεσματικό συνελικτικό νευρωνικό δίκτυο, λόγω της φορητότητας, της ανάγκης μικρής υπολογιστικής ισχύος για εκτέλεση και της γρήγορης εκπαίδευσης του μέσω της εκπαίδευσης μεταφοράς.

### 4.3.2 Αρχιτεκτονική Μοντέλου MobileNet

Το MobileNet είναι προ-εκπαιδευμένο στη βάση του ImageNet και διατίθεται από τις εφαρμογές της βιβλιοθήκης Keras-TensorFlow. Στο μοντέλο προστέθηκαν πυκνά στρώματα (Dense) έτσι ώστε να μπορεί να μάθει πιο πολύπλοκες λειτουργίες και να προσφέρει καλύτερα αποτελέσματα κατά την ταξινόμηση. Το μοντέλο λαμβάνει ως είσοδο μια RGB εικόνα από τις εικόνες που δημιουργήθηκαν από το εργαλείο Bivins.io. με διατάσεις 128x128x3. Ακολούθως στην έξοδο του υπάρχει το στρώμα ταξινόμησης το οποίο αποτελείται από τις δύο τάξεις (phishing ή legitimate) με συνάρτηση ενεργοποίησης softmax.

### 4.3.3 Εισαγωγή και Προ επεξεργασία Εικόνας

Για την εισαγωγή και προεπεξεργασία εικόνας χρησιμοποιείται το ImageDataGenerator εντός της μεθόδου get_train_val_generator(). Η Keras παρέχει την κλάση ImageDataGenerator η οποία καθορίζει τη διαμόρφωση και προετοιμασία των δεδομένων εικόνας. Όταν φορτώνεται μια μεμονωμένη εικόνα ορίζεται το σχήμα της εικόνας, ύψος(height), πλάτος(width) και κανάλια χρωμάτων (channels). Εντός του ImageDataGenerator χρησιμοποιήθηκε η preprocess_input λειτουργία η οποία προορίζεται να προσαρμόσει την κάθε εικόνα εισόδου στη μορφή που απαιτεί το MobileNet μοντέλο . Η κλάση ImageDataGenerator έχει μια μέθοδο που ονομάζεται flow_from_directory() η οποία χρησιμοποιείται για να διαβάσει εικόνες από φακέλους. Για την υλοποίηση εκπαίδευσης, επικύρωσης και δοκιμής των μοντέλων, χρησιμοποιήθηκε η ακόλουθη δομή φακέλων για τον καθένα από τους τρεις (3) τύπους εικόνων (Hilbert,Zigzag, Zorder) όπως φαίνεται στο ακόλουθο Σχήμα 1. Τα ονόματα των φακέλων Phishing και Legitimate είναι σημαντικά γιατί δίνονται αντίστοιχα στις ετικέτες κατηγοριοποίησης.




**Σχήμα 1.** Δομή Φακέλων

Για την εισαγωγή εικόνων σε όλα τα μοντέλα εκπαίδευσης χρησιμοποιήθηκε ο κώδικας που φαίνεται παρακάτω :

```
def get_train_val_generator(batch_size=32):

  train_datagen=ImageDataGenerator(preprocessing_function=preprocess_input)
  train_generator=train_datagen.flow_from_directory(train_data_path,
                                target_size=(img_width,img_height),
                                batch_size=batch_size,
                                color_mode='rgb',
                                class_mode='categorical',
                                shuffle=True)

  val_datagen=ImageDataGenerator(preprocessing_function=preprocess_input)
  val_generator=val_datagen.flow_from_directory(validation_data_path,
                                target_size=(img_width,img_height),
                                batch_size=batch_size,
                                color_mode='rgb',
                                class_mode='categorical',
                                shuffle=True)
  print("BATCH SIZE=",batch_size)
  return train_generator, val_generator
```

### 4.4.4 Εκπαίδευση MobileNet Μοντέλου

Στο MobileNet δίκτυο προστέθηκαν 3 στρώματα. Το πρώτο πυκνό (Dense) στρώμα, λαμβάνει στοιχεία από τους νευρώνες της τελευταίας συνέλιξης του δικτύου και στην έξοδο του παράγεται ένα σχήμα μεγέθους 1024 με συνάρτηση ενεργοποίησης (ReLu). Έπειτα το δεύτερο πυκνό στρώμα λαμβάνει στοιχεία από το πρώτο πυκνό στρώμα και στην έξοδο του παράγεται και πάλι ένα σχήμα μεγέθους 1024 με συνάρτηση ενεργοποίησης ReLu. Το τρίτο στρώμα αποτελείται από ένα πυκνό Dense στρώμα το

οποίο παράγει στην έξοδο του σχήμα μεγέθους 512 με συνάρτηση ενεργοποίησης ReLu . Τέλος η έξοδος του τρίτου στρώματος εισάγεται στο τελευταίο στρώμα ταξινόμησης το οποίο αποτελείται από ένα πυκνό στρώμα (Dense) το οποίο παράγει στην έξοδο ένα σχήμα μεγέθους 2 με συνάρτηση ενεργοποίησης softmax. Το μοντέλο στη συνέχεια μεταγλωττίστηκε (compiled) χρησιμοποιώντας αλγόριθμο βελτιστοποίησης Adam. Ο αλγόριθμος βελτιστοποίησης βοηθάει στη μέγιστη δυνατή μείωση του κόστους. Οι εικόνες εκπαίδευσης εισήχθησαν ανά παρτίδα των τριάντα δύο (32 batch_size) σε κάθε επανάληψη και το κόστος υπολογίστηκε βάσει των εικόνων επικύρωσης (validation images). Το μοντέλο μετά από αρκετές πειραματικές προσπάθειες αποφασίσθηκε να περιοριστεί στις τριάντα εποχές (30) εκπαίδευσης(epochs) γιατί πέραν τον τριάντα δεν αλλοιώνονταν περεταίρω τα αποτελέσματα. Για τον υπολογισμό των βημάτων εκπαίδευσης, διαιρέθηκε το πλήθος των εικόνων εκπαίδευσης με το μέγεθος παρτίδας, έτσι προέκυψαν σαράντα έξι (46) βήματα εκπαίδευσης ανά εποχή. Κατά τη φάση της εκπαίδευσης σε κάθε εποχή υλοποιήθηκε σύγκριση του ποσοστό ακριβείας επικύρωσης με των προηγούμενων εποχών και έγινε αποθήκευση της καλύτερης μέγιστης τιμής. Ο κώδικας που χρησιμοποιήθηκε για την πρώτη φάση εκπαίδευσης φαίνεται παρακάτω:

```
# Φορτώνονται δύο Γεννήτορες με μέγεθος παρτίδας 32
train_generator, val_generator = get_train_val_generator(batch_size)
#Υπολογισμός βημάτων εκπαίδευση
train_steps=train_generator.n//train_generator.batch_size
val_samples=val_generator.n//val_generator.batch_size


# Φόρτωση του MobileNet Μοντέλου με βάρη εκπαίδευσης από ImageNet
MobileNet_model=MobileNet(weights='imagenet',include_top=False) #

x=MobileNet_model.output
x=GlobalAveragePooling2D()(x)
x=Dense(1024,activation='relu')(x) #Πρόσθεση περεταίρω στρωμάτων
x=Dense(1024,activation='relu')(x) #Dense layer 2
x=Dense(512,activation='relu')(x) #Dense layer 3
predictions=Dense(2,activation='softmax')(x) #Τελευταίο Dense στρώμα με συνάρτηση ενεργοποίησης softmax
model=Model(inputs=MobileNet_model.input,outputs=predictions)
```

```
# Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης Adam
model.compile(optimizer=Adam(lr=LR),loss='categorical_crossentropy',metrics=['accuracy'])

# Σημείο ελέγχου
filepath="MobileNet_weights_lr"+str(LR)+".h5"

#Αποθήκευση της καλύτερης μέγιστης τιμής val_accuracy
checkpoint = ModelCheckpoint(filepath, monitor='val_accuracy', verbose=1, save_best_only=True, mode='max')
callbacks_list = [checkpoint]

history=model.fit_generator(generator=train_generator,
            steps_per_epoch=train_steps,
            epochs=30,
            validation_data=val_generator,
            validation_steps=val_samples,
            callbacks=callbacks_list)

print("Training done")
# Αποθήκευση MobileNet Μοντέλου
model.save('MobileNet_Model_lr'+str(LR)+'.h5')
print("Saved model to disk")
```

Για τη διερεύνηση της βέλτιστής ακριβείας επικύρωσης το μοντέλο έτυχε εκπαίδευσης (training), επικύρωσης(validation) και δοκιμής (test) από τρεις (3) ρυθμούς εκπαίδευσης lr0.01, lr.0.001 και lr0.0001 ανά τύπο σετ δεδομένων (Hilbert, Zigzag, Zorder) . Κατά την ολοκλήρωση της διαδικασίας εκπαίδευσης, καταγράφηκαν τα αποτελέσματα τα οποία παρουσιάζονται στα Παραρτήματα Γ1,Δ1,Ε1 . Για την παρουσίαση των αποτελεσμάτων σε γράφημα καθώς και την αποθήκευση των αποτελεσμάτων εκπαίδευσης σε txt αρχείο χρησιμοποιήθηκε ο ακόλουθος κώδικας:

```
# Δημιουργία Γραφήματος και Αποθήκευση Αποτελεσμάτων
acc = history.history['accuracy']
val_acc = history.history['val_accuracy']
loss=history.history['loss']
val_loss=history.history['val_loss']
epochs_range = range(30)
plt.figure(figsize=(20, 10))
```

```
plt.subplot(1, 2, 1)
plt.plot(epochs_range, acc, label='Training Accuracy')
plt.plot(epochs_range, val_acc, label='Validation Accuracy')
plt.legend(loc='lower right')
plt.title('Training and Validation Accuracy')
plt.subplot(1, 2, 2)
plt.plot(epochs_range, loss, label='Training Loss')
plt.plot(epochs_range, val_loss, label='Validation Loss')
plt.legend(loc='upper right')
plt.title('Training and Validation Loss')
#Αποθήκευση Γραφήματος
plt.savefig("MobileNet"+curves+" lr"+str(LR)+ " 128x128 .png")

scores = model.evaluate_generator(val_generator, val_samples=val_samples)
print(model.metrics_names, scores)
print("%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100))
file_score=model.metrics_names, scores
file_score1= "%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100)

f = open("info_lr"+str(LR)+".txt", "a")
f.write("Train \n\n"+ str(file_score)+"\n\n" + str(file_score1)+"\n\n")
f.close()
```

## 4.4 Δεύτερο Στάδιο Πειράματος

Για την ανάπτυξη του πρώτου μέρους της πειραματικής διαδικασίας δημιουργήθηκε σε γλώσσα προγραμματισμού Python ένα CNN-RNN μοντέλο με σκοπό τη βελτίωση της ακρίβειας ταξινόμησης των εικόνων. Χρησιμοποιήθηκε το μοντέλο MobileNet που χρησιμοποιήθηκε στο πρώτο στάδιο του πειράματος και παράλληλα προσαρμόστηκε με ένα Αναδρομικό Νευρωνικό Δίκτυο RNN με αρχιτεκτονική δικτύου LSTM. Τα LSTM δίκτυα αποτελούν μια αρχιτεκτονική νευρωνικών δικτύων με ανατροφοδότηση RNN και χρησιμοποιούνται στον τομέα της βαθιάς μάθησης. Μπορούν να επεξεργαστούν μεμονωμένα σημεία δεδομένων καθώς και ακολουθίες δεδομένων. Αυτό οφείλεται στην ιδιότητα τους να θυμούνται επιλεκτικά μοτίβα για μεγάλες χρονικές περιόδους.

### 4.4.1 Αρχιτεκτονική Μοντέλου MobileNet-RNN

Το μοντέλο αποτελείται από δύο παράλληλα συνδεδεμένα υπο-μοντέλα. Το ένα υπο-μοντέλο είναι όπως προαναφέρθηκε το MobileNet, το οποίο είναι προ-εκπαιδευμένο στη βάση του ImageNet και διατίθεται από τις εφαρμογές της βιβλιοθήκης Keras-TensorFlow. Το δεύτερο υπο-μοντέλο είναι ένα ανεξάρτητο RNN που περιέχει δύο LSTM επίπεδα με έξοδο batch_size 1024. Στην αρχή το μοντέλο λαμβάνει μια RGB εικόνα από τις εικόνες που δημιουργήθηκαν από το εργαλείο Bivins.io. με διατάσεις 128x128x3. Στο υπο-μοντέλο MobileNet η εικόνα λαμβάνεται ως έχει και περνά μέσα μέχρι να φτάσει στο τελικό μπλοκ συνέλιξης που έχει τα χαρακτηριστικά συμφόρησης που έχει μέγεθος batch_size 1024. Στο άλλο παράλληλο υπο-μοντέλο γίνεται μετατροπή της RGB εικόνας (128x128x3), σε εικόνα κλίμακας του γκρι ίδιου μεγέθους, για να είναι δυνατός ο διαχωρισμός της ώστε να καταχωρηθεί ορθά στον RNN. Στη συνέχεια η εικόνα αυτή ανατροφοδοτείται σε (16, 1024) όπου 16 είναι τα χρονικά βήματα και 1024 το μέγεθος του δείγματος σε κάθε βήμα. Οι τιμές αυτές επιλέχθηκαν γιατί το αποτέλεσμα του πολλαπλασιασμού 16*1024 =16.384=128*128 που είναι οι διαστάσεις της εικόνας. Στη συνέχεια η αναμορφωμένη εικόνα περνά μέσα από τα δύο LSTM κάθε ένα από το οποίο έχει έξοδο batch_size=1024. Στη συνέχεια οι δύο έξοδοι των υπό μοντέλων CNN και RNN συγχωνεύονται με τη χρήση πολλαπλασιασμού. Το αποτέλεσμα του πολλαπλασιασμού τροφοδοτείται στο στρώμα ταξινόμησης το οποίο αποτελείται από τις δύο τάξεις (phishing ή legitimate) με συνάρτηση ενεργοποίησης softmax.

### 4.4.2 Εισαγωγή και Προ επεξεργασία Εικόνας

Για την εισαγωγή και προεπεξεργασία εικόνας χρησιμοποιήθηκε το ImageDataGenerator εντός της μεθόδου get_train_val_generator() , όπως και στην πρώτη πειραματική διαδικασία. Για την εισαγωγή εικόνων στο LSTM μοντέλο χρησιμοποιήθηκαν οι μέθοδοι rgb_to_grayscale( ) και rgb_to_grayscale_output_shape() οι οποίες μετατρέπουν την κάθε εικόνα σε κλίμακα του γκρι έτσι ώστε να είναι δυνατός ο διαχωρισμός της εικόνας και να καταχωρηθεί ορθά στο RNN υπομοντέλο. Για την εισαγωγή εικόνων στα μοντέλα εκπαίδευσης χρησιμοποιήθηκε ο κώδικας που φαίνεται παρακάτω:

```
def get_train_val_generator(batch_size=32):
  train_datagen=ImageDataGenerator(preprocessing_function=preprocess_input)

  train_generator=train_datagen.flow_from_directory(train_data_path,
                                target_size=(img_width,img_height),
                                batch_size=batch_size,
                                color_mode='rgb',
                                class_mode='categorical',
                                shuffle=True)

  val_datagen=ImageDataGenerator(preprocessing_function=preprocess_input)

  val_generator=val_datagen.flow_from_directory(validation_data_path,
                                target_size=(img_width,img_height),
                                batch_size=batch_size,
                                color_mode='rgb',
                                class_mode='categorical',
                                shuffle=True)
  return train_generator, val_generator

def rgb_to_grayscale(input):     #Μέσος όρος από κάθε pixel σε 3 RGB στρώματα έχει ως αποτέλεσμα μια εικόνα κλίμακας του γκρι
  return K.mean(input, axis=3)

def rgb_to_grayscale_output_shape(input_shape):
  return input_shape[:-1]
```

### 4.4.3 Εκπαίδευση MobileNet-LSTN Μοντέλου

Το MobileNet-LSTN μοντέλο εκπαιδεύτηκε σε δύο φάσεις:

- Κατά την πρώτη φάση όλα τα στρωματά του MobileNet δικτύου απενεργοποιήθηκαν πλην του τελευταίου στρώματος ταξινόμησης και εκπαιδεύτηκε μαζί με το RNN δίκτυο χρησιμοποιώντας αλγόριθμο βελτιστοποίησης RMSProp ο οποίος σχεδιάστηκε για βελτιστοποίηση των τιμών των βαρών (weights) των νευρωνικών δικτύων. Ο αλγόριθμος βελτιστοποίησης βοηθάει στη μέγιστη δυνατή μείωση του κόστους. Οι εικόνες εκπαίδευσης εισήχθησαν ανά παρτίδα των τριάντα δύο (32 batch_size) σε κάθε επανάληψη και το κόστος υπολογίστηκε βάσει των εικόνων επικύρωσης (validation images). Το μοντέλο μετά από αρκετές πειραματικές

προσπάθειες όπως και στο μοντέλο MobileNet στο (4.1 Πρώτο Στάδιο του Πειράματος) αποφασίσθηκε να περιοριστεί στις τριάντα εποχές (30) εκπαίδευσης(epochs) γιατί πέραν τον τριάντα δεν αλλοιώνονταν περαιτέρω τα αποτελέσματα. Για τον υπολογισμό των βημάτων εκπαίδευσης, διαιρέθηκε το πλήθος των εικόνων εκπαίδευσης με το μέγεθος παρτίδας, έτσι προέκυψαν σαράντα έξι (46) βήματα εκπαίδευσης ανά εποχή. Κατά τη φάση της εκπαίδευσης σε κάθε εποχή υλοποιείτο σύγκριση του ποσοστού ακριβείας επικύρωσης με τις προηγούμενες εποχές και εκτελείτο αποθήκευση της καλύτερης μέγιστης τιμής. Ο κώδικας που χρησιμοποιήθηκε για την πρώτη φάση εκπαίδευσης φαίνεται παρακάτω:

```
# Φορτώνονται δύο Γεννήτορες με μέγεθος παρτίδας 32
print("LOADING IMAGE DATASET WITH BATCH SIZE OF {}...".format(batch_size_train_one))
train_generator, val_generator = get_train_val_generator(batch_size_train_one)


#Υπολογισμός βημάτων εκπαίδευση
train_steps=train_generator.n//train_generator.batch_size
val_samples=val_generator.n//val_generator.batch_size


print("LOAD MobileNet Model / Createting RNN Parallel Model...")
input_tensor = Input(shape=(img_width, img_height,3))

# Φόρτωση του MobileNet Μοντέλου με βάρη εκπαίδευσης από Imagenet
cnn_model= MobileNet(weights='imagenet', include_top=False, input_tensor=input_tensor)
x = cnn_model.output
CNN_bottleneck = GlobalAveragePooling2D()(x)

# Απενεργοποίηση των στρωμάτων του Xception μοντέλου για εκπαίδευση
for layer in cnn_model.layers:
   layer.trainable = False


# Δημιουργία του RNN μοντέλου με δύο LSTM μεγέθους 1024
x = Lambda(rgb_to_grayscale, rgb_to_grayscale_output_shape)(input_tensor)
x = Reshape((16,1024))(x)  # 16 χονικά βήματα timesteps, με είσοδο δείγμα μεγέθους 1024
x = LSTM(1024, return_sequences=True)(x)
RNN_output = LSTM(1024)(x)
```

```
# Οι δύο έξοδοι CNN_bottleneck και RNN_output συγχωνεύονται με πολλαπλασιασμό. Η έξοδος αυτού του
#πολλαπλασιασμού τροφοδοτείται στο  στρώμα ταξινόμησης που αποτελείται από 2 κόμβους  (2 κλάσεις) και
#συνάρτηση ενεργοποίησης softmax

x = Multiply()([CNN_bottleneck, RNN_output])


predictions = Dense(classes, activation='softmax')(x)
model = Model(inputs=[input_tensor], outputs=predictions)


# Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης RMSProp
model.compile(optimizer='rmsprop',loss='categorical_crossentropy' ,metrics=['accuracy'])

print("Starting training")

#Σημείο ελέγχου 1
filepath="weights.h5"
checkpoint = ModelCheckpoint(filepath, monitor='val_accuracy', verbose=1, save_best_only=True, mode='max')
callbacks_list = [checkpoint]

history=model.fit_generator(train_generator,
                            steps_per_epoch=train_steps,
                            epochs=nba_epochs,
                            verbose=1,
                            validation_data=val_generator,
                            validation_steps=val_samples,
                            callbacks=callbacks_list)
```

- Κατά τη δεύτερη φάση όλα τα επίπεδα ολόκληρου του δικτύου ενεργοποιήθηκαν και πραγματοποιήθηκε επανεκπαίδευση του μοντέλου χρησιμοποιώντας αλγόριθμο ενεργοποίησης Adam και ρυθμό εκμάθηση 0,01. Λόγω έλλειψης μνήμης οι εικόνες εκπαίδευσης ανά παρτίδα μειώθηκαν στις δεκαέξι (16 batch_size) σε κάθε επανάληψη και σε αυτή τη φάση το κόστος επανεκτιμήθηκε βάσει των εικόνων επικύρωσης (validation images).  Λόγω μείωσης του μεγέθους παρτίδας ο αριθμός των βημάτων εκπαίδευσης ανά εποχή αυξήθηκε στα ενενήντα δύο (92) βήματα. Ο αριθμός εποχών παρέμεινε ο ίδιος με την πρώτη φάση, λόγω του ότι μετά από προσπάθειες που έγιναν με μεγαλύτερο αριθμό εποχών  δεν παρουσιάστηκε  μεταβολή στο τελικό αποτέλεσμα. Ο κώδικας που χρησιμοποιήθηκε για τη δεύτερη φάση εκπαίδευσης φαίνεται παρακάτω:

```
print("LOADING IMAGE DATASET WITH BATCH SIZE OF {}...".format(batch_size_train_two))
train_generator, val_generator = get_train_val_generator(batch_size_train_two)
#Υπολογισμός βημάτων εκπαίδευσης
train_steps=train_generator.n//train_generator.batch_size
val_samples=val_generator.n//val_generator.batch_size
print("\n Dataset loaded \n")
#Φόρτωση βαρών από τη πρώτη φάση εκπαίδευσης
model.load_weights(filepath)
# Ενεργοποίηση όλων των στρωμάτων για εκπαίδευση
for layer in model.layers:
   layer.trainable = True
# Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης Adam
model.compile(optimizer=Adam(lr=LR), loss='categorical_crossentropy',
          metrics=['accuracy', 'top_k_categorical_accuracy'])
# Σημείο ελέγχου 2
filepath="Finetuned_weights_MobileNet_RNN.h5"
#Αποθήκευση της καλύτερης μέγιστης τιμής val_accuracy
checkpoint = ModelCheckpoint(filepath, monitor='val_accuracy', verbose=1, save_best_only=True, mode='max')
callbacks_list1 = [checkpoint]
history=model.fit_generator(train_generator,
                steps_per_epoch=step_size_train,
                epochs=nbb_epochs,
                verbose=1,
                validation_data=val_generator,
                validation_steps=val_samples,
                callbacks=callbacks_list1)
# Αποθήκευση CNN-RNN μοντέλου
save.model('MobileNet-RNN-Model.h5')
print("Training done")
```

Για τη διερεύνηση της βέλτιστης ακριβείας επικύρωσης το μοντέλο έτυχε εκπαίδευσης (training), επικύρωσης(validation) και δοκιμής (test) από τρεις (3) ρυθμούς εκπαίδευσης lr0.01, lr.0.001 και lr0.0001 ανά τύπο σετ δεδομένων (Hilbert, Zigzag, Zorder) . Κατά την ολοκλήρωση της διαδικασίας εκπαίδευσης, καταγράφηκαν τα αποτελέσματα οποία παρουσιάζονται στα Παραρτήματα Γ1,Δ2 και Ε2 .

Για την παρουσίαση των αποτελεσμάτων σε γράφημα καθώς και την αποθήκευση των αποτελεσμάτων εκπαίδευσης σε .txt αρχείο χρησιμοποιήθηκε ο ακόλουθος κώδικας:

```
# Δημιουργία Γραφήματος και Αποθήκευση Αποτελεσμάτων

acc = history.history['accuracy']
val_acc = history.history['val_accuracy']
loss=history.history['loss']
val_loss=history.history['val_loss']
epochs_range = range(nba_epochs)

plt.figure(figsize=(20, 10))
plt.subplot(1, 2, 1)
plt.plot(epochs_range, acc, label='Training Accuracy')
plt.plot(epochs_range, val_acc, label='Validation Accuracy')
plt.legend(loc='lower right')
plt.title('Training and Validation Accuracy')
plt.subplot(1, 2, 2)
plt.plot(epochs_range, loss, label='Training Loss')
plt.plot(epochs_range, val_loss, label='Validation Loss')
plt.legend(loc='upper right')
plt.title('Training and Validation Loss')
#Αποθήκευση Γραφήματος
plt.savefig("MobileNet-RNN "+curves+" lr"+str(LR)+ " 128x128.png")

#Υπολογισμός αποτελέσματος εκπαίδευσης επί της εκατό.
scores = model.evaluate_generator(val_generator, val_samples=val_samples)
print(model.metrics_names, scores)
print("%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100))
file_score=model.metrics_names, scores
file_score1= "%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100)

#Αποθήκευση αποτελεσμάτων στο αρχείο info.txt
f = open("info.txt", "a")
f.write("Train \n\n"+ str(file_score)+"\n\n" + str(file_score1)+"\n\n")
f.close()
```

## 4.5 Τρίτο Στάδιο Πειράματος

Για την ανάπτυξη του δεύτερου μέρους της πειραματικής διαδικασίας δημιουργήθηκε σε γλώσσα προγραμματισμού Python ένα άλλο CNN-RNN μοντέλο με σκοπό την εξόρυξη συγκριτικών αποτελεσμάτων αναφορικά με την ακρίβεια ταξινόμησης των εικόνων. Για την υλοποίηση αυτού του μοντέλου χρησιμοποιήθηκε το μοντέλο Xception που ανήκει στην κατηγορία των συνελικτικών νευρωνικών δικτυών CNN και παρέχεται από το

Keras, παράλληλα με ένα Αναδρομικό Νευρωνικό Δίκτυο RNN με αρχιτεκτονική δικτύου LSTM όπως και στο δεύτερο πειραματικό στάδιο .

### 4.5.1 Xception -LSTM Μοντέλο

Το μοντέλο Xception δημιουργήθηκε από την Google και αποτελεί μια εξελιγμένη έκδοση του Interception μοντέλου. Η τροποποιημένη σε βάθος ξεχωριστή συνέλιξη στο μοντέλο Xception, παράγει καλύτερα αποτελέσματα ακόμη και από το μοντέλο Interception-V3 και για σύνολα δεδομένων του ImageNet σύμφωνα τα αποτελέσματα για την ταξινόμηση εικόνας στο (ILSVRC 2015). Με τη χρήση ενός υποσυνόλου της βάσης εικόνων του ImageNet , με 1000 εικόνες σε καθεμιά από τις 1000 κατηγορίες κατέληξε στα ακόλουθα συγκριτικά αποτελέσματα. Το Xception υπερισχύει των Vignettes, RestNet και Inception-V3 κυρίως όσον αφορά το ποσοστό σφάλματος. Όσον αφορά την ακρίβεια η βελτίωση είναι δεν είναι πολύ μεγάλη όπως παρατηρούμε στον ακόλουθο Πίνακα 2.

| | Top-1 accuracy | Top-5 accuracy |
|---|---|---|
| VGGNet – 1st Runner Up in ILSVRC 2014 — **VGG-16** | 0.715 | 0.901 |
| ResNet – Winner in ILSVRC 2015 — **ResNet-152** | 0.770 | 0.933 |
| Inception-v3 – 1st Runner Up in ILSVRC 2015 — **Inception V3** | 0.782 | 0.941 |
| **Xception** | **0.790** | **0.945** |

**Πίνακας 2.** Συγκριτικά αποτελέσματα Xception Μοντέλου

Το Xception το οποίο είναι διαθέσιμο στο Keras και είναι ένα πιο βαρύ με περισσότερες παραμέτρους και βάθος μοντέλο από τον MobileNet. Χρησιμοποιήθηκε παράλληλα με LSTM δίκτυα τα οποία αποτελούν μια αρχιτεκτονική νευρωνικών δικτύων με ανατροφοδότηση RNN και χρησιμοποιούνται στον τομέα της βαθιάς μάθησης. Στόχος του μοντέλου αυτού είναι να επιτευχθούν υψηλότερα αποτελέσματα αναφορικά με την ακρίβεια ταξινόμησης εικόνας.

### 4.5.2 Αρχιτεκτονική Μοντέλου

Το μοντέλο αποτελείται όπως και στην πρώτη πειραματική διαδικασία, από δύο παράλληλα συνδεδεμένα υπο-μοντέλα, άλλα υλοποιούνται μερικές τροποποιήσεις όσον αφορά το RNN υπομοντέλο.

Το ένα υπο-μοντέλο είναι όπως προαναφέρθηκε το Xception το οποίο είναι προ-εκπαιδευμένο στη βάση του ImageNet και διατίθεται από τις εφαρμογές της βιβλιοθήκης Keras-TensorFlow. Το δεύτερο υπο-μοντέλο είναι ένα ανεξάρτητο RNN που περιέχει δύο LSTM επίπεδα με μέγεθος παρτίδας εξόδου δύο χιλιάδες σαράντα οκτώ (batch_size 2048). Στην αρχή το μοντέλο λαμβάνει μια RGB εικόνα από τις εικόνες που δημιουργήθηκαν από το εργαλείο Bivins.io. με διατάσεις 128x128x3. Στο υπο-μοντέλο Xception η εικόνα λαμβάνεται ως έχει και περνά μέσα μέχρι να φτάσει στο τελικό μπλοκ συνέλιξης που έχει τα χαρακτηριστικά συμφόρησης που έχει μέγεθος παρτίδας (batch_size 2048). Στο άλλο παράλληλο υπο-μοντέλο γίνεται μετατροπή της RGB εικόνας (128x128x3) , σε εικόνα κλίμακας του γκρι ίδιου μεγέθους, για να είναι δυνατός ο διαχωρισμός της ώστε να καταχωρηθεί ορθά στον RNN. Στη συνέχεια η εικόνα αυτή ανατροφοδοτείται σε (16, 1024) όπου 16 είναι τα χρονικά βήματα και 1024 το μέγεθος του δείγματος σε κάθε βήμα. Οι τιμές αυτές επιλέχθηκαν γιατί το αποτέλεσμα του πολλαπλασιασμού 16*1024=16.384 είναι ίσο με το αποτέλεσμα του πολλαπλασιασμού 128*128=16.384 που είναι οι διαστάσεις της εικόνας. Στη συνέχεια η αναμορφωμένη εικόνα περνά μέσα από τα δύο LSTM κάθε ένα από το οποίο έχει έξοδο παρτίδας (batch_size=2048). Ακολούθως οι δύο έξοδοι των υπο-μοντέλων CNN και RNN συγχωνεύονται με τη χρήση πολλαπλασιασμού. Το αποτέλεσμα του πολλαπλασιασμού τροφοδοτείται στη συνέχεια στο στρώμα ταξινόμησης το οποίο αποτελείται από τις δύο τάξεις (phishing ή legitimate) με συνάρτηση ενεργοποίησης softmax.

### 4.5.3 Εισαγωγή και Προ επεξεργασία Εικόνας

Για την εισαγωγή εικόνων και προ-επεξεργασία εικόνας χρησιμοποιείται το ImageDataGenerator εντός της μεθόδου get_train_val_generator()όπως και την πρώτη πειραματική διαδικασία με τη μόνη διαφορά σε αυτή την περίπτωση, εντός του ImageDataGenerator χρησιμοποιήθηκε η preprocess_input λειτουργία η οποία προορίζεται να προσαρμόσει την κάθε εικόνα εισόδου στη μορφή που απαιτεί το Xception μοντέλο. Ο κώδικας για την εισαγωγή εικόνων στα μοντέλα εκπαίδευσης που χρησιμοποιήθηκε παραμένει ο ίδιος με την πρώτη πειραματική διαδικασία.

### 4.5.4 Εκπαίδευση Xception-LSTN Μοντέλου

Το Xception-LSTN μοντέλο εκπαιδεύτηκε σε δύο φάσεις κατά τον ίδιο τρόπο με το μοντέλο της πρώτης πειραματικής διαδικασίας. Ο αλγόριθμος βελτιστοποίησης , το μέγεθος παρτίδας, οι εποχές εκπαίδευσης καθώς και ο αριθμός βημάτων εκπαίδευσης παρέμειναν τα ίδια. Η βασική τροποποίηση αφορά τον κώδικα υλοποίησης του RNN μοντέλου. Σύμφωνα με τον ακόλουθο κώδικα τροποποιήθηκε το μέγεθος παρτίδας του LSTM σε (2048 batch_size):

```
# Φορτώνονται δύο Γεννήτορες με μέγεθος παρτίδας 32
print("LOADING IMAGE DATASET WITH BATCH SIZE OF {}...".format(batch_size_train_one))
train_generator, val_generator = get_train_val_generator(batch_size_train_one)

#Υπολογισμός βημάτων εκπαίδευση
train_steps=train_generator.n//train_generator.batch_size
val_samples=val_generator.n//val_generator.batch_size

print("LOAD Xception Model / Createting RNN Parallel Model...")
input_tensor = Input(shape=(img_width, img_height,3))

# Φόρτωση του Xception Μοντέλου με βάρη εκπαίδευσης από ImageNet
cnn_model= Xception(weights='imagenet', include_top=False, input_tensor=input_tensor)
x = cnn_model.output
CNN_bottleneck = GlobalAveragePooling2D()(x)

# Απενεργοποίηση των στρωμάτων του Xception μοντέλου για εκπαίδευση
for layer in cnn_model.layers:
   layer.trainable = False

# Δημιουργία του RNN μοντέλου με δύο LSTM μεγέθους 2048
x = Lambda(rgb_to_grayscale, rgb_to_grayscale_output_shape)(input_tensor)
x = Reshape((16, 1024))(x)  # 16 χρονικές στιγμές, με μέγεθος δείγματος είσοδου1024 σε κάθε βήμα
x = LSTM(2048, return_sequences=True)(x) #LSTM με Batch Size 2048
RNN_output = LSTM(2048)(x) #LSTM με Batch Size 2048

# Οι δύο έξοδοι CNN_bottleneck και RNN_output συγχωνεύονται με πολλαπλασιασμό. Η έξοδος #αυτού του πολλαπλασιασμού τροφοδοτείται στο στρώμα ταξινόμησης που αποτελείται από #2 κόμβους (2 κλάσεις) και την συνάρτηση ενεργοποίησης softmax

x = Multiply()([CNN_bottleneck, RNN_output])
predictions = Dense(2, activation='softmax')(x)
```

```
model = Model(inputs=[input_tensor], outputs=predictions)
# Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης RMSProp
model.compile(optimizer='rmsprop',loss='categorical_crossentropy' ,metrics=['accuracy'])
print("Starting training")

# Σημείο ελέγχου 1
filepath="weights_xception_rnn.h5"
#Αποθήκευση της καλύτερης μέγιστης τιμής val_accuracy
checkpoint = ModelCheckpoint(filepath, monitor='val_accuracy', verbose=1, save_best_only=True, mode='max')
callbacks_list = [checkpoint]

#Έναρξη της πρώτης φάσης εκπαίδευσης του CNN-RNN μοντέλου
model.fit_generator(train_generator,
                    steps_per_epoch=train_steps,
                    epochs=nba_epochs,
                    verbose=1,
                    validation_data=val_generator,
                    validation_steps=val_samples,
                    callbacks=callbacks_list)
```

- Κατά τη δεύτερη φάση δεν έχει γίνει κάποια αλλαγή σε σχέση με την πρώτη πειραματική διαδικασία.

```
#Φορτώνονται δύο νέοι Γεννήτορες με μικρότερο μέγεθος παρτίδας 16 για να μην προκληθεί #εξάντληση της μνήμης της GPU
print("LOADING IMAGE DATASET WITH BATCH SIZE OF {}...".format(batch_size_train_two))
train_generator, val_generator = get_train_val_generator(batch_size_train_two)

train_steps=train_generator.n//train_generator.batch_size
val_samples=val_generator.n//val_generator.batch_size
print("\n Dataset loaded \n")

#Φόρτωση βαρών από τη πρώτη φάση εκπαίδευσης
model.load_weights(filepath)

# Ενεργοποίηση όλων των στρωμάτων για εκπαίδευση
for layer in model.layers:
   layer.trainable = True
# Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης Adam
model.compile(optimizer=Adam(lr=LR), loss='categorical_crossentropy',
          metrics=['accuracy', 'top_k_categorical_accuracy'])
# Σημείο Ελέγχου 2
filepath="finetuned_weights_xception_rnn.h5"
```

```
#Αποθήκευση της καλύτερης μέγιστης τιμής val_accuracy
checkpoint = ModelCheckpoint(filepath, monitor='val_accuracy', verbose=1, save_best_only=True, mode='max')
callbacks_list1 = [checkpoint]

print("\n----------Fit Xception-RNN Model---------- \n")

#Έναρξη της δεύτερης φάσης εκπαίδευσης του CNN-RNN μοντέλου
history=model.fit_generator(train_generator,
            steps_per_epoch=train_steps,
            epochs=nbb_epochs,
            verbose=1,
            validation_data=val_generator,
            validation_steps=val_samples,
            callbacks=callbacks_list1)

# Αποθήκευση CNN-RNN μοντέλου
save.model('Xception-RNN-Model.h5')

print("Training done")
model.load_weights(filepath)

model.compile(optimizer=Adam(lr=LR), loss='categorical_crossentropy',
        metrics=['accuracy', 'top_k_categorical_accuracy'])
```

Για τη διερεύνηση της βέλτιστης ακριβείας επικύρωσης το μοντέλο έτυχε εκπαίδευσης (training), επικύρωσης(validation) και δοκιμής (test) από τρεις (3) ρυθμούς εκπαίδευσης lr0.01, lr.0.001 και lr0.0001 ανά τύπο σετ δεδομένων (Hilbert, Zigzag, Zorder) . Κατά την ολοκλήρωση της διαδικασίας εκπαίδευσης, καταγράφηκαν τα αποτελέσματα τα οποία παρουσιάζονται στα Παραρτήματα Γ3,Δ3 και Ε3 .

Για την παρουσίαση των αποτελεσμάτων σε γράφημα καθώς και την αποθήκευση των αποτελεσμάτων εκπαίδευσης σε .txt αρχείο χρησιμοποιήθηκε ο ακόλουθος κώδικας:

```
# Δημιουργία Γραφήματος και Αποθήκευση Αποτελεσμάτων
acc = history.history['accuracy']
val_acc = history.history['val_accuracy']
loss=history.history['loss']
val_loss=history.history['val_loss']
epochs_range = range(nbb_epochs)

plt.figure(figsize=(20, 10))
```

```
plt.subplot(1, 2, 1)
plt.plot(epochs_range, acc, label='Training Accuracy')
plt.plot(epochs_range, val_acc, label='Validation Accuracy')
plt.legend(loc='lower right')
plt.title('Training and Validation Accuracy')
plt.subplot(1, 2, 2)
plt.plot(epochs_range, loss, label='Training Loss')
plt.plot(epochs_range, val_loss, label='Validation Loss')
plt.legend(loc='upper right')
plt.title('Training and Validation Loss')
#Αποθήκευση Γραφήματος
plt.savefig("Xception-RNN "+curves+" lr"+str(LR)+ " 128x128.png")
#Υπολογισμός αποτελέσματος εκπαίδευσης επί της εκατό.
scores = model.evaluate_generator(val_generator, val_samples=val_samples)
print(model.metrics_names, scores)
print("%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100))
file_score=model.metrics_names, scores
file_score1= "%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100)
#Αποθήκευση αποτελεσμάτων στο αρχείο info.txt
f = open("info.txt", "a")
f.write("Train \n\n"+ str(file_score)+"\n\n" + str(file_score1)+"\n\n")
f.close()
```

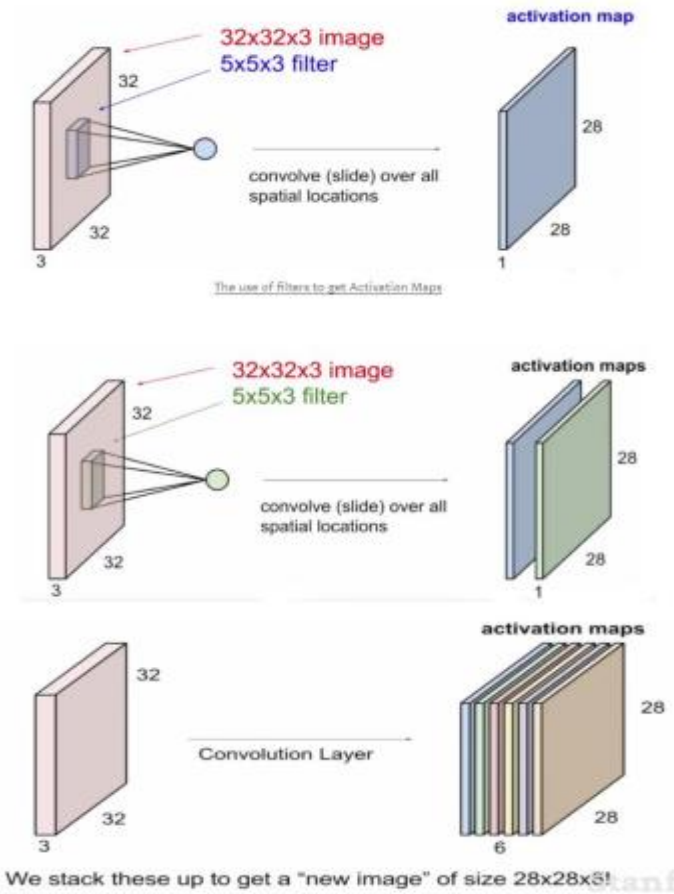
## 4.6 Τέταρτο Στάδιο Πειράματος

Για την ανάπτυξη του τρίτου μέρους της πειραματικής διαδικασίας δημιουργήθηκε σε γλώσσα προγραμματισμού Python και με τη χρήση της βιβλιοθήκης Keras-TensorFlow ένα Συνελικτικό Νευρωνικό Δίκτυο (Convolutional Neural Network). Τα Συνελικτικά Νευρωνικά Δίκτυα έχουν μεγάλη ομοιότητα με τα συνήθη Νευρωνικά Δίκτυα και έχουν καθιερωθεί να χρησιμοποιούνται κυρίως σε συστήματα τα οποία ασχολούνται με θέματα ταξινόμησης και αναγνώρισης εικόνων, λόγω εξαγωγής καλών αποτελεσμάτων. Για την εξόρυξη συγκριτικών αποτελεσμάτων ακρίβειας ταξινόμησης εικόνων, υλοποιήθηκε ένα Συνελικτικό Νευρωνικό Δίκτυο το οποίο περιέχει εννέα (9) στρώματα εκ των οποίων τα τέσσερα (4) είναι επίπεδα συνέλιξης.

