Ανοικτό Πανεπιστήμιο Κύπρου

Θετικών και Εφαρμοσμένων

Επιστημών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Digital Commerce Security Awareness Training & Assessments

Νίκος Μούζουρας

Επιβλέπουσα Καθηγήτρια
Περατικού Αδαμαντίνη

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Digital Commerce Security Awareness Training & Assessments

Νίκος Μούζουρας

Επιβλέπουσα Καθηγήτρια
Περατικού Αδαμαντίνη

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών
στ. 13/06/2022
από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2022

Περίληψη

Η Μεταπτυχιακή Διατριβή περιγραφή την υλοποίηση της πλατφόρμας Be Cyber Aware και του εργαλείου MASCARA που αναπτύχθηκε ως μέρος του έργου ENSURESEC που χρηματοδοτείται από την ΕΕ στο πλαίσιο του προγράμματος Horizon 2020 .

Στόχος της παρούσας μεταπτυχιακής διατριβής είναι να παρουσιάσει τον σχεδιασμό και την εκτέλεση εκστρατειών ευαισθητοποίησης σχετικά με την ασφάλεια για τον έλεγχο συγκεκριμένων ανθρώπινων τρωτών σημείων στο πλαίσιο του ψηφιακού εμπορίου.

Για τους πιο πάνω στόχους αναπτύχθηκε το εργαλείο MASCARA που μας βοηθά να δημιουργήσουμε και να αναπτύξουμε εύκολα εφαρμογές ιστού, από απλούς ιστότοπους, ιστότοπους WordPress ή εφαρμογές Django έως πιο περίπλοκες υπηρεσίες όπως διακομιστές αλληλογραφίας ή διαδικασίες όπως η αποστολή αυτοματοποιημένων μηνυμάτων ηλεκτρονικού ταχυδρομείου σε συγκεκριμένες ομάδες-στόχους χωρίς υπερβολικά περίπλοκες διαμορφώσεις που απαιτούνται από χειροκίνητη εγκατάσταση τέτοιων συστημάτων. Επίσης, το MASCARA υποστηρίζει την καταγραφή και την παρακολούθηση των υπηρεσιών μέσω μιας ανάπτυξης στοίβας ELK ικανή να καταγράφει τυπικά αρχεία καταγραφής εφαρμογών ή ακόμα και προσαρμοσμένα μηνύματα καταγραφής που παράγονται από εφαρμογές που αναπτύσσονται από το MASCARA.

Τέλος δημιουργήθηκε η διαδικτυακή πλατφόρμα Be Cyber Aware με στόχο την εκπαίδευση και ευαισθητοποίησης για την ασφάλεια του ψηφιακού εμπορίου. Παρέχει δωρεάν εκπαιδευτικό περιεχόμενο για την ευαισθητοποίηση στον κυβερνοχώρο (βίντεο και κείμενο) καθώς και αξιολογήσεις σχετικά με τη επίγνωση στην κυβερνοασφάλεια καθώς και μια επιλογή εγγραφής για σειρά προσομοιωμένων (ψευδών) απατών.

Ευχαριστίες

Με το πέρας της ακαδημαϊκής χρονιάς και με την ολοκλήρωση της μεταπτυχιακής διατριβής, θα ήθελα να ευχαριστήσω θερμά την επιβλέποντα καθηγήτρια μου, κυρία Περατικού Αδαμαντίνη, για την δυνατότητα που μου έδωσε να αναπτύξω την παρούσα διατριβή. Τόσο η στήριξη όσο και η καθοδήγηση που δέχτηκα καθ' όλη την διάρκεια ήταν πραγματικά πολύτιμη.

Επιπρόσθετα, θα ήθελα να ευχαριστήσω τον κύριο George Nicalou, επικεφαλής του τμήματος έρευνας και ανάπτυξης στην εταιρία Silensec, τον κύριο Almerindo Graziano, CEO στην εταιρία Silensec και την Γιουλιάνα Καλαιτζίδου, για τον χρόνο και την συμβολή τους στην ανάπτυξη του έργου αυτού.

Τέλος, οφείλω να ευχαριστήσω την οικογένεια και τους φίλους μου που ήταν πάντα κοντά μου και με στήριξαν καθ' όλη την διάρκεια.

Περιεχόμενα

Εισαγωγή

Προβληματισμός και κίνητρα

Ένα από τα μέτρα κατά της πανδημίας COVID-19 [1] ήταν η εφαρμογή της τηλεργασίας και η παρότρυνση του κόσμου για αγορές μέσο του διαδικτύου με επακόλουθο την μια επιταχυνόμενη μετακίνηση επιχειρήσεων, μέσων ενημέρωσης, κοινωνικής αλληλεπίδρασης, εκπαίδευσης κ.λπ. σε πλατφόρμες στο Διαδίκτυο.

Ως επακόλουθο των πιο πάνω έχουν οδηγήσει σε αυξημένη εγκληματική δραστηριότητα στον κυβερνοχώρο, παραβιάσεις δεδομένων, μόλυνση με κακόβουλο λογισμικό, ransomware και επιθέσεις κοινωνικής μηχανικής τύπου phishing.

Η κοινωνική μηχανική, είναι η χειραγώγηση και η εξαπάτηση ατόμων για να αποκτήσουν πρόσβαση σε κατά τα άλλα ασφαλή συστήματα και πληροφορίες, έχει γίνει ένας σημαντικός φορέας που θέτει σε κίνδυνο την ασφάλεια στο διαδίκτυο.

Ο στόχος της παρούσας μεταπτυχιακής διατριβής είναι να αναπτύξει εκστρατείες αξιολόγησης και ανάπτυξης ευαισθητοποίησης για την ασφάλεια που μπορούν να προσεγγίσουν, να αξιολογήσουν και να εκπαιδεύσουν με επιτυχία όσο το δυνατόν περισσότερα άτομα, προκειμένου να βελτιώσουν την ανθεκτικότητά τους σε κακόβουλες πρακτικές ηλεκτρονικού εμπορίου.

Ιστορία της κοινωνικής μηχανικής

Η ιστορία της κοινωνικής μηχανικής

Οι άνθρωποι είναι ο πιο αδύναμος κρίκος όσον αφορά την ασφάλεια στον κυβερνοχώρο. Για να εκμεταλλευτούν αυτή την ευπάθεια, πολλοί χάκερ ασχολούνται με την κοινωνική μηχανική για να υποστηρίξουν τις προσπάθειές τους για κυβερνοεπίθεση και να λάβουν πολύτιμες πληροφορίες. Οι κοινωνικοί μηχανικοί στοχεύουν τους ανθρώπους και όχι την τεχνολογία, για να συγκεντρώσουν χρήσιμες πληροφορίες [2] [3].

Το Χόλιγουντ συχνά δοξάζει τον έξυπνο απατεώνα για την ικανότητά του να γοητεύει και να αφοπλίζει. Στην ταινία «Catch Me If You Can», ο Leonardo DiCaprio υποδύεται έναν νεαρό τον Frank Abegnale, έναν διαβόητο απατεώνα, ο οποίος υποδύθηκε το προσωπικό της αεροπορικής εταιρείας, έναν δικηγόρο και διάφορους άλλους ρόλους για να διαπράξει πλαστογραφία επιταγών. Ο Abegnale αργότερα χρησιμοποίησε τα ταλέντα του για να γίνει σύμβουλος ασφαλείας [4].

Η κοινωνική μηχανική φέρνει την απάτη στην ψηφιακή εποχή. Αντί να χρησιμοποιεί προσωπικές αλληλεπιδράσεις για τη δημιουργία σχέσεων και τη γοητεία των χρηστών σε συγκεκριμένες ενέργειες, η κοινωνική μηχανική αξιοποιεί την έλλειψη ευαισθητοποίησης σχετικά με τα ψηφιακά εργαλεία και την προθυμία για κοινή χρήση σε ψηφιακές πλατφόρμες. Το τελικό αποτέλεσμα είναι το ίδιο: ψυχολογική χειραγώγηση που οδηγεί στην παράδοση ευαίσθητων πληροφοριών.

Η πρώτη καταγραφή της Κοινωνικής Μηχανικής είναι η επίθεση με δούρειο ίππο [5]. Στο διάσημο μυθιστόρημα «Η Οδύσσεια» το έτος 1184 π.Χ. οι Τρώες και οι Έλληνες βυθίστηκαν σε έναν μακρύ, φαινομενικά ατέρμονο πόλεμο.

Μετά από 10ετή πολιορκία, οι Έλληνες συνειδητοποίησαν ότι έπρεπε να γίνουν πονηροί για να

νικήσουν τους Τρώες. Κατασκεύασαν ένα γιγάντιο ξύλινο άλογο και έκρυψαν μέρος του στρατού τους μέσα σε αυτό. Οι υπόλοιποι στρατιωτικοί απέπλευσαν, εμφανιζόμενοι ηττημένοι. Οι Τρώες έπεσαν στο κόλπο. σέρνοντας το ξύλινο άγαλμα πέρα από τα προστατευτικά τους εμπόδια ως τρόπαιο για τη νίκη τους που είχε καθυστερήσει εδώ και καιρό.

Αφού έπεσε ο ήλιος και οι Τρώες πήγαν για ύπνο, οι Έλληνες στρατιώτες που περίμεναν μέσα στο άλογο βγήκαν κρυφά έξω και ξεκλείδωσαν τις πύλες γύρω από την πόλη. Οι Έλληνες χρησιμοποίησαν τότε το στοιχείο του αιφνιδιασμού για να καταστρέψουν την πόλη της Τροίας από μέσα, τερματίζοντας επίσημα τον πόλεμο.

Και εκεί βρίσκεται η πρώτη καταγεγραμμένη περίπτωση κοινωνικής μηχανικής.

Κεφάλαιο 1

1 Ανασκόπηση των Τεχνικών Επιθέσεων Ψηφιακού Εμπορίου

Υπάρχουν διαφορετικοί τύποι τεχνικών επιθέσεων ψηφιακού εμπορίου, όπως επιβεβαιώνεται από την ίδια βιβλιογραφία για το θέμα. Υπάρχει μια κοινή προσέγγιση που χωρίζει αυτές τις τεχνικές σε δύο κύριες ομάδες:

1. Πρακτική κοινωνικής μηχανικής
2. Παραπλάνηση στις πρακτικές μάρκετινγκ

1.1 Πρακτική κοινωνικής μηχανικής

Η κοινωνική μηχανική, που ορίζεται ως η πράξη της προφορικής χειραγώγησης ατόμων με σκοπό την απόσπαση πληροφοριών, μαζί και με άλλες τεχνικές «ψαρέματος» γνωστό και ως phishing, εκμεταλλεύονται κατά κύριο λόγο την ανθρώπινη αφέλεια για να υποκλέψουν προσωπικές πληροφορίες, όπως αριθμούς πιστωτικής κάρτας, τραπεζικές πληροφορίες ή αριθμούς πρόσβασης, σε ισοτόπους που μοιάζουν νόμιμοι [2].

Τα άτομα που δεν διαθέτουν τις κατάλληλες γνώσεις και δεξιότητες στην ασφάλεια των πληροφοριών γίνονται εύκολη λεία για τους Hackers και άλλους εγκληματίες στον κυβερνοχώρο. Εξίσου επικίνδυνη θεωρείται η ανεπαρκής χρηστικότητα των κρίσιμων για την ασφάλεια συστημάτων πληροφοριών και του λογισμικού anti-phishing, η οποία εμποδίζει την απόδοση των χρηστών και οδηγεί τους χρήστες σε αμέλεια σχετικά με την ασφάλεια με αποτέλεσμα να υποπίπτουν σε λάθη και παγίδες.

Παραδείγματα επιθέσεων κοινωνικής μηχανικής περιλαμβάνουν το phishing, την πλαστοπροσωπία σε κλήσεις από γραφεία βοήθειας, «καταδύσεις» σε σκουπίδια, κλοπή σημαντικών εγγράφων, ψεύτικο λογισμικό, δόλωμα, pretexting, tailgating, αναδυόμενα παράθυρα, Robocalls, ransomware, online κοινωνική μηχανική, αντίστροφη κοινωνική μηχανική και κοινωνική μηχανική τηλεφώνου [6].

Επίσης, είναι δυνατό να εμπλέκεται κακόβουλη χρήση διαφημίσεων [7] για τη διάδοση κακόβουλου λογισμικού και την απόκτηση προσωπικών πληροφοριών που αφορούν τον πελάτη. Υπάρχουν χιλιάδες έως εκατομμύρια μολυσμένοι ιστότοποι που προβάλλουν εν αγνοία τους κακόβουλες διαφημίσεις ή κακόβουλο λογισμικό που στοχεύει εκατομμύρια ανυποψίαστα θύματα. Αυτή είναι μια από τις μεθόδους διάδοσης κακόβουλου λογισμικού με απόκρυψη και, στη συνέχεια, εκτέλεση κακόβουλου κώδικα μέσα στις κακόβουλες διαφημίσεις. Στη συνέχεια, αυτές οι διαφημίσεις οδηγούν τα ανυποψίαστα θύματα σε μια σελίδα φιλοξενίας εκμετάλλευσης που έχει περιεχόμενο που μολύνει απευθείας τον υπολογιστή του θύματος χωρίς να απαιτείτε καμία επιπρόσθετη ενέργεια από το θύμα και επιτρέπει στον εισβολέα να αποκτήσει απομακρυσμένη πρόσβαση.

Σε αυτή την ομάδα υπάρχουν δύο κύριες στρατηγικές κοινωνικής μηχανικής:

- Τεχνική phishing [8]

Το phishing είναι μια τεχνική κοινωνικής μηχανικής που, μέσω της χρήσης διαφόρων μεθοδολογιών, στόχο έχει να αποκτήσει προσωπικές και εμπιστεύτηκες πληροφορίες, όπως ηλεκτρονική διεύθυνση, όνομα χρήστη, κωδικό πρόσβασης ή οικονομικές και άλλες οποιασδήποτε

χρήσιμες πληροφορίες. Αυτές οι πληροφορίες χρησιμοποιούνται στη συνέχεια από τον εισβολέα εις βάρος του θύματος και οδηγούν σε κλοπή.

- Κακόβουλη διαφήμιση [7]

Ο όρος «κακόβουλη διαφήμιση» επινοήθηκε για πρώτη φορά το 2007 και αναφέρεται στην διαδικτυακή διαφήμιση που στοχεύει στη διάδοση κακόβουλου λογισμικού.

Υπάρχουν δύο κύριοι τύποι επιθέσεων κακόβουλης διαφήμισης [9]:

1. Ενσωμάτωση κώδικα σε διαφήμιση
   Στον πρώτο τύπο, ο εισβολέας ενσωματώνεικώδικα, μέσα στη διαφήμιση, που αναζητά «κενά» σημεία στη συσκευή του χρήστη για να την μολύνει. Αυτή η επίθεση δεν απαιτεί προληπτική δράση από την μεριά του χρήστη.
2. Ενσωμάτωση σύνδεσμου που οδηγεί σε τρίτο ιστότοπο
   Στον δεύτερο τύπο επίθεσης, οι κακόβουλοι διαφημιστές προβάλλουν (ελκυστικές) διαφημίσεις για να πείσουν τον χρήστη να ακολουθήσει έναν σύνδεσμο και να τον προωθήσει σε έναν ιστότοπο που διαχειρίζεται ο κακόβουλος διαφημιζόμενος. Αυτό στην πραγματικότητα μιμείται την ίδια προσέγγιση που χρησιμοποιείται στις επιθέσεις phishing. Μόλις εισέλθει στον ιστότοπο, ο κακόβουλος διαφημιζόμενος μπορεί να αναζητήσει αδυναμίες στη συσκευή του χρήστη και να εγκαταστήσει ένα κακόβουλο λογισμικό ή ακόμη και να πείσει τον χρήστη να κατεβάσει και να εγκαταστήσει κάποιο κακόβουλο λογισμικό ο ίδιος εμφάνιση ενός μηνύματος που υποδεικνύει ότι η συσκευή έχει μολυνθεί και προτείνει την εγκατάσταση ενός λογισμικού που θα καθαρίσει το σύστημα).

   Σε αυτήν την προσέγγιση, ο hacker χρησιμοποιεί μια υπηρεσία φιλοξενίας διαφημίσεων για να φιλοξενήσει μια διαφήμιση που περιέχει κακόβουλο λογισμικό και ενεργοποιείται όταν το θύμα πατήσει πάνω στη διαφήμιση. Αυτό το κακόβουλο λογισμικό μολύνει τη συσκευή του θύματος για να κλέψει προσωπικά δεδομένα και να διοχετεύσει αυτά τα δεδομένα στον hacker.

Υπάρχουν διαφορετικοί τύποι τεχνικών κακόβουλου λογισμικού [10]: Όπως για παράδειγμα το Trojan, το waterholing, το ramsomware, τα αναδυόμενα παράθυρα, το QRishing και το click jacking.

1.2 Παραπλάνηση στις πρακτικές μάρκετινγκ

Η εξαπάτηση θεωρείται ως εγγενής στοιχείο των σύγχρονων δραστηριοτήτων μάρκετινγκ [11]. Η εμφάνιση νέων τεχνολογιών επικοινωνίας και επεξεργασίας δεδομένων προσφέρει στους εμπόρους ολοένα και πιο αποτελεσματικά μέσα εξαπάτησης των στόχων τους και μαζί με την έλευση του ηλεκτρονικού εμπορίου, η δυνατότητα των νέων τεχνολογιών του Διαδικτύου να παραπλανούν ή να εξαπατούν τους καταναλωτές έχει αυξηθεί σημαντικά.

Η εξαπάτηση των καταναλωτών είναι σαφώς μια σημαντική ανησυχία για το ηλεκτρονικό εμπόριο. Ο κύριος στόχος είναι η χειραγώγηση των πελατών με κύριο στόχο την παρακίνηση στην διαδικασία της αγοράς.

Τα μοναδικά χαρακτηριστικά του Διαδικτύου, όπως το ψηφιακό περιβάλλον, τα χαμηλά εμπόδια εισόδου, ο χωρικός/χρονικός διαχωρισμός και η ανωνυμία, το έχουν καταστήσει πρόσφορο έδαφος για εξαπάτηση. Το Διαδίκτυο είναι ένα ψηφιακό περιβάλλον, το οποίο μειώνει την προσπάθεια των διαδικτυακών εταιρειών να δημιουργήσουν και να αλλάξουν περιεχόμενο πληροφοριών καθώς και να χειραγωγήσουν την παρουσίαση και παραγωγή τέτοιου

πληροφοριακού περιεχομένου προκειμένου να επιτύχουν εξαπάτηση [12]. Για παράδειγμα, οι ιστοσελίδες μπορούν να κατασκευαστούν για να προσελκύουν/ αποσπούν την προσοχή, να ενθαρρύνουν ή να αποθαρρύνουν τις διασταυρούμενες συγκρίσεις, να αναγκάζουν επιλογές και να δημιουργούν πίεση για άμεση αγορά.