### 4.6.1 Αρχιτεκτονική Μοντέλου

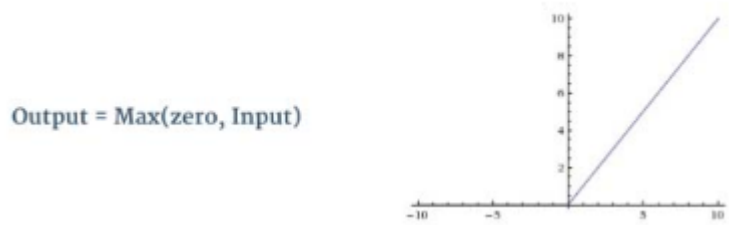
Αρχικά ορίζουμε το μοντέλο μας ως μια γραμμική στοίβα επιπέδων Sequential( ). Στη συνέχεια το Συνελικτικό Νευρωνικό Δίκτυο (CNN) λειτουργεί σε τρία στάδια.

Στο πρώτο στάδιο υπάρχει το στρώμα συνέλιξης που λαμβάνει ως είσοδο εικόνες με ύψος 128, πλάτος 128 και αριθμό καναλιών εικόνας 3. Ο αριθμός καναλιών χαρακτηρίζει τα τρία (3) χρώματα της εικόνας, κόκκινο, μπλε και πράσινο. Το πρώτο στρώμα αποτελείται από μια συνέλιξη η οποία χρησιμοποιεί φίλτρα τα οποία εντοπίζουν τα κύρια χαρακτηριστικά που παρουσιάζονται στην εικόνα εισόδου. Στο παρόν δίκτυο δημιουργούνται 32 φίλτρα με σχήμα (3,3,3). Κάθε φίλτρο σαρώνει κατά πλάτος και κατά ύψος τα εικονοστοιχεία (pixels) της εικόνας. Κάθε φορά υπολογίζεται ένα γινόμενο εσωτερικά για να εξαχθεί ακολούθως ένας χάρτης χαρακτηριστικών. Τέλος από όλα τα φίλτρα, προκύπτει στην έξοδο ένα σύνολο από χάρτες χαρακτηριστικών στους οποίους περιέχονται τα κύρια χαρακτηριστικά της εικόνας εισόδου. Στο Σχήμα 2 παρουσιάζεται ένα παράδειγμα παραγωγής τέτοιων χαρτών .




**Σχήμα 2.** Εφαρμογή φίλτρων στην αρχική εικόνα και παραγωγή χαρτών χαρακτηριστικών.

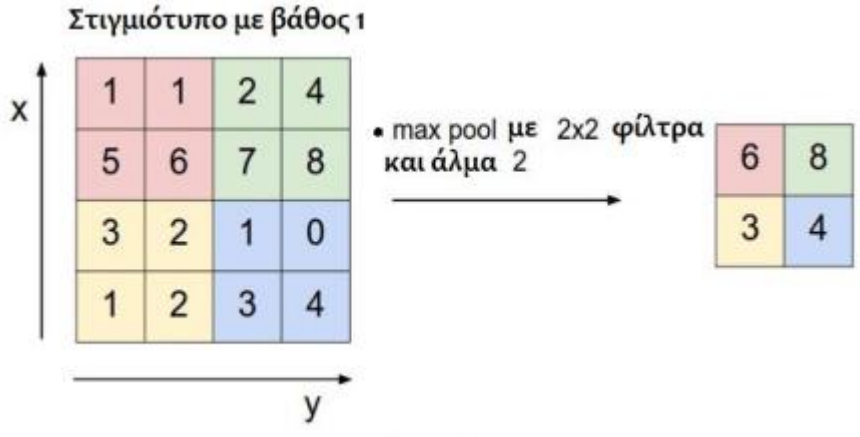
Επίσης στο πρώτο στρώμα χρησιμοποιείται και η συνάρτηση ενεργοποίησης Relu (μη γραμμική) η οποία εκτελεί μια συγκεκριμένη πράξη με σκοπό να αντικαταστήσει με μηδέν (0) τις αρνητικές τιμές έτσι ώστε οι εκάστοτε νευρώνες να μην ενεργοποιηθούν. Αυτή η συνάρτηση καθιστά πιο αποδοτικό το δίκτυο γιατί δε λειτουργούν όλοι οι νευρώνες κάθε φορά.
Η παραγωγή της συνάρτησης ενεργοποίησης Relu δίνεται από:




**Εικόνα 19.** Γραφική απεικόνιση της συνάρτησης Relu.

Στο δεύτερο στάδιο χρησιμοποιείται ένα στρώμα ομαλοποίησης της παρτίδας (Batch Normalization) το οποίο ομαλοποιεί κάθε κανάλι εισόδου σε μια μίνι παρτίδα. Η ομαλοποίηση παρτίδας επιταχύνει την εκπαίδευση των συνελικτικών νευρωνικών δικτύων και σε ορισμένες περιπτώσεις μειώνει κατά το ήμισυ τις εποχές μειώνοντας το σφάλμα γενίκευσης.

Το τρίτο στάδιο είναι το στάδιο της ομαδοποίησης (pooling) στο οποίο γίνεται απομείωση της διάστασης του κάθε χαρακτηριστικού και στην περίπτωση αυτή διαλέγεται μόνο η μέγιστη τιμή από το (pool) γι' αυτό και ονομάζεται (Max-pooling). Αυτό πρακτικά γίνεται με τον ίδιο τρόπο όπως συμβαίνει στα φίλτρα στο επίπεδο συνέλιξης. Κάθε φίλτρο σαρώνει την εικόνα εισόδου και αποθηκεύει μόνο τη μέγιστη τιμή. Το σχήμα του φίλτρου σε αυτή την περίπτωση είναι (2,2). Ένα (Max- pooling) παράδειγμα διαφαίνεται στο Σχήμα 3 .




**Σχήμα 3.** Παράδειγμα Max Pooling

Ακολούθως στο τέταρτο στάδιο εισάχθηκε το στάδιο της απόσυρσης (Dropout (0.2)). Στο στάδιο αυτό ένα ποσοστό (0.2) αποσύρεται τυχαία από το δίκτυο, ορίζοντας την τιμή εξόδου του το μηδέν (0). Αυτό βοηθά στην αποφυγή της υπερεκπαίδευσης (overfitting).

Ο ακόλουθος κώδικας αποτελεί το πρώτο επίπεδο του συνελικτικού δικτύου:

```
model= Sequential()
model.add(Conv2D(32,kernel_size=3,activation='relu',input_shape=(128,128,3)))
model.add(BatchNormalization())
model.add(MaxPool2D(strides=(2,2)))
model.add(Dropout(0.2))
```

Ο πιο πάνω κώδικας επαναλαμβάνεται ακόμη τρεις διαδοχικές φορές, μόνο που στις δύο τελευταίες γίνεται αύξηση του μεγέθους του φίλτρου συνέλιξης όπως φαίνεται πιο κάτω.

```
model.add(Conv2D(32,kernel_size=3,activation='relu'))
model.add(BatchNormalization())
model.add(MaxPool2D(strides=(2,2)))
model.add(Dropout(0.2))

model.add(Conv2D(64,kernel_size=3,activation='relu'))
model.add(BatchNormalization())
model.add(MaxPool2D(strides=(2,2)))
model.add(Dropout(0.2))
```

```
model.add(Conv2D(64,kernel_size=3,activation='relu'))
model.add(BatchNormalization())
model.add(MaxPool2D(strides=(2,2)))
model.add(Dropout(0.2))
```

Στη συνέχεια μετά τα τέσσερα επίπεδα εφαρμόζεται το επίπεδο συμπίεσης (Flatten Layer) όπου η έξοδος του τέταρτου συνελικτικού στρώματος μετατρέπεται από έναν πολυδιάστατο (tensor) σε έναν μονοδιάστατο πίνακα.

Εισάγονται δύο πυκνά (Dense) στρώματα. Τα πυκνά (Dense) στρωματά είναι συνηθισμένα στρωματά του νευρωνικού δικτύου. Σε αυτά τα στρωματά κάθε νευρώνας λαμβάνει ως είσοδο στοιχεία από τους προηγούμενους συνδεδεμένους νευρώνες δημιουργώντας πυκνές συνδέσεις, εξού και το όνομα Dense. Το κάθε στρώμα περιέχει έναν πίνακα βαρών W, έναν φορέα πόλωσης b και τη συνάρτηση ενεργοποίησης του προηγούμενου στρώματος. Τα πυκνά στρώματα είναι επίσης ευπροσάρμοστα, καθώς μπορούν να χρησιμοποιηθούν ως κρυμμένα στρώματα και ως στρώματα εισόδου και εξόδου.

Το πρώτο πυκνό (Dense) στρώμα, λαμβάνει στοιχεία από τους προηγούμενος συνδεδεμένους νευρώνες και στην έξοδο του παράγεται ένα σχήμα μεγέθους 512 με συνάρτηση ενεργοποίησης Softmax. Το επόμενο πυκνό (Dense) στρώμα λαμβάνει ένα σχήμα εισόδου 512 και με ενεργοποίηση Softmax και παράγει στην έξοδό του ένα σχήμα 128 . Ακολούθως εισάχθηκε το στάδιο της απόσυρσης (Dropout (0.2)) με στόχο την αποφυγή υπερεκπαίδευσης (overfitting). Τέλος εισάχθηκε ένα πυκνό (Dense) στρώμα το οποίο παρείχε στην έξοδο του ένα σχήμα μεγέθους δύο (2) όσος και αριθμός των κλάσεων ταξινόμησης, με συνάρτηση ενεργοποίησης Softmax. Η Softmax συνάρτηση είναι μια γενίκευση της λογιστικής συνάρτησης σε πολλαπλές διαστάσεις και χρησιμοποιείται ως η τελευταία συνάρτηση ενεργοποίησης στο συνελικτικό νευρωνικό δίκτυο με σκοπό την ομαλοποίηση της εξόδου και την κατανομή πιθανοτήτων στις κλάσεις εξόδου του δικτύου (Wikipedia 200).

```
model.add(Flatten())
model.add(Dense(512,activation="softmax"))
model.add(Dense(128,activation="softmax"))
model.add(Dropout(0.2))
model.add(Dense(2, activation="softmax"))
```

### 4.6.2 Εισαγωγή και Προ επεξεργασία Εικόνας

Για την εισαγωγή και προ επεξεργασία εικόνας χρησιμοποιείται όπως και στις προηγούμενες πειραματικές διαδικασίες η κλάση ImageDataGenerator του Keras εντός της μεθόδου get_train_val_generator(). Εντός του ImageDataGenerator χρησιμοποιείται η λειτουργία rescale=1./255 η οποία μετατρέπει κάθε τιμή εικονοστοιχείο (pixel) της εικόνας από το εύρος [0,255] σε [0,1]. Η κλάση ImageDataGenerator έχει μια μέθοδο που ονομάζεται flow_from_directory() η οποία χρησιμοποιείται για να διαβάσει εικόνες από φακέλους. Για την υλοποίηση εκπαίδευσης, επικύρωσης και δοκιμής των μοντέλων, χρησιμοποιήθηκε η ίδια δομή φακέλων με τις προηγούμενες πειραματικές.

```
def get_train_val_generator(batch_size=32):
  train_datagen=ImageDataGenerator(rescale=1./255)

  train_generator=train_datagen.flow_from_directory(train_data_path,
                              target_size=(img_width,img_height),
                              batch_size=batch_size,
                              color_mode='rgb',
                              class_mode='categorical',
                              shuffle=True)

  val_datagen=ImageDataGenerator(rescale=1./255)

  val_generator=val_datagen.flow_from_directory(validation_data_path,
                              target_size=(img_width,img_height),
                              batch_size=batch_size,
                              color_mode='rgb',
                              class_mode='categorical',
                              shuffle=True)
  return train_generator, val_generator
```

### 4.6.3 Εκπαίδευση (CNN) Μοντέλου

Το προαναφερθέν Συνελικτικό Νευρωνικό Δίκτυο εκπαιδεύτηκε με τη χρήση του αλγόριθμου βελτιστοποίησης RMSProp ο οποίος σχεδιάστηκε με στόχο τη βελτιστοποίηση των τιμών των βαρών (weights) των νευρώνων καθώς και τη μέγιστη δυνατή μείωση του κόστους (loss) εκπαίδευσης και επικύρωσης. Οι εικόνες εκπαίδευσης εισήχθησαν ανά παρτίδα των δεκαέξι (16 batch_size) σε κάθε επανάληψη και το κόστος υπολογίστηκε βάσει των εικόνων επικύρωσης (validation images). Το μοντέλο μετά από αρκετές πειραματικές προσπάθειες αποφασίσθηκε να περιοριστεί στις διακόσιες εποχές (200) εκπαίδευσής (epochs). Πέραν των διακοσίων (200) εποχών δεν παρουσιαζόταν περεταίρω βελτίωση. Για τον υπολογισμό των βημάτων εκπαίδευσης, διαιρέθηκε το πλήθος των εικόνων εκπαίδευσης με το μέγεθος παρτίδας, έτσι προέκυψαν σαράντα έξι (46) βήματα εκπαίδευσης ανά εποχή. Κατά τη φάση της εκπαίδευσης σε κάθε εποχή υλοποιείτο σύγκριση του ποσοστό ακριβείας επικύρωσης με τις προηγούμενες εποχές και εκτελείτο αποθήκευση της καλύτερης μέγιστης τιμής. Ο κώδικας που χρησιμοποιήθηκε για την εκπαίδευση φαίνεται παρακάτω:

```
# Φορτώνονται δύο Γεννήτορες με μέγεθος παρτίδας 16
train_generator, val_generator =  get_train_val_generator(batch_size)
#Υπολογισμός βημάτων εκπαίδευση
train_steps=train_generator.n//train_generator.batch_size
val_samples=val_generator.n//val_generator.batch_size

model= Sequential()
model.add(Conv2D(32,kernel_size=3,activation='relu',input_shape=(128,128,3)))
model.add(BatchNormalization())
model.add(MaxPool2D(strides=(2,2)))
model.add(Dropout(0.2))
model.add(Conv2D(32,kernel_size=3,activation='relu'))
model.add(BatchNormalization())
model.add(MaxPool2D(strides=(2,2)))
model.add(Dropout(0.2))
model.add(Conv2D(64,kernel_size=3,activation='relu'))
model.add(BatchNormalization())
```

```
model.add(MaxPool2D(strides=(2,2)))
model.add(Dropout(0.2))
model.add(Conv2D(64,kernel_size=3,activation='relu'))
model.add(BatchNormalization())
model.add(MaxPool2D(strides=(2,2)))
model.add(Dropout(0.2))
model.add(Flatten())
model.add(Dense(512,activation="softmax"))
model.add(Dense(128,activation="softmax"))
model.add(Dropout(0.2))
model.add(Dense(2, activation="softmax"))

rms=keras.optimizers.RMSprop(learning_rate=LR, rho=0.9)
# Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης RMSProp
model.compile(loss='categorical_crossentropy',optimizer=rms, metrics=['accuracy'])

# Σημείο ελέγχου
filepath="my_cnn_model_weights.h5"
#Αποθήκευση της καλύτερης μέγιστης τιμής val_accuracy
checkpoint = ModelCheckpoint(filepath, monitor='val_accuracy', verbose=1, save_best_only=True, mode='max')
callbacks_list = [checkpoint]

#Έναρξη εκπαίδευσης του CNN μοντέλου
history=model.fit_generator(train_generator,
                            steps_per_epoch=train_steps,
                            epochs=epochs,
                            callbacks=callbacks_list,
                            validation_data=val_generator,
                            validation_steps=val_samples
                            )
#Αποθήκευση CNN Μοντέλου
model.save('my_cnn_model.h5')
```

Για τη διερεύνηση της βέλτιστής ακριβείας επικύρωσης το μοντέλο έτυχε εκπαίδευσης (training), επικύρωσης(validation) και δοκιμής (test) από τρεις (3) ρυθμούς εκπαίδευσης lr0.01, lr.0.001 και lr0.0001 ανά τύπο σετ δεδομένων (Hilbert, Zigzag, Zorder) . Κατά την

ολοκλήρωση της διαδικασίας εκπαίδευσης, καταγράφηκαν τα αποτελέσματα τα οποία παρουσιάζονται στα Παραρτήματα Γ4,Δ4 και Ε4 .

Για την παρουσίαση των αποτελεσμάτων σε γράφημα καθώς και την αποθήκευση των αποτελεσμάτων εκπαίδευσης σε .txt αρχείο χρησιμοποιήθηκε ο ακόλουθος κώδικας:

```
# Δημιουργία Γραφήματος και Αποθήκευση Αποτελεσμάτων
acc = history.history['accuracy']
val_acc = history.history['val_accuracy']
loss=history.history['loss']
val_loss=history.history['val_loss']
epochs_range = range(epochs)
plt.figure(figsize=(20, 10))
plt.subplot(1, 2, 1)
plt.plot(epochs_range, acc, label='Training Accuracy')
plt.plot(epochs_range, val_acc, label='Validation Accuracy')
plt.legend(loc='lower right')
plt.title('Training and Validation Accuracy')

plt.subplot(1, 2, 2)
plt.plot(epochs_range, loss, label='Training Loss')
plt.plot(epochs_range, val_loss, label='Validation Loss')
plt.legend(loc='upper right')
plt.title('Training and Validation Loss')
#Αποθήκευση Γραφήματος
plt.savefig("My_CNN_Model "+curves+" lr"+str(LR)+ " 128x128.png")

#Υπολογισμός αποτελέσματος εκπαίδευσης επί της εκατό.
scores = model.evaluate_generator(val_generator, val_samples=val_samples)
print(model.metrics_names, scores)
print("%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100))
file_score=model.metrics_names, scores
file_score1= "%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100)

#Αποθήκευση αποτελεσμάτων στο αρχείο info.txt
f = open("info.txt", "a")
f.write("lr= " + str(LR) + "\n\n1st step Train \n\n"+ str(file_score)+"\n\n" + str(file_score1)+"\n\n")
f.close()
```

## 4.7 Παρουσίαση Αποτελεσμάτων και Συμπεράσματα

Κατά το πέρας εκπαίδευσης των προαναφερθέντων μοντέλων καταγράφηκαν τα ακόλουθα αποτελέσματα εκπαίδευσης χρησιμοποιώντας εικόνες οπτικοποίησης του πηγαίου κώδικα ιστότοπων με καμπύλες Hilbert, Zigzag και Zorder αντίστοιχα. Τα αποτελέσματα όπως φαίνεται στον Πίνακα 3, 4 και 5 αφορούν την ακρίβεια επικύρωσης (validation accuracy) των τεσσάρων μοντέλων.

| Learning Rate | MobileNet | MobileNet-RNN | Xception-RNN | Custom CNN |
|---|---|---|---|---|
| 0.01 | 95.83% | 98.26% | 96.88% | 76.74% |
| 0.001 | 97.57% | 98.26% | 93.40% | 97.22% |
| 0.0001 | 94.10% | **98.61%** | 93.75% | 95.83% |

**Πίνακας 3.** Ποσοστό Ακρίβειας Επικύρωσης Μοντέλων με Εικόνες Καμπύλης Hilbert

| Learning Rate | MobileNet | MobileNet-RNN | Xception-RNN | Custom CNN |
|---|---|---|---|---|
| 0.01 | 94.14% | 97.06% | 93.75% | 77.57% |
| 0.001 | 97.27% | 96.32% | 94.12% | 92.28% |
| 0.0001 | 92.97% | 95.22% | 94.12% | 94.85% |

**Πίνακας 4.** Ποσοστό Ακρίβειας Επικύρωσης Μοντέλων με Εικόνες Καμπύλης Zigzag

| Learning Rate | MobileNet | MobileNet-RNN | Xception-RNN | Custom CNN |
|---|---|---|---|---|
| 0.01 | 95.31% | 95.59% | 94.49% | 66.18% |
| 0.001 | 96.09% | 98.53% | 92.65% | 97.06% |
| 0.0001 | 94.92% | 96.32% | 94.49% | 89.71% |

**Πίνακας 5.** Ποσοστό Ακρίβειας Επικύρωσης Μοντέλων με Εικόνες Καμπύλης Zorder

Ακολούθως, τα εκπαιδευμένα μοντέλα δοκιμάστηκαν σε ένα σετ δοκιμών από εικόνες οπτικοποίησης του HTML πηγαίου κώδικα όπως παρουσιάζεται στο Παράρτημα Β, με καμπύλες Hilbert, Zigzag και Zorder αντίστοιχα . Το αποδεκτό πιθανό όριο επικύρωσης που ορίστηκε διαφαίνεται στον πιο κάτω Πίνακα 6. Τα αποτελέσματα όπως φαίνεται

στους Πίνακες 7, 8 και 9, αφορούν την ακρίβεια επικύρωσης (Validation Accuracy) του σετ δοκιμών των τεσσάρων μοντέλων. Ακολούθως στους Πίνακες 10, 11, και 12 παρουσιάζονται συγκριτικά αποτελέσματα επικύρωσης κατά την εκπαίδευση και κατά τη δοκιμή.

| **Πιθανά Όρια Επικύρωσης** | **Περιγραφή** |
|---|---|
| 0% μέχρι 50% | Εξαιρετικά Κακή Ταξινόμηση |
| 50% μέχρι 70% | Πολύ Κακή Ταξινόμηση |
| 70% μέχρι 80% | Κακή Ταξινόμηση |
| 80% μέχρι 90% | Αποδεκτή Ταξινόμηση |
| 90% μέχρι 95% | Πολύ Καλή Ταξινόμηση |
| 95% μέχρι 100% | Εξαιρετική Ταξινόμηση |

**Πίνακας 6.** Αποδεκτά Όρια Επικύρωσης

| **Μοντέλο** | **Lr.** | **Αληθής Επικυρώσεις Πάνω του 80%** | **Αληθής Επικυρώσεις Κάτω του 80%** | **Ψευδής Επικυρώσεις** | **Μέσος Όρος Ακρίβειας Αληθών Επικυρώσεων** | **Ποσοστό Ταξινόμηση Εικόνων** |
|---|---|---|---|---|---|---|
| MobileNet | 0.01 | 70 | - | 5 | 0,946253557 | 93,33% |
| **MobileNet** | **0.001** | **75** | **-** | **-** | **0,999985043** | **100%** |
| MobileNet | 0.0001 | 71 | - | 4 | 0,99371298 | 94,66% |
| MobileNet-RNN | 0.01 | 70 | 2 | 3 | 0,996106912 | 96% |
| **MobileNet-RNN** | **0.001** | **73** | **-** | **2** | **0,998498665** | **97,33%** |
| MobileNet-RNN | 0.0001 | 73 | - | 2 | 0,997736238 | 97,33% |
| Xception-RNN | 0.01 | 68 | - | 7 | 0,994775229 | 90,66% |
| Xception-RNN | 0.001 | 69 | 1 | 5 | 0,993881709 | 93,33% |
| Xception-RNN | 0,0001 | 72 | - | 3 | 0,999524403 | 96% |
| Custom-CNN | 0.01 | 43 | - | 32 | 0,867196192 | 57,33% |
| Custom-CNN | 0.001 | 73 | - | 2 | 0,982807324 | 97,33% |
| Custom-CNN | 0.0001 | 72 | 1 | 2 | 0,879223074 | 96% |
| | | | | **Συνολικός Μέσος Όρος ->** | **0,970808444** | **92,44%** |

**Πίνακας 7.** Αποτελέσματα σετ Δοκιμών από Εικόνες Καμπύλης Hilbert

| Μοντέλο | Lr. | Αληθής Επικυρώσεις Πάνω του 80% | Αληθής Επικυρώσεις Κάτω του 80% | Ψευδής Επικυρώσεις | Μέσος Όρος Ακρίβειας Αληθών Επικυρώσεων | Ποσοστό Ταξινόμηση Εικόνων |
|---|---|---|---|---|---|---|
| MobileNet | 0.01 | 68 | 2 | 5 | 0,983303621 | 93,33% |
| **MobileNet** | **0.001** | **75** | **-** | **-** | **0,996989355** | **100%** |
| MobileNet | 0.0001 | 71 | 1 | 3 | 0,991445187 | 94,66% |
| **MobileNet-RNN** | **0.01** | **74** | **-** | **1** | **0,996568472** | **98,66%** |
| MobileNet-RNN | 0.001 | 71 | - | 4 | 0,998176944 | 94,66% |
| MobileNet-RNN | 0.0001 | 71 | - | 4 | 0,99891812 | 94,66% |
| Xception-RNN | 0.01 | 71 | 2 | 2 | 0,979511879 | 94,66% |
| Xception-RNN | 0.001 | 70 | 1 | 4 | 0,995077651 | 93,33% |
| Xception-RNN | 0,0001 | 72 | - | 3 | 0,99999999 | 96% |
| Custom-CNN | 0.01 | 57 | 2 | 16 | 0,851514265 | 76% |
| Custom-CNN | 0.001 | 72 | - | 3 | 0,987777641 | 96% |
| Custom-CNN | 0.0001 | 74 | - | 1 | 0,863701999 | 98,66% |
| | | | | **Συνολικός Μέσος Όρος ->** | **0,97024876** | **94,21%** |

**Πίνακας 8.** Αποτελέσματα σετ Δοκιμών από Εικόνες Καμπύλης Zigzag

| Μοντέλο | Lr. | Αληθής Επικυρώσεις Πάνω του 80% | Αληθής Επικυρώσεις Κάτω του 80% | Ψευδής Επικυρώσεις | Μέσος Όρος Ακρίβειας Αληθών Επικυρώσεων | Ποσοστό Ταξινόμηση Εικόνων |
|---|---|---|---|---|---|---|
| MobileNet | 0.01 | 72 | - | 3 | 0,992762548 | 96% |
| MobileNet | 0.001 | 72 | 1 | 2 | 0,995020434 | 96% |
| **MobileNet** | **0.0001** | **74** | **-** | **1** | **0,999615845** | **98,66%** |
| MobileNet-RNN | 0.01 | 71 | 1 | 3 | 0,991945092 | 94,66% |
| MobileNet-RNN | 0.001 | 71 | 1 | 3 | 0,995200505 | 94,66% |
| MobileNet-RNN | 0.0001 | 70 | 1 | 4 | 0,999344703 | 93,33% |
| Xception-RNN | 0.01 | 71 | - | 4 | 0,990745661 | 94,66% |
| Xception-RNN | 0.001 | 69 | - | 6 | 0,998917979 | 92% |
| **Xception-RNN** | **0,0001** | **71** | **-** | **4** | **0,999760701** | **94,66%** |
| Custom-CNN | 0.01 | 65 | - | 10 | 0,875755801 | 86,66% |
| Custom-CNN | 0.001 | 66 | 1 | 8 | 0,954005681 | 88% |
| Custom-CNN | 0.0001 | 69 | - | 6 | 0,916535914 | 92% |
| | | | | **Συνολικός Μέσος Όρος ->** | **0,975800905** | **85,55%** |

**Πίνακας 9.** Αποτελέσματα σετ Δοκιμών από Εικόνες Καμπύλης Zorder

| Lr. | Μοντέλο | Επικύρωση Εκπαίδευσης | Επικύρωση Δοκιμών |
|---|---|---|---|
| 0.01 | MobileNet | 95,83% | 93,33% |
| 0.001 | MobileNet | 97,57% | **100%** |
| 0.0001 | MobileNet | 94,10% | 94,66% |
| 0.01 | MobileNet-RNN | **98,26%** | 96% |
| 0.001 | MobileNet-RNN | **98,26%** | **97,33%** |
| 0.0001 | MobileNet-RNN | **98,61%** | 97,33% |
| 0.01 | Xception-RNN | 96,88% | 90,66% |
| 0.001 | Xception-RNN | 93,40% | 93,33% |
| 0.0001 | Xception-RNN | 93,75% | 96% |
| 0.01 | Custom-CNN | 76,74% | 57,33% |
| 0.001 | Custom-CNN | 97,22% | 97,33% |
| 0.0001 | Custom-CNN | 95,83% | 96% |

**Πίνακας 10.** Συγκριτικά Αποτελέσματα Επικύρωσης Κατά την Εκπαίδευση και Αποτελέσματα Επικύρωσης Κατά τη Δοκιμή σε Εικόνες Hilbert.

| Lr. | Μοντέλο | Επικύρωση Εκπαίδευσης | Επικύρωση Δοκιμών |
|---|---|---|---|
| 0.01 | MobileNet | 94,14% | 93,33% |
| **0.001** | **MobileNet** | **97,27%** | **100%** |
| 0.0001 | MobileNet | 92,97% | 94,66% |
| **0.01** | **MobileNet-RNN** | **97,06%** | **98,66%** |
| 0.001 | MobileNet-RNN | 96,32% | 94,66% |
| 0.0001 | MobileNet-RNN | 95,22% | 94,66% |
| 0.01 | Xception-RNN | 93,75% | 94,66% |
| 0.001 | Xception-RNN | 94,12% | 93,33% |
| 0.0001 | Xception-RNN | 94,12% | 96% |
| 0.01 | Custom-CNN | 77,57% | 76% |
| 0.001 | Custom-CNN | 92,28% | 96% |
| 0.0001 | Custom-CNN | 94,85% | 98,66% |

**Πίνακας 11.** Συγκριτικά Αποτελέσματα Επικύρωσης Κατά την Εκπαίδευση και Αποτελέσματα Επικύρωσης Κατά τη Δοκιμή σε Εικόνες Zigzag.

| Lr. | Μοντέλο | Επικύρωση Εκπαίδευσης | Επικύρωση Δοκιμών |
|---|---|---|---|
| 0.01 | MobileNet | 95,31% | 96% |
| 0.001 | MobileNet | 96,09% | 96% |
| 0.0001 | MobileNet | 94,92% | **98,66%** |
| 0.01 | MobileNet-RNN | 95,59% | 94,66% |
| 0.001 | MobileNet-RNN | **98,53%** | 94,66% |
| 0.0001 | MobileNet-RNN | 96,32% | 93,33% |
| 0.01 | Xception-RNN | 94,49% | 94,66% |
| 0.001 | Xception-RNN | 92,65% | 92% |
| 0.0001 | Xception-RNN | 94,49% | **94,66%** |
| 0.01 | Custom-CNN | 66,18% | 86,66% |
| 0.001 | Custom-CNN | **97,06%** | 88% |
| 0.0001 | Custom-CNN | 89,71% | 92% |

**Πίνακας 12.** Συγκριτικά Αποτελέσματα Επικύρωσης Κατά την Εκπαίδευση και Αποτελέσματα Επικύρωσης Κατά τη Δοκιμή σε Εικόνες Zorder.

Σύμφωνα με τα πιο πάνω προαναφερθέντα αποτελέσματα στους Πίνακες 3, 4 και 5, τα αποτελέσματα εκπαίδευσης στο μοντέλο MobileNet-RNN με ρυθμό εκμάθησης lr 0.0001 και με σετ δεδομένων εικόνες καμπύλης Hilbert έχει πετύχει το υψηλότερο ποσοστό ακρίβειας επικύρωσης με 98,53%. Ωστόσο κατά τη φάση της διεξαγωγής της δοκιμής (test) δεν αντλήθηκαν ανάλογα αποτελέσματα με βάση το ποσοστό ακρίβειας επικύρωσης που έχουν ληφθεί κατά την εκπαίδευση. Σύμφωνα με τα αποτελέσματα που παρουσιάζονται στους πιο πάνω Πίνακες 7, 8 και 9 το MobileNet μοντέλο με ρυθμό εκμάθησης lr0.001 και με σετ εικόνων ελέγχου καμπύλης Hilbert παρουσιάζει μέγιστη ακρίβεια ταξινόμησης εικόνων στο 100% σε (phishing) και μέγιστο μέσο όρο ακρίβειας αληθούς πρόβλεψης 99,9% .

Λαμβάνοντας υπόψη τον συνολικό μέσο όρο ακρίβειας επικύρωσης (Validation Accuracy) αληθών προβλέψεων από όλα τα μοντέλα που χρησιμοποιήσαμε, αλλά και τον μέσο όρο ακρίβειας ταξινόμησης των δύο κλάσεων (phishing) και (legitimate), καταλήγουμε στο συμπέρασμα ότι οι εικόνες οι οποίες έχουν παραχθεί με Zigzag καμπύλες κατέχουν τον υψηλότερο μέσο όρο ακρίβειας επικύρωσης (Validation Accuracy) με 97,58%, ενώ ωστόσο κατέχουν το χαμηλότερο ποσοστό ταξινόμησης

εικόνων με βάση το σετ δοκιμών μας με μόλις 85,55% . Οι εικόνες οι οποίες έχουν παραχθεί με καμπύλες Hilbert και Zigzag παρουσιάζουν μέσο όρο ακρίβειας επικύρωσης (Validation Accuracy) στο 97% ο οποίος έχει μικρή απόσταση από το ποσοστό της Zorder καμπύλης. Όμως πετυχαίνουν αρκετά ψηλές αποδόσεις σε ό,τι αφορά τον μέσο όρο ακρίβειας ταξινόμησης των δύο κλάσεων με την καμπύλη Hilbert να πετυχαίνει το 92,44% και την καμπύλη Zigzag να πετυχαίνει το 94,21% που είναι και το υψηλότερο ποσοστό.

Επίσης παρατηρώντας συγκριτικά τα αποτελέσματα ακρίβειας επικύρωσης (validation accuracy) στους Πίνακες 3, 4 και 5, κατά την εκπαίδευση των μοντέλων MobileNet και MobileNet-RNN, παρουσιάζεται μια αύξηση του ποσοστού της ακρίβειας γύρω στο 2,5% λαμβάνοντας υπόψη τα συνολικά αποτελέσματα και από τους τρεις ρυθμούς εκπαίδευσης.

Από τον Πίνακα 7 στον οποίο παρουσιάζονται αποτελέσματα σετ δοκιμών από εικόνες καμπύλης Hilbert παρατηρούμε ότι το Custom-CNN δίκτυο με ρυθμό lr 0.001 έχει πετύχει υψηλά ικανοποιητικά αποτελέσματα όσον αφορά την ακρίβεια επικύρωσης καθώς και όσον αφορά την ακρίβεια ταξινόμησης με τα ποσοστά να είναι στο 98,28% και 97,33% αντίστοιχα. Αυτό μας οδηγεί στο συμπέρασμα ότι για την ταξινόμηση εικόνων οπτικοποίησης δεν είναι απαραίτητη η χρήση πολύ βαθιών συνελικτικών δικτύων με πολλά στρώματα συνέλιξης.

## 4.8 Σύνοψη Κεφαλαίου

Στο κεφάλαιο αυτό παρουσιάστηκε ο τρόπος υλοποίησης της πειραματικής φάσης της μεταπτυχιακής διατριβής. Παρουσιάστηκε η μεθοδολογία συλλογής και οπτικοποίησης των δεδομένων, η υλοποίηση, εκπαίδευση και δοκιμή των CNN καθώς και CNN-RNN μοντέλων με τη χρήση του Keras TensorFlow με τη βοήθεια της γλώσσας Python. Τέλος κατά το πέρας του πειράματος παρουσιάστηκαν τα αποτελέσματα και εξάχθηκαν συμπεράσματα βάσει αυτών.

# Κεφάλαιο 5
# Επίλογος

## 5.1 Συμπεράσματα

Κύριος στόχος της παρούσας μεταπτυχιακής διατριβής ήταν η απάντηση στο ερώτημα εάν η οπτικοποίηση του πηγαίου κώδικα από ιστότοπους ηλεκτρονικού ψαρέματος σε συνάρτηση με την εκπαίδευση CNN καθώς και CNN-RNN δικτύων μπορεί να χρησιμοποιηθεί με επιτυχία για την ανίχνευση ιστότοπων ηλεκτρονικού ψαρέματος. Η απάντηση στο ερώτημα δόθηκε κατά τη διεξαγωγή της πειραματικής διαδικασίας στην οποία ακολουθήθηκαν τέσσερις φάσεις: α) η φάση συλλογής πηγαίου κώδικα από νόμιμους ιστοτόπους και ιστότοπους ηλεκτρονικού ψαρέματος, β) η φάση οπτικοποίησης του πηγαίου κώδικα σε τρεις (3) διαφορετικές μορφές εικόνας, γ) η φάση της εκπαίδευσης των δικτύων CNN και CNN-RNN ούτως ώστε να κατηγοριοποιηθούν οι εικόνες σε εικόνες νόμιμων ιστότοπων και εικόνες ηλεκτρονικού ψαρέματος και δ) η φάση δοκιμών των εκπαιδευόμενων CNN και CNN-RNN δικτύων όπου υλοποιήθηκε στη βάση ενός συνόλου εικόνων οπτικοποίηση από ιστότοπους ηλεκτρονικού ψαρέματος με στόχο την κατηγοριοποίησή τους από τα εκπαιδευμένα νευρωνικά δίκτυα.

Όπως προέκυψε από την πειραματική διαδικασία, τα CNN δίκτυα παράλληλα με τα RNN προσφέρουν καλύτερα αποτελέσματα ακρίβειας επικύρωσης (validation accuracy). Αυτό φάνηκε κατά τη σύγκριση των αποτελεσμάτων ακρίβειας επικύρωσης (validation accurancy) κατά την εκπαίδευση των μοντέλων MobileNet και MobileNet-RNN όπου παρουσιάστηκε σημαντική βελτίωση.

Θα πρέπει να αναφερθεί επίσης ότι από τα αποτελέσματα της πειραματικής διαδικασίας συμπεραίνω ότι δεν είναι αναγκαία η χρήση πολυεπίπεδων νευρωνικών δικτύων με μεγάλο βάθος. Μπορούν να χρησιμοποιηθούν Συνελικτικά Νευρωνικά Δίκτυα με λίγα στρώματα και να παρουσιάσουν εξίσου ικανοποιητικά αποτελέσματα. Ως αποτέλεσμα

αυτό να παρέχει τη δυνατότητα κατασκευής εφαρμογών εντοπισμού ιστότοπων ηλεκτρονικού ψαρέματος ακόμη και σε συσκευές με χαμηλούς υπολογιστικούς πόρους.

Σε σχέση με τις μελέτες που αναφέρθηκαν στη βιβλιογραφική ανασκόπηση, η μέθοδος που χρησιμοποιήθηκε στην παρούσα μεταπτυχιακή διατριβή βασίστηκε στην απόξεση, στην οπτικοποίηση του HTML πηγαίου κώδικα και στη χρήση δικτύων CNN καθώς και CNN-RNN για την ταξινόμηση των ιστότοπων σε νόμιμους ή ιστότοπους ηλεκτρονικού ψαρέματος. Το ποσοστό ακρίβειας ταξινόμησης που πέτυχε το μοντέλο MobileNet με εικόνες καμπύλης Hilbert και με ρυθμό εκπαίδευσης 0.001 κατά τη φάση των δοκιμών έχει φτάσει στο 99% όπου αποτελεί ένα αρκετά ικανοποιητικό ποσοστό σε σχέση με τα αποτελέσματα των προαναφερθείσων μελετών. Επίσης η παρούσα μέθοδος παρέχει τη δυνατότητα ανίχνευσης ιστότοπων ηλεκτρονικού ψαρέματος που εμφανίζεται για πρώτη φορά (zero_day).

Εν κατακλείδι, η εν λόγω μεθοδολογία που χρησιμοποιήθηκε στην παρούσα μεταπτυχιακή διατριβή απέδειξε ότι είναι δυνατή η αναγνώριση ιστότοπων ηλεκτρονικού ψαρέματος με τη χρήση οπτικοποίησης του πηγαίου κώδικα HTML. Τα αποτελέσματα που λήφθηκαν κατά τη φάση των δοκιμών πρόβλεψης ήταν πολύ υψηλά με το ποσοστό κατηγοριοποίησης να φτάνει στο 100% και το ποσοστό επικύρωσης αληθούς πρόβλεψης στο 99,9%.

## 5.2 Προοπτικές

Για τη μελλοντική βελτίωση της παρούσας μεταπτυχιακής διατριβής θα ήταν δυνατή η προσπάθεια εκπαίδευσης των μοντέλων με περισσότερες κατηγορίες ιστότοπων ηλεκτρονικού ψαρέματος. Μερικές από τις κατηγορίες αυτές είναι: ιστότοποι που περιέχουν φόρμες για συμπλήρωση προσωπικών δεδομένων, ιστότοποι που περιέχουν φόρμες για συμπλήρωση δεδομένων πιστωτικών καρτών καθώς επίσης είναι σημαντικό να συμπεριληφθούν και οι ιστότοποι HTML σφάλματος 404 οι οποίοι ήταν αυξημένοι σε αριθμό κατά τη συλλογή ιστότοπων ηλεκτρονικού ψαρέματος. Τέλος, η συλλογή μεγαλύτερου όγκου δεδομένων για εκπαίδευση των μοντέλων θα συνέβαλλε στη βελτίωση των αποτελεσμάτων όπου η σύγκριση αυτών θα παρουσίαζε πιο ακριβή συμπεράσματα.