Η εξαπάτηση στις πρακτικές μάρκετινγκ ενεργοποιείται μέσω διαφορετικών παραπλανητικών στρατηγικών και συνοψίζονται σε τέσσερις κύριες κατηγορίες [13]:

1. Παραπλανητική διαφήμιση (Deceptive advertising)
2. Τύποι παραπλανητικών πρακτικών κοινωνικών δικτύων (Types of deceptive social network practice)
3. Παραπλανητικές πρακτικές πληροφοριών ηλεκτρονικού εμπορίου που σχετίζονται με προϊόντα (Product-related e-commerce deceptive information practices)
4. Τιμολόγηση (Pricing)

1.2.1 Παραπλανητική διαφήμιση (Deceptive advertising)

Η εξαπάτηση εντοπίζεται όταν μια διαφήμιση είναι η εισροή στην αντιληπτική διαδικασία κάποιου κοινού και το αποτέλεσμα αυτής της αντιληπτικής διαδικασίας [14]

a. διαφέρει από την πραγματικότητα της κατάστασης και
b. επηρεάζει την αγοραστική συμπεριφορά εις βάρος του καταναλωτή

Σε αυτήν την κατηγορία μπορούμε να βρούμε: παραπλάνηση λόγω σημασιολογικής σύγχυσης, ασυνείδητο ψέμα, αυθαίρετο ισχυρισμό, αξιώσεις αξιολόγησης διαφήμισης, stealth marketing, greenwashing, ισχυρισμός μισής αλήθειας, υβριδικά μηνύματα, εγγενής διαφήμιση.

1.2.2 Τύποι παραπλανητικών πρακτικών κοινωνικών δικτύων (Types of deceptive social network practice)

Η μεγάλη δημοτικότητα των Διαδικτυακών Κοινωνικών Δικτύων (OSN) [15] και η ευκολία πρόσβασής τους έχει επίσης ως αποτέλεσμα την κακή χρήση των υπηρεσιών τους. Εκτός από το ζήτημα της διατήρησης του απορρήτου των χρηστών, τα OSN αντιμετωπίζουν την πρόκληση της αντιμετώπισης παραπλανητικών χρηστών και των κακόβουλων δραστηριοτήτων τους στο κοινωνικό δίκτυο.

Η πιο κοινή μορφή κακόβουλης δραστηριότητας που εντοπίζεται στα OSN είναι το spamming [16] . Με τον όρο spamming ορίζουμε τους κακόβουλους χρήστες που μεταδίδουν άσχετες πληροφορίες με τη μορφή μηνυμάτων και αναρτήσεων σε όσο το δυνατόν μεγαλύτερο αριθμό νόμιμων χρηστών.

Το spamming γίνεται κυρίως με στόχο την προώθηση προϊόντων, το viral marketing [17], τη διάδοση της μόδας και σε ορισμένες περιπτώσεις μπορεί να γίνει με στόχο την παρενόχληση νόμιμων χρηστών ενός OSN, προκειμένου να μειωθεί η εμπιστοσύνη τους στη συγκεκριμένη υπηρεσία. Σε αντίθεση με τα παραδοσιακά ηλεκτρονικά μηνύματα (emails), όπου το φιλτράρισμα των μηνυμάτων γίνεται με βάση το περιεχόμενο όπου έχει αποδειχθεί πολλά υποσχόμενο στον εντοπισμό των spammers, η εξαπάτηση στα διαδικτυακά κοινωνικά δίκτυα έχει κάνει ένα βήμα μπροστά.

Το φιλτράρισμα ανεπιθύμητων λογαριασμών σε OSN συχνά αντιμετωπίζει προκλήσεις, όπως η

ύπαρξη λεπτής γραμμής μεταξύ του περιεχομένου που μοιράζονται οι νόμιμοι χρήστες και των κακόβουλων λογαριασμών. Επιπλέον, οι παραπλανητικές λογαριασμοί συχνά τείνουν να μιμούνται τη συμπεριφορά νόμιμων χρηστών, γεγονός που καθιστά δύσκολο τον εντοπισμό και την κατηγοριοποίησή τους. Τέλος, η ψεύτικη κριτική θεωρείται κακόβουλη επίθεση μάρκετινγκ στις πρακτικές μάρκετινγκ. Σε αυτή την ενότητα θα παρουσιάσουμε αυτές τις τεχνικές.

Εδώ μπορούμε να βρούμε άλλες τεχνικές όπως: οι ψεύτικες κριτικές, το μάρκετινγκ πολλαπλών επιπέδων, τα κοινωνικά ανεπιθύμητα μηνύματα, το μάρκετινγκ επιρροών και συνεργατών.

1.2.3 Παραπλανητικές πρακτικές πληροφοριών ηλεκτρονικού εμπορίου που σχετίζονται με προϊόντα (Product-related e-commerce deceptive information practices)

Πληροφορίες που σχετίζονται με προϊόντα που προετοιμάζονται από διαδικτυακούς εμπόρους για να παραπλανήσουν τους καταναλωτές προκειμένου να προκαλέσουν επιθυμητές αλλαγές συμπεριφοράς και συμπεριφοράς στους καταναλωτές—αλλαγές που είναι επιζήμιες για τους καταναλωτές και ωφέλιμες για τους εμπόρους [18].

Η χειραγώγηση μάρκετινγκ ασχολείται με τις τακτικές και τις στρατηγικές που χρησιμοποιούνται από τους εμπόρους του μάρκετινγκ που θηρεύουν τις ανθρώπινες γνωστικές, κοινωνικές προκαταλήψεις και που βασίζονται στη μνήμη και επηρεάζουν τελικά τη συμπεριφορά των καταναλωτών υπέρ τους.

Οι ακαδημαϊκοί του μάρκετινγκ διακρίνουν την εξαπάτηση σε τρεις διαφορετικούς τύπους [18]:

- **a.** απόκρυψη — για απόκρυψη, παράλειψη ή συγκάλυψη σχετικών πληροφοριών.
- **b.** αμφιβολία—για την παρουσίαση πληροφοριών αόριστα και/ή διφορούμενα.
- **c.** παραποίηση—για την παρουσίαση ψευδών ή υπερβολικών πληροφοριών.

Οι τεχνικές εξαπάτησης μάρκετινγκ αναφέρονται στην [19]

1. Χειραγώγηση του πληροφοριακού περιεχομένου, που αναφέρεται στην άμεση αλλοίωση του περιεχομένου των πληροφοριών προϊόντων που παρέχονται σε ιστότοπο ηλεκτρονικού εμπορίου.
2. Χειραγώγηση της παρουσίασης πληροφοριών, η οποία αναφέρεται στη χειραγώγηση του σχεδιασμού του τρόπου με τον οποίο οι πληροφορίες προϊόντων παρουσιάζονται στους καταναλωτές σε έναν ιστότοπο ηλεκτρονικού εμπορίου.
3. Χειραγώγηση της παραγωγής πληροφοριών, η οποία αναφέρεται στη χειραγώγηση της δυναμικής παραγωγής πληροφοριών προϊόντων σε έναν ιστότοπο ηλεκτρονικού εμπορίου, με βάση τα ενδιαφέροντα, τις ανάγκες ή/και τις προτιμήσεις των καταναλωτών που λαμβάνονται ρητά ή σιωπηρά.

Εδώ μπορούμε να βρούμε: απόκρυψη με χειραγώγηση περιεχομένου πληροφοριών, απόκρυψη με χειραγώγηση παρουσίασης πληροφοριών, απόκρυψη με χειραγώγηση παραγωγής πληροφοριών, αμφιβολία με χειραγώγηση, παραποίηση με χειραγώγηση.

1.2.4 Τιμολόγηση (Pricing)

Η εξαπάτηση των τιμών μπορεί να συμβεί όταν οι εταιρείες παρέχουν ενδείξεις ψευδούς

επικοινωνίας που υποδεικνύουν ανταγωνιστικές τιμές για να επιτρέψουν την απόκτηση μεγαλύτερης αξιοπιστίας και ισχύος στην αγορά, η οποία μπορεί να οδηγήσει στην ικανότητα των εταιρειών να χρεώνουν υψηλότερες τιμές για προσφορές που περιλαμβάνουν περισσότερα σημάδια από ανυπόστατες προσφορές, αυτό θα αποθάρρυνε τους πιθανούς αγοραστές από περαιτέρω αναζήτηση για περισσότερες επιλογές και αυξάνει την πιθανότητα λήψης απόφασης αγοράς [20].

Μερικές από τις τεχνικές: strikes through pricing, perpetual sales, price anchoring, compare at pricing, drip pricing, προσφορές [13]ς.

Οι επιλεγμένες τεχνικές

Δεν είναι όλες οι τεχνικές που αναφέρονται στο προηγούμενο σημείο κατάλληλες για τα πειράματα. Ορισμένες είναι πολύ επεμβατικές και μπορεί να προκαλέσουν μόνιμες βλάβες στους χρήστες. Ορισμένες απαιτούν μια πολύ περίπλοκη διαδικασία υλοποίησης.

Επιλέγηκαν λοιπόν αυτές που πληρούν τις πιο κάτω απαιτήσεις:

- Σημαντική σε σχέση με τους σκοπούς των πειραμάτων και της εκπαίδευσης
- Ευκαιρία για παρακολούθηση της συμπεριφοράς των καταναλωτών
- Μη επεμβατική
- Εύκολη στην εφαρμογή

Μπορούμε εύκολα να χωρίσουμε τις επιλεγμένες τεχνικές σε 2 ομάδες:

1. Πρακτική κοινωνικής μηχανικής [2]
    - Πρακτικές ηλεκτρονικού ψαρέματος (phishing)
    - Malvertising (QRishing)
2. Παραπλάνηση στις πρακτικές μάρκετινγκ [7]
    - Παραπλανητικές πρακτικές κοινωνικών δικτύων (ψευδείς κριτικές)
    - Πρακτικές παραπλανητικών πληροφοριών που σχετίζονται με το ηλεκτρονικό εμπόριο (equivocation with manipulation)
    - Παραπλανητικές τιμολογιακές πολιτικές (strike through pricing)

Μετά από προβληματισμούς, **αποφασιστικέ** να μην υλοποιηθεί η τεχνική native advertising.

Αυτή η τεχνική κρίθηκε πολύ δύσκολη να παραδοθεί και να επιτευχθούν αποτελέσματα για τους ακόλουθους λόγους:

- Για την προβολή διαφημίσεων θα πρέπει να στοχεύσουμε εκ νέου άτομα που είχαν ήδη εγγραφεί για να συμμετάσχουν και να τα στοχεύσουμε εκ νέου με εγγενείς διαφημίσεις από διάφορα δίκτυα χρησιμοποιώντας δεδομένα pixel από μια σελίδα ευχαριστιών (οι πλήρως νόμιμες εγγραφές εμφανίζονται μόνο σε αυτήν τη σελίδα). Εναλλακτικά θα μπορούσε να γίνει χρήση της ηλεκτρονικής διεύθυνσης με στόχο τα ίδια άτομα. Οι περισσότερες ποιοτικές πλατφόρμες εγγενών διαφημίσεων απαιτούν δεδομένα pixel για εκ νέου στόχευση.

- Αυτό θα απαιτούσε να μην έχει γίνει εκκαθάριση του ιστορικού της προσωρινής μνήμης του προγράμματος περιήγησής τους και να υποθέσουμε ότι το ηλεκτρονική διεύθυνση εγγραφής στο κοινωνικό δίκτυο είναι το ίδιο με αυτό που χρησιμοποιούσαν για να εγγραφούν στα πειράματα.

- Επιπλέον, οι αλγόριθμοι θα είχαν βρει σε μεγάλο βαθμό τις διαφημιστικές μας ανάγκες να προσφέρουν πολύ χαμηλό CTR [21] (και επομένως χαμηλό κέρδος για το διαφημιστικό δίκτυο), καθώς θα υπήρχε μικρή αναγνωσιμότητα επωνυμίας. Επιπρόσθετα μπορεί να είχαμε διαπιστώσει ότι οι διαφημίσεις επισημάνθηκαν ότι είναι προσποιητή απάτη ή ακόμη και να μην επιτρέπονται από την αρχή, καθώς μπορεί να έχουν επηρεάσει τις οδηγίες διαφημίσεων των διαφόρων δικτύων και να έχουν κάνει τα προϊόντα τους να φαίνονται επικίνδυνα (ακόμα και αν είναι ψεύτικη απάτη), καθώς τα δίκτυα διαφημίσεων είναι εξαιρετικά συντηρητικά σε αυτές τις περιοχές για καλό λόγο.

- Ως αποτέλεσμα αυτού, το αναμενόμενο χαμηλό CTR (υποθέτοντας ότι λάβαμε έγκριση) θα σήμαινε ότι από άλλους ανταγωνιστές που εστιάζουν στο κέρδος/ποιότητα θα μείωναν την αποτελεσματικότητα της καμπάνιας σε μεγάλο βαθμό, τα αποτελέσματα της διαφήμισης θα ήταν αμελητέα.

Ως αποτέλεσμα, θεωρήθηκε ότι υπήρχαν πάρα πολλές αρνητικές μεταβλητές για να επικεντρωθούμε στην παροχή αυτής της τεχνικής και του πειράματος.

Κεφάλαιο 2

2.1 Νομικά θέματα και στοχευμένο κοινό

Νομικά ζητήματα

Στο συγκεκριμένο κεφάλαιο γίνεται παράθεση και περιγραφή των νομικών ζητημάτων που σχετίζονται με την παράδοση των εκστρατειών ευαισθητοποίησης για την ασφάλεια. Στόχος αυτής της ενότητας είναι να αποδειχθεί ότι έχουν εντοπιστεί και συζητηθεί όλα τα απαραίτητα νομικά ζητήματα που σχετίζονται με αυτό το θέμα.

Σύνοψη βασικών νομικών πολιτικών και πρακτικών:

Ο στόχος του έργου είναι να αναπτύξει εκστρατείες αξιολόγησης και ανάπτυξης ευαισθητοποίησης για την κυβερνοασφάλεια που μπορούν να προσεγγίσουν, να αξιολογήσουν και να εκπαιδεύσουν με επιτυχία όσο το δυνατόν περισσότερα άτομα, προκειμένου να βελτιώσουν την ανθεκτικότητά τους σε κακόβουλες πρακτικές ηλεκτρονικού εμπορίου.

Έχει γίνει προσπάθεια να διασφαλιστούν οι νομικές και ηθικές απαιτήσεις στην έρευνα, προκειμένου να διασφαλιστεί ότι δεν θίγονται δικαιώματα και συμφέροντα ατόμων και ότι δεν τίθεται σε κίνδυνο το δημόσιο συμφέρον.

Το έργο σχεδιάστηκε με βάση τη θεμελιώδη ηθική της έρευνας και περιλαμβάνει τους ακόλουθους ειδικούς τομείς που σχετίζονται με το έργο:

Βασική απαίτηση	**Ισχύει**	**Λεπτομέρειες των πληροφοριών**	**Σχετικά έγγραφα (και λήψεις)**
Η συμμετοχή στο έργο επιτυγχάνεται με εθελοντικό τρόπο.	Ναι	Είναι εθελοντικής συμμετοχής. Για τον λόγο αυτό έχει χρησιμοποιηθεί συγκεκριμένο λεξιλόγιο για τους επισκέπτες της σελίδας. Παράδειγμα διατύπωσης όταν ο υποψήφιος εθελοντής ξεκινά να διαβάζει την αρχική σελίδα: "Χρειαζόμαστε εθελοντές σαν εσάς για να συμμετάσχουν στο μεγαλύτερο πείραμα της	https://www.becyberaware.eu/ https://www.becyberaware.eu/sign-up/ https://www.becyberaware.eu/terms-and-conditions/

		ΕΕ για να ελέγξουμε τη γενική ευαισθητοποίηση και την ευαισθησία του κοινού σε διαδικτυακές απάτες και έγκλημα στον κυβερνοχώρο στην ΕΕ"	
Έχει ληφθεί ενημερωμένη και γραπτή συγκατάθεση για κάθε ανθρώπινο συμμετέχοντα.	Ναι	Η σελίδα εγγραφής έχει σχεδιαστεί ώστε να είναι σαφής σε σχέση με το τι συναινούν μέσω διατύπωσης με πρόσβαση σε όλα τα σχετικά έγγραφα σχετικά με τα προσωπικά δεδομένα και τις απαιτήσεις συμμετοχής τους με επιπλέον πληροφορίες σε συνδέσμους σε όλο τον ιστότοπο και στην περιοχή του υποσέλιδου. Υπάρχουν 2 τετράγωνα συγκατάθεσης που πρέπει να επιλεγούν για να γίνει αποδεκτή και να προχωρήσει η εγγραφή. Συμφωνώ με την Πολιτική Προστασίας Δεδομένων Συμφωνώ με το Φύλλο Πληροφοριών Συμμετεχόντων	http://becyberaware.eu/static/files/ENSURESEC_BECYBERAWARE_Data_Protection_Policies-1.docx
Δεν έχει παρασχεθεί χρηματική αποζημίωση στους συμμετέχοντες.	Ναι	Η προσφορά «συμπληρωματικής» εκπαίδευσης για την ασφάλεια στον κυβερνοχώρο δεν έχει χρηματική αξία για τους συμμετέχοντες.	
Το δικαίωμα απόσυρσης από την πιλοτική μελέτη έχει εξηγηθεί στους συμμετέχοντες.	Ναι	Όλα τα δεδομένα υποβάλλονται σε επεξεργασία σύμφωνα με τους νόμους GDPR της ΕΕ και διαγράφονται πλήρως κατόπιν αιτήματος.	
Τα κριτήρια συμετοχίς που ορίζονται έχουν	Ναι	Έχουν στοχεύει μόνο πολίτες της ΕΕ	

τηρηθεί.			
Στο έργο δεν συμμετέχουν ανήλικοι.	Ναι	Αυτό είναι η απαιτούμενο πεδίο της αρχικής σελίδας εγγραφής, κανένας κάτω των 18 δεν θα επιτρέπεται να λάβει μέρος στο έργο	https://www.becyberaware.eu/sign-up/
Οι νόμοι και οι απαιτήσεις περί προστασίας δεδομένων τηρούνται κατά την επεξεργασία ή τη συλλογή προσωπικών δεδομένων.	Ναι	Δεν συλλέχτηκαν προσωπικά ονόματα ή ταυτότητες όπως επίσηςδεν συλλέχτηκαν διευθύνσεις IP ή οποιεσδήποτε ηχογραφήσεις συμμετεχόντων. Ως επίσης, δεν μοιραζόμαστε, μεταγλωττίζουμε ή συγχωνεύουμε δεδομένα ή συνδυάζουμε τα δεδομένα.	
Δεν γίνεται περαιτέρω επεξεργασία προσωπικών δεδομένων που έχουν συλλεχθεί προηγουμένως (δευτερεύουσα χρήση).	Ναι	Δεν συλλέχτηκαν ονόματα ή αναγνωριστικά και δεν συλλέχτηκαν διευθύνσεις IP των συμμετεχόντων.	
Δεν πραγματοποιείται μεταφορά προσωπικών δεδομένων σε τρίτες χώρες.	Ναι	Όλα τα δεδομένα διατηρούνται υπό τον έλεγχο του Υπεύθυνου Επεξεργασίας Δεδομένων	
Θεσπίζονται μέτρα ανωνυμίας και εμπιστευτικότητας	Ναι	Καθώς δεν συλλέγουμε προσωπικά ονόματα, η μόνη αναγνώριση που έχουμε είναι από μια ηλεκτρονική διεύθυνση (email) που ικανοποιεί την απαίτηση της ανωνυμίας και της εμπιστευτικότητας	

2.2 Πώς το έργο επεξεργάζεται προσωπικά δεδομένα

Νομικής βάσης

Η νομική βάση για την επεξεργασία των προσωπικών δεδομένων για αυτήν την έρευνα είναι σύμφωνα με το άρθρο 6 παράγραφος 1 του GDPR [22]. Καθώς η συμμετοχή στην μελέτη είναι εντελώς εθελοντική, βασιζόμαστε στη συγκατάθεσή των χριστών για την επεξεργασία των

προσωπικών τους δεδομένων. Σύμφωνα με το άρθ. 7(3) του GDPR, έχουν το δικαίωμα να αποσύρουν τη συγκατάθεσή τους ανά πάσα στιγμή.