# Παράρτηματα Α
## Εξαρτόμενα Λογισμικά

| | | |
|---|---|---|
| Request | Csv | Sys |
| Optparse | Os | Mysql.connector |
| Base64 | Datetime | Cairo |
| Numpy | Pillow | TensorFlow2.0 |
| imgKit | Keras 2.0 | scurve |

# Παράρτημα Β
# Σετ Δεδομένων Δοκιμών

## Λίστα Συνδέσμων Ιστότοπων και Εικόνων για Δοκιμές.

| A/A | URL | Όνομα Εικόνας |
|---|---|---|
| **Adobe login** | | |
| **1.** | http://readmenw.beget.tech/excel.php | adobelogineadmenw.26.25.jpg |
| **2.** | https://gnoddrc.org/wp-admin/MMM/IK/index.php | adobelogingnoddrc.90.04.jpg |
| **3.** | https://huncoppe.tk/vas/nsw/data/UntitledNotebook1.html?run=login_cmd | adobeloginhuncoppe56.16.jpg |
| **4.** | http://modimedia.in/Adobe-2/quotation/ | adobeloginodimedia82.37.jpg |
| **5.** | https://www.creativecombat.com/wp-admin/network/acct/login.php?rand=13InboxLightaspxn.1774256418 | adobeloginwww.crea16.55.jpg |
| **Alibaba login** | | |
| **1.** | http://ddrevent.com/board/wp-content/themes/alibaba/ | alibabalogindrevent.65.04.jpg |
| **2.** | https://locbien.vn///wp-content/languages/login.alibaba-com | alibabaloginlocbien.01.64.jpg |
| **3.** | http://spinehealthpune.com/wp-content/Alibaba.com/ali/login.php | alibabaloginpineheal56.15.jpg |
| **4.** | http://www.diversepropertysolutions.com/login.alibaba.com.spm.a2700.8293689.scGlobalHomeHeader.355.QqbMrU.tracelog.hd.signin.diversepropertysolutions.com/manufacturers/Login.htm | alibabaloginww.diver49.92.jpg |
| **5.** | https://www.talecafe.com/js/Login.htm | alibabaloginwww.tale61.02.jpg |
| **Amazon login** | | |
| **1.** | https://bestfitter.com//wp-includes/images/wlw | amazonloginbestfitt19.01.jpg |
| **2.** | https://chinchillane62.co.uk/wp-content/uploads/2020/08/hgm/index.php | amazonloginchinchil67.95.jpg |
| **3.** | https://conntectflash.com/vicotfd | amazonloginconntect20.19.jpg |
| **4.** | https://decaiofad.ml/AEFWDFTYR34GVER/zam/saweq | amazonlogindecaiofa52.62.jpg |
| **5.** | http://bizbiz.tech/modules/overlay/swo/gps/file | amazonloginizbiz.te71.9.jpg |
| **AT&T login** | | |
| **1.** | https://docs.google.com/forms/d/e/1FAIpQLSepFB7MQOjzfGV3ugc69ffgXga-sq_PwgWMMWmazuPsYqS8uw/viewform?usp=sf_link | at&tlogindocs.goo12.02.jpg |
| **2.** | https://hilltopcleaners.com/recordede | at&tloginhilltopc34.37.jpg |
| **3.** | http://okletsbuy.com/attRR/adfs/index.html | at&tloginkletsbuy99.14.jpg |
| **4.** | https://mahdistrict.org/olu/att/attiinnddeexx.php | at&tloginmahdistr30.89.jpg |
| **5.** | https://zaroosha.in/journal/att-update/login.php? | at&tloginzaroosha94.26.jpg |
| **Bank of America login** | | |
| **1.** | http://35.188.36.185/bank_of_america/22-03-2020/AS42926/website/bimovia.com/wp-admin/user/www.bankofamerica.com.login.update | bankofamericalogin5.188.3665.04.jpg |
| **2.** | http://security.verify.arixbd.com/login.php?cmd=login_submit&id=47dfd616f6f2721fd849b5a517fd282d47dfd616f6f2721fd849b5a517fd282d&session=47dfd616f6f2721fd849b5a517fd282d47dfd616f6f2721fd849b5a517fd282d | bankofamericaloginecurity.26.59.jpg |
| **3.** | https://edificioplatino.com/boa/urgent/login.php?cmd=login_submit&id=7afcff2b0617b793cf192fb036d199207afcff2b06 | bankofamericaloginedificio77.17.jpg |

| | | |
|---|---|---|
| | 17b793cf192fb036d19920&session=7afcff2b0617b793cf192fb036d199207afcff2b0617b793cf192fb036d19920 | |
| **4.** | https://krjpl.com/BOFA/BankofAmerica_VerifyInformation.html | bankofamericaloginkrjpl.co60.86.jpg |
| **5.** | https://www.72dpi.co.il/wp-includes/js/jquery/ui/x1x/v2/bb9a6f82f38850a/login.php | bankofamericaloginwww.72dp49.28.jpg |
| **Chase Bank login** | | |
| **1.** | http://saigonsportcity.com/wp-content/plugins/Chasesupdate/Logon.php?LOB=RBGverify&_pageLabel=page_verify | chaseloginaigonspo91.35.jpg |
| **2.** | http://bellefontaineduilawyer.com/see/homes/index.php | chaseloginellefont45.61.jpg |
| **3.** | http://fotoblad.com/js/chaseonline/auth/login.php?cmd=login_submit&id=94f3501ed614c0af1bcf21f1479d1d6d94f3501ed614c0af1bcf21f1479d1d6d&session=94f3501ed614c0af1bcf21f1479d1d6d94f3501ed614c0af1bcf21f1479d1d6d | chaseloginotoblad.59.76.jpg |
| **4.** | http://downtowndavis.org/wp-content/plugins/id.html?&eventual-chase-international-dashboard9379487-jhbg76389 | chaseloginowntownd30.71.jpg |
| **5.** | https://track4securityglobal.com/wp-admin/csc/email.php | chaselogintrack4se64.7.jpg |
| **DHL login** | | |
| **1.** | http://macvedas.somee.com/dmlh_hl.html | dhlloginacvedas.27.57.jpg |
| **2.** | https://angelartepasteleria.com/Admin/DHL/dhl.php | dhlloginangelart32.29.jpg |
| **3.** | https://harmonium.co.za/0405/dhl/DHL | dhlloginharmoniu69.96.jpg |
| **4.** | https://hotelgrandpapua.com/enter/parcel/document/invoice/fd0c27b897abc4d22cb4b083fd09b1e2/deliveryform.php | dhlloginhotelgra46.79.jpg |
| **5.** | http://loganseguridad.cl/u.php?l=DHl-dTracking_=_JeHFUq_VJOXK0QWHtoGYDw=_JeHFUq_VJOXK0QWHtoGYDw=_JeHFUq_VJOXK0QWHto= | dhlloginogansegu00.33.jpg |
| **eBay login** | | |
| **1.** | https://7426fbe0d8676fde2cac756c0731ce57.udagwebspace.de/7e08701fe7e22e7e0b0fabe1c449c468ZjZiZDNjMmQxYTNlNWI4MmU2NzRhNjk2NWFmOWIwNTM=/signin/ | ebaylogin7426fbe061.09.jpg |
| **2.** | http://linkverified.uk/www.ebay.co.uk/itm/view/126548795655/ | ebayloginkverif23.96.jpg |
| **3.** | https://paleyprintco.com/ebay_login/indexxx.php | ebayloginpaleypri94.81.jpg |
| **4.** | http://urlsverified.uk/www.ebay.co.uk/itm/view/152499384301/ | ebayloginrlsverif45.47.jpg |
| **5.** | https://thongtinduhocduc.vn/1/1.html?signin.ebay.de/ws/eBayISAPI.dll?SignIn&UsingSSL=1&siteid=77&co_partnerId=2&pageType=2553753&ru=https://www.ebay.de/sh/research | ebayloginthongtin17.67.jpg |
| **Facebook login** | | |
| **1.** | https://adm.rightsbsnsrcvryhlp01.my.id | facebookloginadm.righ42.51.jpg |
| **2.** | http://phx.blewpass.com/direct/aHR0cHM6Ly9tb2JpbGUuZmFjZWJvb2suY29tL2xvZ2luLnBocD9uZXh0PWh0dHBzJTNBJTJGJTJGbW9iaWxlLmZhY2Vib29rLmNvbSUyRm5vdGlmaWNhdGlvbnMucGhwJTNGcmVmX2NvbXBvbmVudCUzRG1iYXNpY19ob21lX2hlYWRlciUyNnJlZl9wYWdlJTNEJTI1MkZ3YXAlMjUyRmhvbWUucGhwJTI2cmVmaWQlM0Q3JnJlZnNyYz1odHRwcyUzQSUyRiUyRm1vYmlsZS5mYWNlYm9vay5jb20lMkZub3RpZmljYXRpb25zLnBocCZyZWZpZD03JnJlZl9jb21wb25lbnQ9bWJhc2ljX2hvbWVfaGVhZGVyJl9yZHI- | facebookloginhx.blewp90.51.jpg |
| **3.** | https://joingrupwhatsappbokep2020.wagroupx.com/login.php | facebookloginjoingrup15.72.jpg |
| **4.** | https://securlty.be/4qzp2kmj2e06yvcl | facebookloginsecurlty22.26.jpg |
| **5.** | https://xvgbtoplm.cf/1000655841.html?fbclid=IwAR2lXALqGKtEtG7mh23JtMKHrWfz54ZodX3axUnMYasdW1QlFktRcb | facebookloginxvgbtopl00.11.jpg |
| **Google login** | | |
| **1.** | https://drive.google.com/file/d/1tenGIF9DF-oTkACTAg_tNEsT5ZWTZzKc/edit | googlelogindrive.go97.89.jpg |
| **2.** | http://headlampyardk.com/justonedrive.com/Onedrive_popup/verification.php | googlelogineadlampy24.96.jpg |
| **3.** | http://albel.intnet.mu/File/index.php | googleloginlbel.int84.28.jpg |
| **4.** | http://fluidaccountants.co.uk/essen/pg/pge/Project/ | googleloginluidacco20.43.jpg |

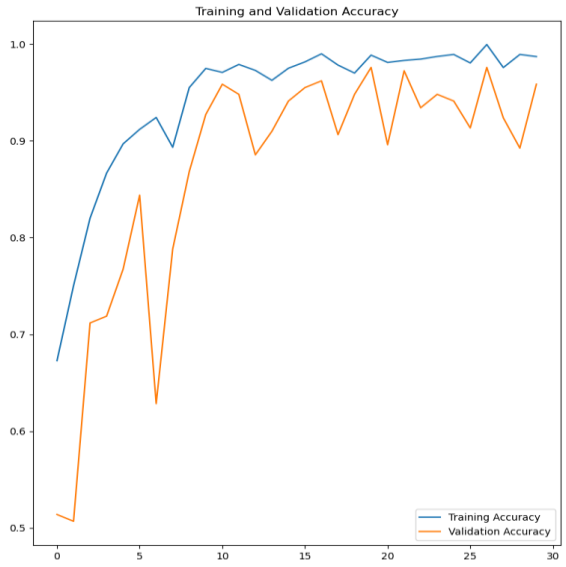
| | | |
|---|---|---|
| **5.** | https://sites.google.com/view/unpublish-unblocker/?ref=tn_tnmn | googleloginsites.go48.39.jpg |
| **LinkedIn login** | | |
| **1.** | http://mauricioynicole.com | linkedinloginauricioy76.35.jpg |
| **2.** | http://advtejas.com/poll/hggjk/hakam new/hakam new/hakam new/piled.php | linkedinlogindvtejas.76.89.jpg |
| **3.** | https://made-in-portsaid.com/wp-content/themes/martfury/new/LinkedinAUT/?email={{email}} | linkedinloginmade-in-59.37.jpg |
| **4.** | https://outlookmorning.com/uj/Linkedin/index2.html | linkedinloginoutlookm27.79.jpg |
| **5.** | http://wowwglass.com/wp-content/plugins/seo-ultimate/sucees/login.php | linkedinloginowwglass82.2.jpg |
| **Microsoft login** | | |
| **1.** | http://kakakakaka-986ff.ts.r.appspot.com/ | microsoftloginakakakak47.63.jpg |
| **2.** | https://dreamy-goldberg-a2a25d.netlify.app/ | microsoftlogindreamy-g35.49.jpg |
| **3.** | https://folhadacidadems.com.br/free/purchase/order.php?email={{email}} | microsoftloginfolhadac33.31.jpg |
| **4.** | https://nazahaco.com/see/outlook_owa/login/?email={{email}} | microsoftloginnazahaco60.47.jpg |
| **5.** | http://arched-elixir-280012.nw.r.appspot.com/ | microsoftloginrched-el31.95.jpg |
| **Netflix login** | | |
| **1.** | https://ahorollno1.com/acc/a3ab4ff8fa4deed2e3bae3a5077675f0 | netflixloginahorolln04.85.jpg |
| **2.** | http://marketinghelper.com.au/themes/sports/wp-content/net/352407221afb776e3143e8a1a0577885 | netflixloginarketing01.44.jpg |
| **3.** | http://flix-flix-update.com | netflixloginlix-flix27.43.jpg |
| **4.** | https://rubibags.com/wp-includes/IXR/nfx/us-en | netflixloginrubibags49.6.jpg |
| **5.** | http://www.stampready.net/click/?t=aHR0cHM6Ly9sYy5jeC8waHZsbEFZX1k1MTg1NTkxODkxMjAw | netflixloginww.stamp24.73.jpg |
| **PayPal login** | | |
| **1.** | http://backyarddelivery.com/wp-includes/pomo/iinformatiion/smarthelp/customer-id-476/myaccount/signin/ | paypalloginackyardd28.63.jpg |
| **2.** | http://paypal.com-webappss-account.keysfishingdirectory.com/128330435faf6ec07af5da8dec5a030eNTM5MmY1YzVjNWZmM2JiNmM4Njc4ZjgwY2ZiZGQ5NmQ= | paypalloginaypal.co74.93.jpg |
| **3.** | https://ppuseralert.com/ | paypalloginppuseral91.68.jpg |
| **4.** | https://shadetreetechnology.com/V4/validation/141ef9684be0a4d6c99321ec6eda79f2 | paypalloginshadetre83.51.jpg |
| **5.** | http://farooqmobiles.com/paypl/xode5nzy=/signin/?country.x=FR&locale.x=fr-FR,fr;q=0.8,en-US;q=0.6,en;q=0.4 | paypalloginarooqmob87.19 |
| **Yahoo login** | | |
| **1.** | http://laesenciaradicaenelsentido.com/wp-admin/network/own/yahoo/1702fdf1f894dc1d2ef993f820a9e6a6 | yahoologinaesencia79.26.jpg |
| **2.** | http://fastfoodgozo.rs/a/yahoo/login.php | yahoologinastfoodg14.91.jpg |
| **3.** | http://bodegascrotta.com.ar/images/Yahoo/index2.php | yahoologinodegascr65.94.jpg |
| **4.** | https://tinyurl.com/y2gnglmc | yahoologintinyurl.03.54.jpg |
| **5.** | http://www.recoveryalert.yahoo.com.diginik.net/login.html | yahoologinww.recov40.92 |

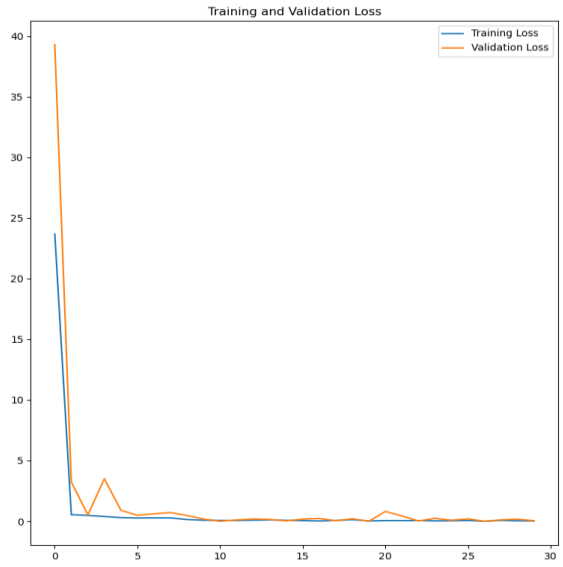
# Παράρτημα Γ
# Δοκιμές Μοντέλων με Καμπύλες Hilbert

## Γ.1 Δοκιμές MobileNet Μοντέλου και Αποτελέσματα Εκπαίδευσης

### Γ.1.1 MobileNet με Ρυθμό Εκμάθησης 0.01

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.01 |
| Μέγεθος Παρτίδας (Batch_size) | 32 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 95.83% |
| Απώλεια Επικύρωσης | 0.04180220142006874 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Hilbert, στο εκπαιδευόμενο μοντέλο MobileNet με lr 0.01.

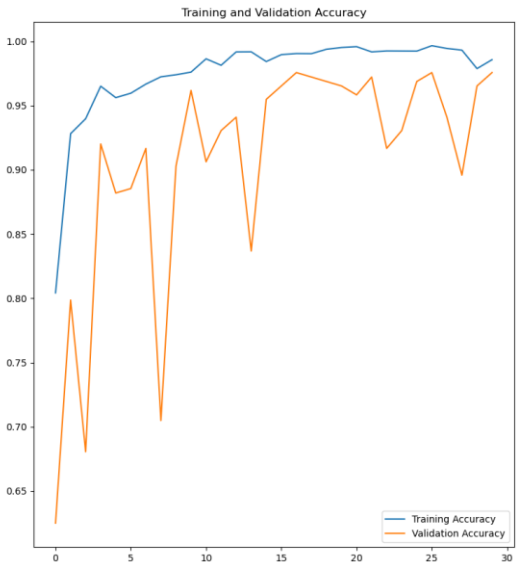
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,9999999 |
| adobelogingnoddrc.90.04.jpg | phishing | 1 |
| adobeloginhuncoppe56.16.jpg | phishing | 1 |
| adobeloginodimedia82.37.jpg | phishing | 1 |

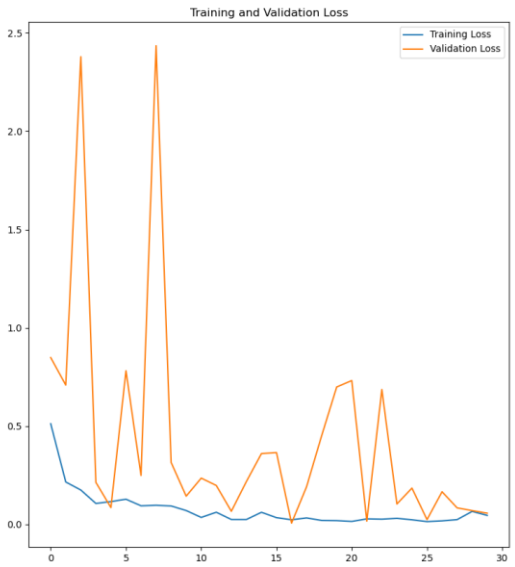
| | | |
|---|---|---|
| adobeloginwww.crea16.55.jpg | phishing | 1 |
| alibabalogindrevent.65.04.jpg | phishing | 1 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9999981 |
| alibabaloginww.diver49.92.jpg | phishing | 0,99999976 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,99999905 |
| amazonloginbestfitt19.01.jpg | phishing | 0,99999654 |
| amazonloginchinchil67.95.jpg | phishing | 1 |
| amazonloginconntect20.19.jpg | phishing | 1 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,9999964 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,99999464 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,8945093** |
| at&tloginhilltopc34.37.jpg | phishing | 0,9999999 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,99999154 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 0,9999999 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,99736005 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,99999964 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9999993 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,99978846 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 0,9999993 |
| chaseloginotoblad.59.76.jpg | phishing | 0,9999993 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,57669634** |
| chaselogintrack4se64.7.jpg | phishing | 1 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9999999 |
| dhlloginangelart32.29.jpg | phishing | 0,9991974 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 0,98325574 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 1 |
| ebayloginkverif23.96.jpg | phishing | 0,9999999 |
| ebayloginpaleypri94.81.jpg | phishing | 0,99996674 |
| ebayloginrlsverif45.47.jpg | phishing | 0,9999999 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9999981 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,9997327 |
| **googlelogindrive.go97.89.jpg** | **legitimate** | **0,99175537** |
| googlelogineadlampy24.96.jpg | phishing | 1 |
| googleloginlbel.int84.28.jpg | phishing | 0,9999999 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| **googleloginsites.go48.39.jpg** | **legitimate** | **0,6574803** |
| linkedinloginauricioy76.35.jpg | phishing | 1 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,9999442 |
| linkedinloginmade-in-59.37.jpg | phishing | 1 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,9999988 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 0,9945129 |

| | | |
|---|---|---|
| microsoftlogindreamy-g35.49.jpg | phishing | 1 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,99999976 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,99845195 |
| microsoftloginrched-el31.95.jpg | phishing | 1 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 0,9999999 |
| netflixloginlix-flix27.43.jpg | phishing | 1 |
| netflixloginrubibags49.6.jpg | phishing | 1 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 1 |
| paypalloginaypal.co74.93.jpg | phishing | 0,9972459 |
| paypalloginppuseral91.68.jpg | phishing | 0,9999907 |
| paypalloginshadetre83.51.jpg | phishing | 1 |
| paypalloginarooqmob87.19 | phishing | 0,9999999 |
| yahoologinaesencia79.26.jpg | phishing | 0,99992883 |
| yahoologinastfoodg14.91.jpg | phishing | 1 |
| yahoologinodegascr65.94.jpg | phishing | 0,9996836 |
| yahoologintinyurl.03.54.jpg | phishing | 0,9999883 |
| yahoologinww.recov40.92 | phishing | 1 |

### Γ.1.2 MobileNet με Ρυθμό Εκμάθησης 0.001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) | 32 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 96.57% |
| Απώλεια Επικύρωσης | 0.05688295140862465 |



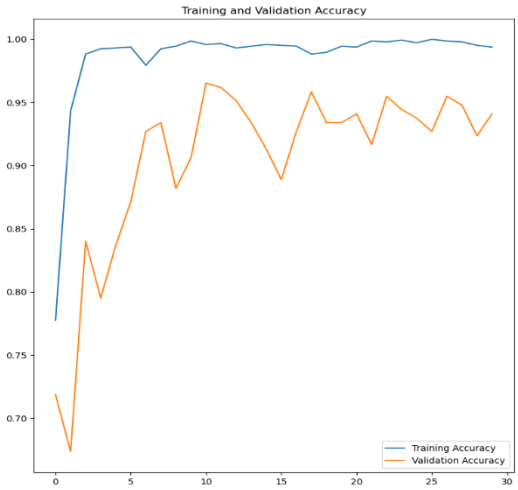

Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Hilbert, στο εκπαιδευόμενο μοντέλο MobileNet με lr 0.001.

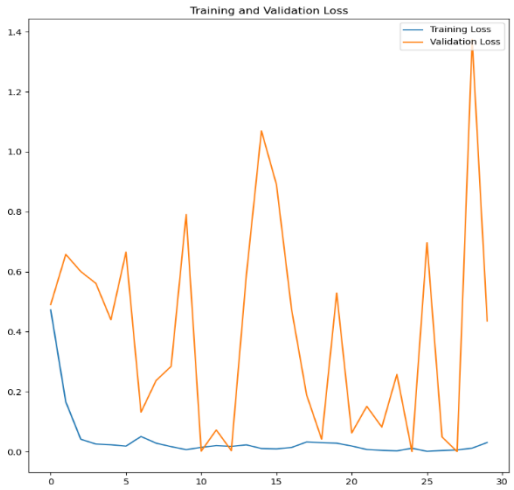
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 1 |
| adobeloginhuncoppe56.16.jpg | phishing | 1 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 1 |
| alibabalogindrevent.65.04.jpg | phishing | 1 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 1 |
| alibabaloginww.diver49.92.jpg | phishing | 1 |
| alibabaloginwww.tale61.02.jpg | phishing | 1 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 1 |
| amazonloginconntect20.19.jpg | phishing | 1 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,999948 |
| at&tloginhilltopc34.37.jpg | phishing | 0,99998677 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9999999 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,99943465 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,9999999 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9999939 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| chaseloginowntownd30.71.jpg | phishing | 0,9999999 |
| chaselogintrack4se64.7.jpg | phishing | 1 |
| dhlloginacvedas.27.57.jpg | phishing | 1 |
| dhlloginangelart32.29.jpg | phishing | 0,9999802 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 1 |
| ebaylogininkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 1 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| facebookloginhx.blewp90.51.jpg | phishing | 1 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,99999964 |
| googlelogindrive.go97.89.jpg | phishing | 0,9997533 |
| googlelogineadlampy24.96.jpg | phishing | 1 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |

| | | |
|---|---|---|
| googleloginsites.go48.39.jpg | phishing | 1 |
| linkedinloginauricioy76.35.jpg | phishing | 0,9997874 |
| linkedinlogindvtejas.76.89.jpg | phishing | 1 |
| linkedinloginmade-in-59.37.jpg | phishing | 1 |
| linkedinloginoutlookm27.79.jpg | phishing | 1 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 1 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,9999999 |
| microsoftloginfolhadac33.31.jpg | phishing | 1 |
| microsoftloginnazahaco60.47.jpg | phishing | 1 |
| microsoftloginrched-el31.95.jpg | phishing | 1 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 1 |
| netflixloginrubibags49.6.jpg | phishing | 0,9999993 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 0,9999968 |
| paypalloginaypal.co74.93.jpg | phishing | 0,9999989 |
| paypalloginppuseral91.68.jpg | phishing | 1 |
| paypalloginshadetre83.51.jpg | phishing | 1 |
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 0,9999999 |
| yahoologinastfoodg14.91.jpg | phishing | 1 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 0,9999999 |
| yahoologinww.recov40.92 | phishing | 1 |

### Γ.1.3 MobileNet με Ρυθμό Εκμάθησης 0.0001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.0001 |
| Μέγεθος Παρτίδας (Batch_size) | 32 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 94.10% |
| Απώλεια Επικύρωσης | 0.4357905685901642 |



Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Hilbert, στο εκπαιδευόμενο μοντέλο MobileNet με lr 0.001.

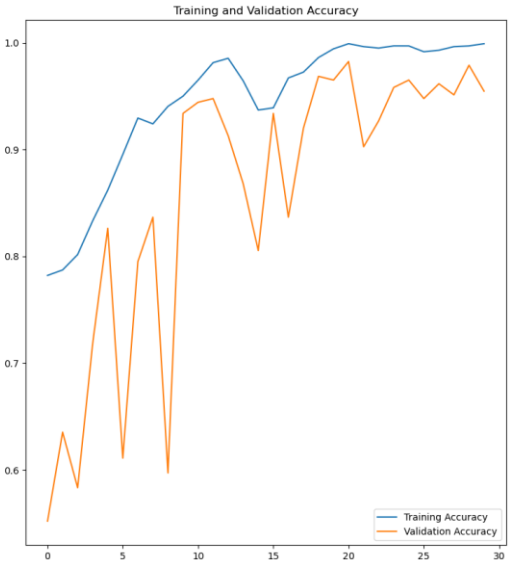
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9999937 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,99998474 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9999999 |
| alibabalogindrevent.65.04.jpg | phishing | 0,97399795 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9999999 |
| alibabaloginww.diver49.92.jpg | phishing | 0,99998903 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,99999774 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 1 |
| amazonloginconntect20.19.jpg | phishing | 0,99999654 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,9964144** |
| at&tloginhilltopc34.37.jpg | phishing | 0,9969989 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9999927 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 0,9999995 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,9999926 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,99998665 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9999956 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| chaseloginowntownd30.71.jpg | phishing | 0,99960774 |
| chaselogintrack4se64.7.jpg | phishing | 0,99999785 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9997216 |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 0,9999999 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,99999976 |
| ebaylogininkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 0,9947502 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,85950845 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 0,99998677 |
| facebookloginxvgbtopl00.11.jpg | phishing | 1 |
| googlelogindrive.go97.89.jpg | phishing | 0,9160339 |
| googlelogineadlampy24.96.jpg | phishing | 1 |

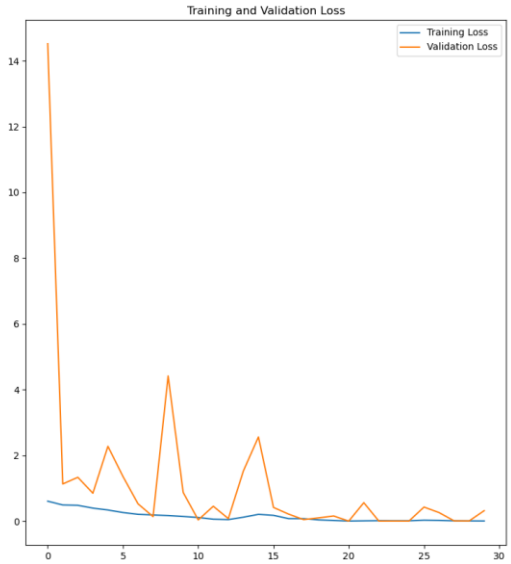
| | | |
|---|---|---|
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 0,9109782 |
| linkedinloginauricioy76.35.jpg | phishing | 0,9017578 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,99969196 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,9999999 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,9999987 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 0,9987992 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,9999975 |
| microsoftloginfolhadac33.31.jpg | phishing | 1 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,983167 |
| microsoftloginrched-el31.95.jpg | phishing | 0,999915 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 1 |
| netflixloginrubibags49.6.jpg | phishing | 0,9999467 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 1 |
| paypalloginaypal.co74.93.jpg | phishing | 0,9999801 |
| paypalloginppuseral91.68.jpg | phishing | 1 |
| paypalloginshadetre83.51.jpg | phishing | 0,9999999 |
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 0,999998 |
| yahoologinastfoodg14.91.jpg | phishing | 0,99999976 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 0,99999917 |

# Γ.2 Δοκιμές MobileNet-RNN Μοντέλου και Αποτελέσματα Εκπαίδευσης

## Γ.2.1 Δοκιμή MobileNet-RNN με Ρυθμό Εκμάθησης 0.01

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.01 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 98.26% |
| Απώλεια Επικύρωσης | 0.009801629930734634 |



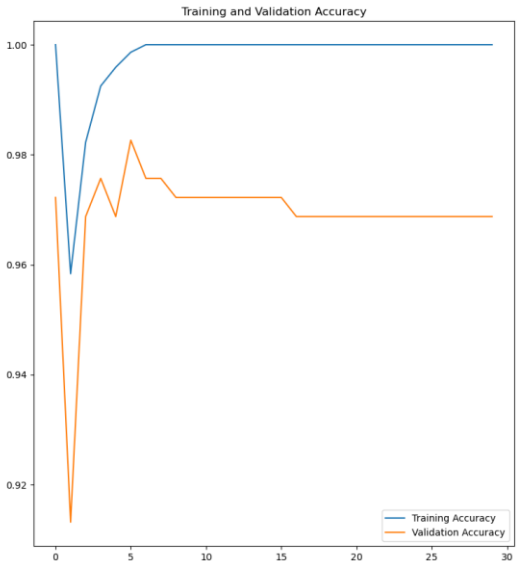

Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Hilbert, στο εκπαιδευόμενο μοντέλο MobileNet -RNNμε lr 0.01.

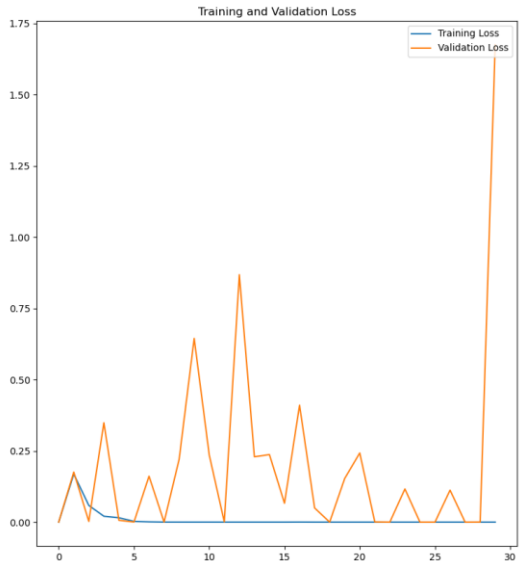
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,9999951 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,99999774 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,9999876 |
| adobeloginodimedia82.37.jpg | phishing | 0,99999976 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9999999 |
| alibabalogindrevent.65.04.jpg | phishing | 0,9999988 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,99999976 |
| alibabaloginpineheal56.15.jpg | phishing | 1 |
| alibabaloginww.diver49.92.jpg | phishing | 0,9999695 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,99999785 |
| amazonloginbestfitt19.01.jpg | phishing | 0,9999989 |
| amazonloginchinchil67.95.jpg | phishing | 0,9999819 |
| amazonloginconntect20.19.jpg | phishing | 0,99999857 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,9999989 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,9999988 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,9999924 |
| **at&tloginhilltopc34.37.jpg** | **legitimate** | **0,7733027** |
| at&tloginkletsbuy99.14.jpg | phishing | 0,99999976 |
| at&tloginmahdistr30.89.jpg | phishing | 0,99999976 |
| at&tloginzaroosha94.26.jpg | phishing | 0,999998 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,9999918 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,9999999 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,9998073 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9999995 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,99999905 |
| chaseloginaigonspo91.35.jpg | phishing | 0,99999905 |
| chaseloginellefont45.61.jpg | phishing | 0,99999964 |

| | | |
|---|---|---|
| chaseloginotoblad.59.76.jpg | phishing | 0,99999964 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,60752547** |
| chaselogintrack4se64.7.jpg | phishing | 0,9999999 |
| dhlloginacvedas.27.57.jpg | phishing | 0,99995494 |
| dhlloginangelart32.29.jpg | phishing | 0,9999958 |
| dhlloginharmoniu69.96.jpg | phishing | 0,99999785 |
| dhlloginhotelgra46.79.jpg | phishing | 0,9999999 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,99999845 |
| ebayloginkverif23.96.jpg | phishing | 0,99999964 |
| ebayloginpaleypri94.81.jpg | phishing | 0,9998622 |
| ebayloginrlsverif45.47.jpg | phishing | 0,99999964 |
| ebayloginthongtin17.67.jpg | phishing | 0,9999999 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,99999225 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,9999907 |
| **googlelogindrive.go97.89.jpg** | **phishing** | **0,77318364** |
| googlelogineadlampy24.96.jpg | phishing | 0,99999905 |
| googleloginlbel.int84.28.jpg | phishing | 0,9999999 |
| googleloginluidacco20.43.jpg | phishing | 0,99999976 |
| googleloginsites.go48.39.jpg | phishing | 0,999949 |
| linkedinloginauricioy76.35.jpg | phishing | 0,99992454 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,99997365 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,99999964 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,9999976 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 0,9999794 |
| **microsoftlogindreamy-g35.49.jpg** | **legitimate** | **0,7431356** |
| microsoftloginfolhadac33.31.jpg | phishing | 0,9999999 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,97885746 |
| microsoftloginrched-el31.95.jpg | phishing | 0,99998915 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 0,9999752 |
| netflixloginrubibags49.6.jpg | phishing | 0,999997 |
| netflixloginww.stamp24.73.jpg | phishing | 0,9999976 |
| paypalloginackyardd28.63.jpg | phishing | 0,9691657 |
| paypalloginaypal.co74.93.jpg | phishing | 0,9994972 |
| paypalloginppuseral91.68.jpg | phishing | 0,9999999 |
| paypalloginshadetre83.51.jpg | phishing | 0,99974555 |
| paypalloginarooqmob87.19 | phishing | 0,9999964 |
| yahoologinaesencia79.26.jpg | phishing | 0,99999917 |
| yahoologinastfoodg14.91.jpg | phishing | 0,9999993 |
| yahoologinodegascr65.94.jpg | phishing | 0,9999993 |
| yahoologintinyurl.03.54.jpg | phishing | 0,99997437 |
| yahoologinww.recov40.92 | phishing | 0,9999982 |

### Γ.2.2 Δοκιμή MobileNet-RNN με Ρυθμό Εκμάθησης 0.001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 98.26% |
| Απώλεια Επικύρωσης | 1.6943540573120117 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Hilbert, στο εκπαιδευόμενο μοντέλο MobileNet -RNNμε lr 0.001.

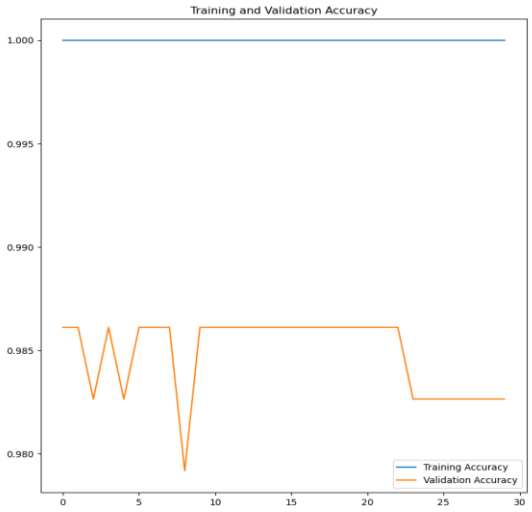
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,99999285 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,9998363 |
| adobeloginodimedia82.37.jpg | phishing | 0,9999999 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9999777 |
| alibabalogindrevent.65.04.jpg | phishing | 0,99999976 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 1 |
| alibabaloginww.diver49.92.jpg | phishing | 1 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,9999945 |
| amazonloginbestfitt19.01.jpg | phishing | 0,99999654 |
| amazonloginchinchil67.95.jpg | phishing | 0,99999785 |
| amazonloginconntect20.19.jpg | phishing | 1 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,9999964 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,9997397 |
| at&tloginhilltopc34.37.jpg | phishing | 0,89835095 |

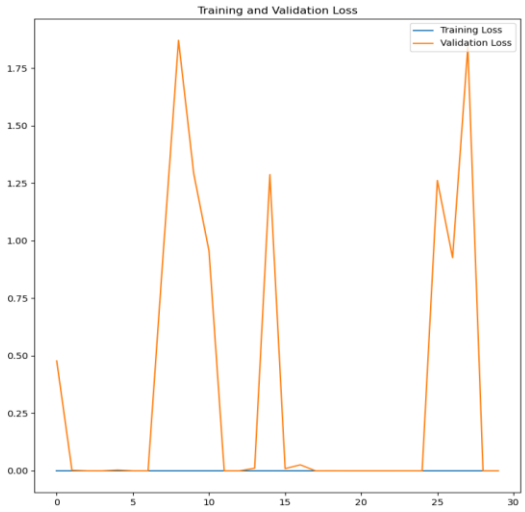
| | | |
|---|---|---|
| at&tloginkletsbuy99.14.jpg | phishing | 0,99999917 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 1 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,9999902 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,9989586 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9999994 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,99999774 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,996005** |
| chaselogintrack4se64.7.jpg | phishing | 1 |
| dhlloginacvedas.27.57.jpg | phishing | 1 |
| dhlloginangelart32.29.jpg | phishing | 0,99999976 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhllogingansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,9997458 |
| ebayloginkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 0,99994946 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 0,9997986 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9999987 |
| facebookloginjoingrup15.72.jpg | phishing | 0,99999976 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,99999964 |
| googlelogindrive.go97.89.jpg | phishing | 1 |
| googlelogineadlampy24.96.jpg | phishing | 0,99997735 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 0,99762684 |
| linkedinloginauricioy76.35.jpg | phishing | 0,99999917 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,9999919 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,9999887 |
| linkedinloginoutlookm27.79.jpg | phishing | 1 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 0,9998733 |
| **microsoftlogindreamy-g35.49.jpg** | **legitimate** | **0,9686142** |
| microsoftloginfolhadac33.31.jpg | phishing | 0,99999905 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,99671483 |
| microsoftloginrched-el31.95.jpg | phishing | 1 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 0,9999976 |
| netflixloginrubibags49.6.jpg | phishing | 0,9999989 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 0,9999988 |
| paypalloginaypal.co74.93.jpg | phishing | 0,9999981 |
| paypalloginppuseral91.68.jpg | phishing | 1 |
| paypalloginshadetre83.51.jpg | phishing | 0,9999913 |

| | | |
|---|---|---|
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 1 |
| yahoologinastfoodg14.91.jpg | phishing | 0,99992955 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 0,99999785 |

### Γ.2.3 Δοκιμή MobileNet-RNN με Ρυθμό Εκμάθησης 0.0001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.0001 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 98.61% |
| Απώλεια Επικύρωσης | 0.0013734073145315 05 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Hilbert, στο εκπαιδευόμενο μοντέλο MobileNet -RNNμε lr 0.0001.

| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,9999999 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9999497 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,998552 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9999993 |
| alibabalogindrevent.65.04.jpg | phishing | 0,99969244 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,9999894 |
| alibabaloginpineheal56.15.jpg | phishing | 0,99786866 |
| alibabaloginww.diver49.92.jpg | phishing | 0,9996418 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,99995685 |
| amazonloginbestfitt19.01.jpg | phishing | 0,9999968 |
| amazonloginchinchil67.95.jpg | phishing | 0,9999932 |

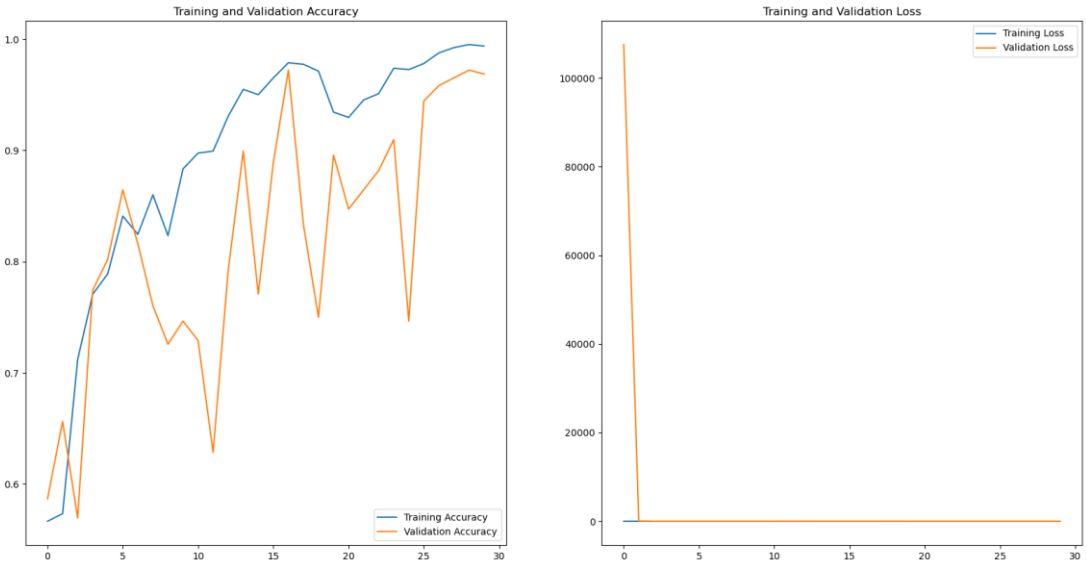
| | | |
|---|---|---|
| amazonloginconntect20.19.jpg | phishing | 0,99999607 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,9999968 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,9999943 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,9783199 |
| at&tloginhilltopc34.37.jpg | phishing | 0,99589324 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,99680495 |
| at&tloginmahdistr30.89.jpg | phishing | 0,9998023 |
| at&tloginzaroosha94.26.jpg | phishing | 0,99997306 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,9999944 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,99977976 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,8939968 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,99998546 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,99999845 |
| chaseloginaigonspo91.35.jpg | phishing | 0,99996686 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,9268453** |
| chaselogintrack4se64.7.jpg | phishing | 0,9938047 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9983588 |
| dhlloginangelart32.29.jpg | phishing | 0,9999676 |
| dhlloginharmoniu69.96.jpg | phishing | 0,99999917 |
| dhlloginhotelgra46.79.jpg | phishing | 0,999967 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,999995 |
| ebaylogininkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 0,99994135 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 0,99999475 |
| facebookloginadm.righ42.51.jpg | phishing | 0,99999285 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9970687 |
| facebookloginjoingrup15.72.jpg | phishing | 0,99978155 |
| facebookloginsecurlty22.26.jpg | phishing | 0,9999881 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,99857926 |
| googlelogindrive.go97.89.jpg | phishing | 0,9999764 |
| googlelogineadlampy24.96.jpg | phishing | 0,99998176 |
| googleloginlbel.int84.28.jpg | phishing | 0,9999796 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 1 |
| linkedinloginauricioy76.35.jpg | phishing | 0,9984072 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,9999747 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,99922705 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,9999182 |
| linkedinloginowwglass82.2.jpg | phishing | 0,9998049 |
| microsoftloginakakakak47.63.jpg | phishing | 0,99993885 |
| **microsoftlogindreamy-g35.49.jpg** | **legitimate** | **0,99849033** |
| microsoftloginfolhadac33.31.jpg | phishing | 0,9998528 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,9916083 |
| microsoftloginrched-el31.95.jpg | phishing | 0,999972 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 0,99998844 |
| netflixloginlix-flix27.43.jpg | phishing | 0,9999838 |
| netflixloginrubibags49.6.jpg | phishing | 0,99921024 |

| | | |
|---|---|---|
| netflixloginww.stamp24.73.jpg | phishing | 0,99999785 |
| paypalloginackyardd28.63.jpg | phishing | 1 |
| paypalloginaypal.co74.93.jpg | phishing | 1 |
| paypalloginppuseral91.68.jpg | phishing | 0,9999716 |
| paypalloginshadetre83.51.jpg | phishing | 0,9998229 |
| paypalloginarooqmob87.19 | phishing | 0,9999894 |
| yahoologinaesencia79.26.jpg | phishing | 0,9999919 |
| yahoologinastfoodg14.91.jpg | phishing | 0,9995665 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 0,99999976 |
| yahoologinww.recov40.92 | phishing | 1 |

# Γ.3 Δοκιμές Xception-RNN Μοντέλου και Αποτελέσματα Εκπαίδευσης

## Γ.3.1 Δοκιμή Xception-RNN με Ρυθμό Εκμάθησης 0.01

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.01 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 96.88% |
| Απώλεια Επικύρωσης | 0.0017365349922329187 |



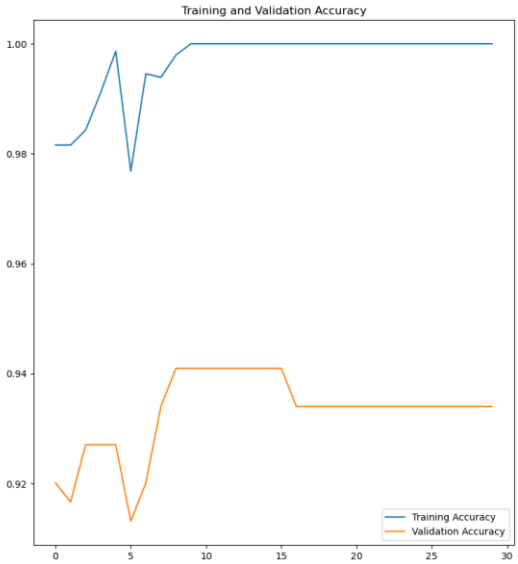

Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Hilbert, στο εκπαιδευόμενο μοντέλο Xception -RNNμε lr 0,01.