Μερικές πληροφορίες για την πολιτική του έργου και για τους τρόπους επεξεργασίας των προσωπικών δεδομένων.

Η επεξεργασία προσωπικών πληροφοριών για τους σκοπούς της παρούσας έρευνας συνεπάγεται ότι λαμβάνονται ορισμένες δικλείδες ασφαλείας για την προστασία των δεδομένων των ατόμων που συμμετείχαν. Για να γίνει αυτό, οι εταίροι του έργου ENSURESEC ξεκινούν κάθε επεξεργασία προσωπικών δεδομένων ακολουθώντας αυτές τις αρχές:

1. **Δικαιοσύνη και νομιμότητα** [23]. Τα προσωπικά δεδομένα υφίστανται δίκαιη επεξεργασία και για τους σκοπούς για τους οποίους συλλέχθηκαν αρχικά. Επιπλέον, οι εργασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα αξιολογούνται ως προς τη νομιμότητα τους από τον συντονιστή του έργου.
2. **Ασφάλεια επεξεργασίας** [24]. Οι εργασίες επεξεργασίας προσωπικών δεδομένων διενεργούνται σύμφωνα με τα διαθέσιμα μέτρα ασφαλείας, τόσο τεχνικά όσο και οργανωτικά. Για παράδειγμα, τα περιβάλλοντα ελέγχου πρόσβασης και ελέγχου ταυτότητας εφαρμόζονται στην πρόσβαση σε σύνολα δεδομένων που περιέχουν προσωπικά δεδομένα και η αρχή της ανάγκης γνώσης εφαρμόζεται στον έλεγχο οποιουδήποτε ερευνητή που εμπλέκεται στη λειτουργία επεξεργασίας προσωπικών δεδομένων.
3. **Minimization** [25]. Η συλλογή και η επεξεργασία προσωπικών δεδομένων, ακολουθεί την αρχή της ελαχιστοποίησης των δεδομένων. Αυτό σημαίνει, για παράδειγμα, τη συλλογή των δεδομένων με τρόπο που να υποβάλλεται σε επεξεργασία μόνο το αυστηρά απαραίτητο ποσό τους. Επιπλέον, όποτε χρειαστούν προσωπικά στοιχεία, θα γίνεται με ψευδώνυμα.
4. **Μη αποκάλυψη σε τρίτους** [26]. Δεν θα γνωστοποιηθούν προσωπικά δεδομένα σε τρίτους (δηλαδή οντότητες που δεν ανήκουν στην κοινοπραξία του έργου), εκτός εάν υπάρχει ρητή εξουσιοδότηση για κάτι τέτοιο από το ενδιαφερόμενο άτομο ή συμβατική υποχρέωση που πρέπει να εκπληρωθεί για λόγους ελέγχου.
5. **Η μακροπρόθεσμη ταυτοποίηση δεν είναι στόχος.** Δεν εμπίπτει στους σκοπούς αυτού του έργου η διατήρηση προσωπικών δεδομένων για μεγάλες περιόδους και η συγκέντρωση τέτοιων δεδομένων για ταυτοποίησή. Όταν τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία για τα τελικά αποτελέσματα της έρευνας, αυτά τα σύνολα θα λειτουργούν ως επί το πλείστων κατά τη διάρκεια της δοκιμής και θα διαγράφονται αμέσως μετά, εκτός εάν αναφέρεται διαφορετικά.
6. **Ακρίβεια**. Το έργο εξετάζει τακτικά σύνολα δεδομένων όπου αποθηκεύονται προσωπικά δεδομένα, προκειμένου να διασφαλίσει την ακρίβεια και την αξιοπιστία των πληροφοριών σε αυτά. Υπάρχουν συστήματα ενημέρωσης των πληροφοριών ώστε να διασφαλίζεται τόσο η ασφάλεια όσο και η ελεγχόμενη πρόσβαση στα σύνολα δεδομένων.

Για πόσο καιρό θα διατηρούμε τα δεδομένα;

Εάν δεν υπάρξει άμεση διαγραφή, αυτό σημαίνει ότι υπάρχει νομική υποχρέωση ή/και ερευνητικό σκοπό να αρχειοθετηθούν τα δεδομένα είτε για συμβατικούς λόγους είτε για σκοπούς επιστημονικής έρευνας. Σε αυτήν την περίπτωση, θα διατηρηθουν τα εν λόγω προσωπικά δεδομένα για το μέγιστο διάστημα 1 έτους μετά τον τερματισμό του έργου, εκτός εάν υποδεικνύεται ή ζητηθεί διαφορετικά από μια εποπτική αρχή ή για σκοπούς ελέγχου.

2.2 Επιλογή κοινού

Προσωπικός παράγοντας που εξαρτάται από το πλαίσιο

2.2.1 Πληροφορίες ασυμμετρίας

Οι ασύμμετρες πληροφορίες [27] είναι μια κατάσταση όπου ένα μέρος έχει ή θα έχει μεγαλύτερο επίπεδο γνώσης σε σχέση με ένα άλλο μέρος σχετικά με τα δικά του χαρακτηριστικά ή ενέργειες.

Η ασυμμετρία των πληροφοριών σε οικονομικές συνθήκες δημιουργεί ανισορροπίες ισχύος και, δεδομένου ότι οι διαδικτυακές τεχνολογίες διευκολύνουν τις επιχειρήσεις να συλλέγουν περισσότερες πληροφορίες σχετικά με τους καταναλωτές, οι επιχειρήσεις μπορούν στη συνέχεια να χρησιμοποιήσουν αυτές τις πληροφορίες προς όφελός τους

Στην περίπτωση των διαδικτυακών αγορών, αυτό μπορεί να οδηγήσει σε αυξημένες περιπτώσεις εξαπάτησης στο μάρκετινγκ, όπως απόκρυψη με χειραγώγηση/παραποίηση παρουσίασης πληροφοριών. Συμβαίνει επίσης με παραπλανητικές πολιτικές τιμολόγησης, όπως οι διακρίσεις τιμών. Το παραπλανητικό μάρκετινγκ μπορεί να επωφεληθεί από εκτενείς πληροφορίες που συλλέγονται στο διαδίκτυο για τους πελάτες και έτσι να συμβάλει στην κερδοφορία των υπηρεσιών ηλεκτρονικού εμπορίου.

2.2.1 Επίπεδο χρήσης του Διαδικτύου

Αριθμός χρήσης του Διαδικτύου και συχνότητα χρήσης του Διαδικτύου.

Η ένταση της χρήσης του Διαδικτύου υπολογίζεται συνδυάζοντας τη συχνότητα χρήσης του Διαδικτύου με τις ώρες που δαπανώνται στο Διαδίκτυο [28]. Αυτό παρέχει μια πιο λεπτή μέτρηση του τρόπου με τον οποίο τα άτομα χρησιμοποιούν το Διαδίκτυο, διαφοροποιώντας αυτά που είναι χρήστες υψηλής συχνότητας και μεγάλης διάρκειας, και εκείνων που είναι λιγότερο έντονοι χρήστες, είτε συνδέονται λιγότερο συχνά είτε/και περνούν λιγότερο χρόνο στο διαδίκτυο. Για τους σκοπούς αυτής της μελέτης, ως χρήστης υψηλής έντασης ορίζεται αυτός που είναι συνδεδεμένος για 5 ή περισσότερες ώρες την εβδομάδα από το σπίτι και χρησιμοποιεί το Διαδίκτυο καθημερινά. Αντίθετα, ως χρήστης χαμηλής έντασης ορίζεται ο οικιακός χρήστης του Διαδικτύου που είτε δεν χρησιμοποιεί το Διαδίκτυο καθημερινά είτε είναι συνδεδεμένος για λιγότερο από 5 ώρες την εβδομάδα. Ο συνδυασμός δεδομένων ταχύτητας και έντασης παράγει τέσσερις τύπους χρηστών (Χρήστης χαμηλής ταχύτητας χαμηλής έντασης, χρήστης χαμηλής ταχύτητας υψηλής έντασης, χρήστης υψηλής ταχύτητας χαμηλής έντασης, χρήστης υψηλής ταχύτητας υψηλής έντασης).

Βρέθηκαν σημαντικές διαφορές μεταξύ συχνών και μη συχνών χρηστών στην επίγνωση κινδύνου [29], των πρακτικών κωδικού πρόσβασης, του εφέ κακόβουλου λογισμικού, της ευαισθητοποίησης για το phishing και της μετάδοσης ιών. Όσον αφορά τη συνειδητοποίηση κινδύνου, οι συχνοί χρήστες φαίνεται να είναι πιο ενημερωμένοι. Αυτό φαίνεται να είναι διαισθητικό, ίσως με βάση το γεγονός ότι οι συχνοί χρήστες είναι περισσότερο συνδεδεμένοι στο διαδίκτυο και, ως εκ τούτου, μπορεί να είναι πιο εξοικειωμένοι με τους διάφορους κινδύνους που ενέχει το κακόβουλο λογισμικό. Σε αντίθεση με ό,τι θα περίμενε κανείς, οι μη συχνοί χρήστες έχουν υψηλότερη βαθμολογία όσον αφορά τις πρακτικές κωδικών πρόσβασης. Αν και ένας λόγος μπορεί να είναι ότι οι μη συχνοί χρήστες είναι γενικά πιο προσεκτικοί με συστήματα και ιστότοπους που απαιτούν κωδικούς πρόσβασης.

2.2.3 Ικανότητες καταναλωτή

Η ικανότητα του καταναλωτή ορίζεται ως η γνώση για τα προϊόντα [30] (π.χ. τιμές, ποιότητα και

μέθοδοι παραγωγής), σε συνδυασμό με την εξοικείωση και τη γνώση του τρόπου λειτουργίας των αγορών. Από αυτή την άποψη, η εξοικείωση και η γνώση λόγω προηγούμενων εμπειριών των καταναλωτών, καθώς και η ενεργή συλλογή πληροφοριών, θεωρούνται σημαντικές για την ικανότητα των καταναλωτών [30]. Η ενημέρωση για συγκεκριμένες αγορές αντιμετωπίζεται ως δείκτης της ικανότητας του καταναλωτή. Η ικανότητα των καταναλωτών δεν εξαρτάται μόνο από τη διαθεσιμότητα επαρκών πληροφοριών, αλλά και από την προθυμία, την ικανότητα και τα κίνητρα των καταναλωτών να αναζητήσουν και να αποκτήσουν ενημερωμένες πληροφορίες.

2.2.4 Έλλειψη προσωπικού ελέγχου

Όταν οι καταναλωτές αδυνατούν να ελέγξουν την προσοχή, τη συμπεριφορά ή τα συναισθήματά τους, τότε οι συμπεριφορά τους είναι πέρα από τον έλεγχό τους [31]. Η έλλειψη προσωπικού ελέγχου θεωρείται ως κύριο συστατικό στο να νιώθουν ευάλωτη. Όταν οι καταναλωτές εμπλέκονται σε συμπεριφορές που έχουν επιλέξει να συμμετάσχουν, οι συμπεριφορές και οι στάσεις τους είναι εθελοντικές και υπό τον έλεγχό τους.

2.2.5 Εμπειρία αγορών μέσω Διαδικτύου

Η εμπειρία ενός καταναλωτή στο Διαδίκτυο αναφέρεται στην εμπειρία απόκτησης δεξιοτήτων ή γνώσεων από την πρακτική. Σύμφωνα με τα χαρακτηριστικά του ηλεκτρονικού εμπορίου, αυτή η εργασία θα ορίσει την εμπειρία του Διαδικτύου για τους καταναλωτές ως την έκταση εξοικείωσης των συναλλαγών ηλεκτρονικού εμπορίου, μετά τις συναλλαγές ηλεκτρονικού εμπορίου, οι καταναλωτές στη διαδικασία αγοράς, στην αναζήτηση πληροφοριών προϊόντος και άλλες πτυχές έχουν κάποια εξοικείωση. Η έρευνα του Luhmann [32] δείχνει ότι οι εμπειρίες αγορών μπορούν να μειώσουν τον κίνδυνο που αντιλαμβάνονται οι καταναλωτές. Οι εμπειρίες μπορούν να βοηθήσουν τους καταναλωτές να εξοικειωθούν με τη λειτουργία, έτσι ώστε η αβεβαιότητα για τις αγορές, η πολυπλοκότητα της εμφάνισης της σελίδας και άλλοι παράγοντες να μειώνονται σημαντικά.

Τα άτομα είναι λιγότερο πιθανό να αισθάνονται ότι οι εταιρείες θα συμμετάσχουν σε παραπλανητικές πρακτικές μάρκετινγκ, όταν πραγματοποιούν αγορές μέσω Διαδικτύου (σε αντίθεση με τις παραδοσιακές αγορές) [33]. Οι άνθρωποι μπορεί επίσης να αισθάνονται λιγότερο καχύποπτοι προς τις εταιρείες όταν πραγματοποιούν αγορές μέσω Διαδικτύου, επειδή ενώ αισθάνονται προσωπικά περισσότερο εμπλεκόμενοι στην εμπειρία αγορών τους, αισθάνονται επίσης ότι οι εταιρείες συμμετέχουν λιγότερο. Οι ηλεκτρονικές αγορές υποτίθεται ότι ωφελούν τους καταναλωτές, καθώς φαίνεται να δίνει στους καταναλωτές περισσότερες ευκαιρίες να αναλάβουν πρωτοβουλίες στη διαδικασία αγορών και να έχουν τα αποτελέσματα που θέλουν. Ακόμη, ορισμένα χαρακτηριστικά του διαδικτυακού εμπορίου (π.χ. πρόσβαση σε κριτικές καταναλωτών) κάνουν τους ανθρώπους να αισθάνονται πιο σίγουροι για την ικανότητά τους να επιτύχουν προσωπικούς στόχους όταν ψωνίζουν. Η εξαπάτηση και η χειραγώγηση μπορούν να παραμείνουν κρυφές σε περιβάλλοντα αγορών στο διαδίκτυο επειδή τα κύρια στοιχεία που σηματοδοτούν τη χειραγώγηση και την εξαπάτηση συχνά συναντώνται μέσω ανθρώπινων αλληλεπιδράσεων.

2.2.6 Εμπειρία εξαπάτησης

Η εμπειρία εξαπάτησης ενός καταναλωτή αναφέρεται στον βαθμό εξοικείωσης του καταναλωτή με τις μεθόδους χειραγώγησης της οντότητας που πουλάει το προϊόν [33].

2.2.7 Γνώση προϊόντος

Είναι μια δεξιότητα όπου οι πελάτες κατανοούν πλήρως και μπορούν να επικοινωνούν αποτελεσματικά με άλλους πελάτες σχετικά με το προϊόν, τα χαρακτηριστικά, τα οφέλη και τις. Όταν αγοράζουν ένα προϊόν, οι πελάτες δεν γνωρίζουν πάντα τα χαρακτηριστικά των προϊόντων

ή παρόμοιων προϊόντων άλλων εμπορικών εταιριών.

2.2.7 Δυνατότητα αγοράς

Αναφέρεται στη διάθεση του προϋπολογισμού του αγοραστή και επηρεάζει τη δυνατότητα να πάρει αυτό που πραγματικά θέλει. Όταν αγοράζουν ένα προϊόν, οι πελάτες συχνά αντιλαμβάνονται ότι υπάρχουν πολύ λίγες επιλογές στο πλαίσιο των δυνατοτήτων τους [34] με ικανότητα αγοράς με το ακόλουθο χαρακτηριστικό: αγοράζουν ένα προϊόν που είναι παρόμοιο με αυτό που θέλουν σε χαμηλότερη τιμή.

2.3 Δημογραφικά χαρακτηριστικά

2.3.1 Γένος

Το φύλο είναι ένας παράγοντας για την ευπάθεια των καταναλωτών σε ψευδείς ή παραπλανητικές διαφημίσεις. Δεν φαίνεται να είναι σημαντικός παράγοντας ευπάθειας στις επιθέσεις phishing [35].