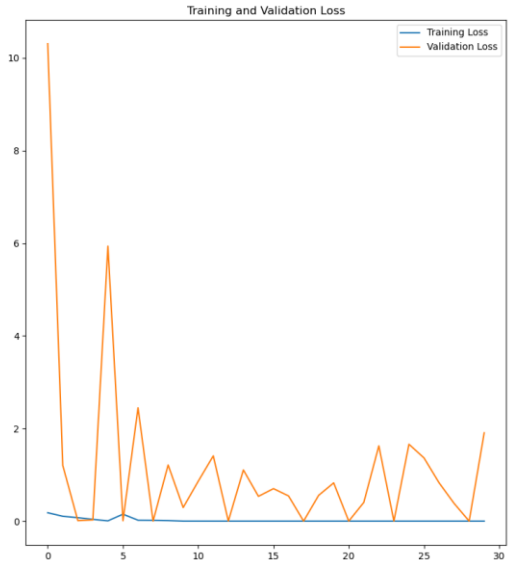
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,9994685 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9942702 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,9999938 |
| adobeloginodimedia82.37.jpg | phishing | 0,99999976 |
| adobeloginwww.crea16.55.jpg | phishing | 0,99999857 |
| alibabalogindrevent.65.04.jpg | phishing | 0,99999225 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,9999502 |
| alibabaloginpineheal56.15.jpg | phishing | 0,999998 |
| alibabaloginww.diver49.92.jpg | phishing | 0,9999267 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,9999994 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 1 |
| amazonloginconntect20.19.jpg | phishing | 0,9999995 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,9999999 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,7971235** |
| **at&tloginhilltopc34.37.jpg** | **legitimate** | **0,84881175** |
| at&tloginkletsbuy99.14.jpg | phishing | 0,999992 |
| at&tloginmahdistr30.89.jpg | phishing | 0,99999917 |
| at&tloginzaroosha94.26.jpg | phishing | 0,9999999 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,9999286 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,9999994 |
| bankofamericaloginedificio77.17.jpg | phishing | 1 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,99999166 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,99990225 |
| chaseloginaigonspo91.35.jpg | phishing | 0,99999964 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| chaseloginowntownd30.71.jpg | phishing | 0,99930763 |
| chaselogintrack4se64.7.jpg | phishing | 0,99899286 |
| **dhlloginacvedas.27.57.jpg** | **legitimate** | **0,63358516** |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 0,99999654 |
| dhlloginhotelgra46.79.jpg | phishing | 0,9999963 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,99827766 |
| ebaylogininkverif23.96.jpg | phishing | 1 |
| **ebayloginpaleypri94.81.jpg** | **legitimate** | **0,7670696** |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,8139809 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 0,99993396 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,99945766 |
| **googlelogindrive.go97.89.jpg** | **legitimate** | **0,9985092** |
| googlelogineadlampy24.96.jpg | phishing | 0,99856085 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 0,9998161 |

| **linkedinloginauricioy76.35.jpg** | **legitimate** | **0,99998724** |
|---|---|---|
| linkedinlogindvtejas.76.89.jpg | phishing | 0,99964225 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,99504673 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,99999607 |
| linkedinloginowwglass82.2.jpg | phishing | 0,99949265 |
| **microsoftloginakakakak47.63.jpg** | **legitimate** | **0,99736804** |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,99997807 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,999793 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,9818865 |
| microsoftloginrched-el31.95.jpg | phishing | 0,99983704 |
| netflixloginahorolln04.85.jpg | phishing | 0,9999993 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 0,99992275 |
| netflixloginrubibags49.6.jpg | phishing | 0,99999654 |
| netflixloginww.stamp24.73.jpg | phishing | 0,9999949 |
| paypalloginackyardd28.63.jpg | phishing | 0,9975924 |
| paypalloginaypal.co74.93.jpg | phishing | 0,96082485 |
| paypalloginppuseral91.68.jpg | phishing | 0,9999951 |
| paypalloginshadetre83.51.jpg | phishing | 0,9999994 |
| paypalloginarooqmob87.19 | phishing | 0,9868037 |
| yahoologinaesencia79.26.jpg | phishing | 0,9999988 |
| yahoologinastfoodg14.91.jpg | phishing | 0,92222285 |
| yahoologinodegascr65.94.jpg | phishing | 0,9999956 |
| yahoologintinyurl.03.54.jpg | phishing | 0,99998593 |
| yahoologinww.recov40.92 | phishing | 0,9999813 |

### Γ.3.2 Δοκιμή Xception-RNN με Ρυθμό Εκμάθησης 0.001

| Ρυθμός Εκμάθησης lr | 0.001 |
|---|---|
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 93.40% |
| Απώλεια Επικύρωσης | 1.3411014379016706e-06 |



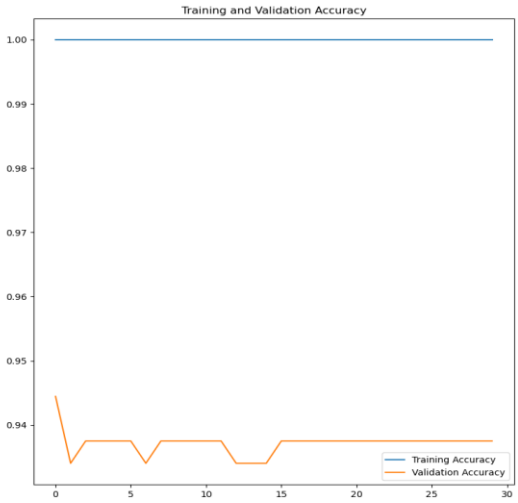

Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Hilbert, στο εκπαιδευόμενο μοντέλο Xception -RNNμε lr 0,001.

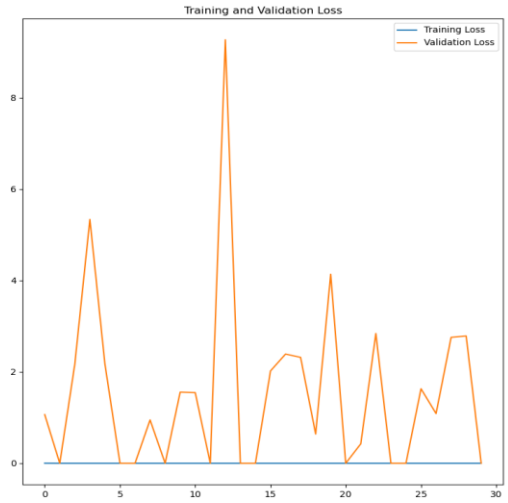
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 1 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,99999976 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9999999 |
| alibabalogindrevent.65.04.jpg | phishing | 0,9999999 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9999999 |
| alibabaloginww.diver49.92.jpg | phishing | 0,9999999 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,9999999 |
| amazonloginbestfitt19.01.jpg | phishing | 0,99999976 |
| amazonloginchinchil67.95.jpg | phishing | 0,9999999 |
| amazonloginconntect20.19.jpg | phishing | 0,99999976 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,99999976 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,9999995 |
| **at&tlogindocs.goo12.02.jpg** | **phishing** | **0,60450536** |
| at&tloginhilltopc34.37.jpg | phishing | 1 |
| at&tloginkletsbuy99.14.jpg | phishing | 1 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 1 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,9999999 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 1 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |

| | | |
|---|---|---|
| chaseloginowntownd30.71.jpg | legitimate | 0,9999906 |
| chaselogintrack4se64.7.jpg | phishing | 0,9999999 |
| dhlloginacvedas.27.57.jpg | phishing | 0,99994266 |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhllogingansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 1 |
| ebayloginkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 1 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| **facebookloginhx.blewp90.51.jpg** | **legitimate** | **0,99999595** |
| facebookloginjoingrup15.72.jpg | phishing | 0,9999995 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,9999999 |
| googlelogindrive.go97.89.jpg | phishing | 0,9673961 |
| googlelogineadlampy24.96.jpg | phishing | 0,9999999 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 0,9999999 |
| linkedinloginauricioy76.35.jpg | phishing | 0,9999999 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,9999993 |
| linkedinloginmade-in-59.37.jpg | phishing | 1 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,9999999 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| **microsoftloginakakakak47.63.jpg** | **legitimate** | **0,99999607** |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,9998815 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,99999976 |
| microsoftloginnazahaco60.47.jpg | legitimate | 0,99998975 |
| microsoftloginrched-el31.95.jpg | phishing | 1 |
| netflixloginahorolln04.85.jpg | phishing | 0,99999976 |
| netflixloginarketing01.44.jpg | phishing | 0,99999976 |
| netflixloginlix-flix27.43.jpg | phishing | 1 |
| netflixloginrubibags49.6.jpg | phishing | 0,9999999 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 0,9999999 |
| **paypalloginaypal.co74.93.jpg** | **legitimate** | **0,99999154** |
| paypalloginppuseral91.68.jpg | phishing | 0,99999976 |
| paypalloginshadetre83.51.jpg | phishing | 0,99999976 |
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 1 |
| yahoologinastfoodg14.91.jpg | phishing | 0,9999999 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 0,9999995 |
| yahoologinww.recov40.92 | phishing | 1 |

### Γ.3.3 Δοκιμή Xception-RNN με Ρυθμό Εκμάθησης 0.0001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.0001 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 93.75% |
| Απώλεια Επικύρωσης | 0.0 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Hilbert, στο εκπαιδευόμενο μοντέλο Xception -RNNμε lr 0,0001.

| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 1 |
| adobeloginhuncoppe56.16.jpg | phishing | 1 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9964818 |
| alibabalogindrevent.65.04.jpg | phishing | 1 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 1 |
| alibabaloginww.diver49.92.jpg | phishing | 1 |
| alibabaloginwww.tale61.02.jpg | phishing | 1 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 1 |
| amazonloginconntect20.19.jpg | phishing | 1 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,99996996 |
| **at&tloginhilltopc34.37.jpg** | **legitimate** | **1** |
| at&tloginkletsbuy99.14.jpg | phishing | 1 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |

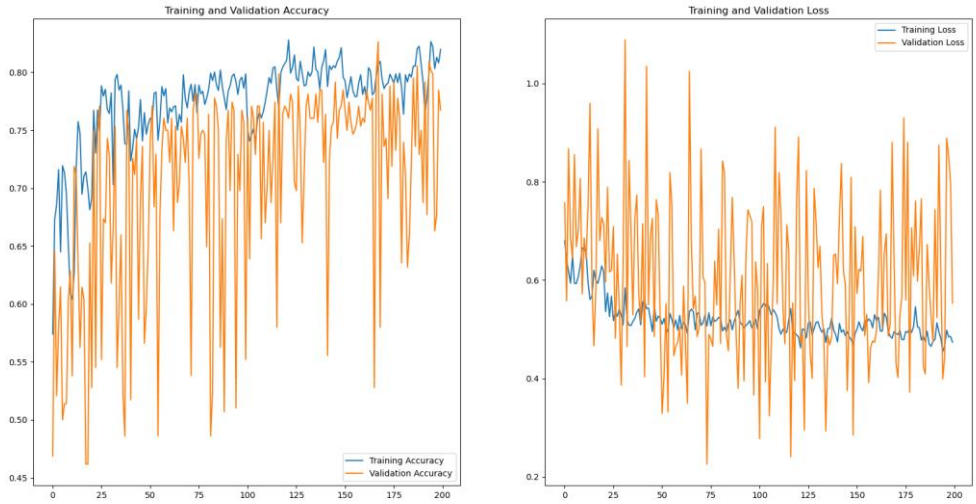
| | | |
|---|---|---|
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 1 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 1 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 1 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,9942063** |
| chaselogintrack4se64.7.jpg | phishing | 1 |
| **dhlloginacvedas.27.57.jpg** | **legitimate** | **0,98812485** |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 1 |
| ebaylogininkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 0,99912995 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,999995 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 1 |
| googlelogindrive.go97.89.jpg | phishing | 1 |
| googlelogineadlampy24.96.jpg | phishing | 1 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 1 |
| linkedinloginauricioy76.35.jpg | phishing | 1 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,99619955 |
| linkedinloginmade-in-59.37.jpg | phishing | 1 |
| linkedinloginoutlookm27.79.jpg | phishing | 1 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 1 |
| microsoftlogindreamy-g35.49.jpg | phishing | 1 |
| microsoftloginfolhadac33.31.jpg | phishing | 1 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,9973494 |
| microsoftloginrched-el31.95.jpg | phishing | 1 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 1 |
| netflixloginrubibags49.6.jpg | phishing | 1 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 0,97663134 |
| paypalloginaypal.co74.93.jpg | phishing | 1 |
| paypalloginppuseral91.68.jpg | phishing | 1 |
| paypalloginshadetre83.51.jpg | phishing | 1 |
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 1 |

| | | |
|---|---|---|
| yahoologinastfoodg14.91.jpg | phishing | 1 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 1 |

# Γ.4 Δοκιμές Custom-CNN Μοντέλου και Αποτελέσματα Εκπαίδευσης

### Γ.4.1 Δοκιμή Custom - CNN με Ρυθμό Εκμάθησης 0.01

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.01 |
| Μέγεθος Παρτίδας (Batch_size) | 16 |
| Εποχές | 200 |
| Ακρίβεια Επικύρωσης | 76.74% |
| Απώλεια Επικύρωσης | 0.5529054403305054 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Hilbert, στο εκπαιδευόμενο μοντέλο Custom-CNN με lr 0,01.

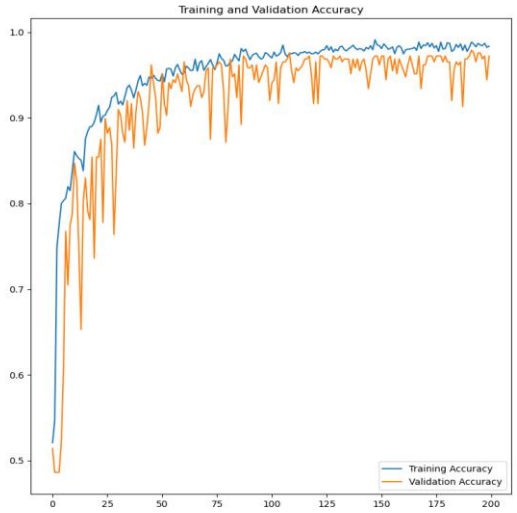
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,8672199 |
| **adobelogingnoddrc.90.04.jpg** | **legitimate** | **0,7968568** |
| **adobeloginhuncoppe56.16.jpg** | **legitimate** | **0,7968568** |
| adobeloginodimedia82.37.jpg | phishing | 0,8672199 |
| **adobeloginwww.crea16.55.jpg** | **legitimate** | **0,7968568** |
| alibabalogindrevent.65.04.jpg | phishing | 0,8672199 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,8672199 |
| **alibabaloginpineheal56.15.jpg** | **legitimate** | **0,7968568** |
| **alibabaloginww.diver49.92.jpg** | **legitimate** | **0,7968568** |

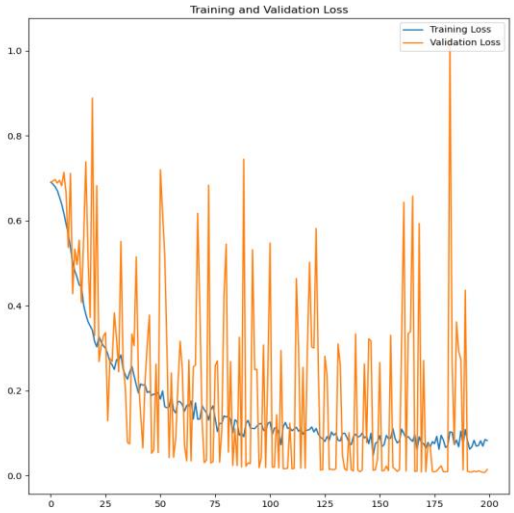
| | | |
|---|---|---|
| **alibabaloginwww.tale61.02.jpg** | **legitimate** | **0,7968568** |
| **amazonloginbestfitt19.01.jpg** | **legitimate** | **0,7968568** |
| amazonloginchinchil67.95.jpg | phishing | 0,8672199 |
| amazonloginconntect20.19.jpg | phishing | 0,8672199 |
| **amazonlogindecaiofa52.62.jpg** | **legitimate** | **0,7968568** |
| **amazonloginizbiz.te71.9.jpg** | **legitimate** | **0,7968568** |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,7968568** |
| at&tloginhilltopc34.37.jpg | phishing | 0,8672199 |
| **at&tloginkletsbuy99.14.jpg** | **legitimate** | **0,7968568** |
| at&tloginmahdistr30.89.jpg | phishing | 0,8672199 |
| at&tloginzaroosha94.26.jpg | phishing | 0,8672199 |
| **bankofamericalogin5.188.3665.04.jpg** | **legitimate** | **0,7968568** |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,8672199 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,8672199 |
| **bankofamericaloginkrjpl.co60.86.jpg** | **legitimate** | **0,7968568** |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,8672199 |
| **chaseloginaigonspo91.35.jpg** | **legitimate** | **0,7968568** |
| chaseloginellefont45.61.jpg | phishing | 0,8672199 |
| chaseloginotoblad.59.76.jpg | phishing | 0,8672199 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,7968568** |
| chaselogintrack4se64.7.jpg | phishing | 0,8672199 |
| dhlloginacvedas.27.57.jpg | phishing | 0,8672199 |
| dhlloginangelart32.29.jpg | phishing | 0,8672199 |
| dhlloginharmoniu69.96.jpg | phishing | 0,8672199 |
| dhlloginhotelgra46.79.jpg | phishing | 0,8672199 |
| dhlloginogansegu00.33.jpg | phishing | 0,8672199 |
| **ebaylogin7426fbe061.09.jpg** | **legitimate** | **0,7968568** |
| ebaylogininkverif23.96.jpg | phishing | 0,8672199 |
| **ebayloginpaleypri94.81.jpg** | **legitimate** | **0,7968568** |
| ebayloginrlsverif45.47.jpg | phishing | 0,8672199 |
| ebayloginthongtin17.67.jpg | phishing | 0,8672199 |
| facebookloginadm.righ42.51.jpg | phishing | 0,8672199 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,8672199 |
| facebookloginjoingrup15.72.jpg | phishing | 0,8672199 |
| facebookloginsecurlty22.26.jpg | phishing | 0,8672199 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,8672199 |
| googlelogindrive.go97.89.jpg | phishing | 0,86620045 |
| **googlelogineadlampy24.96.jpg** | **legitimate** | **0,7968568** |
| googleloginlbel.int84.28.jpg | phishing | 0,8672199 |
| googleloginluidacco20.43.jpg | phishing | 0,8672199 |
| **googleloginsites.go48.39.jpg** | **legitimate** | **0,7968568** |
| **linkedinloginauricioy76.35.jpg** | **legitimate** | **0,7968568** |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,8672199 |
| **linkedinloginmade-in-59.37.jpg** | **legitimate** | **0,7968568** |
| **linkedinloginoutlookm27.79.jpg** | **legitimate** | **0,7968568** |
| linkedinloginowwglass82.2.jpg | phishing | 0,8672199 |
| **microsoftloginakakakak47.63.jpg** | **legitimate** | **0,7968568** |
| **microsoftlogindreamy-g35.49.jpg** | **legitimate** | **0,7968568** |
| microsoftloginfolhadac33.31.jpg | phishing | 0,8672199 |
| **microsoftloginnazahaco60.47.jpg** | **legitimate** | **0,7968568** |
| **microsoftloginrched-el31.95.jpg** | **legitimate** | **0,7968568** |
| netflixloginahorolln04.85.jpg | phishing | 0,8672199 |

| | | |
|---|---|---|
| netflixloginarketing01.44.jpg | phishing | 0,8672199 |
| **netflixloginlix-flix27.43.jpg** | **legitimate** | **0,7968568** |
| netflixloginrubibags49.6.jpg | phishing | 0,8672199 |
| **netflixloginww.stamp24.73.jpg** | **legitimate** | **0,7968568** |
| **paypalloginackyardd28.63.jpg** | **legitimate** | **0,7968568** |
| paypalloginaypal.co74.93.jpg | phishing | 0,8672199 |
| paypalloginppuseral91.68.jpg | phishing | 0,8672199 |
| **paypalloginshadetre83.51.jpg** | **legitimate** | **0,7968568** |
| **paypalloginarooqmob87.19** | **phishing** | **0,8672199** |
| yahoologinaesencia79.26.jpg | phishing | 0,8672199 |
| **yahoologinastfoodg14.91.jpg** | **legitimate** | **0,7968568** |
| yahoologinodegascr65.94.jpg | phishing | 0,8672199 |
| yahoologintinyurl.03.54.jpg | phishing | 0,8672199 |
| **yahoologinww.recov40.92** | **legitimate** | **0,7968568** |

### Γ.4.2 Δοκιμή Custom - CNN με Ρυθμό Εκμάθησης 0.001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) | 16 |
| Εποχές | 200 |
| Ακρίβεια Επικύρωσης | 97.22% |
| Απώλεια Επικύρωσης | 0.014862705022096634 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Hilbert, στο εκπαιδευόμενο μοντέλο Custom-CNN με lr 0,001.

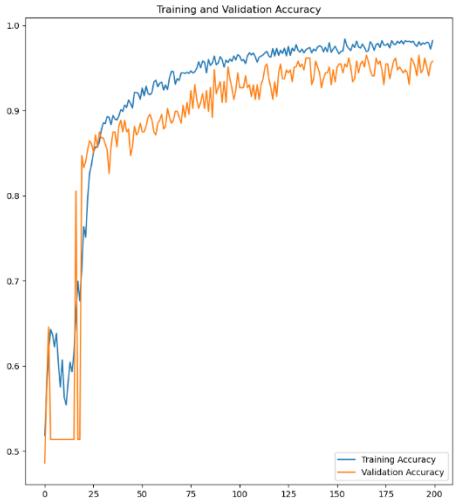
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,98275787 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,98275787 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,9833143 |

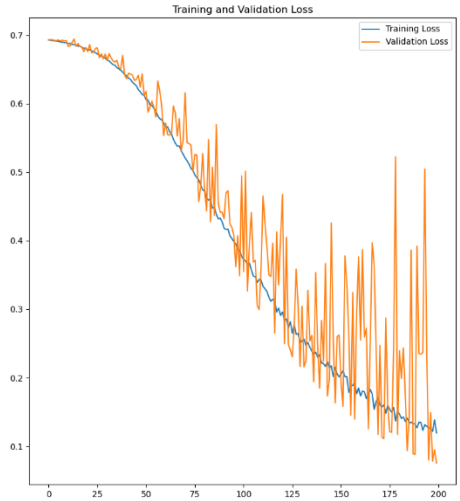
| | | |
|---|---|---|
| adobeloginodimedia82.37.jpg | phishing | 0,98275787 |
| adobeloginwww.crea16.55.jpg | phishing | 0,98275787 |
| alibabalogindrevent.65.04.jpg | phishing | 0,98275787 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,98275787 |
| alibabaloginpineheal56.15.jpg | phishing | 0,98275787 |
| alibabaloginww.diver49.92.jpg | phishing | 0,98275787 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,98275787 |
| amazonloginbestfitt19.01.jpg | phishing | 0,98275787 |
| amazonloginchinchil67.95.jpg | phishing | 0,98275787 |
| amazonloginconntect20.19.jpg | phishing | 0,98275787 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,98275787 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,98275787 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,99706787** |
| at&tloginhilltopc34.37.jpg | phishing | 0,97986 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,98275787 |
| at&tloginmahdistr30.89.jpg | phishing | 0,98275787 |
| at&tloginzaroosha94.26.jpg | phishing | 0,98275787 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,98275787 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,98275787 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,98275787 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,98275787 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,98275787 |
| chaseloginaigonspo91.35.jpg | phishing | 0,98275787 |
| chaseloginellefont45.61.jpg | phishing | 0,98275787 |
| chaseloginotoblad.59.76.jpg | phishing | 0,98275787 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,99666744** |
| chaselogintrack4se64.7.jpg | phishing | 0,98275787 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9814633 |
| dhlloginangelart32.29.jpg | phishing | 0,98275787 |
| dhlloginharmoniu69.96.jpg | phishing | 0,98275787 |
| dhlloginhotelgra46.79.jpg | phishing | 0,98275787 |
| dhlloginogansegu00.33.jpg | phishing | 0,98275787 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,98275787 |
| ebaylogininkverif23.96.jpg | phishing | 0,98275787 |
| ebayloginpaleypri94.81.jpg | phishing | 0,9824661 |
| ebayloginrlsverif45.47.jpg | phishing | 0,98275787 |
| ebayloginthongtin17.67.jpg | phishing | 0,98275787 |
| facebookloginadm.righ42.51.jpg | phishing | 0,98275787 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,98275787 |
| facebookloginjoingrup15.72.jpg | phishing | 0,98275787 |
| facebookloginsecurlty22.26.jpg | phishing | 0,98275787 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,98275787 |
| googlelogindrive.go97.89.jpg | phishing | 0,98485893 |
| googlelogineadlampy24.96.jpg | phishing | 0,98628116 |
| googleloginlbel.int84.28.jpg | phishing | 0,98275787 |
| googleloginluidacco20.43.jpg | phishing | 0,98275787 |
| googleloginsites.go48.39.jpg | phishing | 0,9847519 |
| linkedinloginauricioy76.35.jpg | phishing | 0,98275787 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,98275787 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,98275787 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,98275787 |
| linkedinloginowwglass82.2.jpg | phishing | 0,98275787 |

| | | |
|---|---|---|
| microsoftloginakakakak47.63.jpg | phishing | 0,98275787 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,9827559 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,98275787 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,98275787 |
| microsoftloginrched-el31.95.jpg | phishing | 0,98267937 |
| netflixloginahorolln04.85.jpg | phishing | 0,98275787 |
| netflixloginarketing01.44.jpg | phishing | 0,98275787 |
| netflixloginlix-flix27.43.jpg | phishing | 0,98275787 |
| netflixloginrubibags49.6.jpg | phishing | 0,98275787 |
| netflixloginww.stamp24.73.jpg | phishing | 0,98275787 |
| paypalloginackyardd28.63.jpg | phishing | 0,98275787 |
| paypalloginaypal.co74.93.jpg | phishing | 0,98275787 |
| paypalloginppuseral91.68.jpg | phishing | 0,98275787 |
| paypalloginshadetre83.51.jpg | phishing | 0,98275787 |
| paypalloginarooqmob87.19 | phishing | 0,98275787 |
| yahoologinaesencia79.26.jpg | phishing | 0,98275787 |
| yahoologinastfoodg14.91.jpg | phishing | 0,98275787 |
| yahoologinodegascr65.94.jpg | phishing | 0,98275787 |
| yahoologintinyurl.03.54.jpg | phishing | 0,98275787 |
| yahoologinww.recov40.92 | phishing | 0,98275787 |

### Γ.4.3 Δοκιμή Custom - CNN με Ρυθμό Εκμάθησης 0.0001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.0001 |
| Μέγεθος Παρτίδας (Batch_size) | 16 |
| Εποχές | 200 |
| Ακρίβεια Επικύρωσης | 95.83% |
| Απώλεια Επικύρωσης | 0.07533816993236542 |



Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Hilbert, στο εκπαιδευόμενο μοντέλο Custom-CNN με lr 0,0001.

| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,8830825 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,8830839 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,88307995 |
| adobeloginodimedia82.37.jpg | phishing | 0,8810499 |
| adobeloginwww.crea16.55.jpg | phishing | 0,88308334 |
| alibabalogindrevent.65.04.jpg | phishing | 0,8830839 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,8830709 |
| alibabaloginpineheal56.15.jpg | phishing | 0,88305116 |
| alibabaloginww.diver49.92.jpg | phishing | 0,882962 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,8830837 |
| amazonloginbestfitt19.01.jpg | phishing | 0,8830835 |
| amazonloginchinchil67.95.jpg | phishing | 0,8830827 |
| amazonloginconntect20.19.jpg | phishing | 0,8830835 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,8830835 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,88299406 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,58913165** |
| at&tloginhilltopc34.37.jpg | phishing | 0,8803878 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,8830835 |
| at&tloginmahdistr30.89.jpg | phishing | 0,88308376 |
| at&tloginzaroosha94.26.jpg | phishing | 0,8830766 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,8830466 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,8830839 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,8830839 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,8830739 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,88297474 |
| chaseloginaigonspo91.35.jpg | phishing | 0,8830515 |
| chaseloginellefont45.61.jpg | phishing | 0,8830839 |
| chaseloginotoblad.59.76.jpg | phishing | 0,8830839 |
| **chaseloginowntownd30.71.jpg** | **phishing** | **0,65112305** |
| chaselogintrack4se64.7.jpg | phishing | 0,8830839 |
| dhlloginacvedas.27.57.jpg | phishing | 0,8775527 |
| dhlloginangelart32.29.jpg | phishing | 0,8830821 |
| dhlloginharmoniu69.96.jpg | phishing | 0,87800187 |
| dhlloginhotelgra46.79.jpg | phishing | 0,8830824 |
| dhlloginogansegu00.33.jpg | phishing | 0,8830839 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,8830836 |
| ebayloginkverif23.96.jpg | phishing | 0,8830839 |
| **ebayloginpaleypri94.81.jpg** | **legitimate** | **0,60043544** |
| ebayloginrlsverif45.47.jpg | phishing | 0,8830839 |
| ebayloginthongtin17.67.jpg | phishing | 0,8830839 |
| facebookloginadm.righ42.51.jpg | phishing | 0,8830422 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,8829865 |
| facebookloginjoingrup15.72.jpg | phishing | 0,8830466 |
| facebookloginsecurlty22.26.jpg | phishing | 0,88300765 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,88284624 |
| googlelogindrive.go97.89.jpg | phishing | 0,88298666 |
| googlelogineadlampy24.96.jpg | phishing | 0,8830643 |

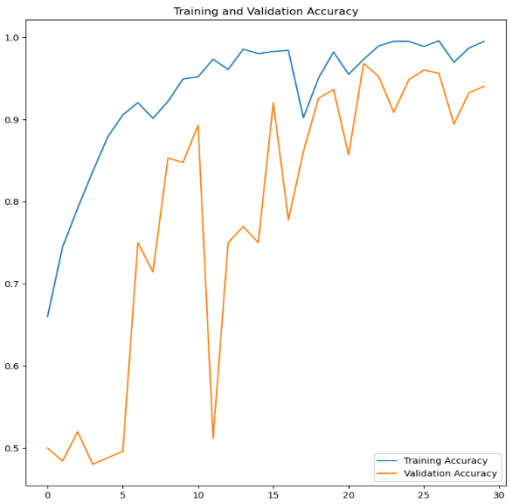
| | | |
|---|---|---|
| googleloginlbel.int84.28.jpg | phishing | 0,88306546 |
| googleloginluidacco20.43.jpg | phishing | 0,8830839 |
| googleloginsites.go48.39.jpg | phishing | 0,87778854 |
| linkedinloginauricioy76.35.jpg | phishing | 0,88221127 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,85865504 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,88308376 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,88308376 |
| linkedinloginowwglass82.2.jpg | phishing | 0,8830839 |
| microsoftloginakakakak47.63.jpg | phishing | 0,88296276 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,8830504 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,8830528 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,8830821 |
| microsoftloginrched-el31.95.jpg | phishing | 0,8825528 |
| netflixloginahorolln04.85.jpg | phishing | 0,8830274 |
| netflixloginarketing01.44.jpg | phishing | 0,88307977 |
| netflixloginlix-flix27.43.jpg | phishing | 0,8830613 |
| netflixloginrubibags49.6.jpg | phishing | 0,8824322 |
| netflixloginww.stamp24.73.jpg | phishing | 0,8830832 |
| paypalloginackyardd28.63.jpg | phishing | 0,8830633 |
| paypalloginaypal.co74.93.jpg | phishing | 0,88289875 |
| paypalloginppuseral91.68.jpg | phishing | 0,88308257 |
| paypalloginshadetre83.51.jpg | phishing | 0,8819853 |
| paypalloginarooqmob87.19 | phishing | 0,8830583 |
| yahoologinaesencia79.26.jpg | phishing | 0,8830333 |
| yahoologinastfoodg14.91.jpg | phishing | 0,8830758 |
| yahoologinodegascr65.94.jpg | phishing | 0,88308185 |
| yahoologintinyurl.03.54.jpg | phishing | 0,8830831 |
| yahoologinww.recov40.92 | phishing | 0,8830839 |

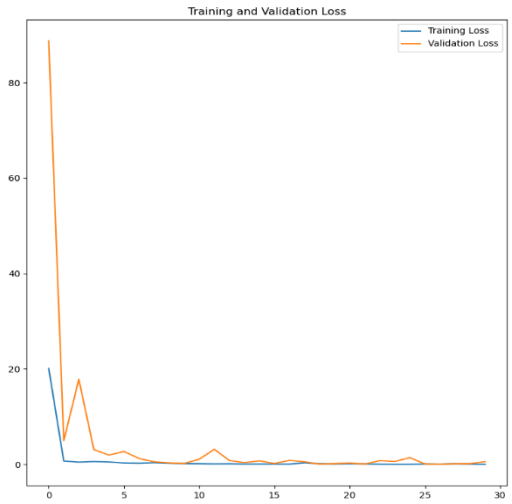
# Παράρτημα Δ
# Δοκιμές Μοντέλων με Καμπύλες Zigzag

## Δ.1 Δοκιμές MobileNet Μοντέλου και Αποτελέσματα Εκπαίδευσης

### Δ.1.1 MobileNet με Ρυθμό Εκμάθησης 0.01

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.01 |
| Μέγεθος Παρτίδας (Batch_size) | 32 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 94.14% |
| Απώλεια Επικύρωσης | 1.9776650667190552 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zigzag, στο εκπαιδευόμενο μοντέλο MobileNet με lr 0,01.

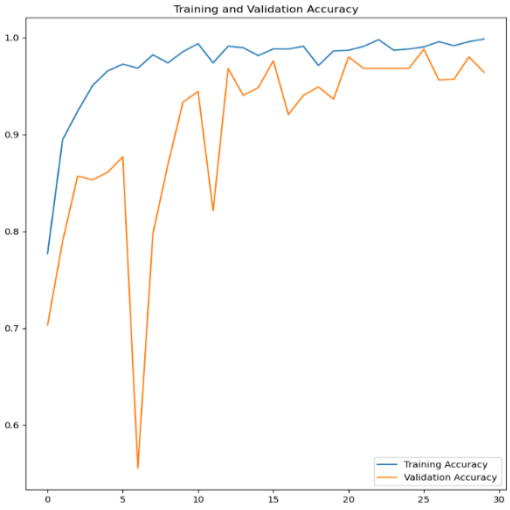
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,9933541 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9997025 |
| **adobeloginhuncoppe56.16.jpg** | **legitimate** | **0,5699004** |
| adobeloginodimedia82.37.jpg | phishing | 0,9999194 |
| adobeloginwww.crea16.55.jpg | phishing | 0,99944645 |
| alibabalogindrevent.65.04.jpg | phishing | 0,9999999 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,9999945 |

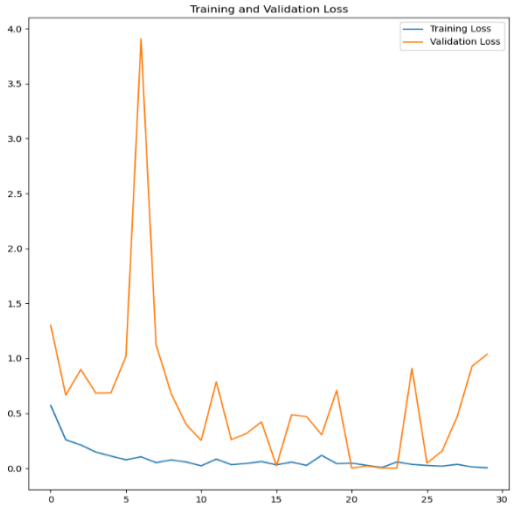
| | | |
|---|---|---|
| alibabaloginpineheal56.15.jpg | phishing | 0,9835254 |
| alibabaloginww.diver49.92.jpg | phishing | 0,9978923 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,99996924 |
| amazonloginbestfitt19.01.jpg | phishing | 0,9999645 |
| amazonloginchinchil67.95.jpg | phishing | 0,9753214 |
| amazonloginconntect20.19.jpg | phishing | 0,9999858 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,9999647 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,99972326 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,7396446** |
| at&tloginhilltopc34.37.jpg | phishing | 0,9959974 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9935539 |
| at&tloginmahdistr30.89.jpg | phishing | 0,9998542 |
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,9992124 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,99991417 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,9999999 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 1 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,9996532 |
| chaseloginaigonspo91.35.jpg | phishing | 0,9540615 |
| chaseloginellefont45.61.jpg | phishing | 0,99999726 |
| chaseloginotoblad.59.76.jpg | phishing | 0,99999726 |
| chaseloginowntownd30.71.jpg | phishing | 0,9955806 |
| chaselogintrack4se64.7.jpg | phishing | 0,99962544 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9999913 |
| dhlloginangelart32.29.jpg | phishing | 0,99999607 |
| dhlloginharmoniu69.96.jpg | phishing | 0,99999976 |
| dhlloginhotelgra46.79.jpg | phishing | 0,9999999 |
| dhlloginogansegu00.33.jpg | phishing | 0,9960145 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,9999763 |
| ebayloginkverif23.96.jpg | phishing | 0,99040097 |
| **ebayloginpaleypri94.81.jpg** | **legitimate** | **0,90154** |
| ebayloginrlsverif45.47.jpg | phishing | 0,99040097 |
| ebayloginthongtin17.67.jpg | phishing | 0,9999943 |
| facebookloginadm.righ42.51.jpg | phishing | 0,9999585 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9999993 |
| facebookloginjoingrup15.72.jpg | phishing | 0,9999964 |
| facebookloginsecurlty22.26.jpg | phishing | 0,9998344 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,9999558 |
| googlelogindrive.go97.89.jpg | phishing | 0,914577 |
| googlelogineadlampy24.96.jpg | phishing | 0,9997837 |
| googleloginlbel.int84.28.jpg | phishing | 0,99997485 |
| googleloginluidacco20.43.jpg | phishing | 0,9982102 |
| googleloginsites.go48.39.jpg | phishing | 0,9887832 |
| linkedinloginauricioy76.35.jpg | phishing | 0,8140912 |
| **linkedinlogindvtejas.76.89.jpg** | **legitimate** | **0,88566667** |
| linkedinloginmade-in-59.37.jpg | phishing | 0,9494447 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,9997769 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 0,999992 |
| **microsoftlogindreamy-g35.49.jpg** | **phishing** | **0,7592009** |
| **microsoftloginfolhadac33.31.jpg** | **legitimate** | **0,57023233** |
| | | |

| | | |
|---|---|---|
| microsoftloginnazahaco60.47.jpg | phishing | 0,9999988 |
| microsoftloginrched-el31.95.jpg | phishing | 0,98994887 |
| netflixloginahorolln04.85.jpg | phishing | 0,9993536 |
| netflixloginarketing01.44.jpg | phishing | 0,9995441 |
| netflixloginlix-flix27.43.jpg | phishing | 0,9750372 |
| **netflixloginrubibags49.6.jpg** | **phishing** | **0,6848015** |
| netflixloginww.stamp24.73.jpg | phishing | 0,9772899 |
| paypalloginackyardd28.63.jpg | phishing | 0,999908 |
| paypalloginaypal.co74.93.jpg | phishing | 0,92450976 |
| paypalloginppuseral91.68.jpg | phishing | 1 |
| paypalloginshadetre83.51.jpg | phishing | 1 |
| paypalloginarooqmob87.19 | phishing | 0,999998 |
| yahoologinaesencia79.26.jpg | phishing | 0,9999993 |
| yahoologinastfoodg14.91.jpg | phishing | 0,9960665 |
| yahoologinodegascr65.94.jpg | phishing | 0,99999726 |
| yahoologintinyurl.03.54.jpg | phishing | 0,99823713 |
| yahoologinww.recov40.92 | phishing | 0,99999976 |

### Δ.1.2 MobileNet με Ρυθμό Εκμάθησης 0.001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) | 32 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 97.27% |
| Απώλεια Επικύρωσης | 9.722941740619717e-07 |



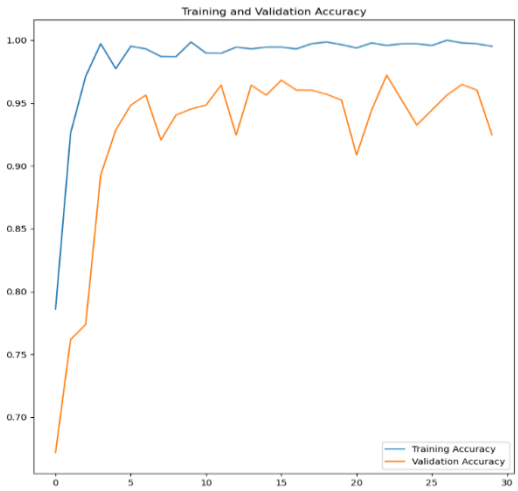

Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zigzag, στο εκπαιδευόμενο μοντέλο MobileNet με lr 0,001.