2.3.1 Αναλφαβητισμός/Ελλειψη γνώσης

Αφορά το επίπεδο εκπαίδευσης του ατόμου.
Οι μορφωμένοι καταναλωτές μπορεί να καταλαβαίνουν καλύτερα από τους αναλφάβητους καταναλωτές σε τεχνικές πληροφορίες για τα προϊόντα που αγοράζουν. Επιπλέον, οι μορφωμένοι καταναλωτές μπορεί να είναι καλύτεροι στην κριτική σκέψη, μαθαίνοντας να σταθμίζουν τα πλεονεκτήματα και τα μειονεκτήματα κάθε μάρκας. Μπορούν επίσης να κάνουν πιο αιτιολογημένες επιλογές με βάση τα χαρακτηριστικά που είναι σημαντικά για αυτούς, παρά με βάση τους ισχυρισμούς που διατυπώνονται από έναν διαφημιζόμενο προϊόν. Για αυτούς τους λόγους, οι παραπλανητικές τακτικές μάρκετινγκ μπορεί να απευθύνονται σε λιγότερο μορφωμένους ή αναλφάβητους καταναλωτές. Οι καταναλωτές χαμηλού επίπεδου εκπαίδευσης δείχνουν ελλείμματα στην κατανόηση όταν αντιμετωπίζουν παραπλανητικά ερεθίσματα, τα οποία θα μπορούσαν να τους κάνουν πιο πιθανό να γίνουν θύματα [36].

2.3.2 Εισόδημα/ κοινωνικοοικονομική κατάσταση

Το άθροισμα όλων των μισθών, ημερομισθίων, κερδών, τόκων, ενοικίων και άλλων μορφών αποδοχών που λαμβάνονται σε κάθε περίπτωση, σε μια συγκεκριμένη περίοδο. Αυτός ο παράγοντας θεωρείται ένας άλλος παράγοντας ευπάθειας. Οι φτωχοί συνήθως αντιμετωπίζουν κοινωνική ανισότητα και δεν έχουν αρκετή δύναμη να ξεφύγουν από τις ασύμμετρες σχέσεις ανταλλαγής [37].

2.3.3 Φυσική κατάσταση

Άτομα με μειωμένη ικανότητα να προβλέπουν, να αντιμετωπίζουν, να αντιστέκονται και να ανακάμπτουν από τις επιπτώσεις φυσικών ή ανθρωπογενών κινδύνων επειδή είναι σωματικά ευάλωτα [38].

2.3.4 Κουλτούρα

Οι συνήθεις πεποιθήσεις, κοινωνικές μορφές και υλικά χαρακτηριστικά μιας φυλετικής,

θρησκευτικής ή κοινωνικής ομάδας. Αποδεικνύεται ότι ο πολιτισμός μπορεί να είναι παράγοντας ευπάθειας. Οι εθνοτικές και φυλετικές μειονότητες και όσοι έχουν γλωσσικά προβλήματα «μπορούν να γίνουν θύματα παραπλανητικών επιθέσεων και υπό αυτή την έννοια μπορεί να είναι ευάλωτοι καταναλωτές.

2.3.5 Ηλικία

Ορισμένες πληθυσμιακές ομάδες (όπως παιδιά, ηλικιωμένοι) μπορεί να είναι ευάλωτοι και στη συνέχεια, θα μπορούσαν να κινδυνεύουν περισσότερο από χειραγώγηση και εξαπάτηση, επειδή μπορεί να μην αναγνωρίζουν πώς οι εταιρείες προσπαθούν να επηρεάσουν τη συμπεριφορά τους. Για παράδειγμα, τα περισσότερα παιδιά δεν αναγνωρίζουν την πρόθεση μιας εταιρείας στη διαφήμιση, επομένως εκδηλώνουν εσφαλμένη κατανόηση και μη σκεπτικιστική στάση απέναντι στις διαφημίσεις. Για τους ηλικιωμένους, το συνεχώς μεταβαλλόμενο περιβάλλον αγορών έχει καταστήσει δύσκολη την αναζήτηση και την αξιολόγηση πληροφοριών, αναγκάζοντάς τους έτσι να λαμβάνουν αποφάσεις χρησιμοποιώντας περιφερειακές ενδείξεις, όπως προσκλήσεις απευθείας αλληλογραφίας και τηλεμάρκετινγκ [39].

2.4 Ψυχολογική / Ατομική κατάσταση

2.4.1 Ντροπαλότητα και Εσωστρέφεια

Η ντροπαλότητα περιλαμβάνει τον φόβο της αρνητικής αξιολόγησης (και είναι μια πιο ήπια μορφή κοινωνικού άγχους), ενώ η εσωστρέφεια αναφέρεται σε μια τάση για υπερδιέγερση και στην ανάγκη να μείνεις μόνος για να κερδίσεις ενέργεια. Τα ντροπαλά ή πολύ εσωστρεφή άτομα ενδέχεται να είναι λιγότερο πιθανό να αμφισβητήσουν μια ασυμφωνία μεταξύ μιας ετικέτας πώλησης και της τιμής που χρεώνεται στον λογαριασμό ή να διαμαρτυρηθούν για την ανάρτηση ειδοποιήσεων πώλησης πολύ μετά τη λήξη της πώλησης [40].

2.4.2 Διάθεση εμπιστοσύνης

Η διάθεση του καταναλωτή στην εμπιστοσύνη αναφέρεται στα μεμονωμένα χαρακτηριστικά ενός πελάτη που οδηγούν σε προσδοκίες σχετικά με την αξιοπιστία. Η διάθεση του καταναλωτή να εμπιστεύεται είναι μια γενική τάση να επιδεικνύει πίστη και να υιοθετεί μια στάση εμπιστοσύνης προς τους άλλους [34].

2.4.3 Αδυναμία

Κατάσταση ανικανότητας που προκύπτει από ανισορροπία στις αλληλεπιδράσεις στην αγορά ή από την κατανάλωση μηνυμάτων και προϊόντων μάρκετινγκ [34].

2.5 Εξωτερικοί παράγοντες

2.5.1 Προώθηση προϊόντων

Είναι η στάση αγοράς προϊόντων με βάση τις συστάσεις της διαφήμισης. Ο καταναλωτής επηρεάζεται να αγοράσει το προϊόν με βάση τα χαρακτηριστικά πληροφοριών και τη μαρτυρία που χρησιμοποιούνται στην επικοινωνία στα μέσα μαζικής ενημέρωσης [34].

2.5.2 Κοινωνική πίεση

Είναι η άμεση επιρροή στους ανθρώπους από τους συνομηλίκους τους ή η επίδραση σε ένα άτομο που ενθαρρύνεται να ακολουθήσει τους συνομηλίκους του αλλάζοντας τις στάσεις, τις αξίες ή τις συμπεριφορές τους για να συμμορφωθούν με αυτές της ομάδας ή του ατόμου που επηρεάζει [34].

2.5.3 Πολιτική επιστροφής

Είναι μια πολιτική που υπαγορεύει τους όρους τυχόν επιστροφών χρημάτων ή επιστροφών που μπορεί να προσφέρονται από τον ιστότοπο ή το κατάστημα ηλεκτρονικού εμπορίου. Πριν γίνει μια αγορά, ο πελάτης μπορεί να αποφασίσει να ελέγξει την πολιτική επιστροφής χρημάτων ενός συγκεκριμένου ιστότοπου ή καταστήματος για να βεβαιωθεί ότι είναι ικανοποιημένος με τους όρους.Η πολιτική επιστροφής χρημάτων μπορεί να θεωρηθεί μια διάσταση της ευπάθειας των πελατών, επειδή θεωρείται ως ένας εξωτερικός παράγοντας που μπορεί να τονώσει ή να δελεάσει και να τους οδηγήσει σε αποφάσεις επιζήμιες για τους ίδιους [34].

2.5.4 Μάρκετινγκ και συναισθηματική πίεση

Είναι ο βαθμός στον οποίο οι καταναλωτές μπορούν να επηρεαστούν από τις τεχνικές μάρκετινγκ της πειθούς [34].

2.5.5 Συμφραζόμενα

Αναφέρεται στην ικανότητα ορισμένων πλαισίων να επηρεάζουν ορισμένους καταναλωτές να λαμβάνουν αποφάσεις μέσω της ενεργοποίησης στερεοτύπων. Σε ορισμένα πλαίσια (π.χ. όταν οι γυναίκες καταναλωτές ψωνίζουν για αυτοκίνητα), η ενεργοποίηση των στερεοτύπων κάνει τους καταναλωτές πιο ευαίσθητους στις τακτικές πωλήσεων, κάτι που μπορεί στη συνέχεια να επηρεάσει αρνητικά τις προθέσεις αγοράς [33].

2.5.6 Κοινωνικά προβλήματα

Αναφέρεται στην ποικιλία των εξωτερικών παραγόντων που μπορεί να επηρεάσουν την καθημερινή ζωή των καταναλωτών που είναι πέρα από τον έλεγχό τους. Αυτοί οι εξωτερικοί παράγοντες συμβάλλουν σε ανισορροπίες δυνάμεων που δεν ευνοούν τους καταναλωτές. Εξωτερικοί παράγοντες όπως δομικά ή κοινωνικά προβλήματα είναι πέρα από τον έλεγχο των ατόμων και συμβάλλουν στον επηρεασμό της διαδικασίας λήψης αποφάσεων.

Κεφάλαιο 3

3.1 Σχεδιασμός καμπάνιας

3.1.1 Τεχνική επίθεσης Phishing

Οι επιθέσεις phishing είναι οι πιο συνηθισμένες επιθέσεις που πραγματοποιούνται από του hackers. Αυτές οι επιθέσεις, που υπάρχουν εδώ και αρκετές δεκαετίες και συνεχίζουν να αποτελούν μείζον πρόβλημα σήμερα, αποτελούν σοβαρή απειλή στον κόσμο του κυβερνοχώρου [41].

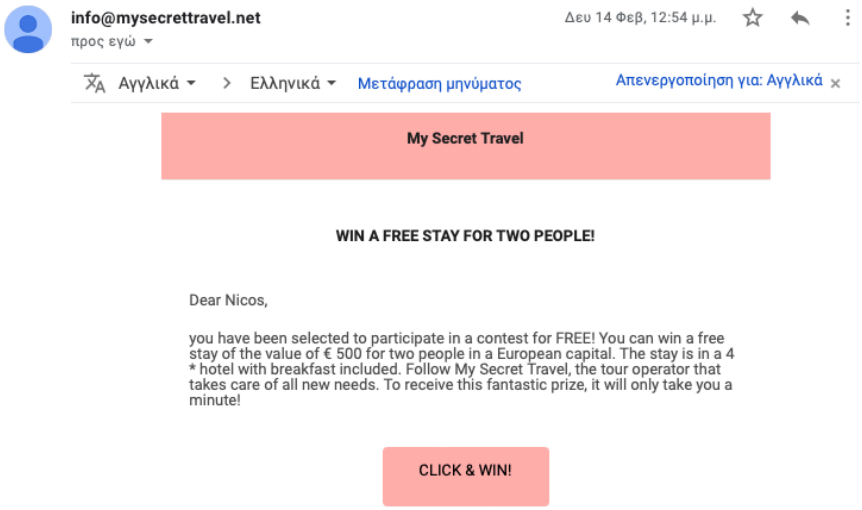
Το phishing είναι μια τεχνική κοινωνικής μηχανικής που, μέσω της χρήσης διαφόρων μεθοδολογιών, στοχεύει να επηρεάσει τον στόχο της επίθεσης για να αποκαλύψει προσωπικές πληροφορίες, όπως διεύθυνση email, όνομα χρήστη, κωδικό πρόσβασης ή οικονομικές πληροφορίες. Αυτές οι πληροφορίες χρησιμοποιούνται στη συνέχεια από τον εισβολέα εις βάρος του θύματος. Στοχεύουν στη δόλια απόκτηση προσωπικών και εμπιστευτικών πληροφοριών από επιδιωκόμενους στόχους μέσω τηλεφωνικών κλήσεων ή email. Οι επιτιθέμενοι παραπλανούν τα θύματα για να αποκτήσουν ευαίσθητες και εμπιστευτικές πληροφορίες [42].

Οι επιτιθέμενοι υιοθετούν πολλαπλές νέες και δημιουργικές μεθόδους μέσω των οποίων διεξάγουν επιθέσεις phishing, οι οποίες αυξάνονται ραγδαία. Επομένως, σε αυτή την ενότητα, παρουσιάζεται μια ανασκόπηση των τεχνικών των επιθέσεων phishing. Αυτή η ενότητα περιλαμβάνει μια ολοκληρωμένη εξέταση των χαρακτηριστικών των υφιστάμενων κλασικών, σύγχρονων και προηγμένων τεχνικών επίθεσης phishing.

Κανάλια: E-Mail

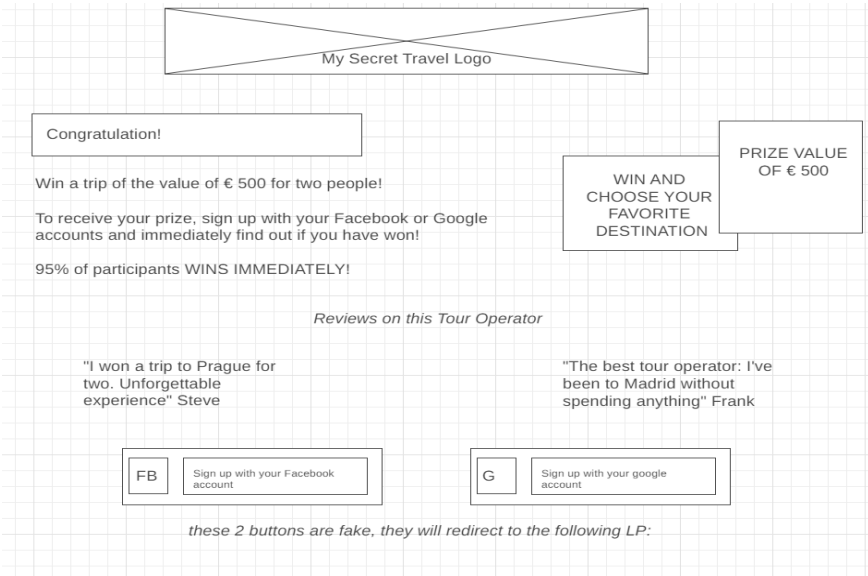
Μηχανισμός Παράδοσης: οι χρήστες θα λάβουν ένα ταξιδιωτικό ηλεκτρονικό μήνυμα ηλεκτρονικού ψαρέματος (Εικόνα 1), είναι ελκυστικό για χρήστες που μπορεί να ενδιαφέρονται για την ιδέα να κερδίσουν ένα ταξίδι. Θα στείλουμε ένα email ζητώντας από τους χρήστες να συμμετάσχουν σε έναν διαγωνισμό για να κερδίσουν ένα ταξίδι (Εικόνα 2).