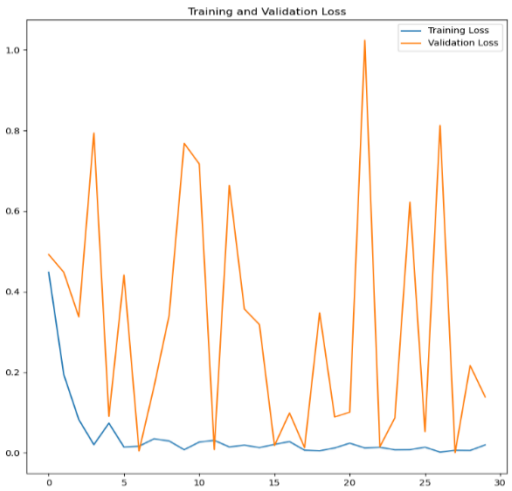
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,99999344 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,99966073 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,9999999 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 0,99999976 |
| alibabalogindrevent.65.04.jpg | phishing | 1 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,9999999 |
| alibabaloginpineheal56.15.jpg | phishing | 1 |
| alibabaloginww.diver49.92.jpg | phishing | 1 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,99999917 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 1 |
| amazonloginconntect20.19.jpg | phishing | 0,99993813 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,82141 |
| at&tloginhilltopc34.37.jpg | phishing | 0,99999774 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,99999964 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 0,9999565 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 1 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 1 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9999999 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,99999976 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| chaseloginowntownd30.71.jpg | phishing | 0,9959031 |
| chaselogintrack4se64.7.jpg | phishing | 0,9999999 |
| dhlloginacvedas.27.57.jpg | phishing | 1 |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 0,9999969 |
| dhlloginhotelgra46.79.jpg | phishing | 0,99990535 |
| dhlloginogansegu00.33.jpg | phishing | 0,99698883 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,9999999 |
| ebayloginkverif23.96.jpg | phishing | 0,9897278 |
| ebayloginpaleypri94.81.jpg | phishing | 0,9999987 |
| ebayloginrlsverif45.47.jpg | phishing | 0,9897278 |
| ebayloginthongtin17.67.jpg | phishing | 0,99997103 |
| facebookloginadm.righ42.51.jpg | phishing | 0,9999869 |
| facebookloginhx.blewp90.51.jpg | phishing | 1 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 1 |
| googlelogindrive.go97.89.jpg | phishing | 0,99999917 |
| googlelogineadlampy24.96.jpg | phishing | 0,99999285 |
| googleloginlbel.int84.28.jpg | phishing | 0,9999888 |
| googleloginluidacco20.43.jpg | phishing | 0,99998987 |
| googleloginsites.go48.39.jpg | phishing | 0,99999917 |

| | | |
|---|---|---|
| linkedinloginauricioy76.35.jpg | phishing | 0,9999769 |
| linkedinlogindvtejas.76.89.jpg | phishing | 1 |
| linkedinloginmade-in-59.37.jpg | phishing | 1 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,99999964 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 1 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,98138213 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,9999242 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,99999785 |
| microsoftloginrched-el31.95.jpg | phishing | 1 |
| netflixloginahorolln04.85.jpg | phishing | 0,99999833 |
| netflixloginarketing01.44.jpg | phishing | 0,99999964 |
| netflixloginlix-flix27.43.jpg | phishing | 0,9999999 |
| netflixloginrubibags49.6.jpg | phishing | 0,9999989 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 1 |
| paypalloginaypal.co74.93.jpg | phishing | 1 |
| paypalloginppuseral91.68.jpg | phishing | 0,9999999 |
| paypalloginshadetre83.51.jpg | phishing | 1 |
| paypalloginarooqmob87.19 | phishing | 0,9999831 |
| yahoologinaesencia79.26.jpg | phishing | 0,9999999 |
| yahoologinastfoodg14.91.jpg | phishing | 0,9999913 |
| yahoologinodegascr65.94.jpg | phishing | 0,9998299 |
| yahoologintinyurl.03.54.jpg | phishing | 0,99999106 |
| yahoologinww.recov40.92 | phishing | 0,99999833 |

### Δ.1.3 MobileNet με Ρυθμό Εκμάθησης 0.0001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.0001 |
| Μέγεθος Παρτίδας (Batch_size) | 32 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 92.97% |
| Απώλεια Επικύρωσης | 1.1033775806427002 |



Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zigzag, στο εκπαιδευόμενο μοντέλο MobileNet με lr 0,0001.

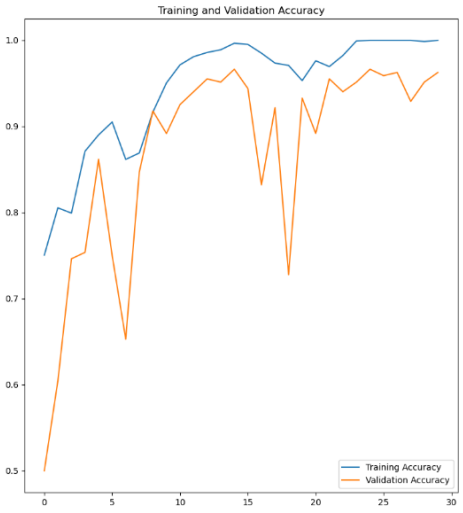
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,9999999 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9900199 |
| adobeloginhuncoppe56.16.jpg | phishing | 1 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9999901 |
| alibabalogindrevent.65.04.jpg | phishing | 0,9999999 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 0,99999905 |
| alibabaloginww.diver49.92.jpg | phishing | 0,9999999 |
| alibabaloginwww.tale61.02.jpg | phishing | 1 |
| amazonloginbestfitt19.01.jpg | phishing | 0,9999995 |
| amazonloginchinchil67.95.jpg | phishing | 0,9999999 |
| amazonloginconntect20.19.jpg | phishing | 1 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,9999995 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,99965847 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,99736303** |
| at&tloginhilltopc34.37.jpg | phishing | 0,9471469 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9999572 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 0,9999999 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 1 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,99999833 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9998204 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 0,9999441 |
| chaseloginellefont45.61.jpg | phishing | 0,99997115 |
| chaseloginotoblad.59.76.jpg | phishing | 0,99997115 |
| chaseloginowntownd30.71.jpg | phishing | 0,99664825 |
| chaselogintrack4se64.7.jpg | phishing | 0,9999999 |
| dhlloginacvedas.27.57.jpg | phishing | 0,99976164 |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 0,9999918 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,9956559 |
| ebayloginkverif23.96.jpg | phishing | 1 |
| **ebayloginpaleypri94.81.jpg** | **legitimate** | **0,99417514** |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 0,99999964 |
| facebookloginadm.righ42.51.jpg | phishing | 0,99999774 |
| facebookloginhx.blewp90.51.jpg | phishing | 1 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 0,9999962 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,99940515 |
| googlelogindrive.go97.89.jpg | phishing | 0,99641955 |

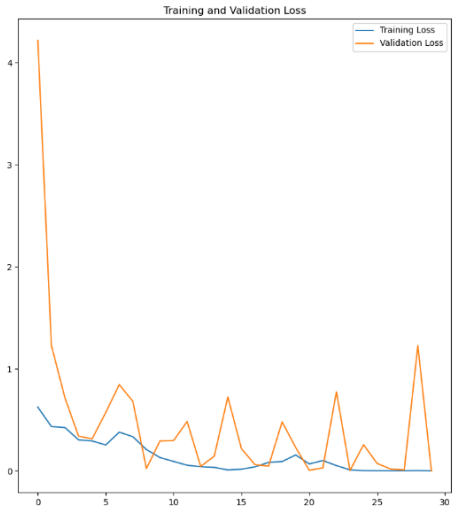
| | | |
|---|---|---|
| googlelogineadlampy24.96.jpg | phishing | 0,9998429 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 0,9987882 |
| **linkedinloginauricioy76.35.jpg** | **legitimate** | **0,99858415** |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,99994695 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,9101489 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,99999964 |
| linkedinloginowwglass82.2.jpg | phishing | 0,99999833 |
| microsoftloginakakakak47.63.jpg | phishing | 0,99894017 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,9999993 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,99999917 |
| **microsoftloginnazahaco60.47.jpg** | **phishing** | **0,55586225** |
| microsoftloginrched-el31.95.jpg | phishing | 0,9994011 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 1 |
| netflixloginrubibags49.6.jpg | phishing | 0,999624 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 0,99999964 |
| paypalloginaypal.co74.93.jpg | phishing | 0,99999845 |
| paypalloginppuseral91.68.jpg | phishing | 1 |
| paypalloginshadetre83.51.jpg | phishing | 0,99999774 |
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 1 |
| yahoologinastfoodg14.91.jpg | phishing | 0,9973769 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 0,9997788 |

# Δ.2 Δοκιμές MobileNet_RNN Μοντέλου και Αποτελέσματα Εκπαίδευσης

## Δ.2.1 MobileNet-RNN με Ρυθμό Εκμάθησης 0.01

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.01 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 97.06% |
| Απώλεια Επικύρωσης | 0.0035601546987891197 |



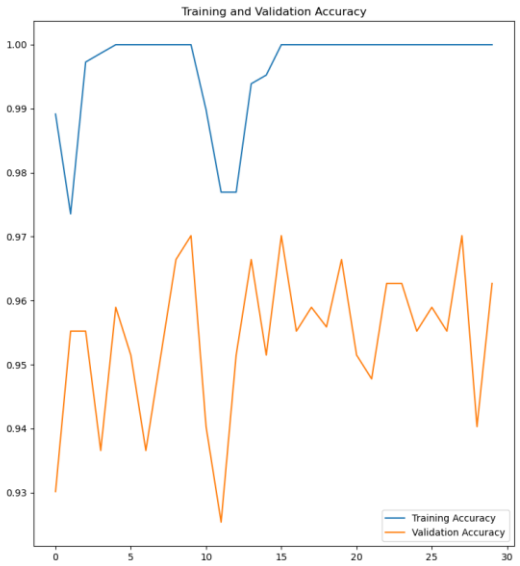

Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zigzag, στο εκπαιδευόμενο μοντέλο MobileNet-RNN με lr 0,01.

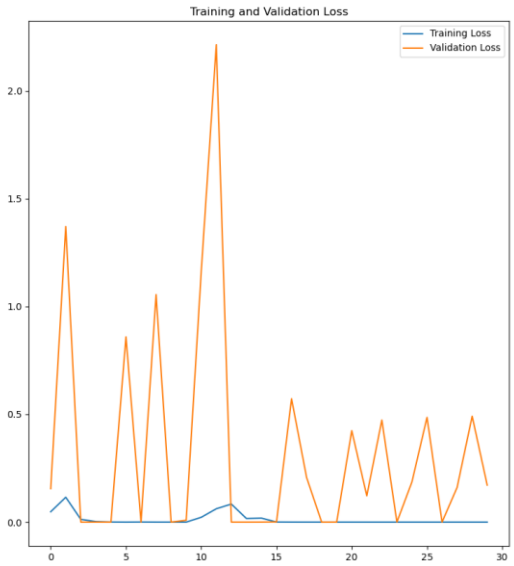
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,9999988 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9999355 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,9993705 |
| adobeloginodimedia82.37.jpg | phishing | 0,99995446 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9997167 |
| alibabalogindrevent.65.04.jpg | phishing | 0,99998975 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,9996798 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9982486 |
| alibabaloginww.diver49.92.jpg | phishing | 0,999474 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,9999478 |
| amazonloginbestfitt19.01.jpg | phishing | 0,999987 |
| amazonloginchinchil67.95.jpg | phishing | 0,99999917 |
| amazonloginconntect20.19.jpg | phishing | 0,99999845 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,999987 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,9999646 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,9999795 |
| at&tloginhilltopc34.37.jpg | phishing | 0,9907205 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9999238 |
| at&tloginmahdistr30.89.jpg | phishing | 0,9999982 |
| at&tloginzaroosha94.26.jpg | phishing | 0,9999819 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,9999958 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,9999995 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,999995 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9999063 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,9998037 |
| chaseloginaigonspo91.35.jpg | phishing | 0,9999542 |
| chaseloginellefont45.61.jpg | phishing | 0,99998724 |
| chaseloginotoblad.59.76.jpg | phishing | 0,99998724 |
| chaseloginowntownd30.71.jpg | phishing | 0,9584365 |

| | | |
|---|---|---|
| chaselogintrack4se64.7.jpg | phishing | 0,9999988 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9999894 |
| dhlloginangelart32.29.jpg | phishing | 0,9999982 |
| dhlloginharmoniu69.96.jpg | phishing | 0,9999598 |
| dhlloginhotelgra46.79.jpg | phishing | 0,99999964 |
| dhlloginogansegu00.33.jpg | phishing | 0,99998116 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,99956065 |
| ebayloginkverif23.96.jpg | phishing | 0,99834716 |
| ebayloginpaleypri94.81.jpg | phishing | 0,99739456 |
| ebayloginrlsverif45.47.jpg | phishing | 0,99834716 |
| ebayloginthongtin17.67.jpg | phishing | 0,9999989 |
| facebookloginadm.righ42.51.jpg | phishing | 0,99993503 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9984812 |
| facebookloginjoingrup15.72.jpg | phishing | 0,99999774 |
| facebookloginsecurlty22.26.jpg | phishing | 0,99955434 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,9999976 |
| googlelogindrive.go97.89.jpg | phishing | 0,99999964 |
| googlelogineadlampy24.96.jpg | phishing | 0,9994215 |
| googleloginlbel.int84.28.jpg | phishing | 0,99988794 |
| googleloginluidacco20.43.jpg | phishing | 0,9998061 |
| googleloginsites.go48.39.jpg | phishing | 0,99902654 |
| linkedinloginauricioy76.35.jpg | phishing | 0,99096876 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,9975349 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,9998517 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,999984 |
| linkedinloginowwglass82.2.jpg | phishing | 0,999982 |
| microsoftloginakakakak47.63.jpg | phishing | 0,99998033 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,8277499 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,99999905 |
| **microsoftloginnazahaco60.47.jpg** | **legitimate** | **0,9933223** |
| microsoftloginrched-el31.95.jpg | phishing | 0,9999472 |
| netflixloginahorolln04.85.jpg | phishing | 0,9999969 |
| netflixloginarketing01.44.jpg | phishing | 0,99995387 |
| netflixloginlix-flix27.43.jpg | phishing | 0,99999464 |
| netflixloginrubibags49.6.jpg | phishing | 0,99999595 |
| netflixloginww.stamp24.73.jpg | phishing | 0,9996308 |
| paypalloginackyardd28.63.jpg | phishing | 0,9999093 |
| paypalloginaypal.co74.93.jpg | phishing | 0,99723345 |
| paypalloginppuseral91.68.jpg | phishing | 0,9999988 |
| paypalloginshadetre83.51.jpg | phishing | 0,99999964 |
| paypalloginarooqmob87.19 | phishing | 0,9999776 |
| yahoologinaesencia79.26.jpg | phishing | 0,9999882 |
| yahoologinastfoodg14.91.jpg | phishing | 0,9989242 |
| yahoologinodegascr65.94.jpg | phishing | 0,9999807 |
| yahoologintinyurl.03.54.jpg | phishing | 0,99999774 |
| yahoologinww.recov40.92 | phishing | 0,9998827 |

### Δ.2.2 MobileNet-RNN με Ρυθμό Εκμάθησης 0.001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 96.32% |
| Απώλεια Επικύρωσης | 3.836948053503875e-06 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zigzag, στο εκπαιδευόμενο μοντέλο MobileNet-RNN με lr 0,001.

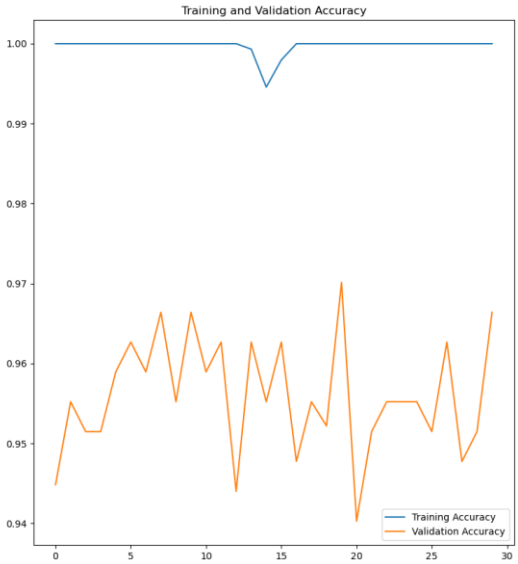
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,99998116 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,99995935 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 0,99999726 |
| alibabalogindrevent.65.04.jpg | phishing | 1 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9999999 |
| alibabaloginww.diver49.92.jpg | phishing | 0,99999666 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,9999994 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 0,9999789 |
| amazonloginconntect20.19.jpg | phishing | 0,9999944 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,9999844 |
| **at&tloginhilltopc34.37.jpg** | **legitimate** | **0,9999956** |

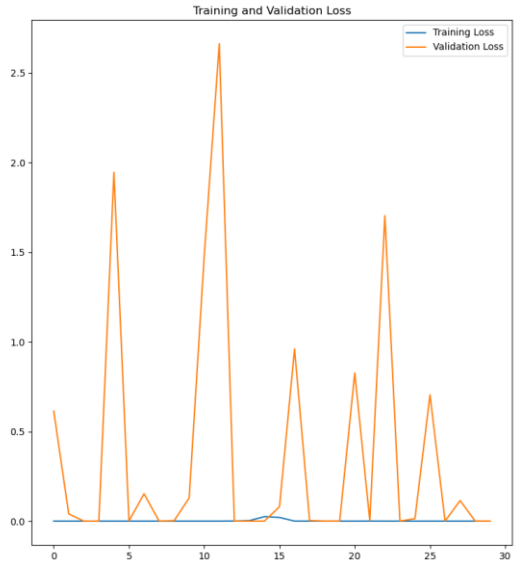
| | | |
|---|---|---|
| at&tloginkletsbuy99.14.jpg | phishing | 0,9999573 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,9999645 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 1 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9999993 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 0,9999999 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,9454928** |
| chaselogintrack4se64.7.jpg | phishing | 0,9999982 |
| dhlloginacvedas.27.57.jpg | phishing | 0,99999905 |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,99999833 |
| ebayloginkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 0,9613118 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 0,99997973 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9999974 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 0,9998331 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,99999726 |
| googlelogindrive.go97.89.jpg | phishing | 0,91096735 |
| googlelogineadlampy24.96.jpg | phishing | 0,99999774 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 0,9999417 |
| **linkedinloginauricioy76.35.jpg** | **legitimate** | **0,9930288** |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,99998355 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,9999975 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,9999907 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 0,9992093 |
| **microsoftlogindreamy-g35.49.jpg** | **legitimate** | **0,9169497** |
| microsoftloginfolhadac33.31.jpg | phishing | 1 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,9999924 |
| microsoftloginrched-el31.95.jpg | phishing | 0,99999726 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 0,99998033 |
| netflixloginrubibags49.6.jpg | phishing | 0,9998579 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 0,99999976 |
| paypalloginaypal.co74.93.jpg | phishing | 0,9999995 |
| paypalloginppuseral91.68.jpg | phishing | 1 |
| paypalloginshadetre83.51.jpg | phishing | 0,9999213 |

| | | |
|---|---|---|
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 1 |
| yahoologinastfoodg14.91.jpg | phishing | 1 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 0,99979943 |

### Δ.2.3 MobileNet-RNN με Ρυθμό Εκμάθησης 0.0001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.0001 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Μέγεθος Παρτίδας (Batch_size) | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 95.22% |
| Απώλεια Επικύρωσης | 2.980764627456665 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zigzag, στο εκπαιδευόμενο μοντέλο MobileNet-RNN με lr 0,0001.

| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9999994 |
| adobeloginhuncoppe56.16.jpg | phishing | 1 |
| adobeloginodimedia82.37.jpg | phishing | 0,9999484 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9937383 |
| alibabalogindrevent.65.04.jpg | phishing | 1 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,9999995 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9999995 |
| alibabaloginww.diver49.92.jpg | phishing | 0,99999917 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,99999547 |
| amazonloginbestfitt19.01.jpg | phishing | 0,99999595 |

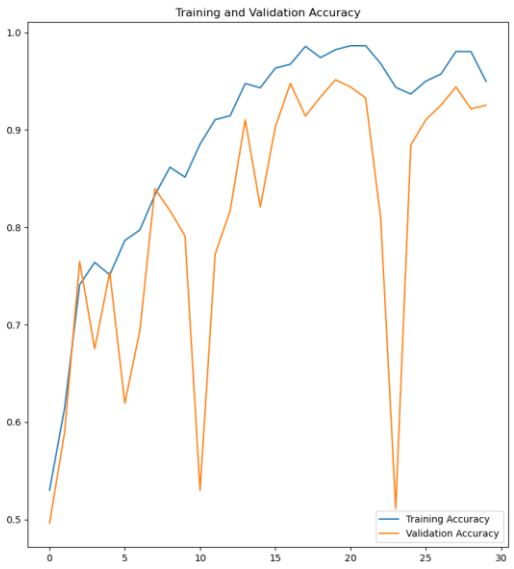
| | | |
|---|---|---|
| amazonloginchinchil67.95.jpg | phishing | 1 |
| amazonloginconntect20.19.jpg | phishing | 1 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,99999535 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,9999987 |
| **at&tloginhilltopc34.37.jpg** | **legitimate** | **0,9989397** |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9999999 |
| at&tloginmahdistr30.89.jpg | phishing | 0,9999957 |
| at&tloginzaroosha94.26.jpg | phishing | 0,9999999 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,99999714 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,99999976 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,99999785 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 1 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,99997234 |
| chaseloginaigonspo91.35.jpg | phishing | 0,9999999 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,91742516** |
| chaselogintrack4se64.7.jpg | phishing | 1 |
| dhlloginacvedas.27.57.jpg | phishing | 0,99999964 |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 0,98684096 |
| dhlloginhotelgra46.79.jpg | phishing | 0,9999763 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 1 |
| ebayloginkverif23.96.jpg | phishing | 0,99999905 |
| ebayloginpaleypri94.81.jpg | phishing | 1 |
| ebayloginrlsverif45.47.jpg | phishing | 0,99999905 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 0,97158086 |
| facebookloginhx.blewp90.51.jpg | phishing | 1 |
| facebookloginjoingrup15.72.jpg | phishing | 0,9999771 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,99999475 |
| **googlelogindrive.go97.89.jpg** | **legitimate** | **0,54855496** |
| googlelogineadlampy24.96.jpg | phishing | 1 |
| googleloginlbel.int84.28.jpg | phishing | 0,9999857 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 0,9999291 |
| linkedinloginauricioy76.35.jpg | phishing | 0,97428924 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,99987173 |
| linkedinloginmade-in-59.37.jpg | phishing | 1 |
| linkedinloginoutlookm27.79.jpg | phishing | 1 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 0,99994147 |
| **microsoftlogindreamy-g35.49.jpg** | **legitimate** | **0,5175193** |
| microsoftloginfolhadac33.31.jpg | phishing | 0,99999964 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,99940336 |
| microsoftloginrched-el31.95.jpg | phishing | 1 |
| netflixloginahorolln04.85.jpg | phishing | 0,99999976 |
| netflixloginarketing01.44.jpg | phishing | 0,99999976 |
| netflixloginlix-flix27.43.jpg | phishing | 1 |

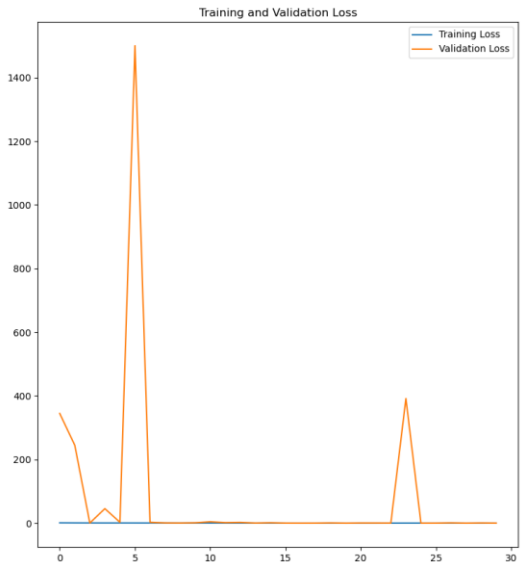
| | | |
|---|---|---|
| netflixloginrubibags49.6.jpg | phishing | 0,9978453 |
| netflixloginww.stamp24.73.jpg | phishing | 0,9999995 |
| paypalloginackyardd28.63.jpg | phishing | 0,99994016 |
| paypalloginaypal.co74.93.jpg | phishing | 0,99999094 |
| paypalloginppuseral91.68.jpg | phishing | 0,99999845 |
| paypalloginshadetre83.51.jpg | phishing | 0,99999845 |
| paypalloginarooqmob87.19 | phishing | 0,9999999 |
| yahoologinaesencia79.26.jpg | phishing | 0,9999994 |
| yahoologinastfoodg14.91.jpg | phishing | 1 |
| yahoologinodegascr65.94.jpg | phishing | 0,99999964 |
| yahoologintinyurl.03.54.jpg | phishing | 0,9999951 |
| yahoologinww.recov40.92 | phishing | 1 |

# Δ.3 Δοκιμές Xception_RNN Μοντέλου και Αποτελέσματα Εκπαίδευσης

## Δ.3.1 Xception-RNN με Ρυθμό Εκμάθησης 0.01

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.01 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 93.75 % |
| Απώλεια Επικύρωσης | 0.005075282417237759 |



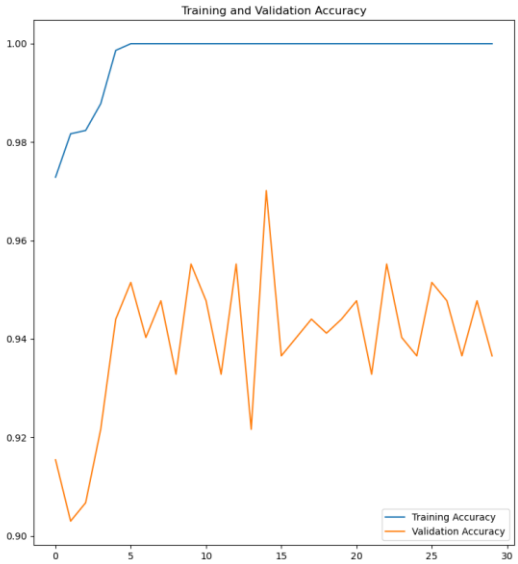
Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zigzag, στο εκπαιδευόμενο μοντέλο Xception-RNN με lr 0,01.

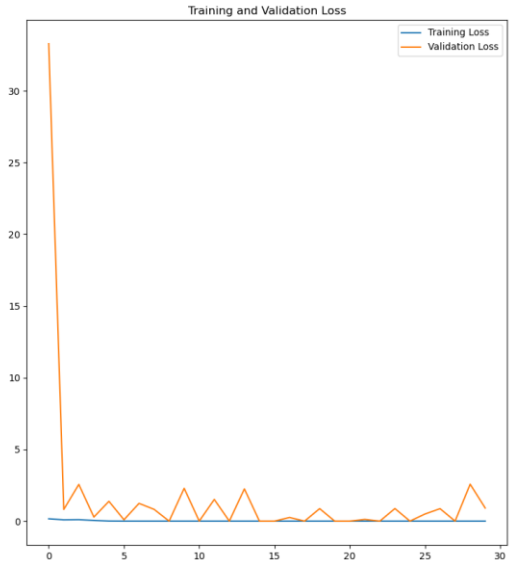
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,99999964 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,97804755 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,9962786 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9997824 |
| alibabalogindrevent.65.04.jpg | phishing | 1 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9999832 |
| alibabaloginww.diver49.92.jpg | phishing | 0,9999784 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,9995566 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 0,9990907 |
| amazonloginconntect20.19.jpg | phishing | 0,91590166 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,8340641 |
| **at&tloginhilltopc34.37.jpg** | **phishing** | **0,7606937** |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9853166 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 0,9999889 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,9754056 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,9999963 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,9979327 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9948285 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 0,9028195 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,7846368** |
| chaselogintrack4se64.7.jpg | phishing | 0,92969877 |
| dhlloginacvedas.27.57.jpg | phishing | 0,99975735 |
| dhlloginangelart32.29.jpg | phishing | 0,9998369 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,998381 |
| ebayloginkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 0,9998554 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9998809 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 0,89666754 |
| facebookloginxvgbtopl00.11.jpg | phishing | 1 |
| googlelogindrive.go97.89.jpg | phishing | 0,9970475 |

| **googlelogineadlampy24.96.jpg** | **phishing** | **0,54408044** |
|---|---|---|
| googleloginlbel.int84.28.jpg | phishing | 0,99999774 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 0,9994029 |
| **linkedinloginauricioy76.35.jpg** | **legitimate** | **0,508715** |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,99830675 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,9940481 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,8912116 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 0,99993443 |
| microsoftlogindreamy-g35.49.jpg | phishing | 1 |
| microsoftloginfolhadac33.31.jpg | phishing | 1 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,998752 |
| microsoftloginrched-el31.95.jpg | phishing | 1 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 0,97302395 |
| netflixloginrubibags49.6.jpg | phishing | 0,99999666 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 0,99999976 |
| paypalloginaypal.co74.93.jpg | phishing | 1 |
| paypalloginppuseral91.68.jpg | phishing | 1 |
| paypalloginshadetre83.51.jpg | phishing | 0,9999932 |
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 1 |
| yahoologinastfoodg14.91.jpg | phishing | 0,94693494 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 0,9978947 |

### Δ.3.2 Xception-RNN με Ρυθμό Εκμάθησης 0.001

| Ρυθμός Εκμάθησης lr | 0.001 |
|---|---|
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 94,12 % |
| Απώλεια Επικύρωσης | 1.4941227436065674 |



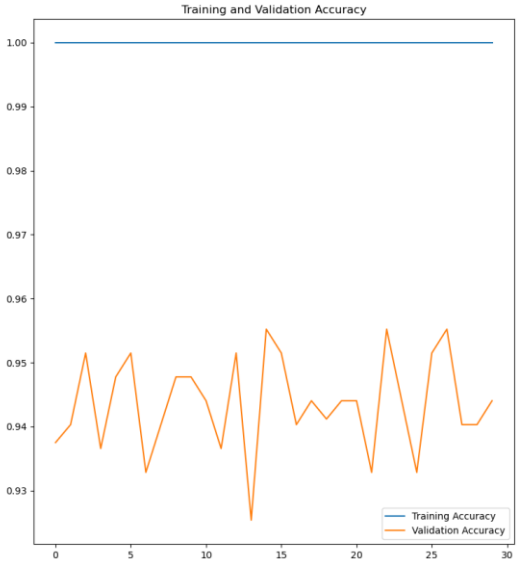

Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zigzag, στο εκπαιδευόμενο μοντέλο Xception-RNN με lr 0,001.

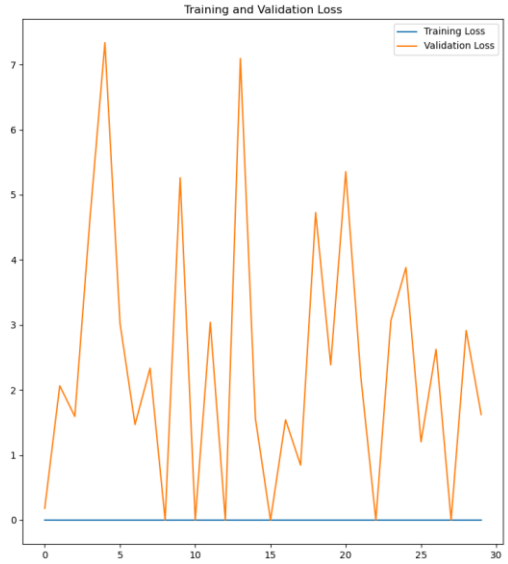
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9999999 |
| adobeloginhuncoppe56.16.jpg | phishing | 1 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| **adobeloginwww.crea16.55.jpg** | **legitimate** | **0,9803452** |
| alibabalogindrevent.65.04.jpg | phishing | 0,9999999 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9999999 |
| alibabaloginww.diver49.92.jpg | phishing | 0,99999976 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,99999976 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 1 |
| amazonloginconntect20.19.jpg | phishing | 1 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| at&tlogindocs.goo12.02.jpg | phishing | 1 |
| at&tloginhilltopc34.37.jpg | phishing | 0,99942255 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,99999654 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 1 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 1 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9999962 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 0,99999964 |
| chaseloginotoblad.59.76.jpg | phishing | 0,99999964 |

| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,99675155** |
|---|---|---|
| chaselogintrack4se64.7.jpg | phishing | 1 |
| dhlloginacvedas.27.57.jpg | phishing | 1 |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,99997044 |
| ebayloginkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 1 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,99999535 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 1 |
| googlelogindrive.go97.89.jpg | phishing | 1 |
| googlelogineadlampy24.96.jpg | phishing | 0,99999857 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 1 |
| **linkedinloginauricioy76.35.jpg** | **legitimate** | **0,9961074** |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,9996649 |
| linkedinloginmade-in-59.37.jpg | phishing | 1 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,9999777 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 1 |
| **microsoftlogindreamy-g35.49.jpg** | **legitimate** | **0,9711978** |
| microsoftloginfolhadac33.31.jpg | phishing | 0,9999995 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,9973584 |
| microsoftloginrched-el31.95.jpg | phishing | 0,99999917 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 1 |
| **netflixloginrubibags49.6.jpg** | **phishing** | **0,65413564** |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 1 |
| paypalloginaypal.co74.93.jpg | phishing | 0,99999976 |
| paypalloginppuseral91.68.jpg | phishing | 1 |
| paypalloginshadetre83.51.jpg | phishing | 1 |
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 1 |
| yahoologinastfoodg14.91.jpg | phishing | 1 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 1 |

### Δ.3.3 Xception-RNN με Ρυθμό Εκμάθησης 0.0001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 94,12 % |
| Απώλεια Επικύρωσης | 2.102830410003662 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zigzag, στο εκπαιδευόμενο μοντέλο Xception-RNN με lr 0,0001.

| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 1 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,99999976 |
| adobeloginodimedia82.37.jpg | phishing | 0,9999995 |
| adobeloginwww.crea16.55.jpg | phishing | 1 |
| alibabalogindrevent.65.04.jpg | phishing | 1 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 1 |
| alibabaloginww.diver49.92.jpg | phishing | 1 |
| alibabaloginwww.tale61.02.jpg | phishing | 1 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 1 |
| amazonloginconntect20.19.jpg | phishing | 1 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| at&tlogindocs.goo12.02.jpg | phishing | 1 |
| **at&tloginhilltopc34.37.jpg** | **legitimate** | **0,9999994** |
| at&tloginkletsbuy99.14.jpg | phishing | 1 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |

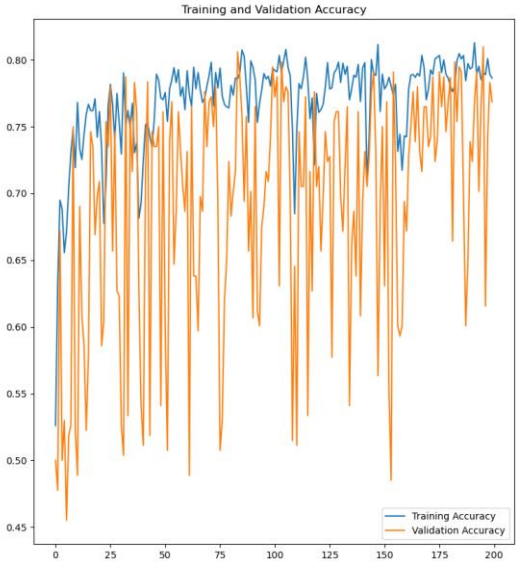
| | | |
|---|---|---|
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 1 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 1 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 1 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| chaseloginowntownd30.71.jpg | phishing | 1 |
| chaselogintrack4se64.7.jpg | phishing | 1 |
| dhlloginacvedas.27.57.jpg | phishing | 1 |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 1 |
| ebaylogininkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 1 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| facebookloginhx.blewp90.51.jpg | phishing | 1 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 1 |
| googlelogindrive.go97.89.jpg | phishing | 1 |
| googlelogineadlampy24.96.jpg | phishing | 1 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 1 |
| linkedinloginauricioy76.35.jpg | phishing | 1 |
| linkedinlogindvtejas.76.89.jpg | phishing | 1 |
| linkedinloginmade-in-59.37.jpg | phishing | 1 |
| linkedinloginoutlookm27.79.jpg | phishing | 1 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | legitimate | 1 |
| **microsoftlogindreamy-g35.49.jpg** | **legitimate** | **1** |
| microsoftloginfolhadac33.31.jpg | phishing | 1 |
| microsoftloginnazahaco60.47.jpg | phishing | 1 |
| microsoftloginrched-el31.95.jpg | phishing | 1 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 1 |
| netflixloginrubibags49.6.jpg | phishing | 1 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 1 |
| paypalloginaypal.co74.93.jpg | phishing | 1 |
| paypalloginppuseral91.68.jpg | phishing | 1 |
| paypalloginshadetre83.51.jpg | phishing | 1 |
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 1 |

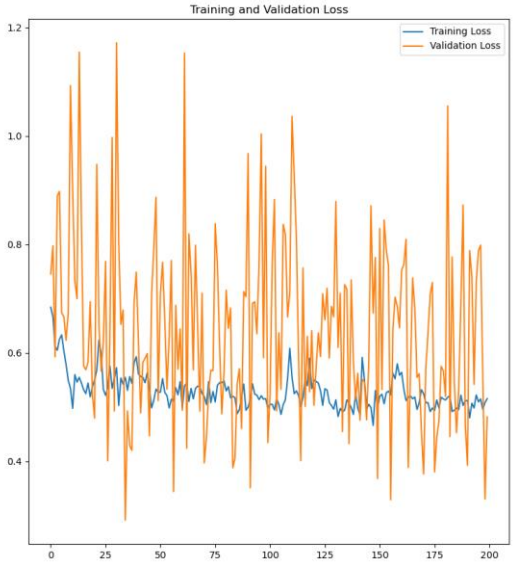
| | | |
|---|---|---|
| yahoologinastfoodg14.91.jpg | phishing | 1 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 1 |

# Δ.4 Δοκιμές Custom CNN Μοντέλου και Αποτελέσματα Εκπαίδευσης

## Δ.4.1 Custom CNN Μοντέλο με Ρυθμό Εκμάθησης 0.01

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.01 |
| Μέγεθος Παρτίδας (Batch_size) | 16 |
| Εποχές | 200 |
| Ακρίβεια Επικύρωσης | 77.57 % |
| Απώλεια Επικύρωσης | 0.40028566122055054 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zigzag, στο εκπαιδευόμενο μοντέλο Custom-CNN με lr 0,01.

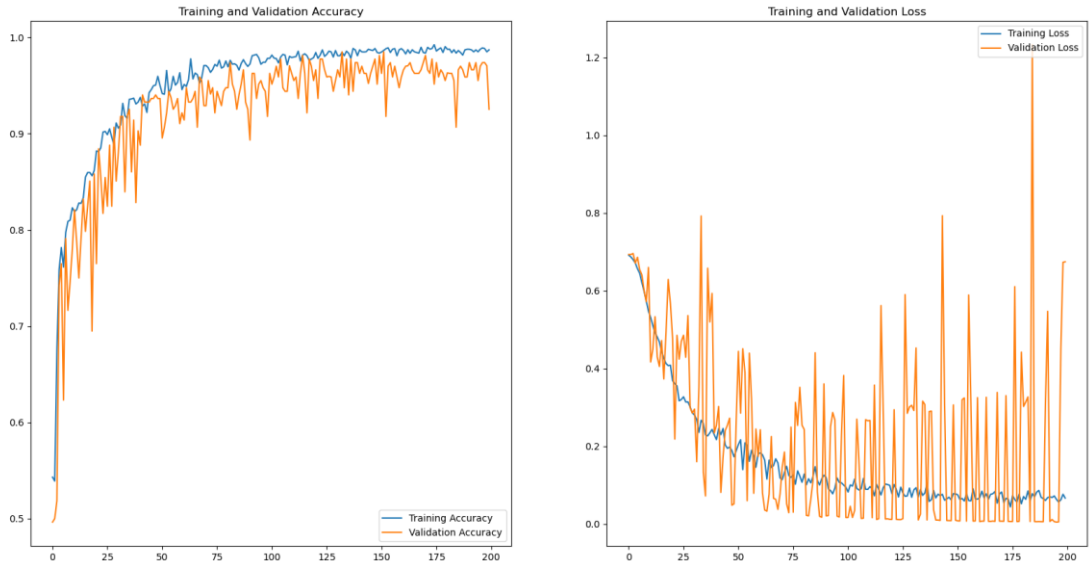
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,8596088 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,8596088 |
| **adobeloginhuncoppe56.16.jpg** | **legitimate** | **0,75002575** |
| adobeloginodimedia82.37.jpg | phishing | 0,8596088 |
| adobeloginwww.crea16.55.jpg | phishing | 0,8596088 |
| alibabalogindrevent.65.04.jpg | phishing | 0,8596088 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,8596088 |

| | | |
|---|---|---|
| alibabaloginpineheal56.15.jpg | phishing | 0,8596088 |
| **alibabaloginww.diver49.92.jpg** | **legitimate** | **0,75002575** |
| **alibabaloginwww.tale61.02.jpg** | **legitimate** | **0,75002575** |
| amazonloginbestfitt19.01.jpg | phishing | 0,8596088 |
| amazonloginchinchil67.95.jpg | phishing | 0,8596088 |
| amazonloginconntect20.19.jpg | phishing | 0,8596088 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,8596088 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,8596088 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,75002575** |
| at&tloginhilltopc34.37.jpg | phishing | 0,8596088 |
| **at&tloginkletsbuy99.14.jpg** | **legitimate** | **0,75002575** |
| at&tloginmahdistr30.89.jpg | phishing | 0,8596088 |
| at&tloginzaroosha94.26.jpg | phishing | 0,8596088 |
| **bankofamericalogin5.188.3665.04.jpg** | **legitimate** | **0,75002575** |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,8596088 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,8596088 |
| **bankofamericaloginkrjpl.co60.86.jpg** | **legitimate** | **0,75002575** |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,8596088 |
| chaseloginaigonspo91.35.jpg | phishing | 0,8596088 |
| chaseloginellefont45.61.jpg | phishing | 0,8596088 |
| chaseloginotoblad.59.76.jpg | phishing | 0,8596088 |
| chaseloginowntownd30.71.jpg | phishing | 0,8596088 |
| chaselogintrack4se64.7.jpg | phishing | 0,8596088 |
| dhlloginacvedas.27.57.jpg | phishing | 0,8596088 |
| dhlloginangelart32.29.jpg | phishing | 0,8596088 |
| dhlloginharmoniu69.96.jpg | phishing | 0,8596088 |
| dhlloginhotelgra46.79.jpg | phishing | 0,8596088 |
| dhlloginogansegu00.33.jpg | phishing | 0,8596088 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,8596088 |
| ebaylogininkverif23.96.jpg | phishing | 0,8596088 |
| **ebayloginpaleypri94.81.jpg** | **legitimate** | **0,75002575** |
| ebayloginrlsverif45.47.jpg | phishing | 0,8596088 |
| ebayloginthongtin17.67.jpg | phishing | 0,8596088 |
| facebookloginadm.righ42.51.jpg | phishing | 0,8596088 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,8596088 |
| facebookloginjoingrup15.72.jpg | phishing | 0,8596088 |
| facebookloginsecurlty22.26.jpg | phishing | 0,8596088 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,8596088 |
| googlelogindrive.go97.89.jpg | phishing | 0,85960865 |
| **googlelogineadlampy24.96.jpg** | **legitimate** | **0,75002575** |
| googleloginlbel.int84.28.jpg | phishing | 0,8596088 |
| googleloginluidacco20.43.jpg | phishing | 0,8596088 |
| **googleloginsites.go48.39.jpg** | **legitimate** | **0,75002575** |
| **linkedinloginauricioy76.35.jpg** | **legitimate** | **0,75002575** |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,8596088 |
| **linkedinloginmade-in-59.37.jpg** | **legitimate** | **0,75002575** |
| linkedinloginoutlookm27.79.jpg | phishing | 0,8596088 |
| linkedinloginowwglass82.2.jpg | phishing | 0,8596088 |
| **microsoftloginakakakak47.63.jpg** | **legitimate** | **0,75002575** |
| **microsoftlogindreamy-g35.49.jpg** | **phishing** | **0,6208201** |
| microsoftloginfolhadac33.31.jpg | phishing | 0,8596088 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,8596088 |

| | | |
|---|---|---|
| **microsoftloginrched-el31.95.jpg** | **phishing** | **0,6208201** |
| netflixloginahorolln04.85.jpg | phishing | 0,8596088 |
| netflixloginarketing01.44.jpg | phishing | 0,8596088 |
| **netflixloginlix-flix27.43.jpg** | **legitimate** | **0,75002575** |
| netflixloginrubibags49.6.jpg | phishing | 0,8596088 |
| **netflixloginww.stamp24.73.jpg** | **legitimate** | **0,75002575** |
| paypalloginackyardd28.63.jpg | phishing | 0,8596088 |
| paypalloginaypal.co74.93.jpg | phishing | 0,8596088 |
| paypalloginppuseral91.68.jpg | phishing | 0,8596088 |
| paypalloginshadetre83.51.jpg | phishing | 0,8596088 |
| paypalloginarooqmob87.19 | phishing | 0,8596088 |
| yahoologinaesencia79.26.jpg | phishing | 0,8596088 |
| **yahoologinastfoodg14.91.jpg** | **legitimate** | **0,74873537** |
| yahoologinodegascr65.94.jpg | phishing | 0,8596088 |
| yahoologintinyurl.03.54.jpg | phishing | 0,8596088 |
| yahoologinww.recov40.92 | phishing | 0,8596088 |

### Δ.4.2 Custom CNN Μοντέλο με Ρυθμό Εκμάθησης 0.001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) | 16 |
| Εποχές | 200 |
| Ακρίβεια Επικύρωσης | 92.28% |
| Απώλεια Επικύρωσης | 0.09222497045993805 |



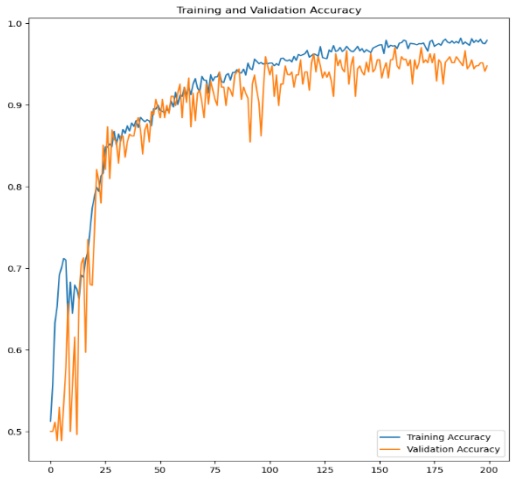

Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zigzag, στο εκπαιδευόμενο μοντέλο Custom-CNN με lr 0,001.