Εικόνα 1:Προσχέδιο προσομοίωσης phishing email

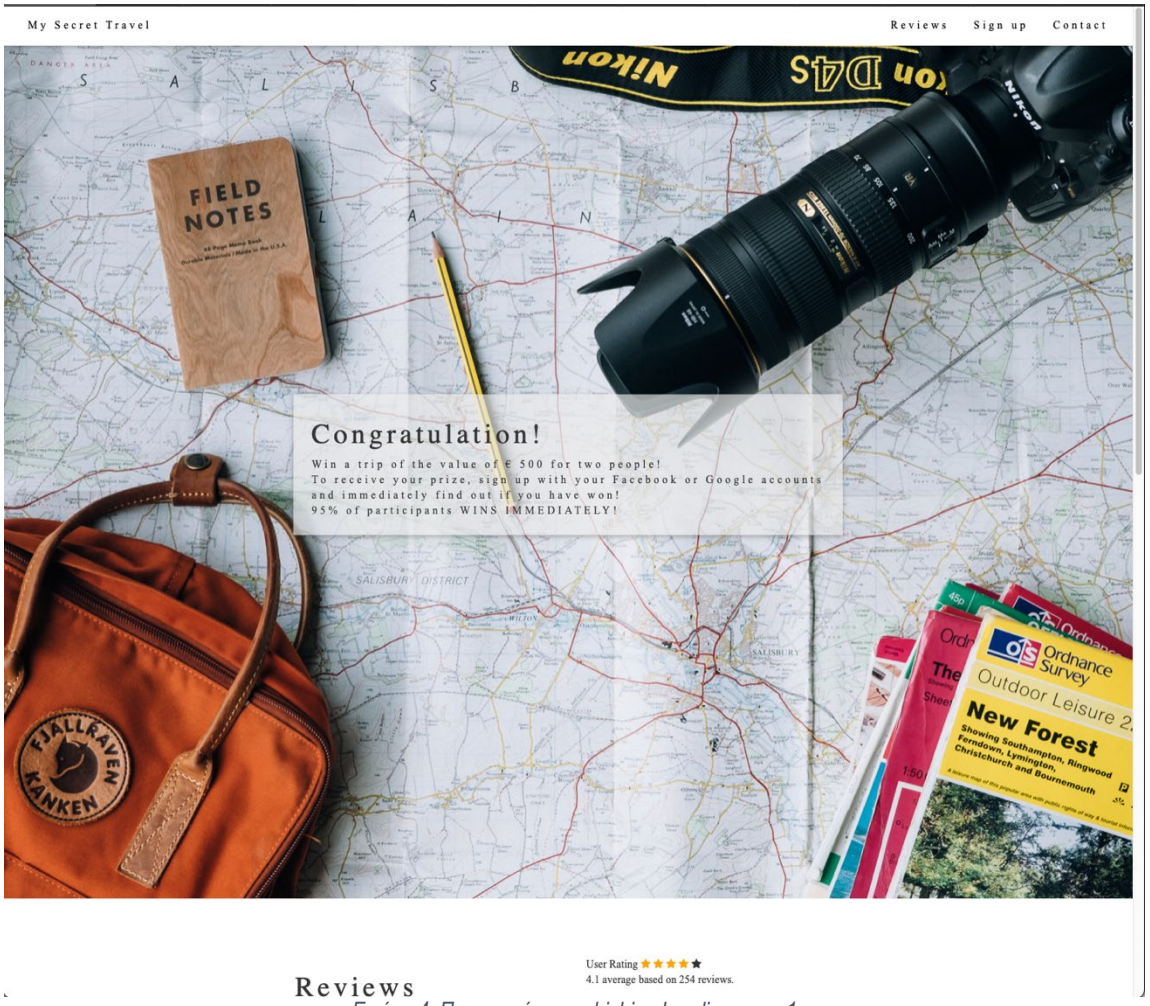


Εικόνα 2:Email προσομοίωσης phishing

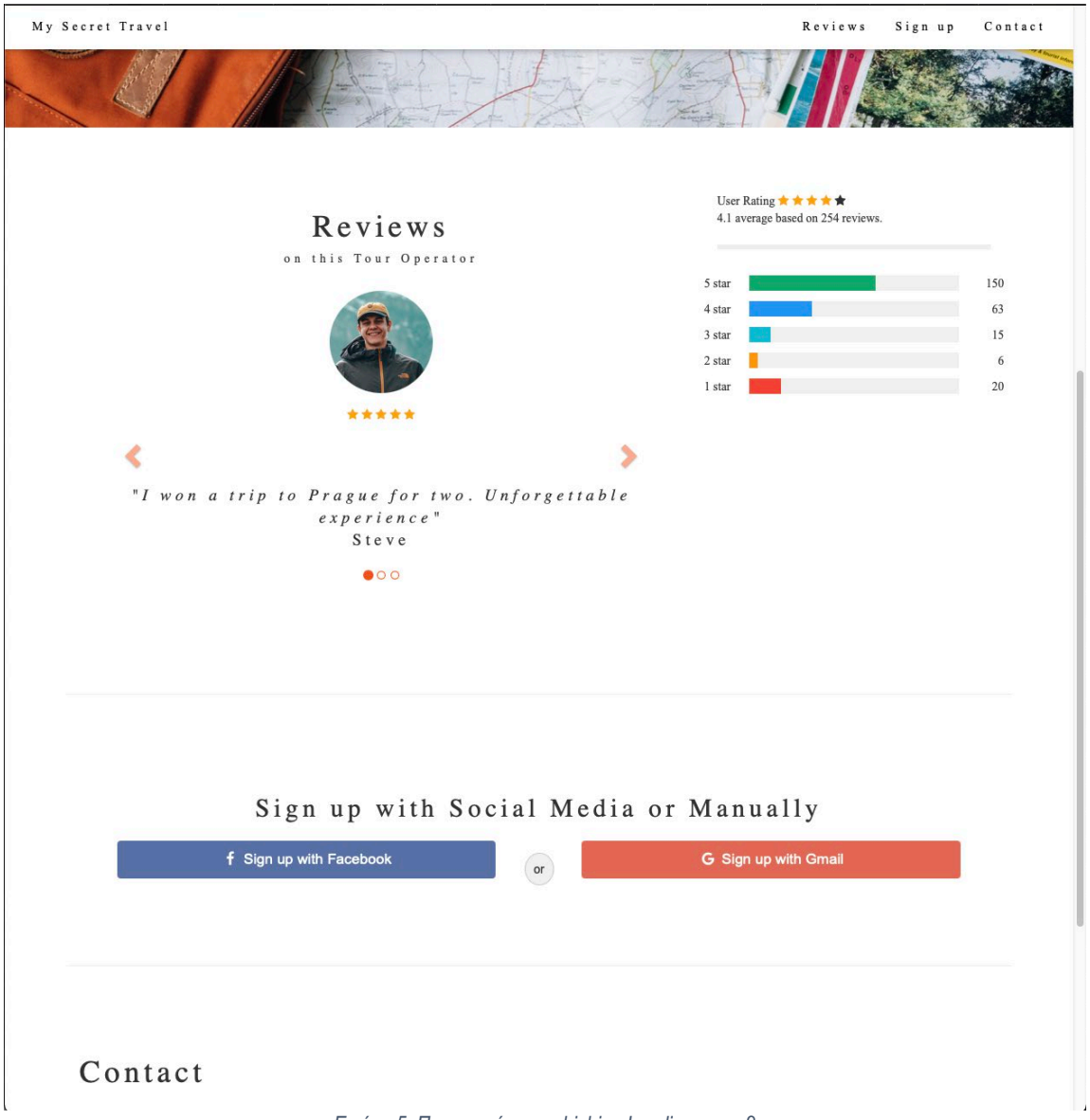
Εάν ο χρήστης κάνει κλικ στην παρότρυνση για δράση που θα βρεθεί στο κάτω μέρος του email, θα φτάσει στη σελίδα προορισμού του πλασματικού ιστότοπου Mysecrettravel (Εικόνα 3). Σε αυτό το σημείο εργαζόμαστε σε διαφορετικούς τύπους εμπλοκής. Το ένα είναι απλώς να εγγραφούν και να αφήσουν τα δεδομένα τους (εγγραφή στο gmail ή στο facebook) (Εικόνα: 5), το άλλο είναι να μοιραστούν τον διαγωνισμό.



Εικόνα 3: Προσχέδιο προσομοίωσης phishing Landing page

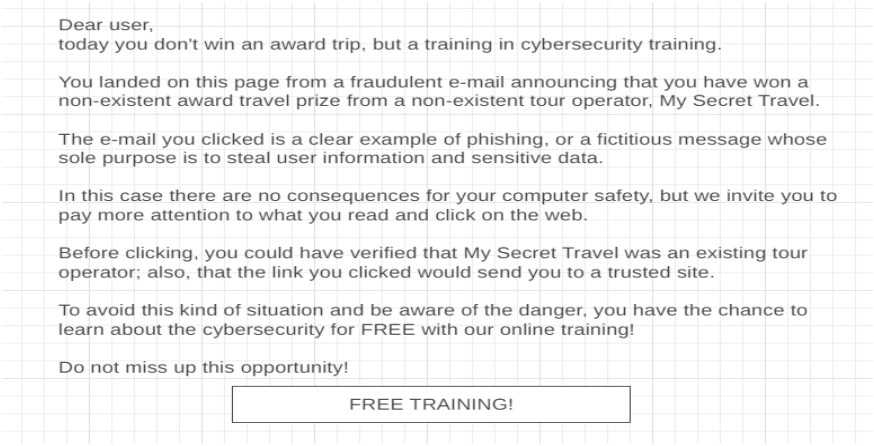


Εικόνα 4: Προσομοίωσης phishing Landing page 1

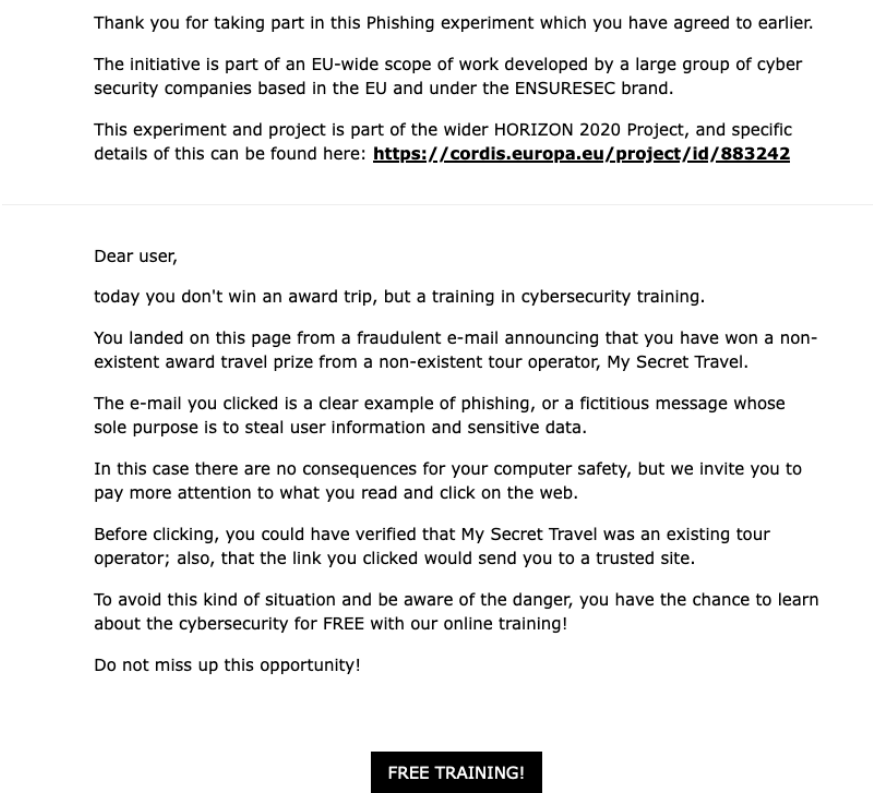


Εικόνα 5: Προσομοίωσης phishing Landing page 2

Μόλις οι χρήστες κάνουν κλικ στο log in, θα ανακατευθυνθεί στη σελίδα όπου θα εξηγήσουμε ότι έπεσε θύμα phishing και του προσφέρουμε τη δωρεάν εκπαίδευση.



Εικόνα 6: Προσχέδιο προσομοίωσης phishing, σελίδα οπού εξηγείται το κόλπο


Thank you for taking part in this Phishing experiment which you have agreed to earlier.

The initiative is part of an EU-wide scope of work developed by a large group of cyber security companies based in the EU and under the ENSURESEC brand.

This experiment and project is part of the wider HORIZON 2020 Project, and specific details of this can be found here: **https://cordis.europa.eu/project/id/883242**

Dear user,

today you don't win an award trip, but a training in cybersecurity training.

You landed on this page from a fraudulent e-mail announcing that you have won a non-existent award travel prize from a non-existent tour operator, My Secret Travel.

The e-mail you clicked is a clear example of phishing, or a fictitious message whose sole purpose is to steal user information and sensitive data.

In this case there are no consequences for your computer safety, but we invite you to pay more attention to what you read and click on the web.

Before clicking, you could have verified that My Secret Travel was an existing tour operator; also, that the link you clicked would send you to a trusted site.

To avoid this kind of situation and be aware of the danger, you have the chance to learn about the cybersecurity for FREE with our online training!

Do not miss up this opportunity!

FREE TRAINING!

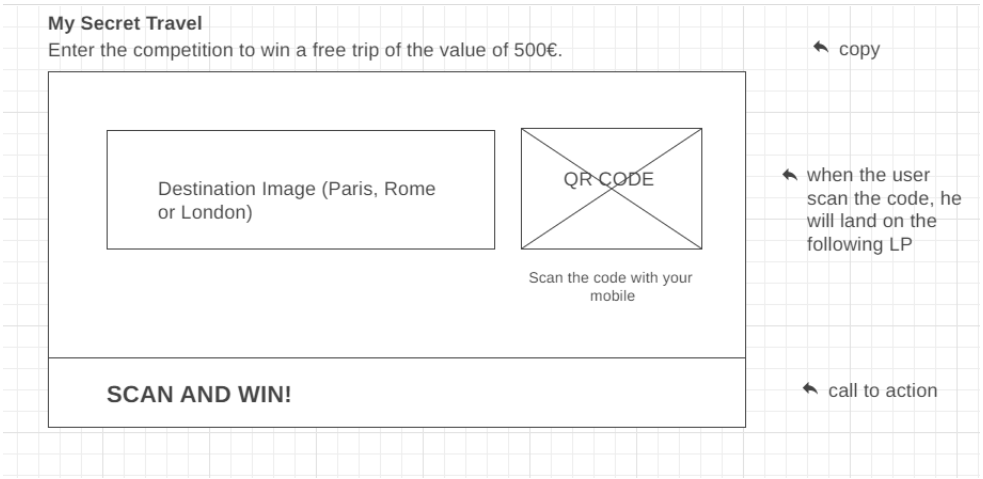
Εικόνα 7: Προσομοίωσης phishing, σελίδα οπού εξηγείται το κόλπο

Στόχος: Χρήστες με χαμηλό επίπεδο συνειδητοποίησης κινδύνου, υψηλή εξωστρέφεια και υψηλή περιέργεια. Υψηλός αναλφαβητισμός και χαμηλή χρήση του διαδικτύου και της τεχνολογικής τεχνογνωσίας.

3.1.2 Τεχνική επίθεσης QRishing

Ένας κώδικας QR (ταχείας απόκρισης) είναι μια εικόνα που περιέχει μια διάταξη ασπρόμαυρων εικονοστοιχείων που χρησιμοποιούνται για την αποθήκευση και την μετάδοση συμπιεσμένων πληροφοριών. Ο hacker θα μπορούσε να δημοσιεύσει κωδικούς QR γύρω από μια περιοχή που προσποιούνταν ότι ήταν διαφημίσεις για ένα νόμιμο προϊόν ή εταιρεία.
Στη συνέχεια, οι κωδικοί QR κατευθύνουν τους σαρωτές αυτών των κωδικών σε μια κακόβουλη διεύθυνση URL, όπου πραγματοποιείται λήψη κακόβουλου λογισμικού, μολύνοντας έτσι τη συσκευή του θύματος, πριν τους ανακατευθύνουν στον νόμιμο ιστότοπο. Το θύμα δεν θα γνώριζε την επίθεση, αλλά θα είχε τώρα μια μολισμένη συσκευή που μεταδίδει τα προσωπικά του δεδομένα στον hacker.
Εναλλακτικά, ο σύνδεσμος θα μπορούσε να τους κατευθύνει σε μια πλαστή πανομοιότυπη ιστοσελίδα του νόμιμου ιστότοπου, ζητώντας τους να συνδεθούν όπου μέσο αυτής της ιστοσελίδας θα γινόταν υποκλοπή των διαπιστευτηρίων τους. Ακόμα κι αν ο αναγνώστης κώδικα QR παρουσιάζει πρώτα τη διεύθυνση URL για επιθεώρηση από το θύμα, με την χρήση τεχνικών συντόμευσης διεύθυνσης URL σημαίνει ότι είναι πιο δύσκολο για τους χρήστες να προσδιορίσουν εάν μια διεύθυνση URL είναι νόμιμη.

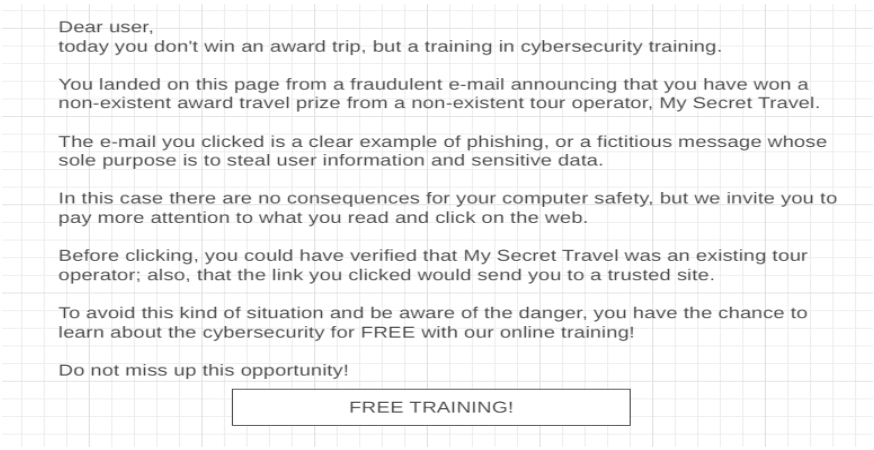
Κανάλια: E-Mail
Μηχανισμός Παράδοσης: Ο χρήστης θα λάβει ένα email όπου καλείται να σαρώσει έναν κωδικό QR προκειμένου να λάβει ένα δωρεάν ταξίδι, το μήνυμα είναι πολύ απλό: «Μπείτε στον διαγωνισμό για να κερδίσετε ένα δωρεάν ταξίδι αξίας 500 ευρώ».



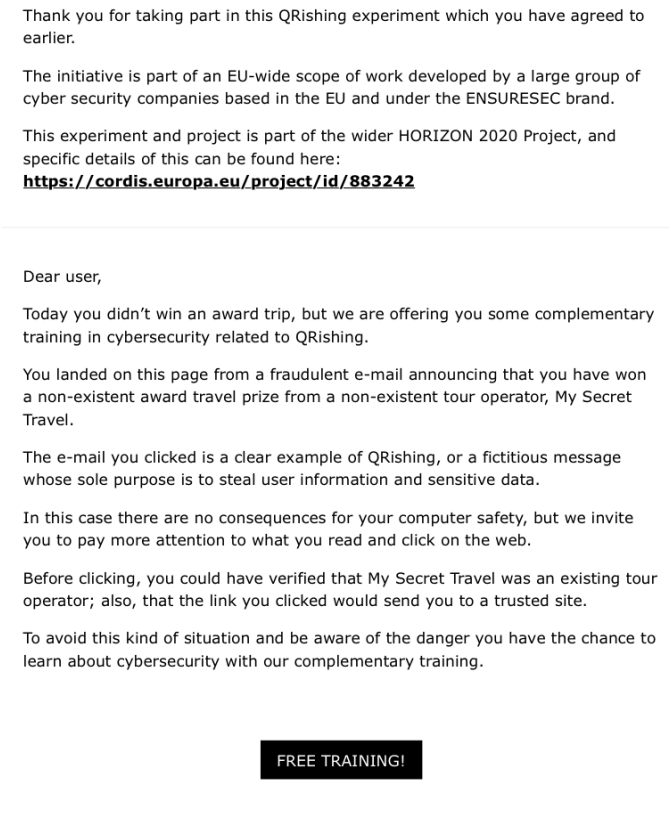
Εικόνα 8: Προσχέδιο προσομοίωσης QRishing email

Εικόνα 9: προσομοίωσης QRishing email

Μόλις ο χρήστης σαρώσει τον κώδικα, θα φτάσει στη σελίδα προορισμού του πλασματικού ιστότοπου Mysecrettravel.
Για άλλη μια φορά καλείται να συνδεθεί και να αφήσει τα προσωπικά του στοιχεία, σε αυτό το στάδιο θα ανακατευθυνθεί στην σελίδα προορισμού όπου εξηγούμε το κόλπο και προσφέρουμε τη δωρεάν εκπαίδευση.



Εικόνα 10: Προσχέδιο προσομοίωσης QRishing, σελίδα οπού εξηγείται το κόλπο



Εικόνα 11: Προσομοίωσης QRishing, σελίδα οπού εξηγείται το κόλπο

Στόχος: Ψυχολογική/Ατομική κατάσταση: Διάθεση εμπιστοσύνης. Αντίληψη απειλής: Περιέργεια. Δημογραφικά χαρακτηριστικά: Αναλφαβητισμός/Έλλειψη γνώσεων.