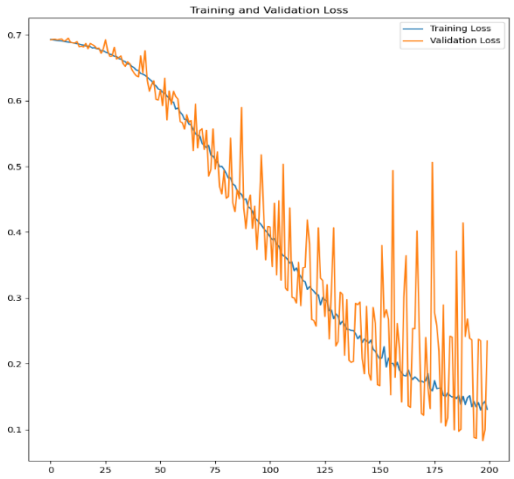
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,9881486 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9881486 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,9881374 |
| adobeloginodimedia82.37.jpg | phishing | 0,9881486 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9881486 |
| alibabalogindrevent.65.04.jpg | phishing | 0,98407346 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,9881486 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9881486 |
| alibabaloginww.diver49.92.jpg | phishing | 0,9881484 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,98493123 |
| amazonloginbestfitt19.01.jpg | phishing | 0,9881486 |
| amazonloginchinchil67.95.jpg | phishing | 0,9881486 |
| amazonloginconntect20.19.jpg | phishing | 0,9881486 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,9881486 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,9881486 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,9881486 |
| at&tloginhilltopc34.37.jpg | phishing | 0,9881486 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9881302 |
| at&tloginmahdistr30.89.jpg | phishing | 0,9881486 |
| at&tloginzaroosha94.26.jpg | phishing | 0,9881486 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,9881486 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,9881486 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,9881486 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9881342 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,9881486 |
| chaseloginaigonspo91.35.jpg | phishing | 0,98814803 |
| chaseloginellefont45.61.jpg | phishing | 0,9881486 |
| chaseloginotoblad.59.76.jpg | phishing | 0,9881486 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,9909389** |
| chaselogintrack4se64.7.jpg | phishing | 0,9881486 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9881486 |
| dhlloginangelart32.29.jpg | phishing | 0,9881486 |
| dhlloginharmoniu69.96.jpg | phishing | 0,9881486 |
| dhlloginhotelgra46.79.jpg | phishing | 0,9881486 |
| dhlloginogansegu00.33.jpg | phishing | 0,9881486 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,9881486 |
| ebayloginkverif23.96.jpg | phishing | 0,9881486 |
| ebayloginpaleypri94.81.jpg | phishing | 0,9881486 |
| ebayloginrlsverif45.47.jpg | phishing | 0,9881486 |
| ebayloginthongtin17.67.jpg | phishing | 0,9881486 |
| facebookloginadm.righ42.51.jpg | phishing | 0,9881486 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9881486 |
| facebookloginjoingrup15.72.jpg | phishing | 0,9881486 |
| facebookloginsecurlty22.26.jpg | phishing | 0,9881486 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,9881486 |
| **googlelogindrive.go97.89.jpg** | **legitimate** | **0,9895257** |
| googlelogineadlampy24.96.jpg | phishing | 0,9760149 |
| googleloginlbel.int84.28.jpg | phishing | 0,9881486 |
| googleloginluidacco20.43.jpg | phishing | 0,9881486 |
| googleloginsites.go48.39.jpg | phishing | 0,9845317 |

| | | |
|---|---|---|
| linkedinloginauricioy76.35.jpg | phishing | 0,9881486 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,9881486 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,9881486 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,9881486 |
| linkedinloginowwglass82.2.jpg | phishing | 0,9881486 |
| microsoftloginakakakak47.63.jpg | phishing | 0,9881486 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,9881486 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,9881486 |
| **microsoftloginnazahaco60.47.jpg** | **legitimate** | **0,9905934** |
| microsoftloginrched-el31.95.jpg | phishing | 0,9845317 |
| netflixloginahorolln04.85.jpg | phishing | 0,9881486 |
| netflixloginarketing01.44.jpg | phishing | 0,9881486 |
| netflixloginlix-flix27.43.jpg | phishing | 0,9881486 |
| netflixloginrubibags49.6.jpg | phishing | 0,9881486 |
| netflixloginww.stamp24.73.jpg | phishing | 0,9881486 |
| paypalloginackyardd28.63.jpg | phishing | 0,9881486 |
| paypalloginaypal.co74.93.jpg | phishing | 0,9881486 |
| paypalloginppuseral91.68.jpg | phishing | 0,9881486 |
| paypalloginshadetre83.51.jpg | phishing | 0,9881486 |
| paypalloginarooqmob87.19 | phishing | 0,9881486 |
| yahoologinaesencia79.26.jpg | phishing | 0,9881486 |
| yahoologinastfoodg14.91.jpg | phishing | 0,9881486 |
| yahoologinodegascr65.94.jpg | phishing | 0,9881486 |
| yahoologintinyurl.03.54.jpg | phishing | 0,9881443 |
| yahoologinww.recov40.92 | phishing | 0,9881486 |

### Δ.4.3 Custom CNN Μοντέλο με Ρυθμό Εκμάθησης 0.001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) | 16 |
| Εποχές | 200 |
| Ακρίβεια Επικύρωσης | 94.85% |
| Απώλεια Επικύρωσης | 0.08079496026039124 |



Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zigzag, στο εκπαιδευόμενο μοντέλο Custom-CNN με lr 0,0001.

| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,86401075 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,86401075 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,86401075 |
| adobeloginodimedia82.37.jpg | phishing | 0,86401075 |
| adobeloginwww.crea16.55.jpg | phishing | 0,86401075 |
| alibabalogindrevent.65.04.jpg | phishing | 0,86401075 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,86401075 |
| alibabaloginpineheal56.15.jpg | phishing | 0,8640088 |
| alibabaloginww.diver49.92.jpg | phishing | 0,86399865 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,8640106 |
| amazonloginbestfitt19.01.jpg | phishing | 0,86401075 |
| amazonloginchinchil67.95.jpg | phishing | 0,86401075 |
| amazonloginconntect20.19.jpg | phishing | 0,8640083 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,86401075 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,86401075 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,85544765 |
| at&tloginhilltopc34.37.jpg | phishing | 0,86401075 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,8640105 |
| at&tloginmahdistr30.89.jpg | phishing | 0,86401075 |
| at&tloginzaroosha94.26.jpg | phishing | 0,86401075 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,86401075 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,86401075 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,86401075 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,86401075 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,86401075 |
| chaseloginaigonspo91.35.jpg | phishing | 0,8640107 |
| chaseloginellefont45.61.jpg | phishing | 0,86401075 |
| chaseloginotoblad.59.76.jpg | phishing | 0,86401075 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,8444344** |
| chaselogintrack4se64.7.jpg | phishing | 0,86401075 |
| dhlloginacvedas.27.57.jpg | phishing | 0,8640098 |
| dhlloginangelart32.29.jpg | phishing | 0,86401075 |
| dhlloginharmoniu69.96.jpg | phishing | 0,86401075 |
| dhlloginhotelgra46.79.jpg | phishing | 0,86401075 |
| dhlloginogansegu00.33.jpg | phishing | 0,86401075 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,8640081 |
| ebayloginkverif23.96.jpg | phishing | 0,86401075 |
| ebayloginpaleypri94.81.jpg | phishing | 0,8640106 |
| ebayloginrlsverif45.47.jpg | phishing | 0,86401075 |
| ebayloginthongtin17.67.jpg | phishing | 0,86401075 |
| facebookloginadm.righ42.51.jpg | phishing | 0,86401075 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,8640106 |
| facebookloginjoingrup15.72.jpg | phishing | 0,86401075 |
| facebookloginsecurlty22.26.jpg | phishing | 0,86401075 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,8640098 |
| googlelogindrive.go97.89.jpg | phishing | 0,8637161 |
| googlelogineadlampy24.96.jpg | phishing | 0,85026336 |

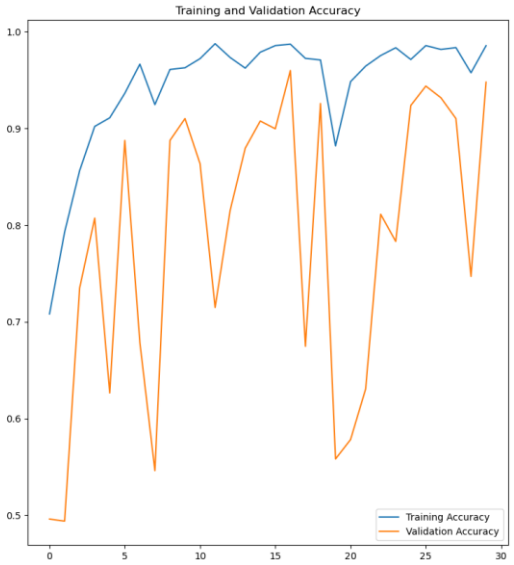
| | | |
|---|---|---|
| googleloginlbel.int84.28.jpg | phishing | 0,86401075 |
| googleloginluidacco20.43.jpg | phishing | 0,86401075 |
| googleloginsites.go48.39.jpg | phishing | 0,8638234 |
| linkedinloginauricioy76.35.jpg | phishing | 0,86401075 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,86400443 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,86401075 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,8640097 |
| linkedinloginowwglass82.2.jpg | phishing | 0,86401075 |
| microsoftloginakakakak47.63.jpg | phishing | 0,86401075 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,8640106 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,86401075 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,86401075 |
| microsoftloginrched-el31.95.jpg | phishing | 0,86401016 |
| netflixloginahorolln04.85.jpg | phishing | 0,86401075 |
| netflixloginarketing01.44.jpg | phishing | 0,86401075 |
| netflixloginlix-flix27.43.jpg | phishing | 0,8640107 |
| netflixloginrubibags49.6.jpg | phishing | 0,86398566 |
| netflixloginww.stamp24.73.jpg | phishing | 0,86401075 |
| paypalloginackyardd28.63.jpg | phishing | 0,86401075 |
| paypalloginaypal.co74.93.jpg | phishing | 0,86401075 |
| paypalloginppuseral91.68.jpg | phishing | 0,86401075 |
| paypalloginshadetre83.51.jpg | phishing | 0,86401075 |
| paypalloginarooqmob87.19 | phishing | 0,86401075 |
| yahoologinaesencia79.26.jpg | phishing | 0,86401075 |
| yahoologinastfoodg14.91.jpg | phishing | 0,86401075 |
| yahoologinodegascr65.94.jpg | phishing | 0,86401075 |
| yahoologintinyurl.03.54.jpg | phishing | 0,86401075 |
| yahoologinww.recov40.92 | phishing | 0,86401075 |

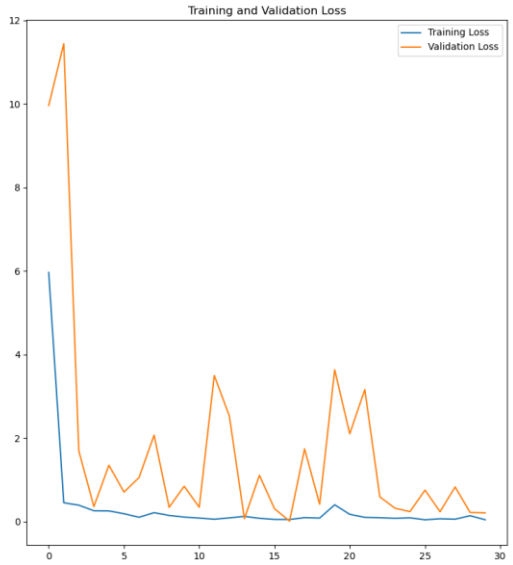
# Παράρτημα Ε
# Δοκιμές Μοντέλων με Καμπύλες Zorder

## Ε.1 Δοκιμές MobileNet Μοντέλου και Αποτελέσματα Εκπαίδευσης

### Ε.1.1 MobileNet με Ρυθμό Εκμάθησης 0.01

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.01 |
| Μέγεθος Παρτίδας (Batch_size) | 32 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 95.31% |
| Απώλεια Επικύρωσης | 0.11346303671598434 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zorder, στο εκπαιδευόμενο μοντέλο MobileNet με lr 0,01.

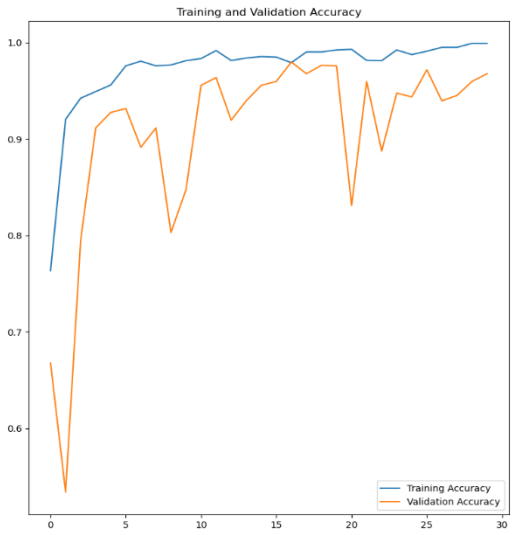
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9999999 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,99999976 |

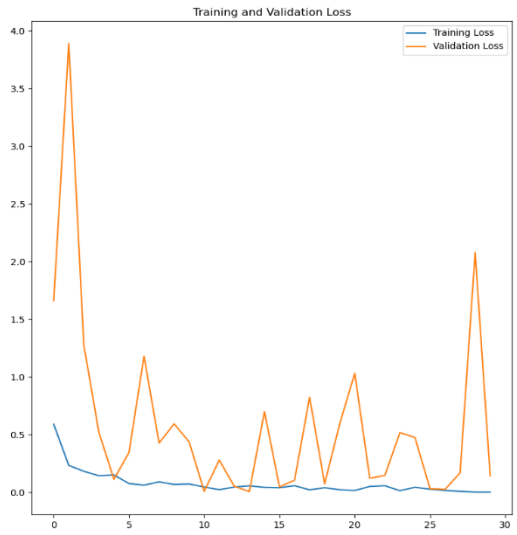
| | | |
|---|---|---|
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 1 |
| alibabalogindrevent.65.04.jpg | phishing | 1 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9998435 |
| alibabaloginww.diver49.92.jpg | phishing | 1 |
| alibabaloginwww.tale61.02.jpg | phishing | 1 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 0,9999082 |
| amazonloginconntect20.19.jpg | phishing | 0,9999932 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,99980825** |
| at&tloginhilltopc34.37.jpg | phishing | 0,9991153 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9999969 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,9724873 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 1 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,99716944 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| chaseloginowntownd30.71.jpg | phishing | 0,9722282 |
| chaselogintrack4se64.7.jpg | phishing | 0,99969697 |
| dhlloginacvedas.27.57.jpg | phishing | 1 |
| dhlloginangelart32.29.jpg | phishing | 0,99993 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,998679 |
| ebaylogininkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 1 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9222138 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,99998546 |
| **googlelogindrive.go97.89.jpg** | **legitimate** | **0,90092576** |
| googlelogineadlampy24.96.jpg | phishing | 0,99993026 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| **googleloginsites.go48.39.jpg** | **legitimate** | **0,9519274** |
| linkedinloginauricioy76.35.jpg | phishing | 0,9172398 |
| linkedinlogindvtejas.76.89.jpg | phishing | 1 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,89216197 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,99996436 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |

| | | |
|---|---|---|
| microsoftloginakakakak47.63.jpg | phishing | 0,8903117 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,9999993 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,99998343 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,9853044 |
| microsoftloginrched-el31.95.jpg | phishing | 0,9993942 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 0,9992986 |
| netflixloginrubibags49.6.jpg | phishing | 0,934081 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 1 |
| paypalloginaypal.co74.93.jpg | phishing | 1 |
| paypalloginppuseral91.68.jpg | phishing | 1 |
| paypalloginshadetre83.51.jpg | phishing | 1 |
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 1 |
| yahoologinastfoodg14.91.jpg | phishing | 0,99998784 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 0,99999964 |

### E.1.2 MobileNet με Ρυθμό Εκμάθησης 0.001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) | 32 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 96.09% |
| Απώλεια Επικύρωσης | 0.4718405604362488 |



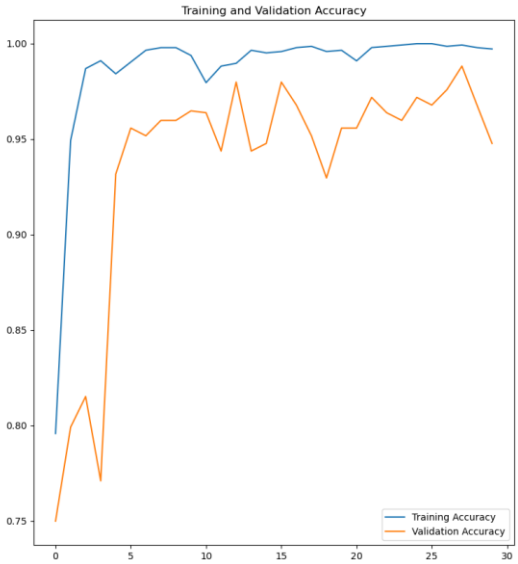

Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zorder, στο εκπαιδευόμενο μοντέλο MobileNet με lr 0,001.

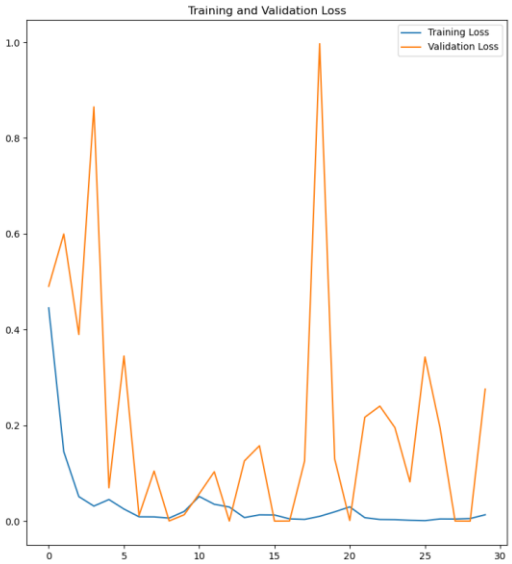
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,99999833 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,999997 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,9999275 |
| adobeloginodimedia82.37.jpg | phishing | 0,9999963 |
| adobeloginwww.crea16.55.jpg | phishing | 0,99560875 |
| alibabalogindrevent.65.04.jpg | phishing | 1 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9999999 |
| alibabaloginww.diver49.92.jpg | phishing | 0,9999999 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,9999858 |
| amazonloginbestfitt19.01.jpg | phishing | 0,9999999 |
| amazonloginchinchil67.95.jpg | phishing | 0,9998907 |
| amazonloginconntect20.19.jpg | phishing | 0,9998642 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,99999905 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,97459954** |
| at&tloginhilltopc34.37.jpg | phishing | 0,9999995 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9999962 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,9951816 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,99999976 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,976061 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,9999993 |
| chaseloginaigonspo91.35.jpg | phishing | 0,99993896 |
| chaseloginellefont45.61.jpg | phishing | 0,9999937 |
| chaseloginotoblad.59.76.jpg | phishing | 0,9999937 |
| chaseloginowntownd30.71.jpg | phishing | 0,79703087 |
| chaselogintrack4se64.7.jpg | phishing | 0,9999895 |
| dhlloginacvedas.27.57.jpg | phishing | 0,998346 |
| dhlloginangelart32.29.jpg | phishing | 0,9999999 |
| dhlloginharmoniu69.96.jpg | phishing | 0,9999999 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhlloginogansegu00.33.jpg | phishing | 0,9998097 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,99999833 |
| ebayloginkverif23.96.jpg | phishing | 0,9999999 |
| ebayloginpaleypri94.81.jpg | phishing | 0,97274673 |
| ebayloginrlsverif45.47.jpg | phishing | 0,9999999 |
| ebayloginthongtin17.67.jpg | phishing | 0,9999999 |
| facebookloginadm.righ42.51.jpg | phishing | 0,9999999 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9997297 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 0,9995987 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,99982893 |
| googlelogindrive.go97.89.jpg | phishing | 0,999992 |
| googlelogineadlampy24.96.jpg | phishing | 0,98439676 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 0,9999999 |

| | | |
|---|---|---|
| googleloginsites.go48.39.jpg | phishing | 0,9822818 |
| **linkedinloginauricioy76.35.jpg** | **legitimate** | **0,8215731** |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,9597949 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,999366 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,9999994 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 0,9993993 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,97857416 |
| microsoftloginfolhadac33.31.jpg | phishing | 1 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,9999862 |
| microsoftloginrched-el31.95.jpg | phishing | 0,99989927 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 0,99999964 |
| netflixloginlix-flix27.43.jpg | phishing | 0,999951 |
| netflixloginrubibags49.6.jpg | phishing | 0,9999958 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 0,9999999 |
| paypalloginaypal.co74.93.jpg | phishing | 1 |
| paypalloginppuseral91.68.jpg | phishing | 0,99990165 |
| paypalloginshadetre83.51.jpg | phishing | 1 |
| paypalloginarooqmob87.19 | phishing | 0,9999999 |
| yahoologinaesencia79.26.jpg | phishing | 0,99999785 |
| yahoologinastfoodg14.91.jpg | phishing | 0,99950993 |
| yahoologinodegascr65.94.jpg | phishing | 0,99999964 |
| yahoologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 0,9999378 |

### Ε.1.3 MobileNet με Ρυθμό Εκμάθησης 0.001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.0001 |
| Μέγεθος Παρτίδας (Batch_size) | 32 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 94.92% |
| Απώλεια Επικύρωσης | 0.012627439573407173 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zorder, στο εκπαιδευόμενο μοντέλο MobileNet με lr 0,0001.

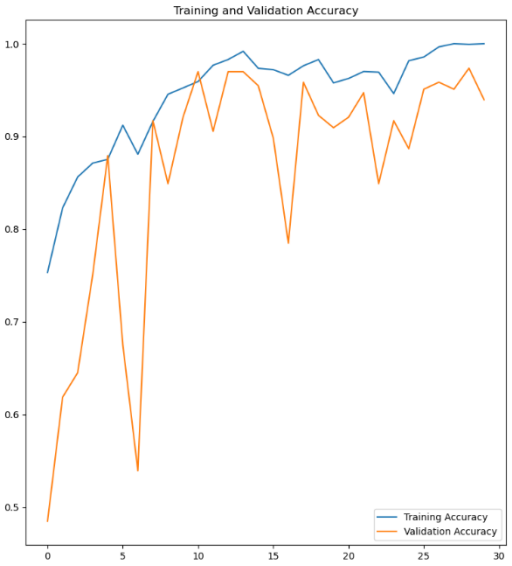
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 1 |
| adobeloginhuncoppe56.16.jpg | phishing | 1 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9999833 |
| alibabalogindrevent.65.04.jpg | phishing | 1 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 1 |
| alibabaloginww.diver49.92.jpg | phishing | 1 |
| alibabaloginwww.tale61.02.jpg | phishing | 1 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 1 |
| amazonloginconntect20.19.jpg | phishing | 1 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,97722113** |
| at&tloginhilltopc34.37.jpg | phishing | 0,9999993 |
| at&tloginkletsbuy99.14.jpg | phishing | 1 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 1 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 1 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,99999976 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |

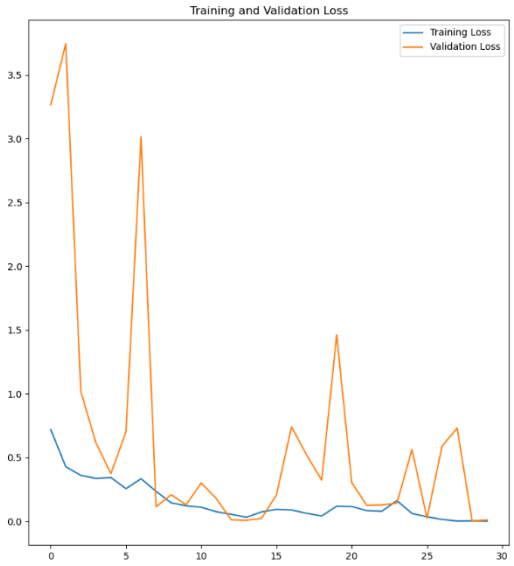
| | | |
|---|---|---|
| chaseloginowntownd30.71.jpg | phishing | 0,9999999 |
| chaselogintrack4se64.7.jpg | phishing | 1 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9999999 |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 1 |
| ebayloginkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 0,9844008 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9999653 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 1 |
| googlelogindrive.go97.89.jpg | phishing | 0,99997604 |
| googlelogineadlampy24.96.jpg | phishing | 1 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 0,9999944 |
| linkedinloginauricioy76.35.jpg | phishing | 0,9999924 |
| linkedinlogindvtejas.76.89.jpg | phishing | 1 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,9999999 |
| linkedinloginoutlookm27.79.jpg | phishing | 1 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 0,9999906 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,98748815 |
| microsoftloginfolhadac33.31.jpg | phishing | 1 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,999783 |
| microsoftloginrched-el31.95.jpg | phishing | 1 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 1 |
| netflixloginrubibags49.6.jpg | phishing | 1 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 1 |
| paypalloginaypal.co74.93.jpg | phishing | 1 |
| paypalloginppuseral91.68.jpg | phishing | 0,99999976 |
| paypalloginshadetre83.51.jpg | phishing | 1 |
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 1 |
| yahoologinastfoodg14.91.jpg | phishing | 1 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 1 |

# Ε.2 Δοκιμές MobileNet-RNN Μοντέλου και Αποτελέσματα Εκπαίδευσης

## Ε.2.1 MobileNet-RNN με Ρυθμό Εκμάθησης 0.01

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.01 |
| Μέγεθος Παρτίδας (Batch_size) | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 95.59% |
| Απώλεια Επικύρωσης | 0.00011436982458690181 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zorder, στο εκπαιδευόμενο μοντέλο MobileNet-RNN με lr 0,01.

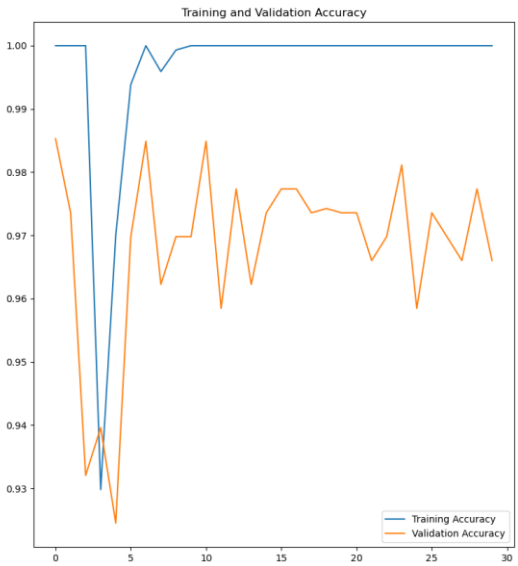
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,9999999 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9996276 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,9999149 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 0,99999964 |
| alibabalogindrevent.65.04.jpg | phishing | 0,99850094 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,99999845 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9999645 |
| alibabaloginww.diver49.92.jpg | phishing | 0,9999683 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,99991596 |
| amazonloginbestfitt19.01.jpg | phishing | 0,99999917 |
| amazonloginchinchil67.95.jpg | phishing | 0,99999964 |
| amazonloginconntect20.19.jpg | phishing | 0,9999995 |

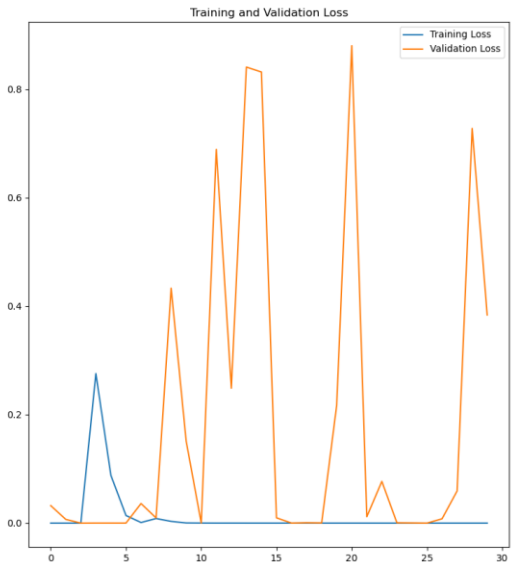
| | | |
|---|---|---|
| amazonlogindecaiofa52.62.jpg | phishing | 0,99999917 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,9999145 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,6433662** |
| at&tloginhilltopc34.37.jpg | phishing | 0,99999225 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9999963 |
| at&tloginmahdistr30.89.jpg | phishing | 0,99999976 |
| at&tloginzaroosha94.26.jpg | phishing | 0,99999774 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,99993956 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,9999994 |
| bankofamericaloginedificio77.17.jpg | phishing | 1 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,99997604 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 0,99987006 |
| chaseloginellefont45.61.jpg | phishing | 0,9999999 |
| chaseloginotoblad.59.76.jpg | phishing | 0,9999999 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,6841016** |
| chaselogintrack4se64.7.jpg | phishing | 0,9999814 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9999442 |
| dhlloginangelart32.29.jpg | phishing | 0,99999905 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 0,999995 |
| dhllogingansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,999992 |
| ebayloginkverif23.96.jpg | phishing | 0,9999999 |
| ebayloginpaleypri94.81.jpg | phishing | 0,99073374 |
| ebayloginrlsverif45.47.jpg | phishing | 0,9999999 |
| ebayloginthongtin17.67.jpg | phishing | 0,99999285 |
| facebookloginadm.righ42.51.jpg | phishing | 1 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9998386 |
| facebookloginjoingrup15.72.jpg | phishing | 0,9999981 |
| facebookloginsecurlty22.26.jpg | phishing | 0,9999392 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,999987 |
| googlelogindrive.go97.89.jpg | phishing | 0,9998399 |
| googlelogineadlampy24.96.jpg | phishing | 0,99997973 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 0,9767268 |
| linkedinloginauricioy76.35.jpg | phishing | 0,98762685 |
| **linkedinlogindvtejas.76.89.jpg** | **legitimate** | **0,8634982** |
| linkedinloginmade-in-59.37.jpg | phishing | 0,99999845 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,99998593 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 0,9974331 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,99209267 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,9999925 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,97854346 |
| microsoftloginrched-el31.95.jpg | phishing | 0,999047 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 0,99999964 |
| netflixloginrubibags49.6.jpg | phishing | 0,50597733 |
| netflixloginww.stamp24.73.jpg | phishing | 0,999974 |

| | | |
|---|---|---|
| paypalloginackyardd28.63.jpg | phishing | 0,9999999 |
| paypalloginaypal.co74.93.jpg | phishing | 0,9999976 |
| paypalloginppuseral91.68.jpg | phishing | 0,9951611 |
| paypalloginshadetre83.51.jpg | phishing | 0,99999917 |
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 1 |
| yahoologinastfoodg14.91.jpg | phishing | 0,9997162 |
| yahoologinodegascr65.94.jpg | phishing | 0,9999964 |
| yahoologintinyurl.03.54.jpg | phishing | 0,99998486 |
| yahoologinww.recov40.92 | phishing | 1 |

### E.2.2 MobileNet-RNN Μοντέλο με Ρυθμό Εκμάθησης 0.001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 98.53% |
| Απώλεια Επικύρωσης | 0.0009643440134823322 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zorder, στο εκπαιδευόμενο μοντέλο MobileNet-RNN με lr 0,001.

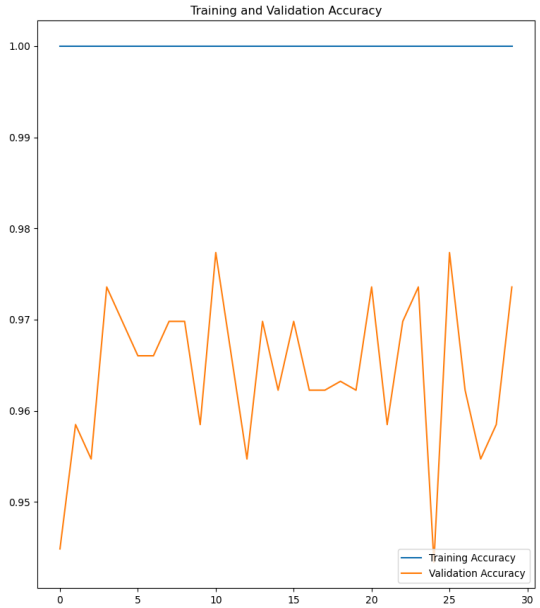
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,99999964 |
| adobelogingnoddrc.90.04.jpg | phishing | 1 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,9999933 |
| adobeloginodimedia82.37.jpg | phishing | 0,9999989 |
| adobeloginwww.crea16.55.jpg | phishing | 0,99999917 |
| alibabalogindrevent.65.04.jpg | phishing | 0,99999094 |

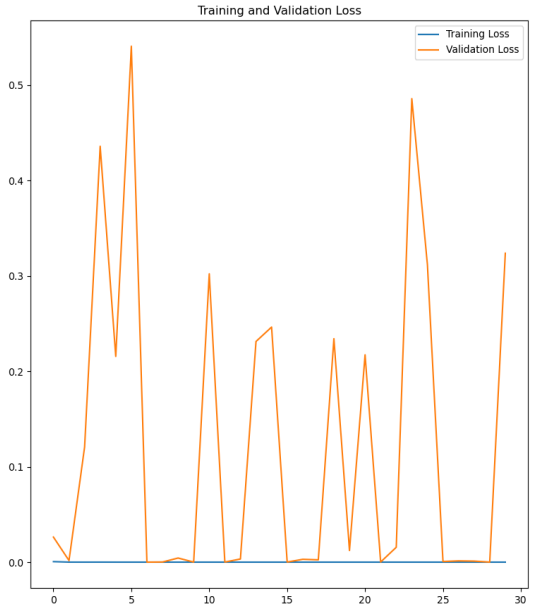
| | | |
|---|---|---|
| alibabaloginlocbien.01.64.jpg | phishing | 0,9999659 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9998128 |
| alibabaloginww.diver49.92.jpg | phishing | 0,9999795 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,9999888 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 0,9999734 |
| amazonloginconntect20.19.jpg | phishing | 1 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,9999995 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,9747507 |
| at&tloginhilltopc34.37.jpg | phishing | 0,9999988 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,99999845 |
| at&tloginmahdistr30.89.jpg | phishing | 0,99996316 |
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 1 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,99999285 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,99870634 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,99999905 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 1 |
| chaseloginaigonspo91.35.jpg | phishing | 0,99992275 |
| chaseloginellefont45.61.jpg | phishing | 0,99999356 |
| chaseloginotoblad.59.76.jpg | phishing | 0,99999356 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,8034912** |
| chaselogintrack4se64.7.jpg | phishing | 0,9999944 |
| dhlloginacvedas.27.57.jpg | phishing | 0,99628 |
| dhlloginangelart32.29.jpg | phishing | 0,99992883 |
| dhlloginharmoniu69.96.jpg | phishing | 0,9993679 |
| dhlloginhotelgra46.79.jpg | phishing | 0,9992841 |
| dhllogingansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 1 |
| ebayloginkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 0,9528847 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 0,99999964 |
| facebookloginadm.righ42.51.jpg | phishing | 0,99999917 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,999995 |
| facebookloginjoingrup15.72.jpg | phishing | 0,99999833 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,99999845 |
| **googlelogindrive.go97.89.jpg** | **legitimate** | **0,97891724** |
| googlelogineadlampy24.96.jpg | phishing | 0,9995127 |
| googleloginlbel.int84.28.jpg | phishing | 0,99998295 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 0,9991841 |
| **linkedinloginauricioy76.35.jpg** | **phishing** | **0,73675936** |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,9996989 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,9999908 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,9999964 |
| linkedinloginowwglass82.2.jpg | phishing | 0,99999464 |
| microsoftloginakakakak47.63.jpg | phishing | 1 |
| **microsoftlogindreamy-g35.49.jpg** | **legitimate** | **0,8822323** |
| microsoftloginfolhadac33.31.jpg | phishing | 0,9999995 |

| | | |
|---|---|---|
| microsoftloginnazahaco60.47.jpg | phishing | 0,99999845 |
| microsoftloginrched-el31.95.jpg | phishing | 1 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 0,99999905 |
| netflixloginrubibags49.6.jpg | phishing | 0,99998355 |
| netflixloginww.stamp24.73.jpg | phishing | 0,9987098 |
| paypalloginackyardd28.63.jpg | phishing | 0,9999995 |
| paypalloginaypal.co74.93.jpg | phishing | 0,999925 |
| paypalloginppuseral91.68.jpg | phishing | 0,9999944 |
| paypalloginshadetre83.51.jpg | phishing | 0,99999464 |
| paypalloginarooqmob87.19 | phishing | 0,9999827 |
| yahoologinaesencia79.26.jpg | phishing | 0,99999976 |
| yahoologinastfoodg14.91.jpg | phishing | 0,9999801 |
| yahoologinodegascr65.94.jpg | phishing | 0,99999976 |
| yahoologintinyurl.03.54.jpg | phishing | 0,9999994 |
| yahoologinww.recov40.92 | phishing | 0,9999993 |

### E.2.3 MobileNet-RNN Μοντέλο με Ρυθμό Εκμάθησης 0.0001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.0001 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 96.32% |
| Απώλεια Επικύρωσης | 7.599558671245177e-07 |



Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zorder, στο εκπαιδευόμενο μοντέλο MobileNet-RNN με lr 0,0001.

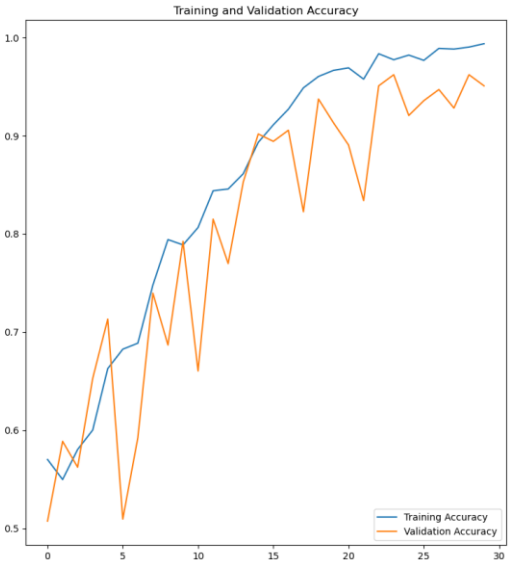
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,99999976 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,99999917 |
| adobeloginhuncoppe56.16.jpg | phishing | 1 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 1 |
| alibabalogindrevent.65.04.jpg | phishing | 1 |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 1 |
| alibabaloginww.diver49.92.jpg | phishing | 1 |
| alibabaloginwww.tale61.02.jpg | phishing | 1 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 0,9999993 |
| amazonloginconntect20.19.jpg | phishing | 1 |
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,9997055 |
| at&tloginhilltopc34.37.jpg | phishing | 1 |
| at&tloginkletsbuy99.14.jpg | phishing | 1 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,99999535 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,9999999 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,9999994 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9999999 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,9999999 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| chaseloginowntownd30.71.jpg | phishing | 0,9719549 |
| chaselogintrack4se64.7.jpg | phishing | 1 |
| dhlloginacvedas.27.57.jpg | phishing | 1 |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhlloginogansegu00.33.jpg | phishing | 0,99999964 |
| ebaylogin7426fbe061.09.jpg | phishing | 1 |
| ebaylogininkverif23.96.jpg | phishing | 0,9999964 |
| ebayloginpaleypri94.81.jpg | legitimate | 0,9481453 |
| ebayloginrlsverif45.47.jpg | phishing | 0,9999964 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 0,9862518 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9999832 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 1 |
| facebookloginxvgbtopl00.11.jpg | phishing | 1 |
| **googlelogindrive.go97.89.jpg** | **legitimate** | **0,9988034** |
| googlelogineadlampy24.96.jpg | phishing | 0,99999917 |

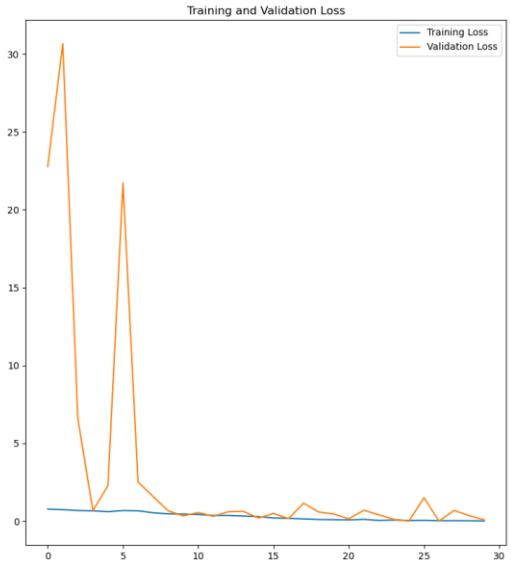
| | | |
|---|---|---|
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| **googleloginsites.go48.39.jpg** | **legitimate** | **0,9300504** |
| linkedinloginauricioy76.35.jpg | phishing | 0,9965879 |
| linkedinlogindvtejas.76.89.jpg | phishing | 1 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,99999964 |
| linkedinloginoutlookm27.79.jpg | phishing | 1 |
| linkedinloginowwglass82.2.jpg | phishing | 0,99999976 |
| microsoftloginakakakak47.63.jpg | phishing | 0,9999167 |
| **microsoftlogindreamy-g35.49.jpg** | **legitimate** | **0,9902714** |
| microsoftloginfolhadac33.31.jpg | phishing | 0,9999999 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,99999917 |
| microsoftloginrched-el31.95.jpg | phishing | 0,99999845 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 0,9999987 |
| netflixloginlix-flix27.43.jpg | phishing | 1 |
| netflixloginrubibags49.6.jpg | phishing | 0,999124 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |
| paypalloginackyardd28.63.jpg | phishing | 0,9999989 |
| paypalloginaypal.co74.93.jpg | phishing | 0,99999106 |
| paypalloginppuseral91.68.jpg | phishing | 0,99999475 |
| paypalloginshadetre83.51.jpg | phishing | 0,9999995 |
| paypalloginarooqmob87.19 | phishing | 0,9999858 |
| yahoologinaesencia79.26.jpg | phishing | 1 |
| yahoologinastfoodg14.91.jpg | phishing | 1 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 1 |

# Ε.3 Δοκιμές Xception-RNN Μοντέλου και Αποτελέσματα Εκπαίδευσης

## Ε.3.1 Xception-RNN Μοντέλο με Ρυθμό Εκμάθησης 0.01

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.01 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 94.49% |
| Απώλεια Επικύρωσης | 1.3032159805297852 |



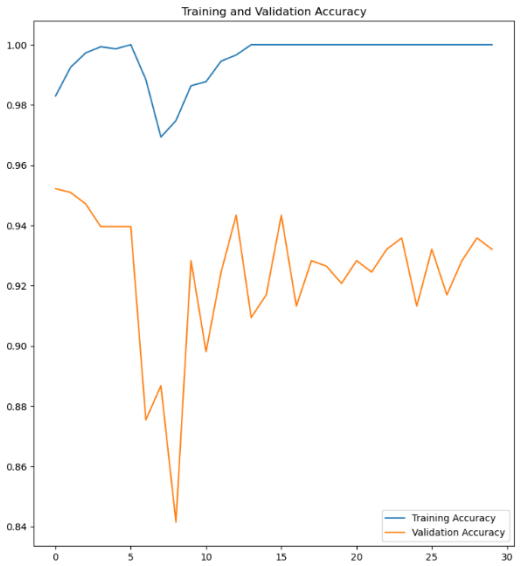

Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zorder, στο εκπαιδευόμενο μοντέλο Xception-RNN με lr 0,01.

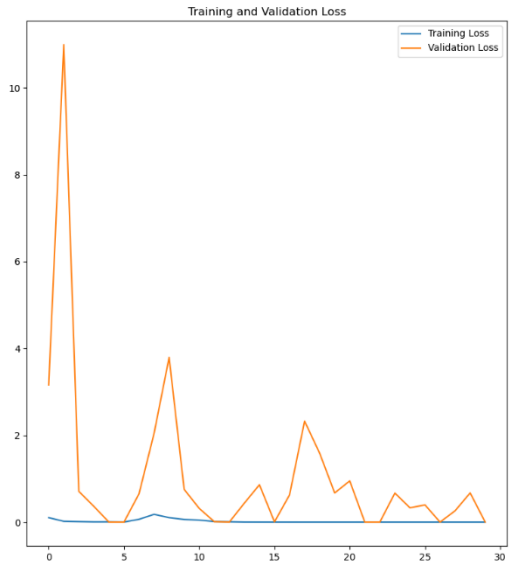
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,8823796 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,99963737 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 0,9997967 |
| alibabalogindrevent.65.04.jpg | phishing | 0,9998859 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,9999794 |
| alibabaloginpineheal56.15.jpg | phishing | 0,99838555 |
| alibabaloginww.diver49.92.jpg | phishing | 0,99982506 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,99822885 |
| amazonloginbestfitt19.01.jpg | phishing | 0,999899 |
| amazonloginchinchil67.95.jpg | phishing | 0,9953004 |
| amazonloginconntect20.19.jpg | phishing | 0,9999447 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,9999075 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,9985312 |
| **at&tlogindocs.goo12.02.jpg** | legitimate | 0,99939823 |
| at&tloginhilltopc34.37.jpg | phishing | 0,97965175 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,93260175 |
| at&tloginmahdistr30.89.jpg | phishing | 0,99999976 |
| at&tloginzaroosha94.26.jpg | phishing | 0,8602572 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,99986255 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,9999999 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,99054503 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,99996793 |
| chaseloginaigonspo91.35.jpg | phishing | 0,9965579 |
| chaseloginellefont45.61.jpg | phishing | 0,9975425 |
| chaseloginotoblad.59.76.jpg | phishing | 0,9975425 |

| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,98416835** |
|---|---|---|
| chaselogintrack4se64.7.jpg | phishing | 0,9999331 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9999542 |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 0,99999905 |
| dhlloginhotelgra46.79.jpg | phishing | 0,9998072 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,99993896 |
| ebayloginkverif23.96.jpg | phishing | 0,9999988 |
| ebayloginpaleypri94.81.jpg | phishing | 0,9780442 |
| ebayloginrlsverif45.47.jpg | phishing | 0,9999988 |
| ebayloginthongtin17.67.jpg | phishing | 0,999928 |
| facebookloginadm.righ42.51.jpg | phishing | 0,9999957 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,98983055 |
| facebookloginjoingrup15.72.jpg | phishing | 0,999627 |
| facebookloginsecurlty22.26.jpg | phishing | 0,9944718 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,9999144 |
| googlelogindrive.go97.89.jpg | phishing | 0,9174487 |
| googlelogineadlampy24.96.jpg | phishing | 0,99641114 |
| googleloginlbel.int84.28.jpg | phishing | 0,99999905 |
| googleloginluidacco20.43.jpg | phishing | 0,99999976 |
| googleloginsites.go48.39.jpg | phishing | 0,94053227 |
| linkedinloginauricioy76.35.jpg | phishing | 0,9997732 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,99692243 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,99985325 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,99989915 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| microsoftloginakakakak47.63.jpg | phishing | 0,99664354 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,99985325 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,99940383 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,93917406 |
| microsoftloginrched-el31.95.jpg | phishing | 0,9998907 |
| netflixloginahorolln04.85.jpg | phishing | 0,9999945 |
| netflixloginarketing01.44.jpg | phishing | 0,9992212 |
| netflixloginlix-flix27.43.jpg | phishing | 0,9989324 |
| **netflixloginrubibags49.6.jpg** | **legitimate** | **0,7674277** |
| netflixloginww.stamp24.73.jpg | phishing | 0,99998176 |
| paypalloginackyardd28.63.jpg | phishing | 0,9998965 |
| paypalloginaypal.co74.93.jpg | phishing | 0,9993149 |
| paypalloginppuseral91.68.jpg | phishing | 0,98016894 |
| paypalloginshadetre83.51.jpg | phishing | 0,99999976 |
| paypalloginarooqmob87.19 | phishing | 0,9999949 |
| yahoologinaesencia79.26.jpg | phishing | 0,99999833 |
| yahoologinastfoodg14.91.jpg | phishing | 0,9935196 |
| yahoologinodegascr65.94.jpg | phishing | 0,99999964 |
| **yahoologintinyurl.03.54.jpg** | **legitimate** | **0,8165745** |
| yahoologinww.recov40.92 | phishing | 0,9984434 |

### E.3.2 Xception-RNN Μοντέλο με Ρυθμό Εκμάθησης 0.001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 92.65% |
| Απώλεια Επικύρωσης | 1.7228362560272217 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zorder, στο εκπαιδευόμενο μοντέλο Xception-RNN με lr 0,001.

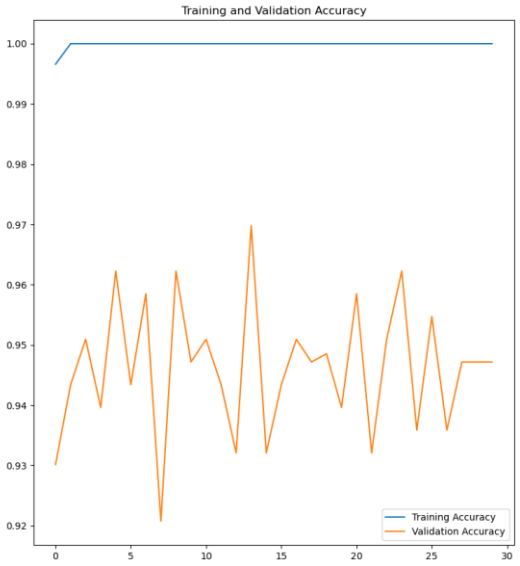
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,99999845 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,9999989 |
| adobeloginodimedia82.37.jpg | phishing | 0,9999999 |
| adobeloginwww.crea16.55.jpg | phishing | 0,99988866 |
| alibabalogindrevent.65.04.jpg | phishing | 0,9995881 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,99999917 |
| alibabaloginpineheal56.15.jpg | phishing | 0,9999639 |
| alibabaloginww.diver49.92.jpg | phishing | 0,9999875 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,999979 |
| amazonloginbestfitt19.01.jpg | phishing | 0,99998367 |
| amazonloginchinchil67.95.jpg | phishing | 0,99999416 |
| amazonloginconntect20.19.jpg | phishing | 0,9999969 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,99998367 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,99997985 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,9999964 |
| at&tloginhilltopc34.37.jpg | phishing | 0,99999285 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9999068 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |

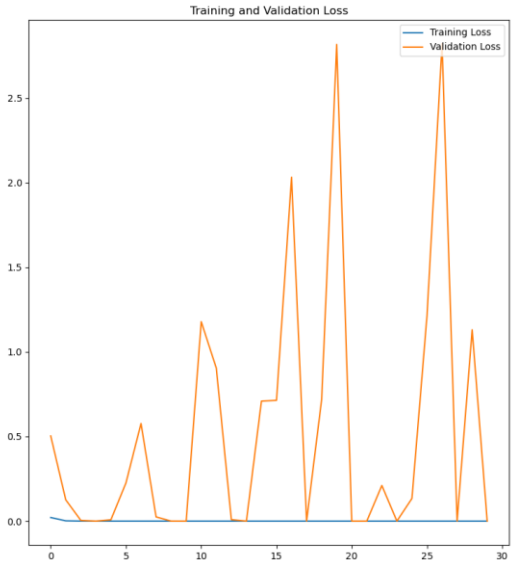
| | | |
|---|---|---|
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,9999825 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,9999993 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,9999845 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,9999987 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,99992096 |
| chaseloginaigonspo91.35.jpg | phishing | 0,99999535 |
| chaseloginellefont45.61.jpg | phishing | 0,9999962 |
| chaseloginotoblad.59.76.jpg | phishing | 0,9999962 |
| **chaseloginowntownd30.71.jpg** | **legitimate** | **0,81274575** |
| chaselogintrack4se64.7.jpg | phishing | 0,9999968 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9999969 |
| dhlloginangelart32.29.jpg | phishing | 0,9999949 |
| dhlloginharmoniu69.96.jpg | phishing | 0,9999964 |
| dhlloginhotelgra46.79.jpg | phishing | 0,9999999 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,9999943 |
| ebayloginkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 0,9999188 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 0,99999535 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,99999726 |
| facebookloginjoingrup15.72.jpg | phishing | 0,99999046 |
| facebookloginsecurlty22.26.jpg | phishing | 0,9999949 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,99979633 |
| googlelogindrive.go97.89.jpg | phishing | 0,92728895 |
| googlelogineadlampy24.96.jpg | phishing | 0,9999809 |
| googleloginlbel.int84.28.jpg | phishing | 0,9999666 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 0,99995756 |
| **linkedinloginauricioy76.35.jpg** | **legitimate** | **0,9999851** |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,99998236 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,99998736 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,99999094 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| **microsoftloginakakakak47.63.jpg** | **legitimate** | **0,99994326** |
| **microsoftlogindreamy-g35.49.jpg** | **legitimate** | **0,99999356** |
| microsoftloginfolhadac33.31.jpg | phishing | 0,99994946 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,99963856 |
| microsoftloginrched-el31.95.jpg | phishing | 0,9999378 |
| netflixloginahorolln04.85.jpg | phishing | 0,9999938 |
| netflixloginarketing01.44.jpg | phishing | 0,99998975 |
| netflixloginlix-flix27.43.jpg | phishing | 0,9999956 |
| **netflixloginrubibags49.6.jpg** | **legitimate** | **0,94844764** |
| netflixloginww.stamp24.73.jpg | phishing | 0,9999962 |
| paypalloginackyardd28.63.jpg | phishing | 0,9999857 |
| paypalloginaypal.co74.93.jpg | phishing | 0,999995 |
| paypalloginppuseral91.68.jpg | phishing | 0,9999511 |
| paypalloginshadetre83.51.jpg | phishing | 0,9999939 |
| paypalloginarooqmob87.19 | phishing | 0,9999881 |
| yahoologinaesencia79.26.jpg | phishing | 1 |

| | | |
|---|---|---|
| yahoologinastfoodg14.91.jpg | phishing | 0,9999937 |
| yahoologinodegascr65.94.jpg | phishing | 0,9999988 |
| **yahoologintinyurl.03.54.jpg** | **legitimate** | **0,9998246** |
| yahoologinww.recov40.92 | phishing | 0,9999945 |

### E.3.3 Xception-RNN Μοντέλο με Ρυθμό Εκμάθησης 0.0001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.0001 |
| Μέγεθος Παρτίδας (Batch_size) 1ης Φάσης Εκπαίδευσης | 32 |
| Μέγεθος Παρτίδας (Batch_size) 2ης Φάσης Εκπαίδευσης | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 94.49% |
| Απώλεια Επικύρωσης | 0.05623584985733032 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zorder, στο εκπαιδευόμενο μοντέλο Xception-RNN με lr 0,0001.

| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 1 |
| adobelogingnoddrc.90.04.jpg | phishing | 1 |
| adobeloginhuncoppe56.16.jpg | phishing | 1 |
| adobeloginodimedia82.37.jpg | phishing | 1 |
| adobeloginwww.crea16.55.jpg | phishing | 1 |
| **alibabalogindrevent.65.04.jpg** | **legitimate** | **0,99442106** |
| alibabaloginlocbien.01.64.jpg | phishing | 1 |
| alibabaloginpineheal56.15.jpg | phishing | 1 |
| alibabaloginww.diver49.92.jpg | phishing | 1 |
| alibabaloginwww.tale61.02.jpg | phishing | 1 |
| amazonloginbestfitt19.01.jpg | phishing | 1 |
| amazonloginchinchil67.95.jpg | phishing | 1 |
| amazonloginconntect20.19.jpg | phishing | 1 |

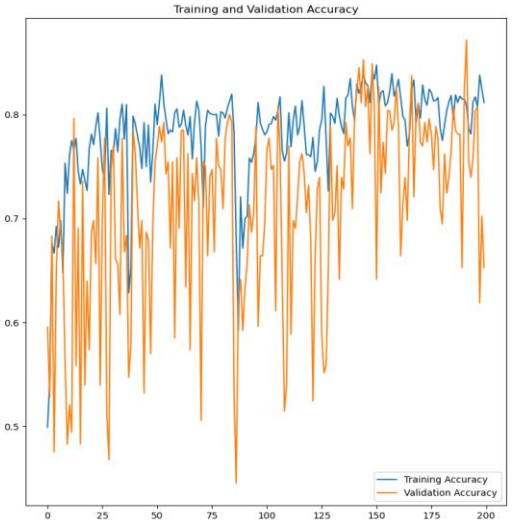
| | | |
|---|---|---|
| amazonlogindecaiofa52.62.jpg | phishing | 1 |
| amazonloginizbiz.te71.9.jpg | phishing | 1 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,9999982 |
| at&tloginhilltopc34.37.jpg | phishing | 0,99999285 |
| at&tloginkletsbuy99.14.jpg | phishing | 1 |
| at&tloginmahdistr30.89.jpg | phishing | 1 |
| at&tloginzaroosha94.26.jpg | phishing | 1 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 1 |
| bankofamericaloginecurity.26.59.jpg | phishing | 1 |
| bankofamericaloginedificio77.17.jpg | phishing | 1 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 1 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,99999964 |
| chaseloginaigonspo91.35.jpg | phishing | 1 |
| chaseloginellefont45.61.jpg | phishing | 1 |
| chaseloginotoblad.59.76.jpg | phishing | 1 |
| chaseloginowntownd30.71.jpg | phishing | 0,9911136 |
| chaselogintrack4se64.7.jpg | phishing | 1 |
| dhlloginacvedas.27.57.jpg | phishing | 1 |
| dhlloginangelart32.29.jpg | phishing | 1 |
| dhlloginharmoniu69.96.jpg | phishing | 1 |
| dhlloginhotelgra46.79.jpg | phishing | 1 |
| dhlloginogansegu00.33.jpg | phishing | 1 |
| ebaylogin7426fbe061.09.jpg | phishing | 1 |
| ebayloginkverif23.96.jpg | phishing | 1 |
| ebayloginpaleypri94.81.jpg | phishing | 1 |
| ebayloginrlsverif45.47.jpg | phishing | 1 |
| ebayloginthongtin17.67.jpg | phishing | 1 |
| facebookloginadm.righ42.51.jpg | phishing | 0,99358493 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,99996686 |
| facebookloginjoingrup15.72.jpg | phishing | 1 |
| facebookloginsecurlty22.26.jpg | phishing | 0,99999976 |
| facebookloginxvgbtopl00.11.jpg | phishing | 1 |
| **googlelogindrive.go97.89.jpg** | **legitimate** | **1** |
| googlelogineadlampy24.96.jpg | phishing | 1 |
| googleloginlbel.int84.28.jpg | phishing | 1 |
| googleloginluidacco20.43.jpg | phishing | 1 |
| googleloginsites.go48.39.jpg | phishing | 1 |
| **linkedinloginauricioy76.35.jpg** | **legitimate** | **0,99917054** |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,9997193 |
| linkedinloginmade-in-59.37.jpg | phishing | 1 |
| linkedinloginoutlookm27.79.jpg | phishing | 1 |
| linkedinloginowwglass82.2.jpg | phishing | 1 |
| **microsoftloginakakakak47.63.jpg** | **legitimate** | **0,9994079** |
| microsoftlogindreamy-g35.49.jpg | phishing | 1 |
| microsoftloginfolhadac33.31.jpg | phishing | 1 |
| microsoftloginnazahaco60.47.jpg | phishing | 1 |
| microsoftloginrched-el31.95.jpg | phishing | 0,99999976 |
| netflixloginahorolln04.85.jpg | phishing | 1 |
| netflixloginarketing01.44.jpg | phishing | 1 |
| netflixloginlix-flix27.43.jpg | phishing | 1 |
| netflixloginrubibags49.6.jpg | phishing | 0,9986381 |
| netflixloginww.stamp24.73.jpg | phishing | 1 |

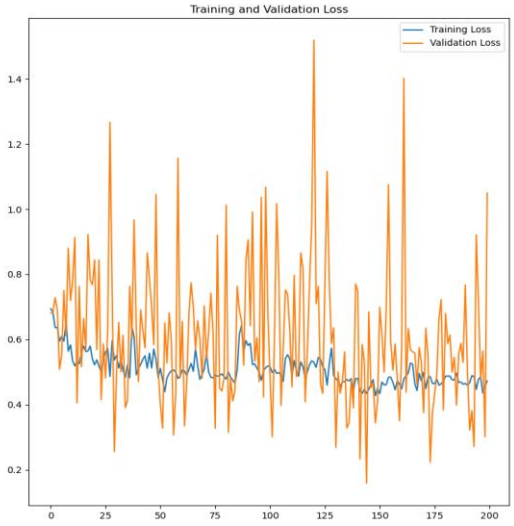
| | | |
|---|---|---|
| paypalloginackyardd28.63.jpg | phishing | 1 |
| paypalloginaypal.co74.93.jpg | phishing | 0,9999968 |
| paypalloginppuseral91.68.jpg | phishing | 1 |
| paypalloginshadetre83.51.jpg | phishing | 1 |
| paypalloginarooqmob87.19 | phishing | 1 |
| yahoologinaesencia79.26.jpg | phishing | 1 |
| yahoologinastfoodg14.91.jpg | phishing | 1 |
| yahoologinodegascr65.94.jpg | phishing | 1 |
| yahoologintinyurl.03.54.jpg | phishing | 1 |
| yahoologinww.recov40.92 | phishing | 1 |

# Ε.4 Δοκιμές Custom-RNN Μοντέλου και Αποτελέσματα Εκπαίδευσης

## Ε.4.1 Custom CNN Μοντέλο με Ρυθμό Εκμάθησης 0.01

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.01 |
| Μέγεθος Παρτίδας (Batch_size) | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 66.18% |
| Απώλεια Επικύρωσης | 0.4922325909137726 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zorder, στο εκπαιδευόμενο μοντέλο Custom_CNN με lr 0,01.

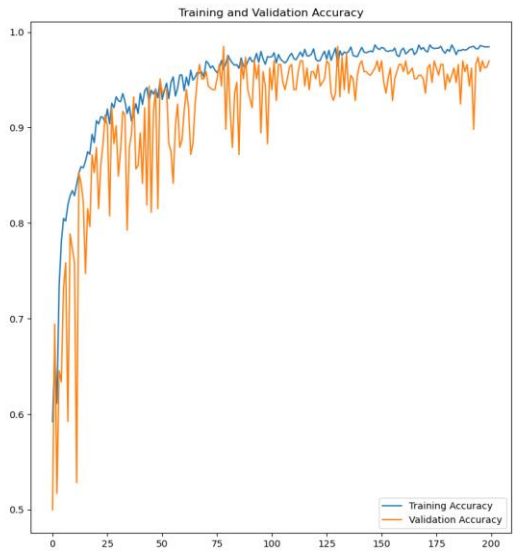
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,8817795 |
| **adobelogingnoddrc.90.04.jpg** | **legitimate** | **0,72448546** |
| **adobeloginhuncoppe56.16.jpg** | **legitimate** | **0,83643186** |

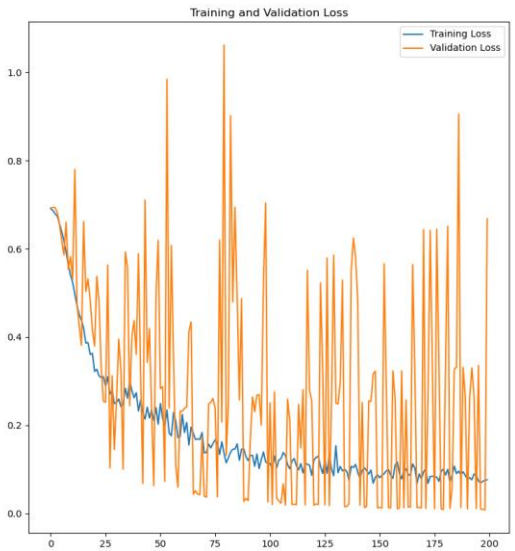
| | | |
|---|---|---|
| adobeloginodimedia82.37.jpg | phishing | 0,8817795 |
| adobeloginwww.crea16.55.jpg | phishing | 0,8817795 |
| alibabalogindrevent.65.04.jpg | phishing | 0,8817795 |
| alibabaloginlocbien.01.64.jpg | phishing | 0,8817795 |
| alibabaloginpineheal56.15.jpg | phishing | 0,8494249 |
| alibabaloginww.diver49.92.jpg | phishing | 0,82466745 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,82466745 |
| amazonloginbestfitt19.01.jpg | phishing | 0,8817795 |
| amazonloginchinchil67.95.jpg | phishing | 0,8817795 |
| amazonloginconntect20.19.jpg | phishing | 0,8494249 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,8817795 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,8817795 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,83643186** |
| at&tloginhilltopc34.37.jpg | phishing | 0,8817795 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,8817795 |
| at&tloginmahdistr30.89.jpg | phishing | 0,8817795 |
| at&tloginzaroosha94.26.jpg | phishing | 0,8817795 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,8817795 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,8817795 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,8817795 |
| **bankofamericaloginkrjpl.co60.86.jpg** | **legitimate** | **0,5885979** |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,8817795 |
| chaseloginaigonspo91.35.jpg | phishing | 0,8817795 |
| chaseloginellefont45.61.jpg | phishing | 0,8817795 |
| chaseloginotoblad.59.76.jpg | phishing | 0,8817795 |
| chaseloginowntownd30.71.jpg | phishing | 0,8246439 |
| chaselogintrack4se64.7.jpg | phishing | 0,8817795 |
| dhlloginacvedas.27.57.jpg | phishing | 0,8817795 |
| dhlloginangelart32.29.jpg | phishing | 0,8817795 |
| dhlloginharmoniu69.96.jpg | phishing | 0,8817795 |
| dhlloginhotelgra46.79.jpg | phishing | 0,8817795 |
| dhlloginogansegu00.33.jpg | phishing | 0,8817795 |
| **ebaylogin7426fbe061.09.jpg** | **legitimate** | **0,83643186** |
| ebaylogininkverif23.96.jpg | phishing | 0,8817795 |
| **ebayloginpaleypri94.81.jpg** | **legitimate** | **0,83643186** |
| ebayloginrlsverif45.47.jpg | phishing | 0,8817795 |
| ebayloginthongtin17.67.jpg | phishing | 0,8817795 |
| facebookloginadm.righ42.51.jpg | phishing | 0,8817795 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,8817795 |
| facebookloginjoingrup15.72.jpg | phishing | 0,8817795 |
| facebookloginsecurlty22.26.jpg | phishing | 0,8817795 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,8817795 |
| googlelogindrive.go97.89.jpg | phishing | 0,8817795 |
| **googlelogineadlampy24.96.jpg** | **legitimate** | **0,83643186** |
| googleloginlbel.int84.28.jpg | phishing | 0,8817795 |
| googleloginluidacco20.43.jpg | phishing | 0,8817795 |
| googleloginsites.go48.39.jpg | phishing | 0,82466745 |
| linkedinloginauricioy76.35.jpg | phishing | 0,8817795 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,8817795 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,8157746 |
| **linkedinloginoutlookm27.79.jpg** | **legitimate** | **0,5885979** |
| linkedinloginowwglass82.2.jpg | phishing | 0,8817795 |

| | | |
|---|---|---|
| microsoftloginakakakak47.63.jpg | phishing | 0,8817795 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,8817795 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,8817795 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,8817795 |
| microsoftloginrched-el31.95.jpg | phishing | 0,8817795 |
| netflixloginahorolln04.85.jpg | phishing | 0,8817795 |
| netflixloginarketing01.44.jpg | phishing | 0,8817795 |
| netflixloginlix-flix27.43.jpg | phishing | 0,8494249 |
| netflixloginrubibags49.6.jpg | phishing | 0,8817795 |
| netflixloginww.stamp24.73.jpg | phishing | 0,8817795 |
| paypalloginackyardd28.63.jpg | phishing | 0,8817795 |
| paypalloginaypal.co74.93.jpg | phishing | 0,8817795 |
| paypalloginppuseral91.68.jpg | phishing | 0,8817795 |
| paypalloginshadetre83.51.jpg | phishing | 0,8817795 |
| paypalloginarooqmob87.19 | phishing | 0,8817795 |
| yahoologinaesencia79.26.jpg | phishing | 0,8817795 |
| **yahoologinastfoodg14.91.jpg** | **legitimate** | **0,83643186** |
| yahoologinodegascr65.94.jpg | phishing | 0,8817795 |
| yahologintinyurl.03.54.jpg | phishing | 0,8817795 |
| **yahoologinww.recov40.92** | **legitimate** | **0,83643186** |

### E.4.2 Custom CNN Μοντέλο με Ρυθμό Εκμάθησης 0.001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 97.06% |
| Απώλεια Επικύρωσης | 0.010514810681343079 |



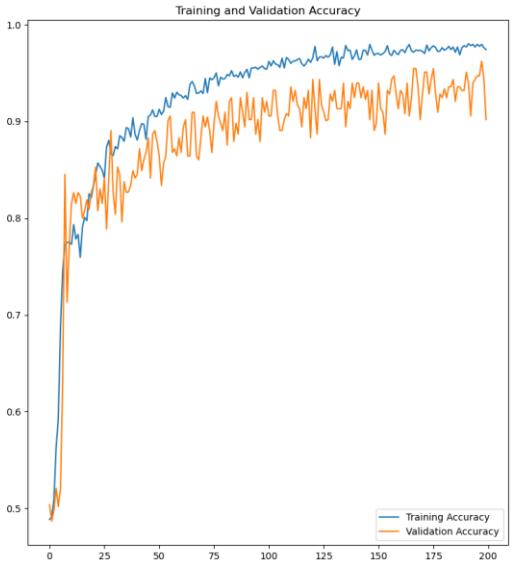
Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zorder, στο εκπαιδευόμενο μοντέλο Custom_CNN με lr 0,001.

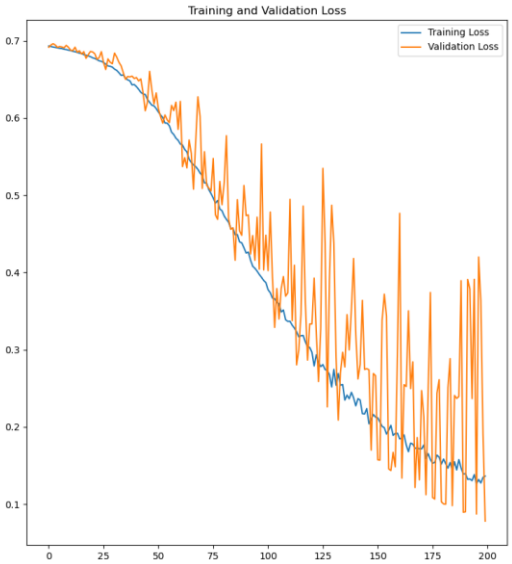
| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,96295375 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9629536 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,94860214 |
| **adobeloginodimedia82.37.jpg** | **legitimate** | **0,87459975** |
| adobeloginwww.crea16.55.jpg | phishing | 0,9629533 |
| **alibabalogindrevent.65.04.jpg** | **legitimate** | **0,97112906** |
| alibabaloginlocbien.01.64.jpg | phishing | 0,96295375 |
| **alibabaloginpineheal56.15.jpg** | **legitimate** | **0,9711322** |
| alibabaloginww.diver49.92.jpg | phishing | 0,96253985 |
| alibabaloginwww.tale61.02.jpg | phishing | 0,9629438 |
| amazonloginbestfitt19.01.jpg | phishing | 0,96294415 |
| amazonloginchinchil67.95.jpg | phishing | 0,9629536 |
| amazonloginconntect20.19.jpg | phishing | 0,96295375 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,96294403 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,95968014 |
| at&tlogindocs.goo12.02.jpg | phishing | 0,96264136 |
| at&tloginhilltopc34.37.jpg | phishing | 0,96295375 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,9629536 |
| at&tloginmahdistr30.89.jpg | phishing | 0,96295375 |
| at&tloginzaroosha94.26.jpg | phishing | 0,96295375 |
| bankofamericalogin5.188.3665.04.jpg | phishing | 0,95752823 |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,95957804 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,9629536 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,82260644 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,96295375 |
| chaseloginaigonspo91.35.jpg | phishing | 0,9629444 |
| chaseloginellefont45.61.jpg | phishing | 0,9629536 |
| chaseloginotoblad.59.76.jpg | phishing | 0,9629536 |
| chaseloginowntownd30.71.jpg | phishing | 0,9629404 |
| chaselogintrack4se64.7.jpg | phishing | 0,96295357 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9586775 |
| dhlloginangelart32.29.jpg | phishing | 0,96215254 |
| dhlloginharmoniu69.96.jpg | phishing | 0,96295375 |
| dhlloginhotelgra46.79.jpg | phishing | 0,96295375 |
| dhlloginogansegu00.33.jpg | phishing | 0,93195885 |
| ebaylogin7426fbe061.09.jpg | phishing | 0,9629536 |
| ebayloginkverif23.96.jpg | phishing | 0,96295375 |
| ebayloginpaleypri94.81.jpg | phishing | 0,9620804 |
| ebayloginrlsverif45.47.jpg | phishing | 0,96295375 |
| ebayloginthongtin17.67.jpg | phishing | 0,96295375 |
| facebookloginadm.righ42.51.jpg | phishing | 0,9629536 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,9629502 |
| facebookloginjoingrup15.72.jpg | phishing | 0,9629536 |
| facebookloginsecurlty22.26.jpg | phishing | 0,9629061 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,9627581 |
| **googlelogindrive.go97.89.jpg** | **legitimate** | **0,9678349** |
| **googlelogineadlampy24.96.jpg** | **legitimate** | **0,9251515** |

| | | |
|---|---|---|
| googleloginlbel.int84.28.jpg | phishing | 0,96295375 |
| googleloginluidacco20.43.jpg | phishing | 0,96295375 |
| **googleloginsites.go48.39.jpg** | **legitimate** | **0,53041804** |
| linkedinloginauricioy76.35.jpg | phishing | 0,96295345 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,96295357 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,9629288 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,96162105 |
| linkedinloginowwglass82.2.jpg | phishing | 0,96295375 |
| microsoftloginakakakak47.63.jpg | phishing | 0,96295255 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,96295375 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,5986574 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,962952 |
| microsoftloginrched-el31.95.jpg | phishing | 0,93411595 |
| netflixloginahorolln04.85.jpg | phishing | 0,96295375 |
| netflixloginarketing01.44.jpg | phishing | 0,9629536 |
| netflixloginlix-flix27.43.jpg | phishing | 0,96295375 |
| netflixloginrubibags49.6.jpg | phishing | 0,96295375 |
| netflixloginww.stamp24.73.jpg | phishing | 0,96295375 |
| paypalloginackyardd28.63.jpg | phishing | 0,96295375 |
| paypalloginaypal.co74.93.jpg | phishing | 0,96295357 |
| **paypalloginppuseral91.68.jpg** | **legitimate** | **0,9711149** |
| paypalloginshadetre83.51.jpg | phishing | 0,96295375 |
| paypalloginarooqmob87.19 | phishing | 0,9629536 |
| yahoologinaesencia79.26.jpg | phishing | 0,9626784 |
| **yahoologinastfoodg14.91.jpg** | **legitimate** | **0,70978945** |
| yahoologinodegascr65.94.jpg | phishing | 0,96295077 |
| yahoologintinyurl.03.54.jpg | phishing | 0,96295375 |
| yahoologinww.recov40.92 | phishing | 0,96295375 |

### Ε.4.3 Custom CNN Μοντέλο με Ρυθμό Εκμάθησης 0.0001

| | |
|---|---|
| Ρυθμός Εκμάθησης lr | 0.001 |
| Μέγεθος Παρτίδας (Batch_size) | 16 |
| Εποχές | 30 |
| Ακρίβεια Επικύρωσης | 89.71% |
| Απώλεια Επικύρωσης | 0.4946260452270508 |




Κατωτέρω παρουσιάζονται αναλυτικά αποτελέσματα του σετ δοκιμών με εικόνες καμπύλης Zorder, στο εκπαιδευόμενο μοντέλο Custom_CNN με lr 0,0001.

| Όνομα Εικόνας | Phishing /Legitimate | Πιθανότητα |
|---|---|---|
| adobelogineadmenw.26.25.jpg | phishing | 0,919926 |
| adobelogingnoddrc.90.04.jpg | phishing | 0,9199284 |
| adobeloginhuncoppe56.16.jpg | phishing | 0,91991657 |
| **adobeloginodimedia82.37.jpg** | **legitimate** | **0,92417765** |
| adobeloginwww.crea16.55.jpg | phishing | 0,91906506 |
| alibabalogindrevent.65.04.jpg | phishing | 0,91987723 |
| **alibabaloginlocbien.01.64.jpg** | **phishing** | **0,9199282** |
| **alibabaloginpineheal56.15.jpg** | **legitimate** | **0,9205428** |
| alibabaloginww.diver49.92.jpg | phishing | 0,8432151 |
| alibabaloginwww.tale61.02.jpg | legitimate | 0,7477353 |
| amazonloginbestfitt19.01.jpg | phishing | 0,9199184 |
| amazonloginchinchil67.95.jpg | phishing | 0,91990405 |
| amazonloginconntect20.19.jpg | phishing | 0,91992795 |
| amazonlogindecaiofa52.62.jpg | phishing | 0,9199181 |
| amazonloginizbiz.te71.9.jpg | phishing | 0,91992795 |
| **at&tlogindocs.goo12.02.jpg** | **legitimate** | **0,8898083** |
| at&tloginhilltopc34.37.jpg | phishing | 0,91404355 |
| at&tloginkletsbuy99.14.jpg | phishing | 0,919911 |
| at&tloginmahdistr30.89.jpg | phishing | 0,9199065 |
| at&tloginzaroosha94.26.jpg | phishing | 0,9199285 |
| **bankofamericalogin5.188.3665.04.jpg** | **legitimate** | **0,9267028** |
| bankofamericaloginecurity.26.59.jpg | phishing | 0,9199284 |
| bankofamericaloginedificio77.17.jpg | phishing | 0,9199283 |
| bankofamericaloginkrjpl.co60.86.jpg | phishing | 0,91555583 |
| bankofamericaloginwww.72dp49.28.jpg | phishing | 0,9193129 |
| chaseloginaigonspo91.35.jpg | phishing | 0,91986513 |
| chaseloginellefont45.61.jpg | phishing | 0,9199282 |

| | | |
|---|---|---|
| chaseloginotoblad.59.76.jpg | phishing | 0,9199282 |
| chaseloginowntownd30.71.jpg | phishing | 0,90655655 |
| chaselogintrack4se64.7.jpg | phishing | 0,91992617 |
| dhlloginacvedas.27.57.jpg | phishing | 0,9197787 |
| dhlloginangelart32.29.jpg | phishing | 0,91902244 |
| dhlloginharmoniu69.96.jpg | phishing | 0,9199285 |
| dhlloginhotelgra46.79.jpg | phishing | 0,9199285 |
| **dhlloginogansegu00.33.jpg** | **legitimate** | **0,92663467** |
| ebaylogin7426fbe061.09.jpg | phishing | 0,9199285 |
| ebayloginkverif23.96.jpg | phishing | 0,9199283 |
| ebayloginpaleypri94.81.jpg | phishing | 0,8664744 |
| ebayloginrlsverif45.47.jpg | phishing | 0,9199283 |
| ebayloginthongtin17.67.jpg | phishing | 0,9193768 |
| facebookloginadm.righ42.51.jpg | phishing | 0,9198813 |
| facebookloginhx.blewp90.51.jpg | phishing | 0,91384727 |
| facebookloginjoingrup15.72.jpg | phishing | 0,9199285 |
| facebookloginsecurlty22.26.jpg | phishing | 0,9199096 |
| facebookloginxvgbtopl00.11.jpg | phishing | 0,91992736 |
| googlelogindrive.go97.89.jpg | phishing | 0,9195727 |
| googlelogineadlampy24.96.jpg | phishing | 0,9199278 |
| googleloginlbel.int84.28.jpg | phishing | 0,9199285 |
| googleloginluidacco20.43.jpg | phishing | 0,9199281 |
| googleloginsites.go48.39.jpg | phishing | 0,8898619 |
| linkedinloginauricioy76.35.jpg | phishing | 0,919918 |
| linkedinlogindvtejas.76.89.jpg | phishing | 0,91985583 |
| linkedinloginmade-in-59.37.jpg | phishing | 0,91992795 |
| linkedinloginoutlookm27.79.jpg | phishing | 0,91986513 |
| linkedinloginowwglass82.2.jpg | phishing | 0,9199284 |
| microsoftloginakakakak47.63.jpg | phishing | 0,90620106 |
| microsoftlogindreamy-g35.49.jpg | phishing | 0,9199284 |
| microsoftloginfolhadac33.31.jpg | phishing | 0,91990256 |
| microsoftloginnazahaco60.47.jpg | phishing | 0,9199283 |
| microsoftloginrched-el31.95.jpg | phishing | 0,9198118 |
| netflixloginahorolln04.85.jpg | phishing | 0,91992676 |
| netflixloginarketing01.44.jpg | phishing | 0,9145295 |
| netflixloginlix-flix27.43.jpg | phishing | 0,9199081 |
| netflixloginrubibags49.6.jpg | phishing | 0,9199273 |
| netflixloginww.stamp24.73.jpg | phishing | 0,9198953 |
| paypalloginackyardd28.63.jpg | phishing | 0,9196859 |
| paypalloginaypal.co74.93.jpg | phishing | 0,9199284 |
| paypalloginppuseral91.68.jpg | phishing | 0,91098464 |
| paypalloginshadetre83.51.jpg | phishing | 0,9198345 |
| paypalloginarooqmob87.19 | phishing | 0,91984314 |
| yahoologinaesencia79.26.jpg | phishing | 0,90838575 |
| yahoologinastfoodg14.91.jpg | phishing | 0,9198992 |
| yahoologinodegascr65.94.jpg | phishing | 0,91992545 |
| yahoologintinyurl.03.54.jpg | phishing | 0,9199285 |
| yahoologinww.recov40.92 | phishing | 0,9199285 |