Κεφάλαιο 4

Εργαλεία για την Εκστρατεία Ευαισθητοποίησης για την Ασφάλεια

4.1 MASCARA

4.1.1 Τι είναι η MASCARA

Το MASCARA είναι ένα εργαλείο που μας βοηθά να δημιουργήσουμε και να αναπτύξουμε εύκολα εφαρμογές ιστού, από απλούς ιστότοπους, ιστότοπους WordPress ή εφαρμογές Django έως πιο περίπλοκες υπηρεσίες όπως διακομιστές αλληλογραφίας ή διαδικασίες όπως η αποστολή αυτοματοποιημένων μηνυμάτων ηλεκτρονικού ταχυδρομείου σε συγκεκριμένες ομάδες-στόχους χωρίς υπερβολικά περίπλοκες διαμορφώσεις που απαιτούνται από χειροκίνητη εγκατάσταση τέτοιων συστημάτων. Επίσης, το MASCARA υποστηρίζει την καταγραφή και την παρακολούθηση των αναπτυσσόμενων υπηρεσιών μέσω μιας ανάπτυξης στοίβας ELK ικανή να καταγράφει τυπικά αρχεία καταγραφής εφαρμογών ή ακόμα και προσαρμοσμένα μηνύματα καταγραφής που παράγονται από εφαρμογές που αναπτύσσονται από το MASCARA.

Απαιτήσεις χρήστη

Ο χρήστης πρέπει να μπορεί να εγγραφεί και να συνδεθεί στην πλατφόρμα. Οι πληροφορίες που πρέπει να συλλέγει η πλατφόρμα από τον χρήστη κατά την εγγραφή θα πρέπει να είναι:

- Email
- Κωδικός πρόσβασης
- Όνομα και Επώνυμο

Ο διαχειριστής πρέπει να εγκρίνει μη αυτόματα τους νέους εγγεγραμμένους χρήστες για πρόσβαση στη δημιουργία, προβολή και διαχείριση καμπανιών.
Ο χρήστης πρέπει να μπορεί να δημιουργήσει ένα Έργο, οι πληροφορίες σχετικά με το Έργο πρέπει να περιλαμβάνουν:

- Όνομα
- Περιγραφή
- Ετικέτες

Ο χρήστης πρέπει να μπορεί να δημιουργήσει μια καμπάνια, οι πληροφορίες σχετικά με την καμπάνια πρέπει να περιλαμβάνουν:

- Όνομα
- Περιγραφή
- Αναγνωριστικό έργου
- Ετικέτες

Ο χρήστης πρέπει να μπορεί να δημιουργήσει ένα Widget, οι πληροφορίες σχετικά με το Widget πρέπει να περιλαμβάνουν:

- Όνομα προσθήκης
- Ευρετήριο
- Περιγραφή

- Αναγνωριστικό καμπάνιας
- Διαμόρφωση

Ο χρήστης πρέπει να μπορεί να ανεβάσει ένα Αρχείο, οι πληροφορίες σχετικά με το Αρχείο πρέπει να περιλαμβάνουν:

- Αρχείο
- Όνομα αρχείου
- Περιγραφή
- Ετικέτες

1. Ο χρήστης πρέπει να μπορεί να δει τον αριθμό των Έργων, των Καμπανιών και των Γραφικών στοιχείων που δημιουργήθηκαν από αυτόν και να μπορεί να δει πληροφορίες όπως η κατάσταση μιας Καμπάνιας (Ενεργή ή Ανενεργή).
2. Ο χρήστης πρέπει επίσης να μπορεί να ανεβάζει αρχεία που μπορούν να χρησιμοποιηθούν σε μεταγενέστερο στάδιο, κατά τη διαμόρφωση των widget.
3. Ο χρήστης πρέπει να μπορεί να ξεκινά και να διακόπτει μια καμπάνια όποτε θέλει.

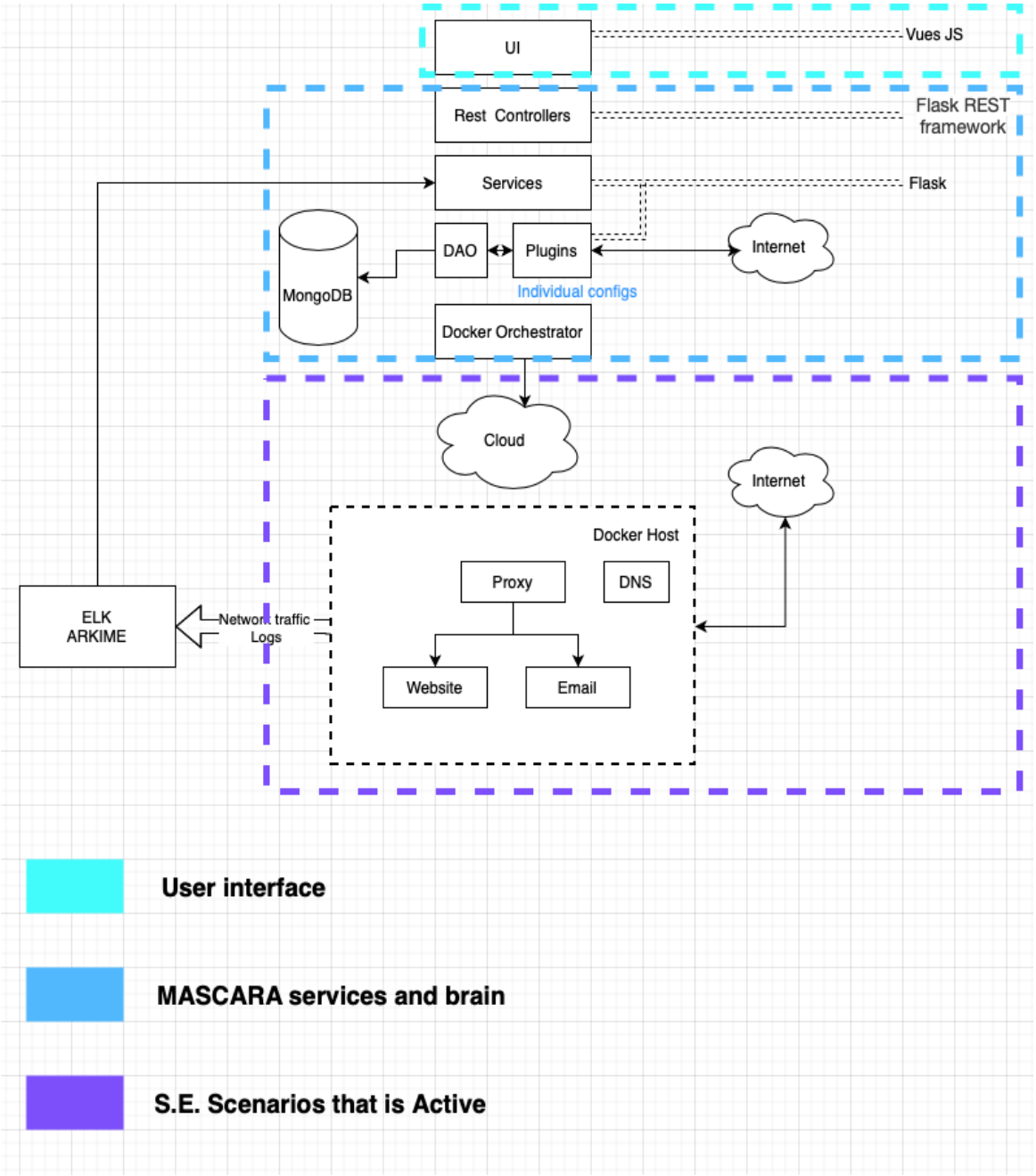
4.1.2 MASCARA Αρχιτεκτονική και Σχεδιασμός

Η αρχιτεκτονική του MASCARA χωρίζεται σε τρεις κύριες ενότητες.

1. **Διεπαφή χρήστη (Frontend):**
   Η διεπαφή χρήστη έχει κατασκευαστεί χρησιμοποιώντας το πλαίσιο Quasar, ένα σύγχρονο κιτ εργαλείων που βασίζεται στην έκδοση 3 του VueJS. Μέσω του UI ένας πιστοποιημένος χρήστης μπορεί εύκολα να δημιουργήσει και να αναπτύξει S.E. σενάρια μέσα σε λίγα λεπτά χρησιμοποιώντας ένα σετ προκατασκευασμένων γραφικών στοιχείων.

2. **Υπηρεσίες (Backend):**
   Για την ανάπτυξη του Backend έγινε χρήση του Domain driven RESTful design. Με αυτόν τον σχεδιασμό έχουμε ευελιξία σε οποιεσδήποτε αλλαγές, καθώς οι νέες λειτουργικές απαιτήσεις θα ταιριάζουν φυσικά και είναι ευκολότερο να συντηρηθούν.
   Ο πυρήνας του backend είναι γραμμένος στην γλώσσα προγραμματισμού Python 3 χρησιμοποιώντας το πλαίσιο Flask REST. Ένα σύνολο ελεγκτών εκθέτει τα τελικά σημεία API που θα χρησιμοποιηθούν από τη διεπαφή χρήστη για τη διαχείριση του κύκλου ζωής του S.E. σενάρια. Η υπηρεσία υποστηρίζεται από mongo DB ως «business logic store».

3. **Σενάρια Κοινωνικής Μηχανικής (Docker containers stack)**
   Κάθε S.E. αποτελείται από έναν ορισμό καμπάνιας που περιλαμβάνει πρότυπα email για αποστολή στους χρήστες-στόχους και ένα πρότυπο στοίβας docker ανάλογα με τα επιλεγμένα γραφικά στοιχεία/προσθήκες. Αυτά τα γραφικά στοιχεία χρησιμοποιούνται για την υλοποίηση σελίδων προορισμού και για την παρακολούθηση της εκτέλεσης της καμπάνιας. Κάθε παρουσία καμπάνιας, μόλις εκτελεστεί, αναπτύσσει μια παρουσία της στοίβας που γίνεται προσβάσιμη με ένα έγκυρο πιστοποιητικό SSL σε έναν διαμορφωμένο τομέα μέσω ενός διακομιστή μεσολάβησης εισόδου διεπαφής.



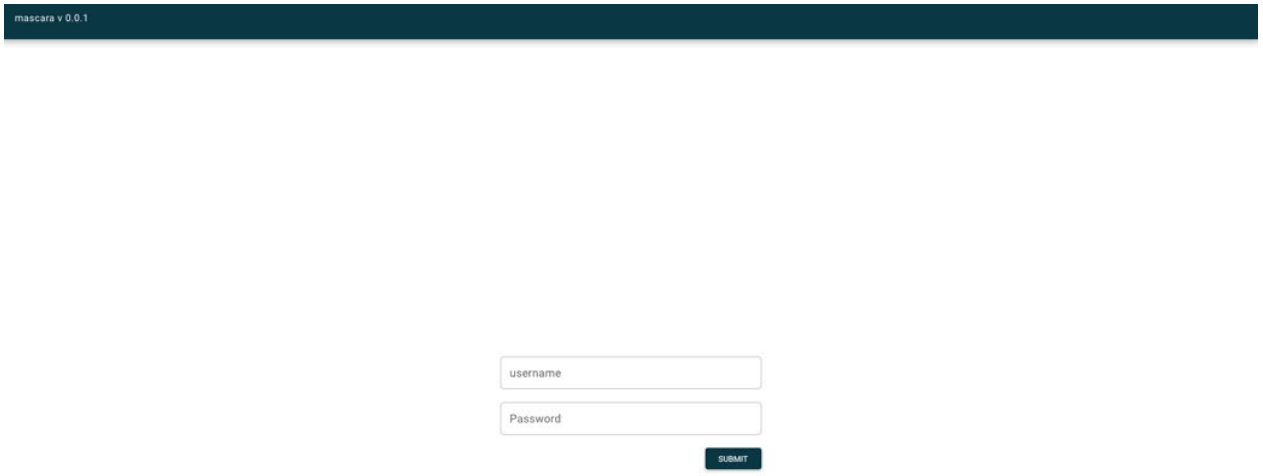
Εικόνα 12: αρχιτεκτονική του MASCARA

Επίσης, έχει αναπτυχθεί ένας κεντρικός διακομιστής αναμετάδοσης postfix με TLS και DKIM διαμορφωμένα για κάθε όνομα(domain name) τομέα καμπάνιας, έτσι ώστε να επιτρέπεται η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου στους στόχους της καμπάνιας ως νόμιμοι αποστολείς.

Έχουν αναπτυχθεί περισσότερα από έναν κεντρικό διακομιστή apache για να λειτουργεί ως αντίστροφος διακομιστής μεσολάβησης σε ιστότοπους που αναπτύσσονται με docker για κάθε περίπτωση καμπάνιας. Ένα νέο αρχείο διαμόρφωσης virtualhost προστίθεται αυτόματα στη διαμόρφωση του διακομιστή μεσολάβησης κατά τη δημιουργία μιας νέας παρουσίας καμπάνιας.

4.1.3 Τεκμηρίωση διεπαφής χρήστη

Εάν ο χρήστης δεν έχει πιστοποιηθεί και προσπαθήσει να αποκτήσει πρόσβαση στην πλατφόρμα MASCARA, θα τον ανακατευθύνει στη σελίδα ελέγχου ταυτότητας

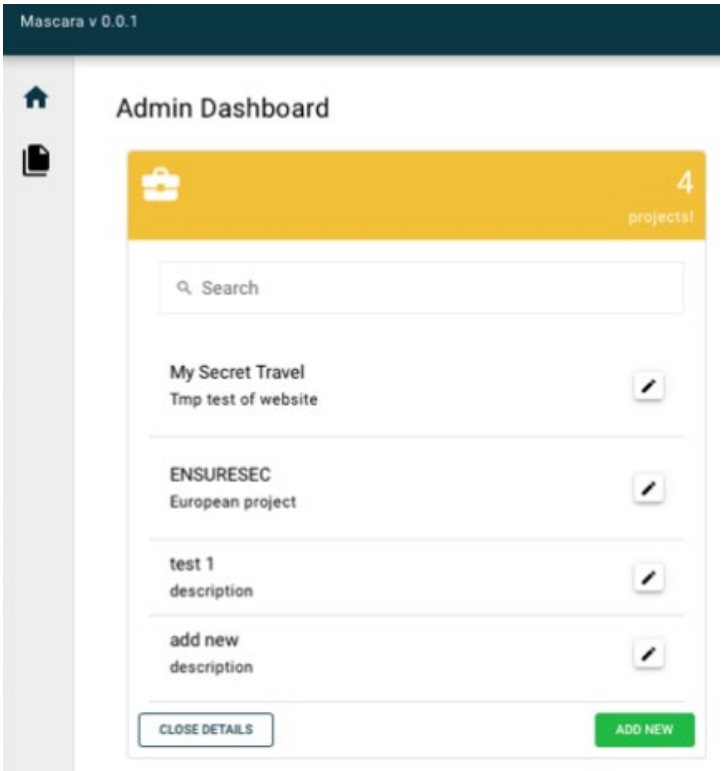


Εικόνα 13

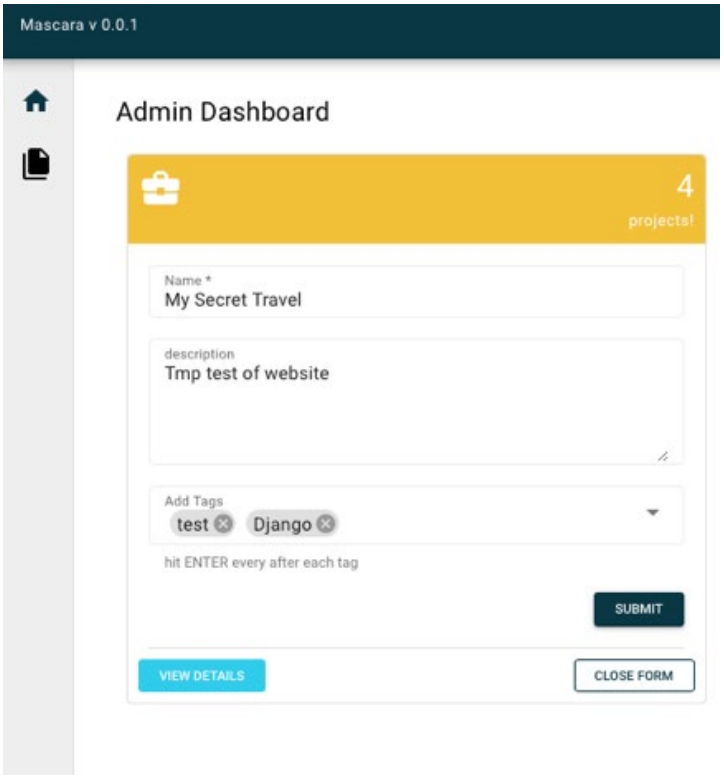
Όταν ένας χρήστης πραγματοποιεί έλεγχο ταυτότητας επιτυχώς, έχει πρόσβαση στον Πίνακα ελέγχου διαχειριστή. Εκεί μπορεί να δει πόσα έργα, και καμπάνιες έχουν ήδη δημιουργηθεί. Επίσης, μπορεί να δημιουργήσει και να διαμορφώσει νέα έργα και καμπάνιες ή να ενημερώσουν ένα υπάρχον έργο. Τέλος, μπορούν να ξεκινήσουν ή να σταματήσουν καμπάνιες.

Εικόνα 14

Ο χρήστης μπορεί να δει λεπτομέρειες για τα έργα κάνοντας κλικ στο κουμπί VIEW DETAILS στην ενότητα του Project και, αν χρειαστεί, μπορεί να επεξεργαστεί ένα υπάρχον Project.

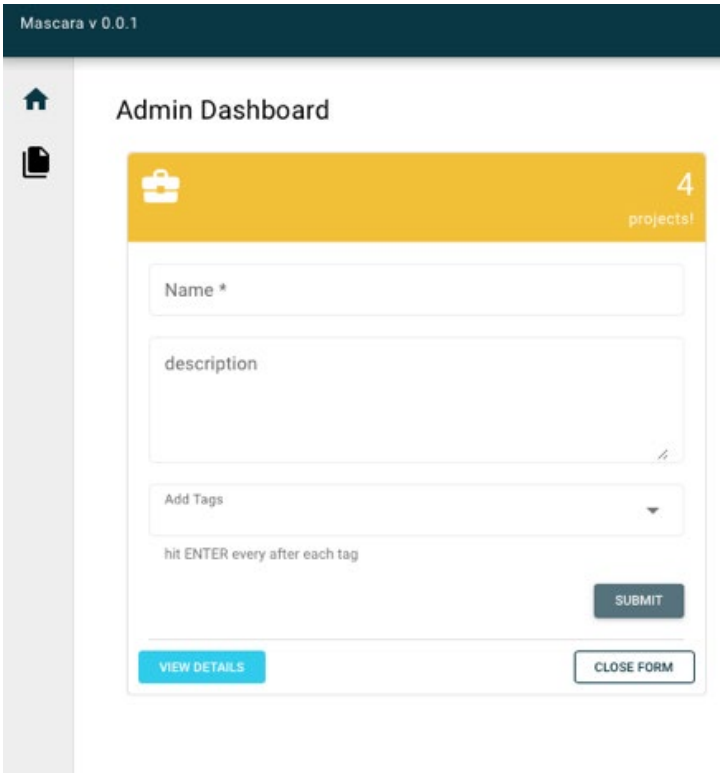


Εικόνα 15



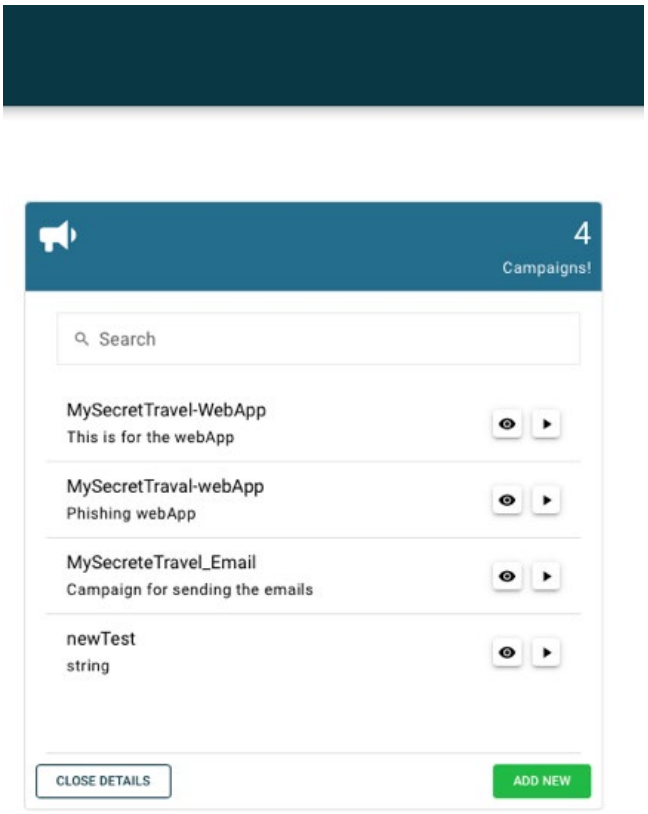
Εικόνα 16

Ο χρήστης μπορεί να δημιουργήσει ένα νέο έργο κάνοντας κλικ στο κουμπί ADD NEW στην ενότητα του έργου και να συμπληρώσει τα απαιτούμενα πεδία.

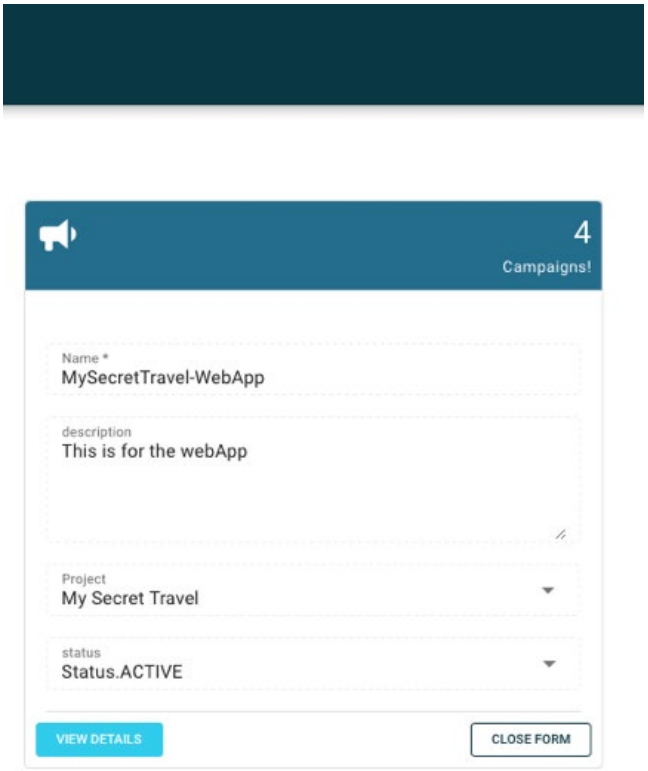


Εικόνα 17

Ο χρήστης μπορεί να δει λεπτομέρειες σχετικά με τις καμπάνιες κάνοντας κλικ στο κουμπί VIEW DETAILS στην ενότητα καμπάνιες και «περισσότερες λεπτομέρειες» για μια συγκεκριμένη καμπάνια όπως η περιγραφή, το έργο που είναι συνδεδεμένο μαζί της ή την κατάσταση της καμπάνιας κάνοντας κλικ το εικονίδιο του ματιού στη συγκεκριμένη καμπάνια. Επιπλέον, εάν ο χρήστης θέλει να ξεκινήσει ή να σταματήσει μια καμπάνια, μπορεί να εκτελέσει αυτήν την ενέργεια κάνοντας κλικ στο εικονίδιο αναπαραγωγής.

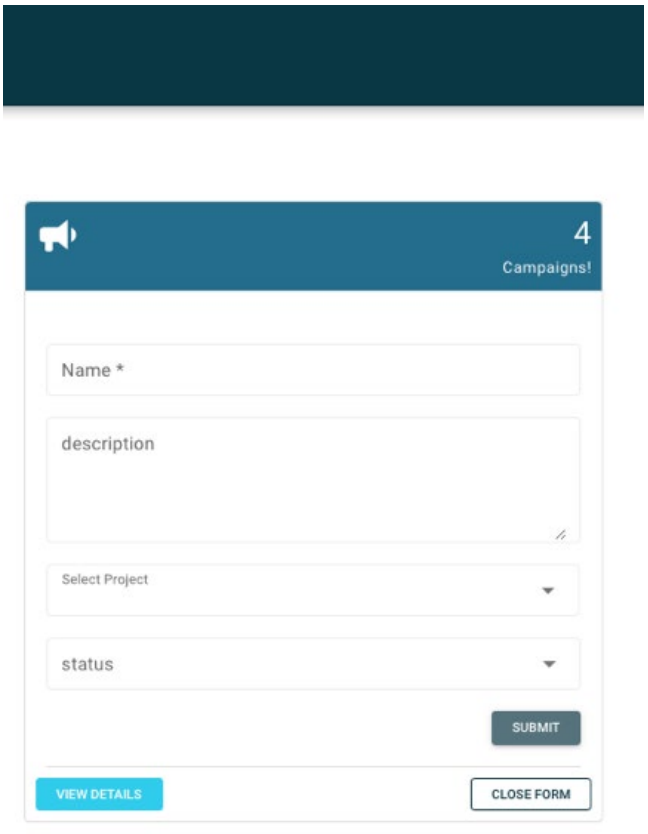


Εικόνα 18



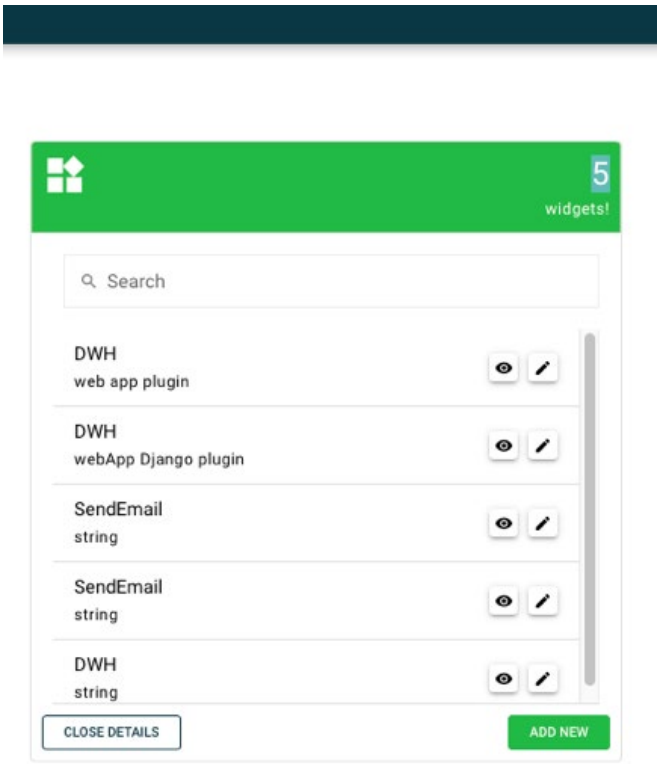
Εικόνα 19

Ο χρήστης μπορεί να δημιουργήσει μια νέα καμπάνια κάνοντας κλικ στο κουμπί ADD NEW στην ενότητα καμπάνιας και να συμπληρώσει τα απαιτούμενα πεδία.

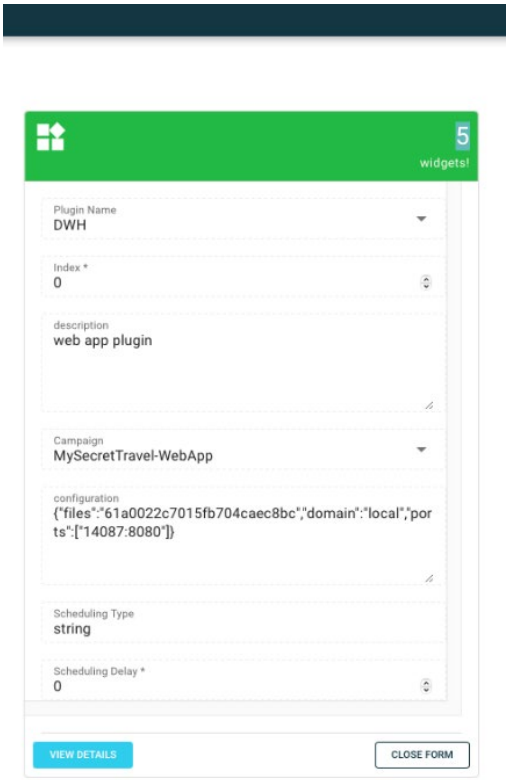


Εικόνα 20

Ο χρήστης μπορεί να δει λεπτομέρειες σχετικά με τα widget κάνοντας κλικ στο κουμπί VIEW DETAILS στην ενότητα widget και περισσότερες λεπτομέρειες για ένα συγκεκριμένο widget, όπως το όνομα της προσθήκης, η συνδεδεμένη καμπάνια ή μια διαμόρφωση, κάνοντας κλικ στο εικονίδιο ματιού στο συγκεκριμένο widget. Εάν είναι απαραίτητο, ο χρήστης μπορεί να επεξεργαστεί ένα υπάρχον widget.

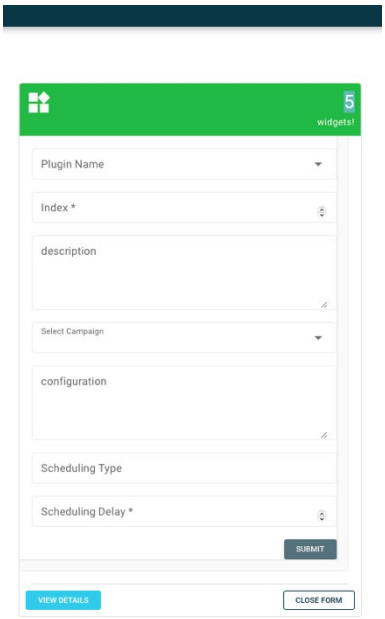


Εικόνα 21



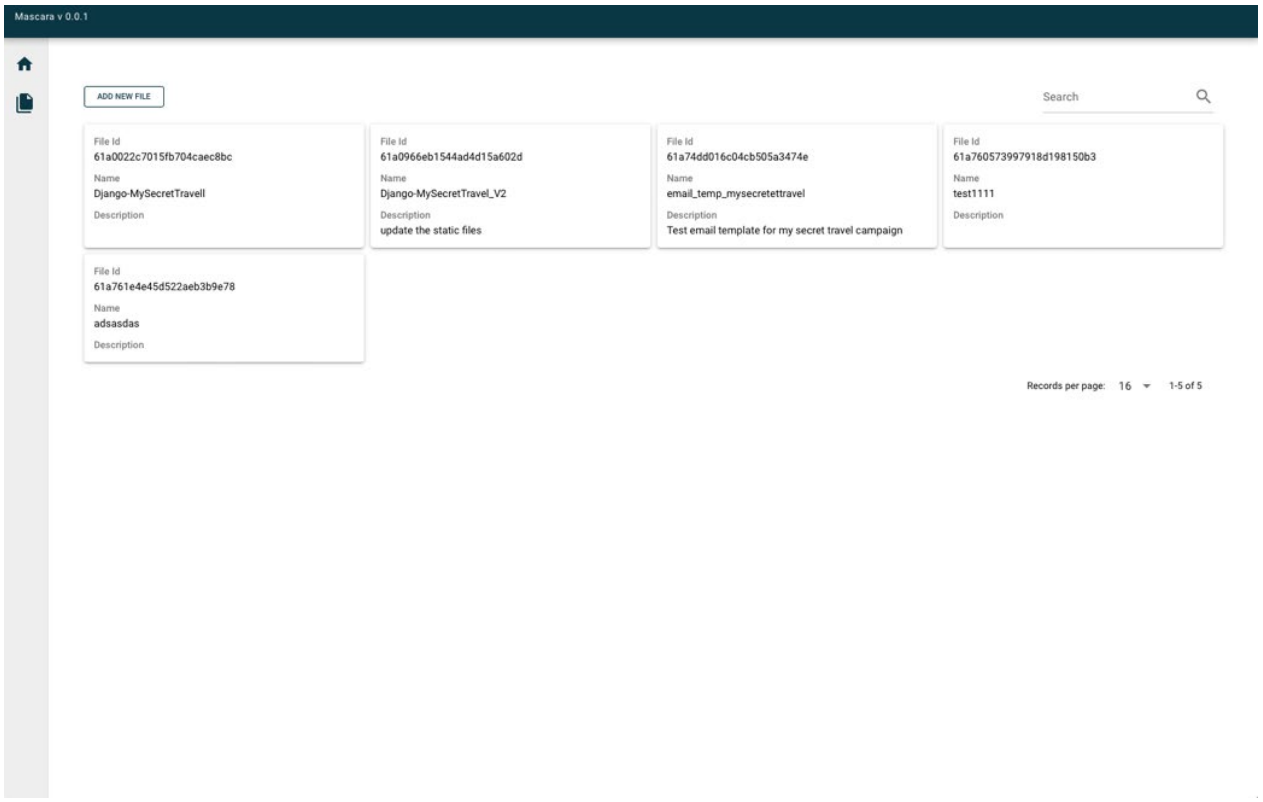
Εικόνα 22

Ο χρήστης μπορεί να δημιουργήσει ένα νέο widget κάνοντας κλικ στο κουμπί ADD NEW στην ενότητα widgets και να συμπληρώσει τα απαιτούμενα πεδία.



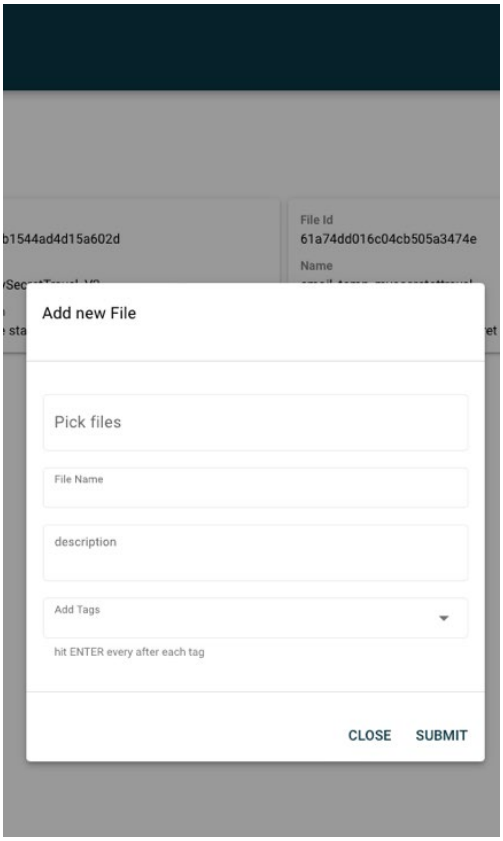
Εικόνα 23

Ο χρήστης μπορεί να δει όλα τα μεταφορτωμένα αρχεία με ορισμένες λεπτομέρειες, όπως αναγνωριστικό αρχείου, όνομα και περιγραφή από την οθόνη Αρχεία.



Εικόνα 24

Ο χρήστης μπορεί να ανεβάσει νέα αρχεία ή περισσότερα από ένα αρχεία σε μορφή zip κάνοντας κλικ στο κουμπί ADD NEW FILE συμπληρώνοντας τα απαιτούμενα πεδία.



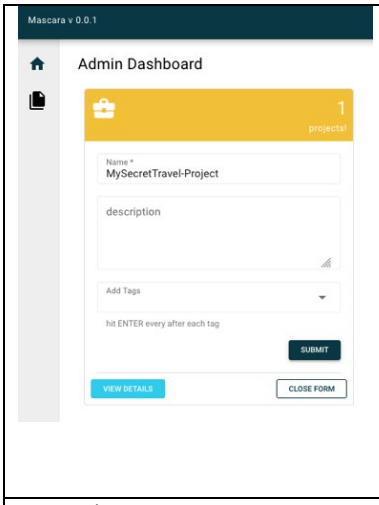
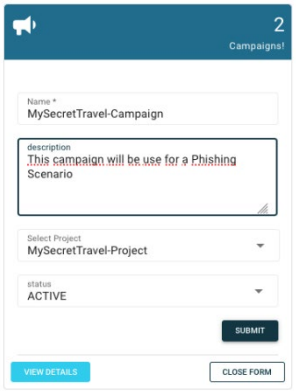
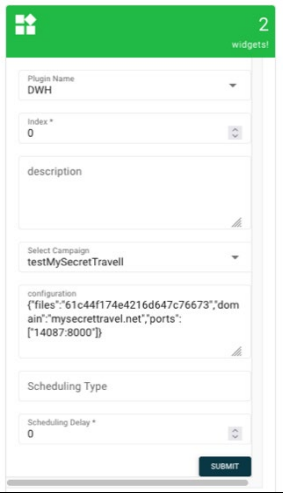
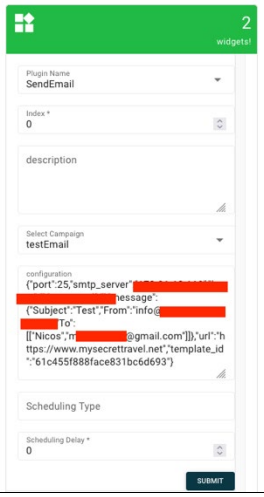
Εικόνα 25

Μία από τις πιο ισχυρές υπηρεσίες που παρέχει το έργο MASCARA, είναι η δυνατότητα συλλογής δεδομένων και δημιουργίας αναλυτικών στοιχείων για κάθε καμπάνια. Αυτά τα αναλυτικά στοιχεία μπορούν να μας βοηθήσουν να κατανοήσουμε την αφοσίωση του χρήστη με τις εφαρμογές phishing, μέσω της αλληλεπίδρασης και της συμπεριφοράς τους σε κάθε καμπάνια.