# Παράρτημα Z
# Κώδικες

## Z.1 Κώδικας Συλλογής και Οπτικοποίησης Δεδομένων

### Z.1.1 Κώδικας main.py

```
import csv
import sys
from process import *
import optparse
import os
import mysql.connector
import base64
from datetime import datetime
import requests
import re
import imgkit
import time

# Global
content = []
os.environ['TF_CPP_MIN_LOG_LEVEL'] = '2'

try:
   mydb = mysql.connector.connect(host = 'localhost', user='root',
    database='SpamDetection', password='root123')
   print('----------------------------------')
   print('')
   print('--------URL Scraping Tool -------- ')
   print('')
   print('-- [I] Database Connected Well --')
   print('')
   print('----------------------------------')
except:
   print ('Database Connection Failed ')


# Used to grab HTML of target page and send to image creation.
#METHOD FOR SINGLE STRING INPUT

def siteCheck(url):

        # CHECK IF URL EXISTS
        cursor = mydb.cursor()
        sql_select_query = """ select * from Legitimate where url = %s """
        cursor.execute(sql_select_query, (url, ))
        record_Legitimate = cursor.fetchall()
```

```
        if cursor.rowcount > 0:
            cursor.close()
            return 1
        else:
            cursor = mydb.cursor()
            sql_select_query = """ select * from Phishing where url = %s """
            cursor.execute(sql_select_query, (url, ))
            record_Legitimate = cursor.fetchall()
                    if cursor.rowcount > 0:
                        cursor.close()
                        return 1
                    else:
                        cursor.close()
                        return 0
#CREATE URLs SCREENSHOOT
def image_def(url,path):

        try:
            imgkit.from_url(url,path)
        except:
            print("\n error with",url,"----imgkit----\n")
        return(path)


# USED TO COLLECT TRAINING DATA
def importUrls(urlType,kind):
        with open(urlType, mode='r') as csv_file:
            csv_reader = csv.DictReader(csv_file)
            for row in csv_reader:
                    name = row['name']
                    url = row['url']
                    lang = row['lang']
                    content.append([name,url,lang])

        print('[I] Prog - Begining Scan of ' + str(len(content)) + ' sites')
        try:
            if not os.path.exists('data/Images'):
                    os.makedirs('data/Images')
            for p in content:
                if siteCheck(p[1]) == 1:
                    print('\n URL_EXIST')
                    print('---------------------------')
                    print(p[0])
                    print(p[1])
                    print('---------------------------')
                else:
                    try:
                        r = requests.get(p[1])
                        error=0
                    except:
                        print('\n' + '[!] Error - Site Read Error - [' + p[1] + ']')
                        error=1

                    try:
                        if error==0 :
                            print('\n'"GOOD")

                            if  kind == "good":
```

```
    type_is="legitimate"
else:
    type_is="phishing"

iso_code=p[2]
y=p[1]

 #CREATE IMAGE NAME
 new_Name = p[0] + y[8:16] + str(time.time())[8:] + '.jpg'
 new_Path="data/Images/"+type_is+"/screenshoot/"+new_Name
 print("CREATE SCREENSHOT IMAGE")
 path_photo = image_def(p[1],new_Path)
 #CREATE SCREENSHOT IMAGE
 print("\n CREATE HILBERT IMAGE")
 path_hilbert = siteInput(r.text,p[0],p[1],type_is,"hilbert",new_Name)
#CREATE HILBERT IMAGE
 print("\n CERATE ZIGZAG IMAGE")
 path_zigzag = siteInput(r.text,p[0],p[1],type_is,"zigzag",new_Name)
 #CREATE ZIGZAG IMAGE
 print("\n CREATE ZORDER IMAGE")
 path_zorder = siteInput(r.text,p[0],p[1],type_is,"zorder",new_Name)
 #CREATE ZORDER IMAGE

    source_code=r.text
    print('\n' + '[I] Prog - Successfull Site Read -  [' + p[1] + ']')
    #Photos encode
    with open(path_hilbert, "rb") as image_file:
            encoded_string = base64.b64encode(image_file.read())
    with open(path_zigzag, "rb") as image_file:
            encoded_string_1 = base64.b64encode(image_file.read())
    with open(path_zorder, "rb") as image_file:
            encoded_string_2= base64.b64encode(image_file.read())
    with open(path_photo, "rd") as image_file:
            encoded_string_3=base64.b64encode(image_file.read())

    ## CREATE RECORD OF NEW SITE
    if "good" == kind :
        status = "Safe"
        cursor = mydb.cursor()
        query = "INSERT INTO Legitimate (url, url_name, language, status,"+
    "date, path_hilbert,path_zigzag,path_zorder,path_screenshoot,imgPath_hilbert,"+
    "imgPath_zigzag,imgPath_zorder, screenshoot,source_code)"+
     " VALUES (%s, %s, %s,%s, %s, %s, %s, %s, %s, %s, %s, %s, %s)"
    ## storing values in a variable
         values = (p[1], p[0], iso_code, status,
          datetime.now().strftime('%Y-%m-%d %H:%M:%S'),
          path_hilbert,path_zigzag,path_zorder,
          path_photo,encoded_string,encoded_string_1,
          encoded_string_2,encoded_string_3,source_code)
    ## executing the query with values
          try:
               cursor.execute(query, values)
               mydb.commit()
         except mysql.connector.Error as err:
               print("Something went wrong: {}".format(err))
          cursor.close()
     else:
           status = "Phishing"
           cursor = mydb.cursor()
```

```
                                query = "INSERT INTO Phishing (url, url_name, language, status,"+
                            " date, path_hilbert,path_zigzag,path_zorder,path_screenshoot,imgPath_hilbert,"+
                            "imgPath_zigzag,imgPath_zorder, screenshoot,source_code)"+
                            " VALUES (%s, %s, %s,%s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s)"
                               ## storing values in a variable
                                values = (p[1], p[0], iso_code, status,
                                    datetime.now().strftime('%Y-%m-%d %H:%M:%S'),
                                    path_hilbert,path_zigzag,path_zorder,path_photo,encoded_string,
                                    encoded_string_1,encoded_string_2,encoded_string_3,source_code)
                                ## executing the query with values
                                try:
                                    cursor.execute(query, values)
                                    mydb.commit()
                                except mysql.connector.Error as err:
                                    print("Something went wrong: {}".format(err))
                                cursor.close()
                        except:
                                print('\n' + '[!] Error - Site Read Error - [' + p[1] + ']')
                except:
                        print('[!] Error - Folder Creation Error')

def Main():
   ## PARSER - USER INPUT - Used during create dataset for selecting urls data input.
        parser = optparse.OptionParser('usage: python v1 -S [good OR bad]')
        parser.add_option('-S', dest='urlType', type='string', help='Select what type of urls you wish to
read in.')
        (options, args) = parser.parse_args()
        urlType = ''
        if (options.urlType == None):
            print("EXIT")
            exit(0)
        else:
            if (options.urlType == 'good'):
                temp = importUrls('data/goodurls.csv','good')
            else:
                temp = importUrls('data/badurls.csv','bad')

if __name__ == '__main__':
        Main()
```

## Ζ.1.2 Τροποποιημένος Κώδικας process.py του Binvis

```
import os.path, math, string, sys
import scurve
from scurve import progress, utils, draw
from PIL import Image, ImageDraw
import shutil
import time

name_type=[]

# Binvis Image Creations
class _Color:
   def __init__(self, data, block):
      self.data, self.block = data, block
      s = list(set(data))
      s.sort()
      self.symbol_map = {v : i for (i, v) in enumerate(s)}

   def __len__(self):
      return len(self.data)

   def point(self, x):
      if self.block and (self.block[0]<=x<self.block[1]):
         return self.block[2]
      else:
         return self.getPoint(x)
class ColorGradient(_Color):
   def getPoint(self, x):
      c = ord(self.data[x])/255.0
      return [
         int(255*c),
         int(255*c),
         int(255*c)
      ]
class ColorHilbert(_Color):
   def __init__(self, data, block):
      _Color.__init__(self, data, block)
      self.csource = scurve.fromSize("hilbert", 3, 256**3)
      self.step = len(self.csource)/float(len(self.symbol_map))

   def getPoint(self, x):
      c = self.symbol_map[self.data[x]]
      return self.csource.point(int(c*self.step))

class ColorClass(_Color):
   def getPoint(self, x):
      c = ord(self.data[x])
      if c == 0:
         return [0, 0, 0]
      elif c == 255:
         return [255, 255, 255]
      elif chr(c) in string.printable:
         return [55, 126, 184]
      return [228, 26, 28]

#Function used from Binvis Libary to create Images from passed in data from siteInput.
## Could be sped up with binvis maths alteration.
```

```
def drawmap_unrolled(map, size, csource, name, prog):
   prog.set_target((size**2)*4)
   map = scurve.fromSize(map, 2, size**2)
   c = Image.new("RGB", (size, size*4))
   cd = ImageDraw.Draw(c)
   step = len(csource)/float(len(map)*4)

   sofar = 0
   for quad in range(4):
      for i, p in enumerate(map):
         off = (i + (quad * size**2))
         color = csource.point(
                  int(off * step)
               )
         x, y = tuple(p)
         cd.point(
            (x, y + (size * quad)),
            fill=tuple(color)
         )
         if not sofar%100:
            prog.tick(sofar)
         sofar += 1
   c.save(name)

# Used to create a record of phishing sites passed through,

def record(name, url, name_t, curve_name ):
   path = 'data/Images/'+ name_t +'/'+curve_name +'/'+ name
   shutil.move(name,path)
   return path


# Function used to force hilbert colour creation using passed in URL data.
def siteInput(input, output, url,name_type,curve_type,newName):
   block = None
   d = input
   csource = ColorHilbert(d, block)
   prog = progress.Progress(None)
   #newName = output + url[8:16] + str(time.time())[8:] + '.jpg'
   drawmap_unrolled(curve_type, 128, csource, newName, prog)
   return record(newName, url,name_type,curve_type)
```

# Ζ.2 Κώδικας Εκπαίδευσης MobileNet Μοντέλου

```
import time
import random
import numpy as np
import matplotlib.pyplot as plt
import keras
from keras.layers import Dense,GlobalAveragePooling2D
from keras.optimizers import Adam
from keras.metrics import categorical_crossentropy
from keras.preprocessing.image import ImageDataGenerator
from keras.preprocessing import image
from keras.models import Model
from keras.applications import imagenet_utils,MobileNet
from keras.callbacks import ModelCheckpoint
from keras.models import load_model


curves="hilbert"
img_width, img_height = 128 , 128
train_data_path = 'C:/Users/USER/Desktop/phish_or_not/data_'+curves+'/training'
validation_data_path = 'C:/Users/USER/Desktop/phish_or_not/data_'+curves+'/validation'
batch_size=32
epochs= 30
LR=0.01


def get_train_val_generator(batch_size=32):
  train_datagen=ImageDataGenerator(rescale=1./255)

  train_generator=train_datagen.flow_from_directory(train_data_path,
                                target_size=(img_width,img_height),
                                batch_size=batch_size,
                                color_mode='rgb',
                                class_mode='categorical',
                                shuffle=True)

  val_datagen=ImageDataGenerator(rescale=1./255) #included in our dependencies

  val_generator=val_datagen.flow_from_directory(validation_data_path,
                                target_size=(img_width,img_height),
                                batch_size=batch_size,
                                color_mode='rgb',
                                class_mode='categorical',
                                shuffle=True)
  print("BATCH SIZE=",batch_size)
  return train_generator, val_generator


# Φορτώνονται δύο Γεννήτορες με μέγεθος παρτίδας 32
train_generator, val_generator = get_train_val_generator(batch_size)
#Υπολογισμός βημάτων εκπαίδευση
train_steps=train_generator.n//train_generator.batch_size
val_samples=val_generator.n//val_generator.batch_size
```

```
# Φόρτωση του MobileNet Μοντέλου με βάρη εκπαίδευσης από ImageNet
MobileNet_model=MobileNet(weights='imagenet',include_top=False) #

x=MobileNet_model.output
x=GlobalAveragePooling2D()(x)
x=Dense(1024,activation='relu')(x) #Πρόσθεση περεταίρω στρωμάτων
x=Dense(1024,activation='relu')(x) #Dense layer 2
x=Dense(512,activation='relu')(x) #Dense layer 3
predictions=Dense(2,activation='softmax')(x) #Τελευταίο Dense στρώμα με συνάρτηση ενεργοποίησης
softmax
model=Model(inputs=MobileNet_model.input,outputs=predictions)

# Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης Adam
model.compile(optimizer=Adam(lr=LR),loss='categorical_crossentropy',metrics=['accuracy'])

# Σημείο ελέγχου
filepath="MobileNet_weights_lr"+str(LR)+".h5"

#Αποθήκευση της καλύτερης μέγιστης τιμής val_accuracy
checkpoint = ModelCheckpoint(filepath, monitor='val_accuracy', verbose=1, save_best_only=True,
mode='max')
callbacks_list = [checkpoint]

history=model.fit_generator(generator=train_generator,
            steps_per_epoch=train_steps,
            epochs=30,
            validation_data=val_generator,
            validation_steps=val_samples,
            callbacks=callbacks_list)

print("Training done")
# Αποθήκευση MobileNet Μοντέλου
model.save('MobileNet_Model_lr'+str(LR)+'.h5')

print("Saved model to disk")


# Δημιουργία Γραφήματος και Αποθήκευση Αποτελεσμάτων
acc = history.history['accuracy']
val_acc = history.history['val_accuracy']

loss=history.history['loss']
val_loss=history.history['val_loss']

epochs_range = range(30)

plt.figure(figsize=(20, 10))
plt.subplot(1, 2, 1)
plt.plot(epochs_range, acc, label='Training Accuracy')
plt.plot(epochs_range, val_acc, label='Validation Accuracy')
plt.legend(loc='lower right')
plt.title('Training and Validation Accuracy')

plt.subplot(1, 2, 2)
plt.plot(epochs_range, loss, label='Training Loss')
plt.plot(epochs_range, val_loss, label='Validation Loss')
plt.legend(loc='upper right')
plt.title('Training and Validation Loss')
#Αποθήκευση Γραφήματος
```

```
plt.savefig("MobileNet"+curves+" lr"+str(LR)+ " 128x128 .png")


scores = model.evaluate_generator(val_generator, val_samples=val_samples)
print(model.metrics_names, scores)
print("%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100))
file_score=model.metrics_names, scores
file_score1= "%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100)

f = open("info_lr"+str(LR)+".txt", "a")
f.write("Train \n\n"+ str(file_score)+"\n\n" + str(file_score1)+"\n\n")
f.close()
```

# Z.3 Κώδικας Εκπαίδευσης MobileNet-RNN Μοντέλου

```
import keras
from keras.applications import MobileNet
from keras.applications.mobilenet import preprocess_input
from keras.layers import GlobalAveragePooling2D, Dense, Reshape, Lambda, LSTM, Multiply,Input
from keras import backend as K
from keras.preprocessing.image import ImageDataGenerator
from keras.models import Model, load_model
from keras.optimizers import Adam
from keras.callbacks import ModelCheckpoint
import numpy as np
import matplotlib.pyplot as plt

curves="hilbert"
img_width = 128
img_height = 128
LR=0.01
batch_size_train_one = 32
batch_size_train_two = 16
nba_epochs = 30
nbb_epochs = 30
classes=2
train_data_path = 'C:/Users/USER/Desktop/phish_or_not/data_'+curves+'/training'
validation_data_path = 'C:/Users/USER/Desktop/phish_or_not/data_'+curves+'/validation'



def get_train_val_generator(batch_size=32):
  train_datagen=ImageDataGenerator(preprocessing_function=preprocess_input)

  train_generator=train_datagen.flow_from_directory(train_data_path,
                                target_size=(img_width,img_height),
                                batch_size=batch_size,
                                color_mode='rgb',
                                class_mode='categorical',
                                shuffle=True)

  val_datagen=ImageDataGenerator(preprocessing_function=preprocess_input)

  val_generator=val_datagen.flow_from_directory(validation_data_path,
                                target_size=(img_width,img_height),
                                batch_size=batch_size,
```

```
                                color_mode='rgb',
                                class_mode='categorical',
                                shuffle=True)
    return train_generator, val_generator


def rgb_to_grayscale(input):    #Μέσος όρος από κάθε pixel σε 3 RGB στρώματα έχει ως αποτέλεσμα μια εικόνα κλίμακας του γκρι
    return K.mean(input, axis=3)


def rgb_to_grayscale_output_shape(input_shape):
    return input_shape[:-1]


# Φορτώνονται δύο Γεννήτορες με μέγεθος παρτίδας 32
print("LOADING IMAGE DATASET WITH BATCH SIZE OF {}...".format(batch_size_train_one))
train_generator, val_generator = get_train_val_generator(batch_size_train_one)


#Υπολογισμός βημάτων εκπαίδευση
train_steps=train_generator.n//train_generator.batch_size
val_samples=val_generator.n//val_generator.batch_size


print("LOAD MobileNet Model / Createting RNN Parallel Model...")
input_tensor = Input(shape=(img_width, img_height,3))

# Φόρτωση του MobileNet Μοντέλου με βάρη εκπαίδευσης από ImageNet
cnn_model= MobileNet(weights='imagenet', include_top=False, input_tensor=input_tensor)
x = cnn_model.output
CNN_bottleneck = GlobalAveragePooling2D()(x)

# Απενεργοποίηση των στρωμάτων του Xception μοντέλου για εκπαίδευση
for layer in cnn_model.layers:
    layer.trainable = False


# Δημιουργία του RNN μοντέλου με δύο LSTM μεγέθους 1024
x = Lambda(rgb_to_grayscale, rgb_to_grayscale_output_shape)(input_tensor)
x = Reshape((16,1024))(x)  # 16 χρονικά βήματα, με είσοδο δείγμα μεγέθους 1024
x = LSTM(1024, return_sequences=True)(x)
RNN_output = LSTM(1024)(x)


# Οι δύο έξοδοι CNN_bottleneck και RNN_output συγχωνεύονται με πολλαπλασιασμό. Η έξοδος αυτού του πολλαπλασιασμού
# τροφοδοτείται στο  στρώμα ταξινόμησης που αποτελείται από 2 κόμβους  (2 κλάσεις) και συνάρτηση ενεργοποίησης softmax

x = Multiply()([CNN_bottleneck, RNN_output])


predictions = Dense(classes, activation='softmax')(x)
model = Model(inputs=[input_tensor], outputs=predictions)


# Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης RMSProp
model.compile(optimizer='rmsprop',loss='categorical_crossentropy' ,metrics=['accuracy'])
```

```
print("Starting training")

#Σημείο ελέγχου 1
filepath="weights.h5"
checkpoint = ModelCheckpoint(filepath, monitor='val_accuracy', verbose=1, save_best_only=True,
mode='max')
callbacks_list = [checkpoint]

history=model.fit_generator(train_generator,
                                                steps_per_epoch=train_steps,
                                                epochs=nba_epochs,
                                                verbose=1,
                                                validation_data=val_generator,
                                                validation_steps=val_samples,
                                                callbacks=callbacks_list)


print("----------------------------------------------1st Training Step Done---------------------------------------------- \n\n")
print("----------------------------------------------2nd Training Step Starting ----------------------------------------------")
print("\n----------------------------------------------Loaded model---------------------------------------------------------- \n")

#Φορτώνονται δύο νέοι Γεννήτορες με μικρότερο μέγεθος παρτίδας 16 για να μην προκληθεί εξάντληση
#της μνήμης της GPU
print("LOADING IMAGE DATASET WITH BATCH SIZE OF {}...".format(batch_size_train_two))
train_generator, val_generator = get_train_val_generator(batch_size_train_two)
#Υπολογισμός βημάτων εκπαίδευσης
train_steps=train_generator.n//train_generator.batch_size
val_samples=val_generator.n//val_generator.batch_size
print("\n Dataset loaded \n")

#Φόρτωση βαρών από τη πρώτη φάση εκπαίδευσης
model.load_weights(filepath)

# Ενεργοποίηση όλων των στρωμάτων για εκπαίδευση
for layer in model.layers:
   layer.trainable = True

# Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης Adam
model.compile(optimizer=Adam(lr=LR), loss='categorical_crossentropy',
          metrics=['accuracy', 'top_k_categorical_accuracy'])



# Σημείο ελέγχου 2
filepath="Finetuned_weights_MobileNet_RNN.h5"
#Αποθήκευση της καλύτερης μέγιστης τιμής val_accuracy

checkpoint = ModelCheckpoint(filepath, monitor='val_accuracy', verbose=1, save_best_only=True,
mode='max')
callbacks_list1 = [checkpoint]


history=model.fit_generator(train_generator,
                steps_per_epoch=step_size_train,
                epochs=nbb_epochs,
                verbose=1,
                validation_data=val_generator,
```

```
            validation_steps=val_samples,
            callbacks=callbacks_list1)

# Αποθήκευση CNN-RNN μοντέλου
save.model('MobileNet-RNN-Model.h5')
print("Training done")
model.load_weights(filepath)



model.compile(optimizer=Adam(lr=LR), loss='categorical_crossentropy',
          metrics=['accuracy', 'top_k_categorical_accuracy'])


# Δημιουργία Γραφήματος και Αποθήκευση Αποτελεσμάτων

acc = history.history['accuracy']
val_acc = history.history['val_accuracy']

loss=history.history['loss']
val_loss=history.history['val_loss']

epochs_range = range(nba_epochs)

plt.figure(figsize=(20, 10))
plt.subplot(1, 2, 1)
plt.plot(epochs_range, acc, label='Training Accuracy')
plt.plot(epochs_range, val_acc, label='Validation Accuracy')
plt.legend(loc='lower right')
plt.title('Training and Validation Accuracy')

plt.subplot(1, 2, 2)
plt.plot(epochs_range, loss, label='Training Loss')
plt.plot(epochs_range, val_loss, label='Validation Loss')
plt.legend(loc='upper right')
plt.title('Training and Validation Loss')
#Αποθήκευση Γραφήματος
plt.savefig("MobileNet-RNN "+curves+" lr"+str(LR)+ " 128x128.png")

#Υπολογισμός αποτελέσματος εκπαίδευσης επί της εκατό.
scores = model.evaluate_generator(val_generator, val_samples=val_samples)
print(model.metrics_names, scores)
print("%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100))
file_score=model.metrics_names, scores
file_score1= "%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100)

#Αποθήκευση αποτελεσμάτων στο αρχείο info.txt
f = open("info.txt", "a")
f.write("Train \n\n"+ str(file_score)+"\n\n" + str(file_score1)+"\n\n")
f.close()
```

# Ζ.4 Κώδικας Εκπαίδευσης Xception-RNN Μοντέλου

```
import keras
import matplotlib.pyplot as plt
import time
import numpy as np
from keras.applications.xception import Xception,preprocess_input
from keras.layers import Input
from keras.layers import GlobalAveragePooling2D, Dense, Reshape, Lambda, LSTM, Multiply
from keras import backend as K
from keras.preprocessing.image import ImageDataGenerator
from keras.models import Model
from keras.models import load_model
from keras.optimizers import Adam
from keras.callbacks import ModelCheckpoint
from keras.metrics import categorical_crossentropy
np.random.seed(1337)

curves="hilbert"
img_width = 128
img_height = 128
LR=0.01
batch_size_train_one = 32
batch_size_train_two = 16
nba_epochs = 30
nbb_epochs = 30
classes=2
train_data_path = 'C:/Users/USER/Desktop/phish_or_not/data_'+curves+'/training'
validation_data_path = 'C:/Users/USER/Desktop/phish_or_not/data_'+curves+'/validation'


def get_train_val_generator(batch_size=32):
   train_datagen=ImageDataGenerator(preprocessing_function=preprocess_input)

   train_generator=train_datagen.flow_from_directory(train_data_path,
                                 target_size=(img_width,img_height),
                                 batch_size=batch_size,
                                 color_mode='rgb',
                                 class_mode='categorical',
                                 shuffle=True)

   val_datagen=ImageDataGenerator(preprocessing_function=preprocess_input)

   val_generator=val_datagen.flow_from_directory(validation_data_path,
                                 target_size=(img_width,img_height),
                                 batch_size=batch_size,
                                 color_mode='rgb',
                                 class_mode='categorical',
                                 shuffle=True)
   return train_generator, val_generator


def rgb_to_grayscale(input):        #Μέσος όρος από κάθε pixel σε 3 RGB στρώματα έχει ως αποτέλεσμα
μια εικόνα κλίμακας του γκρι
   return K.mean(input, axis=3)

def rgb_to_grayscale_output_shape(input_shape):
```

```
    return input_shape[:-1]


# Φορτώνονται δύο Γεννήτορες με μέγεθος παρτίδας 32
print("LOADING IMAGE DATASET WITH BATCH SIZE OF {}...".format(batch_size_train_one))
train_generator, val_generator = get_train_val_generator(batch_size_train_one)


#Υπολογισμός βημάτων εκπαίδευση
train_steps=train_generator.n//train_generator.batch_size
val_samples=val_generator.n//val_generator.batch_size



print("LOAD Xception Model / Createting RNN Parallel Model...")
input_tensor = Input(shape=(img_width, img_height,3))


# Φόρτωση του Xception Μοντέλου με βάρη εκπαίδευσης από ImageNet
cnn_model= Xception(weights='imagenet', include_top=False, input_tensor=input_tensor)
x = cnn_model.output
CNN_bottleneck = GlobalAveragePooling2D()(x)

# Απενεργοποίηση των στρωμάτων του Xception μοντέλου για εκπαίδευση
for layer in cnn_model.layers:
    layer.trainable = False

# Δημιουργία του RNN μοντέλου με δύο LSTM μεγέθους 2048
x = Lambda(rgb_to_grayscale, rgb_to_grayscale_output_shape)(input_tensor)
x = Reshape((16, 1024))(x)  # 16 χρονικές στιγμές, με μέγεθος δείγματος είσοδου1024 σε κάθε βήμα
x = LSTM(2048, return_sequences=True)(x) #LSTM με Batch Size 2048
RNN_output = LSTM(2048)(x) #LSTM με Batch Size 2048


# Οι δύο έξοδοι CNN_bottleneck και RNN_output συγχωνεύονται με πολλαπλασιασμό. Η έξοδος #αυτού
του πολλαπλασιασμού  τροφοδοτείται στο  στρώμα ταξινόμησης που αποτελείται από #2 κόμβους  (2
κλάσεις) και  την συνάρτηση ενεργοποίησης softmax

x = Multiply()([CNN_bottleneck, RNN_output])

predictions = Dense(2, activation='softmax')(x)
model = Model(inputs=[input_tensor], outputs=predictions)

# Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης RMSProp
model.compile(optimizer='rmsprop',loss='categorical_crossentropy' ,metrics=['accuracy'])

print("Starting training")

# Σημείο ελέγχου 1
filepath="weights_xception_rnn.h5"
#Αποθήκευση της καλύτερης μέγιστης τιμής val_accuracy
checkpoint = ModelCheckpoint(filepath, monitor='val_accuracy', verbose=1, save_best_only=True,
mode='max')
callbacks_list = [checkpoint]


#Έναρξη της πρώτης φάσης εκπαίδευσης του CNN-RNN μοντέλου
model.fit_generator(train_generator,
                    steps_per_epoch=train_steps,
```

```
                                epochs=nba_epochs,
                                verbose=1,
                                validation_data=val_generator,
                                validation_steps=val_samples,
                                callbacks=callbacks_list)

print("----------------------------------------1st Training Step Done---------------------------------------- \n\n")
print("----------------------------------------2nd Training Step Starting ----------------------------------------")
print("\n----------------------------------------Loaded model---------------------------------------- \n")

#Φορτώνονται δύο νέοι Γεννήτορες με μικρότερο μέγεθος παρτίδας 16 για να μην προκληθεί #εξάντληση της μνήμης της GPU
print("LOADING IMAGE DATASET WITH BATCH SIZE OF {}...".format(batch_size_train_two))
train_generator, val_generator = get_train_val_generator(batch_size_train_two)

train_steps=train_generator.n//train_generator.batch_size
val_samples=val_generator.n//val_generator.batch_size
print("\n Dataset loaded \n")

#Φόρτωση βαρών από τη πρώτη φάση εκπαίδευσης
model.load_weights(filepath)

# Ενεργοποίηση όλων των στρωμάτων για εκπαίδευση
for layer in model.layers:
   layer.trainable = True


# Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης Adam
model.compile(optimizer=Adam(lr=LR), loss='categorical_crossentropy',
          metrics=['accuracy', 'top_k_categorical_accuracy'])

# Σημείο Ελέγχου 2
filepath="finetuned_weights_xception_rnn.h5"
#Αποθήκευση της καλύτερης μέγιστης τιμής val_accuracy
checkpoint = ModelCheckpoint(filepath, monitor='val_accuracy', verbose=1, save_best_only=True,
mode='max')
callbacks_list1 = [checkpoint]

print("\n----------------------------------Fit Xception-RNN Model---------------------------------------- \n")

#Έναρξη της δεύτερης φάσης εκπαίδευσης του CNN-RNN μοντέλου
history=model.fit_generator(train_generator,
                steps_per_epoch=train_steps,
                epochs=nbb_epochs,
                verbose=1,
                validation_data=val_generator,
                validation_steps=val_samples,
                callbacks=callbacks_list1)

# Αποθήκευση CNN-RNN μοντέλου
save.model('Xception-RNN-Model.h5')

print("Training done")
model.load_weights(filepath)

model.compile(optimizer=Adam(lr=LR), loss='categorical_crossentropy',
          metrics=['accuracy', 'top_k_categorical_accuracy'])

# Δημιουργία Γραφήματος και Αποθήκευση Αποτελεσμάτων
```

```
acc = history.history['accuracy']
val_acc = history.history['val_accuracy']

loss=history.history['loss']
val_loss=history.history['val_loss']
epochs_range = range(nbb_epochs)

plt.figure(figsize=(20, 10))
plt.subplot(1, 2, 1)
plt.plot(epochs_range, acc, label='Training Accuracy')
plt.plot(epochs_range, val_acc, label='Validation Accuracy')
plt.legend(loc='lower right')
plt.title('Training and Validation Accuracy')

plt.subplot(1, 2, 2)
plt.plot(epochs_range, loss, label='Training Loss')
plt.plot(epochs_range, val_loss, label='Validation Loss')
plt.legend(loc='upper right')
plt.title('Training and Validation Loss')
#Αποθήκευση Γραφήματος
plt.savefig("Xception-RNN "+curves+" lr"+str(LR)+ " 128x128.png")

#Υπολογισμός αποτελέσματος εκπαίδευσης επί της εκατό.
scores = model.evaluate_generator(val_generator, val_samples=val_samples)
print(model.metrics_names, scores)
print("%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100))
file_score=model.metrics_names, scores
file_score1= "%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100)

#Αποθήκευση αποτελεσμάτων στο αρχείο info.txt
f = open("info.txt", "a")
f.write("Train \n\n"+ str(file_score)+"\n\n" + str(file_score1)+"\n\n")
f.close()
```

# Z.5 Κώδικας Εκπαίδευσης Custom-CNN Μοντέλου

```
import keras
from keras.models import *
from keras.layers import *
from keras.optimizers import *
from keras.preprocessing.image import ImageDataGenerator
import matplotlib.pyplot as plt
from keras.callbacks import History
from keras.callbacks import *
import os



curves="hilbert"
img_width, img_height = 128 , 128
classes=2
train_data_path = 'C:/Users/USER/Desktop/phish_or_not/data_'+curves+'/training'
validation_data_path = 'C:/Users/USER/Desktop/phish_or_not/data_'+curves+'/validation'
batch_size=16
epochs= 200
```

```
LR=0.0001


def get_train_val_generator(batch_size=128):
  train_datagen=ImageDataGenerator(rescale=1./255)

  train_generator=train_datagen.flow_from_directory(train_data_path,
                                target_size=(img_width,img_height),
                                batch_size=batch_size,
                                color_mode='rgb',
                                class_mode='categorical',
                                shuffle=True)

  val_datagen=ImageDataGenerator(rescale=1./255)

  val_generator=val_datagen.flow_from_directory(validation_data_path,
                                target_size=(img_width,img_height),
                                batch_size=batch_size,
                                color_mode='rgb',
                                class_mode='categorical',
                                shuffle=True)
  return train_generator, val_generator


# Φορτώνονται δύο Γεννήτορες με μέγεθος παρτίδας 16
train_generator, val_generator =  get_train_val_generator(batch_size)
#Υπολογισμός βημάτων εκπαίδευση
train_steps=train_generator.n//train_generator.batch_size
val_samples=val_generator.n//val_generator.batch_size

model= Sequential()
model.add(Conv2D(32,kernel_size=3,activation='relu',input_shape=(128,128,3)))
model.add(BatchNormalization())
model.add(MaxPool2D(strides=(2,2)))
model.add(Dropout(0.2))
model.add(Conv2D(32,kernel_size=3,activation='relu'))
model.add(BatchNormalization())
model.add(MaxPool2D(strides=(2,2)))
model.add(Dropout(0.2))
model.add(Conv2D(64,kernel_size=3,activation='relu'))
model.add(BatchNormalization())
model.add(MaxPool2D(strides=(2,2)))
model.add(Dropout(0.2))
model.add(Conv2D(64,kernel_size=3,activation='relu'))
model.add(BatchNormalization())
model.add(MaxPool2D(strides=(2,2)))
model.add(Dropout(0.2))

model.add(Flatten())
model.add(Dense(512,activation="softmax"))
model.add(Dense(128,activation="softmax"))
model.add(Dropout(0.2))

model.add(Dense(2, activation="softmax"))


rms=keras.optimizers.RMSprop(learning_rate=LR, rho=0.9)
# Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης RMSProp
model.compile(loss='categorical_crossentropy',optimizer=rms, metrics=['accuracy'])
```

```
# Σημείο ελέγχου
filepath="my_cnn_model_weights.h5"
#Αποθήκευση της καλύτερης μέγιστης τιμής val_accuracy
checkpoint = ModelCheckpoint(filepath, monitor='val_accuracy', verbose=1, save_best_only=True,
mode='max')
callbacks_list = [checkpoint]

#Έναρξη εκπαίδευσης του CNN μοντέλου
history=model.fit_generator(train_generator,
                                                steps_per_epoch=train_steps,
                                                epochs=epochs,
                                                callbacks=callbacks_list,
                                                validation_data=val_generator,
                                                validation_steps=val_samples
                                                )

#Αποθήκευση CNN Μοντέλου
model.save('my_cnn_model.h5')

# Δημιουργία Γραφήματος και Αποθήκευση Αποτελεσμάτων
acc = history.history['accuracy']
val_acc = history.history['val_accuracy']

loss=history.history['loss']
val_loss=history.history['val_loss']

epochs_range = range(epochs)

plt.figure(figsize=(20, 10))
plt.subplot(1, 2, 1)
plt.plot(epochs_range, acc, label='Training Accuracy')
plt.plot(epochs_range, val_acc, label='Validation Accuracy')
plt.legend(loc='lower right')
plt.title('Training and Validation Accuracy')

plt.subplot(1, 2, 2)
plt.plot(epochs_range, loss, label='Training Loss')
plt.plot(epochs_range, val_loss, label='Validation Loss')
plt.legend(loc='upper right')
plt.title('Training and Validation Loss')
#Αποθήκευση Γραφήματος
plt.savefig("My_CNN_Model "+curves+" lr"+str(LR)+ " 128x128.png")

#Υπολογισμός αποτελέσματος εκπαίδευσης επί της εκατό.
scores = model.evaluate_generator(val_generator, val_samples=val_samples)
print(model.metrics_names, scores)
print("%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100))
file_score=model.metrics_names, scores
file_score1= "%s: %.2f%%" % (model.metrics_names[1], scores[1] * 100)

#Αποθήκευση αποτελεσμάτων στο αρχείο info.txt
f = open("info.txt", "a")
f.write("lr= " + str(LR) + "\n\n1st step Train \n\n"+ str(file_score)+"\n\n" + str(file_score1)+"\n\n")
f.close()
```

# Ζ.6 Κώδικας Δοκιμών Μοντέλων

```
import numpy as np
import keras
import os
import csv
from keras.applications.xception import preprocess_input
from keras.optimizers import Adam
from keras.metrics import categorical_crossentropy
from keras.preprocessing.image import ImageDataGenerator
from keras.models import load_model
from keras.layers.core import Dense, Activation


curves="hilbert"
LR=0.01
test_path=r"C:/Users/USER/Desktop/phish_or_not/data_"+curves+"/test"


#Φόρτωση του μοντέλου και των βαρών
model = keras.models.load_model('model_xception_rnn.h5')
model.load_weights('finetuned_weights_xception_rnn.h5')

#Μεταγλώττιση του μοντέλου με αλγόριθμο βελτιστοποίησης Adam
model.compile(optimizer=Adam(lr=LR), loss='categorical_crossentropy',metrics=['accuracy',
'top_k_categorical_accuracy'])

#Γεννήτορας παρτίδας Εικόνων
test_datagen=ImageDataGenerator(preprocessing_function=preprocess_input)

test_generator = test_datagen.flow_from_directory(
   directory=test_path,
   target_size=(128,128),
   color_mode="rgb",
   batch_size=1,
   class_mode=None,
   shuffle=False,
   seed=42)



STEP_SIZE_TEST=test_generator.n//test_generator.batch_size
test_generator.reset()

pred=model.predict_generator(test_generator,steps=STEP_SIZE_TEST,verbose=1)


pithanotita=pred.max(axis=1)#Παρουσίαση της Μέγιστης Πιθανότητας


predicted_class_indices=np.argmax(pred,axis=1)
#Ορισμός Ετικετών
labels={'legitimate':0,
            'phishing':1,
                    }
```

```
labels = dict((v,k) for k,v in labels.items())
predictions = [labels[k] for k in predicted_class_indices]

# Αποθήκευση αποτελεσμάτων σε CSV αρχείο
filenames=test_generator.filenames

l=0
myFile = open('Xception_RNN_lr'+str(LR)+'_results.csv', 'w')

with myFile:
	myFields = ['Filename', 'Predictions','Predictions_Persent']
	writer = csv.DictWriter(myFile, fieldnames=myFields)
	writer.writeheader()

	while l < len(pred):
		Filename=filenames[l]
		Predictions=predictions[l]
		Predictions_Persent=pithanotita[l]

	writer.writerow({'Filename':Filename,'Predictions':Predictions,'Predictions_Persent':Predictions_
Persent})
		print("\nFilename : ",filenames[l],"\nPredictions :",predictions[l],"\nPredictions Persent
:",pithanotita[l],"\n")
		l+=1
```

# Βιβλιογραφία


*Anti-Phishing Working Group.* 2020. https://apwg.org/.

Basnet, Ram B, και Tenzin Doleck. «Towards Developing a Tool to Detect Phishing URLs: A Machine Learning Approach.» *IEEE*, 2015: 220-223.

Bhagyashree, E, και K. Tanuja. «Phishing URL Detection: A Machine Learning and Web Mining-based Approach.» *International Journal of Computer Applications* 123, αρ. 13 (August 2015): 46-50.

Cao, Ye, Weili Han, και Yuerna Le. «Anti-Phishing Based on Automated Individual White-List.» *Proceedings of the 4th ACM workshop on Digital Identity Management*, October 2008: 51-60.

Cortesi, Aldo . *Github.* 3 Mar 2015. https://github.com/cortesi/scurve.

Feng, Fang , Qingguo Zhou, Zebang Shen, Xuhui Yang, Lihong Han, and Jin Qiang Wang. "The Application of a Novel Neural Network in the Detection of Phishing Websites." April 2018.

*Google Safe Browsing.* 2012. https://developers.google.com/safe-browsing/?csw=1 (πρόσβαση 2018).

Group Anti Phishing Reoporting. "Phishing Activity Trends Report 1st Quarter." 2018.

Group, Anti Phishing Working. *Phishing Activity Trends Report 1st Quarter.* Group, Anti Phishing Working, 2019, 6.

*Help Net Security .* χ.χ. https://www.helpnetsecurity.com/2020/02/26/phishing-ssl/.

Hoon, Lee Chang, Dong Hyun Kim, και Jin Lee Lee. «Heuristic Based Approach for Phishing Site Detection Using URL Features.» *Third International Conference on Advances in Computing, Electronics and Electrical Technology - CEET.* 2015. 131-135.

ILSVRC. *Imagenet Larger Scale Visial Recognition Challenge.* 2015. http://www.image-net.org/challenges/LSVRC/.

Isitphishing. *https://isitphishing.org/.* χ.χ. https://isitphishing.org/.

Jain, Ankit Kumar , και B B Gupta. «A Novel Approach to Protect Against Phishing Attacks at Client Side Using Auto-Updated White-List.» *EURASIP Journal on Information Security*, 2018: 687—700.

Jain, Ankit Kumar , και B B Gupta. «Towards Detection Of Phishing Websites On Client-Side Using Machine Learning Based Approach.» *Telecommunication Systems volume*, Dec 2017: 687-700.

Khonji, Mahmoud , Youssef Iraqi, και Andrew Jones. «Phishing Detection: A Literature Survey.» *IEEE Communications Surveys & Tutorials* 15, αρ. 4 (April 2013): 2091-2121.

Le, Anh , Athina Markopoulou, και Michalis Faloutsos. «PhishDef: URL Names Say It All.» *IEEE .* 2011. 191-195.

Marchal, Samuel , François Jérôme, State Radu, και Engel Thomas. «PhishStorm: Detecting Phishing With Streaming Analytics.» *IEEE*, 2014: 458-471.

OpenPhish. *https://openphish.com/.* χ.χ. https://openphish.com/.

Peng, Tianrui , Ian Harris, και Yuki Sawa. «Detecting Phishing Attacks Using Natural Language Processing and Machine Learning.» *IEEE 12th International Conference on Semantic Computing*, 2018: 300-301.

PhishTank. *https://www.phishtank.com/.* χ.χ. https://www.phishtank.com/.

Prakash, Pawan , Manish Kumar, Ramana Rao Kompella, και Minaxi Gupta. «Phishnet: Predictive Blacklisting to Detect Pphishing Attacks.» *IEEE.* 2010. 1-5.

Rao, Routhu Srinivasa, και Alwyn Roshan Roshan Pais . «Detection of Phishing Websites Using an Efficient Feature-Based Machine Learning Framework.» *Springer*, 2018.

Reporting, Consumer Fraud. *Phishing Examples.* χ.χ. http://www.consumerfraudreporting.org/phishing_examples.php.

RSA. *RSA Quarterly Fraud Report, Q1 2018.* RSA, 2018.

Sharifi, Mohsen , και Seyed Hossein Siadati. «A Phishing Sites Blacklist Generator.» *ACS/IEEE International Conference on Computer Systems and Applications.* 2008.

Sheng, Steve , Brad Wardman, Gary Warner, Lorrie Faith Cranor, Jason Hong, και Chengshan Zhang. «An Empirical Analysis of Phishing Blacklists.» *Sixth Conference on Email and Anti-Spam.* 2009.

Sheng, Steve , Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Cranor, and Julie Downs. "Who Falls for Phish? A Demographic Analysis of Phishing." *Proceedings of the SIGCHI Conference on Human Factors in Computer Systems.* 2010. 373-382.

Shinde, Amitkumar , Angad Pandey, Rahul Pawar, και Vinayak Gangule. «Clustering and Bayesian Approach-based Model for Detection of Phishing.» *International Journal of Computer Applications*, 2015: 30-33.

Suryavanshi, Nirmala , and Anurag Jain. "A Review of Various Techniques for Detection and Prevention." *International Journal of Advanced Computer Technology*, 2015: 41-46.

Wikipedia. 12 November 200. https://en.wikipedia.org/wiki/Softmax_function.

Wombat. «State of the Phish Report_Final.» 2019.