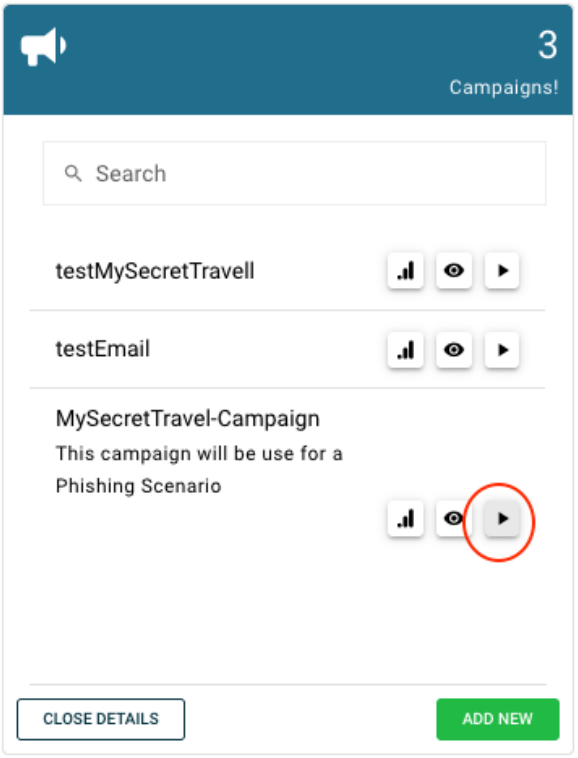
Εικόνα 26

4.1.4 Παράδειγμα στον πραγματικό κόσμο

Παρακάτω περιγράφεται ένα πραγματικό παράδειγμα μιας καμπάνιας Κοινωνικής Μηχανικής και πιο συγκεκριμένα ενός σεναρίου Phishing.
Πρώτα από 'όλα πρέπει να ρυθμίσουμε το σενάριο δημιουργώντας ένα έργο, μια καμπάνια και στη συνέχεια να διαμορφώσουμε τα απαραίτητα widget.

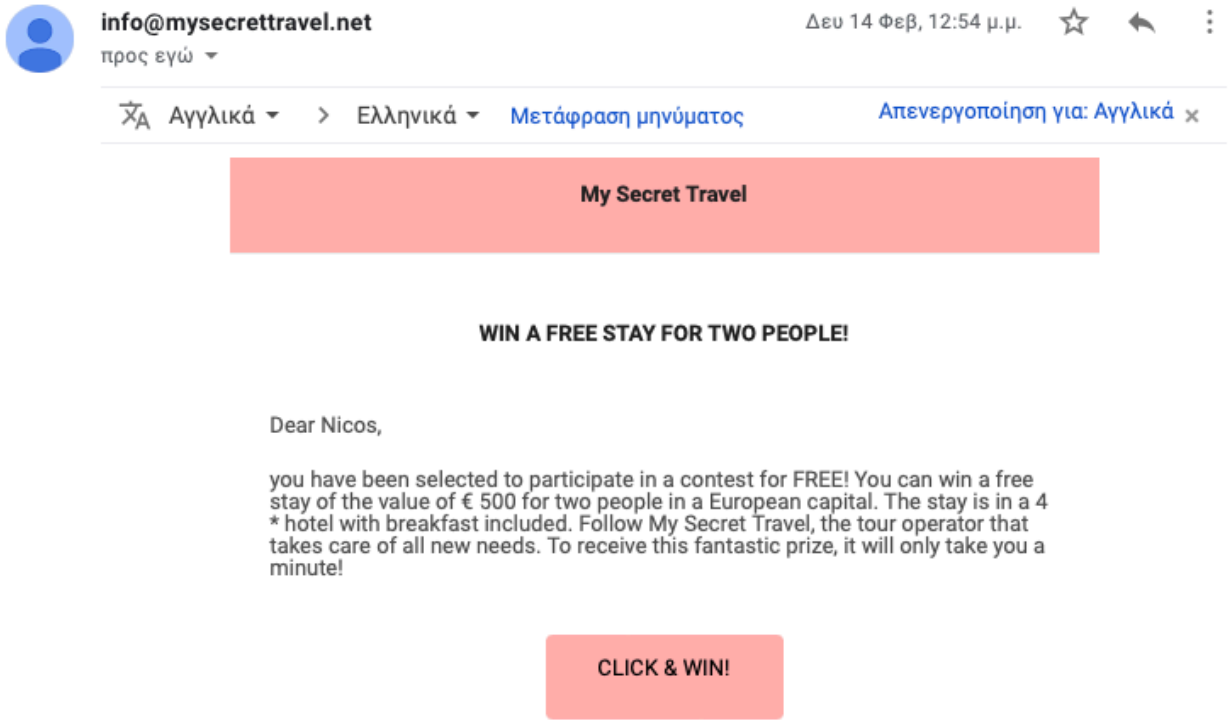
			
Βήμα 1 Δημιουργία έργου	Βήμα 2 Δημιουργία καμπάνιας	Βήμα 3.1 Διαμόρφωση του widget της εφαρμογής web.	Βήμα 3.2 Διαμόρφωση του widget αυτοματοποιημένης αποστολής email.

Μετά τη ρύθμιση της καμπάνιας, πατώντας το κουμπί εκτέλεσης από τη λειτουργική ενότητα Campaigns η καμπάνια μπαίνει σε λειτουργία.



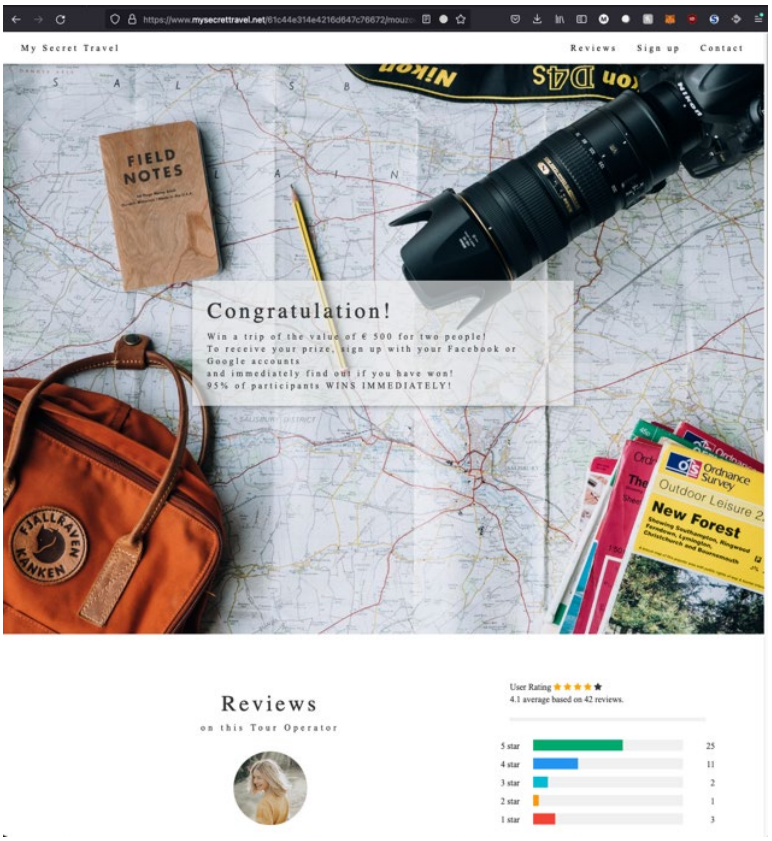
Εικόνα 27

Ο χρήστης-στόχος θα λάβει ένα email που τον ενημερώνει ότι μπορεί να κερδίσει ένα κουπόνι 500 ευρώ για δύο άτομα για διαμονή σε ξενοδοχείο 4 αστέρων.

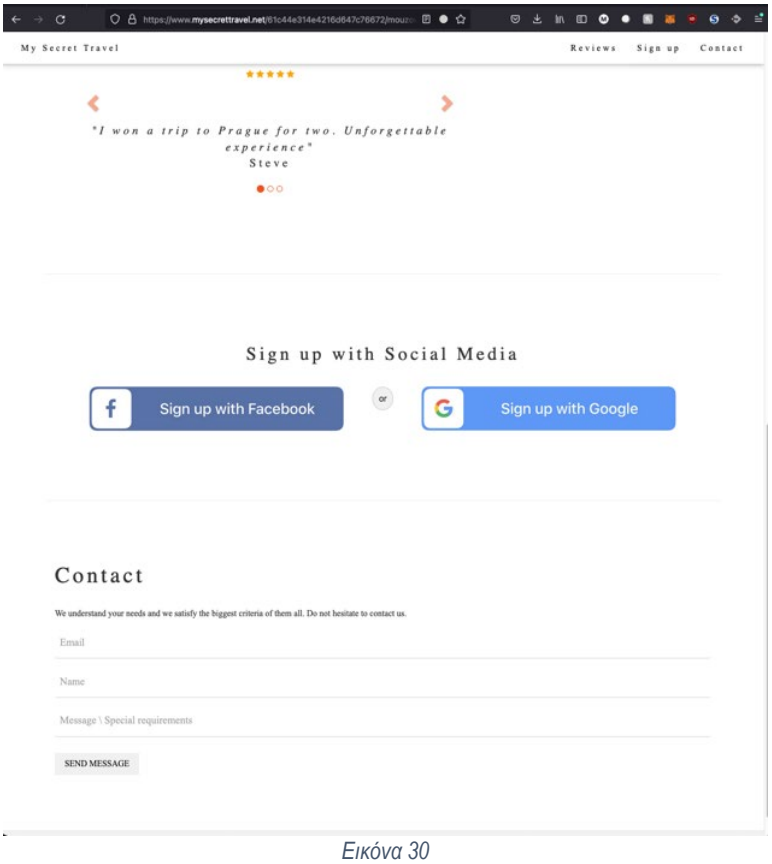


Εικόνα 28

Όταν ο χρήστης κάνει κλικ στο κουμπί, θα ανοίξει ένα νέο παράθυρο του ιστότοπου phishing.

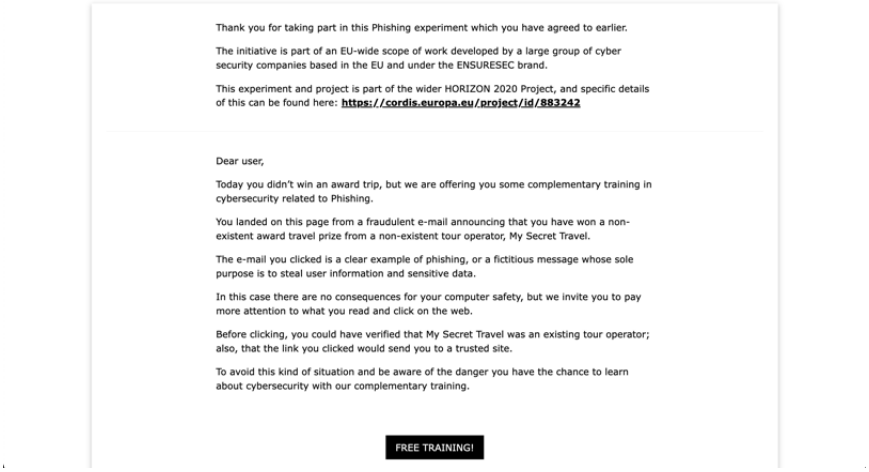


Εικόνα 29



Εικόνα 30

Η συμπεριφορά του χρήστη καταγράφεται και είμαστε σε θέση να γνωρίζουμε πότε και πού κάνει κλικ ο χρήστης στον ιστότοπο. Αυτά τα δεδομένα αποθηκεύονται και διοχετεύονται στην πλατφόρμα MASCARA.
Εάν ο χρήστης εκτελέσει μια ενέργεια που έχει ως αποτέλεσμα παραβίασης των διαπιστευτηρίων του, π.χ.: κάνοντας κλικ στην εγγραφή στο Facebook, θα ανακατευθύνει μετά από λίγα δευτερόλεπτα σε μια νέα σελίδα όπου θα ενημερώσει τον χρήστη πως συμμετέχει σε μια καμπάνια ηλεκτρονικού "ψαρέματος" και θα του παρέχει με δωρεάν εκπαίδευση.


Thank you for taking part in this Phishing experiment which you have agreed to earlier.

The initiative is part of an EU-wide scope of work developed by a large group of cyber security companies based in the EU and under the ENSURESEC brand.

This experiment and project is part of the wider HORIZON 2020 Project, and specific details of this can be found here: **https://cordis.europa.eu/project/id/883242**

Dear user,

Today you didn't win an award trip, but we are offering you some complementary training in cybersecurity related to Phishing.

You landed on this page from a fraudulent e-mail announcing that you have won a non-existent award travel prize from a non-existent tour operator, My Secret Travel.

The e-mail you clicked is a clear example of phishing, or a fictitious message whose sole purpose is to steal user information and sensitive data.

In this case there are no consequences for your computer safety, but we invite you to pay more attention to what you read and click on the web.

Before clicking, you could have verified that My Secret Travel was an existing tour operator; also, that the link you clicked would send you to a trusted site.

To avoid this kind of situation and be aware of the danger you have the chance to learn about cybersecurity with our complementary training.

FREE TRAINING!

Εικόνα 31

4.2 Πλατφόρμα εκπαίδευσης και αξιολόγησης

4.2.1 Σκοπός

Σκοπός της πλατφόρμας είναι η εκπαίδευση και ευαισθητοποίησης για την ασφάλεια του ψηφιακού εμπορίου. Παρέχει δωρεάν εκπαιδευτικό περιεχόμενο για την ευαισθητοποίηση στον κυβερνοχώρο (βίντεο και κείμενο) καθώς και αξιολογήσεις σχετικά με τη επίγνωση στην κυβερνοασφάλεια καθώς και μια επιλογή εγγραφής για σειρά προσομοιωμένων (ψευδών) απατών.

Τα εκπαιδευτικά βίντεο έχουν διάρκεια δύο με τριών λεπτών και αναφέρονται στα κύρια σημεία των επιθέσεων και τρόπους προς αποφυγής τους.

4.2.2 Ανατομία της πλατφόρμας

Η πλατφόρμα αποτελείται από τρεις κύριες σελίδες:

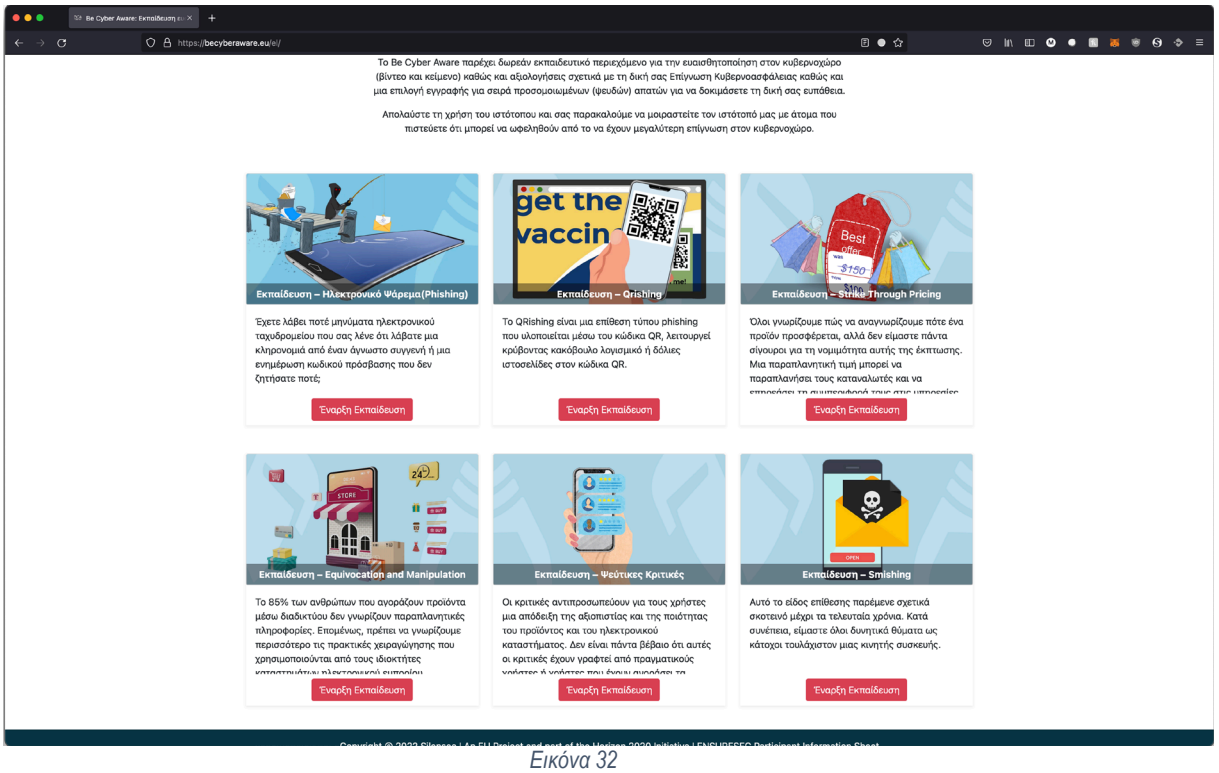
1. **Αρχική**
2. **Αξιολογήσεις**
3. **Εγγραφή για Προσομοίωση**

Ακόμη όλο το περιεχόμενο της πλατφόρμας τόσο το κείμενο όσο και τα videos είναι μεταφρασμένο σε 6 γλώσσες:

1. Αγγλικά
2. Ελληνικά
3. Ιταλικά
4. Ισπανικά
5. Ρουμανικά
6. Γερμανικά

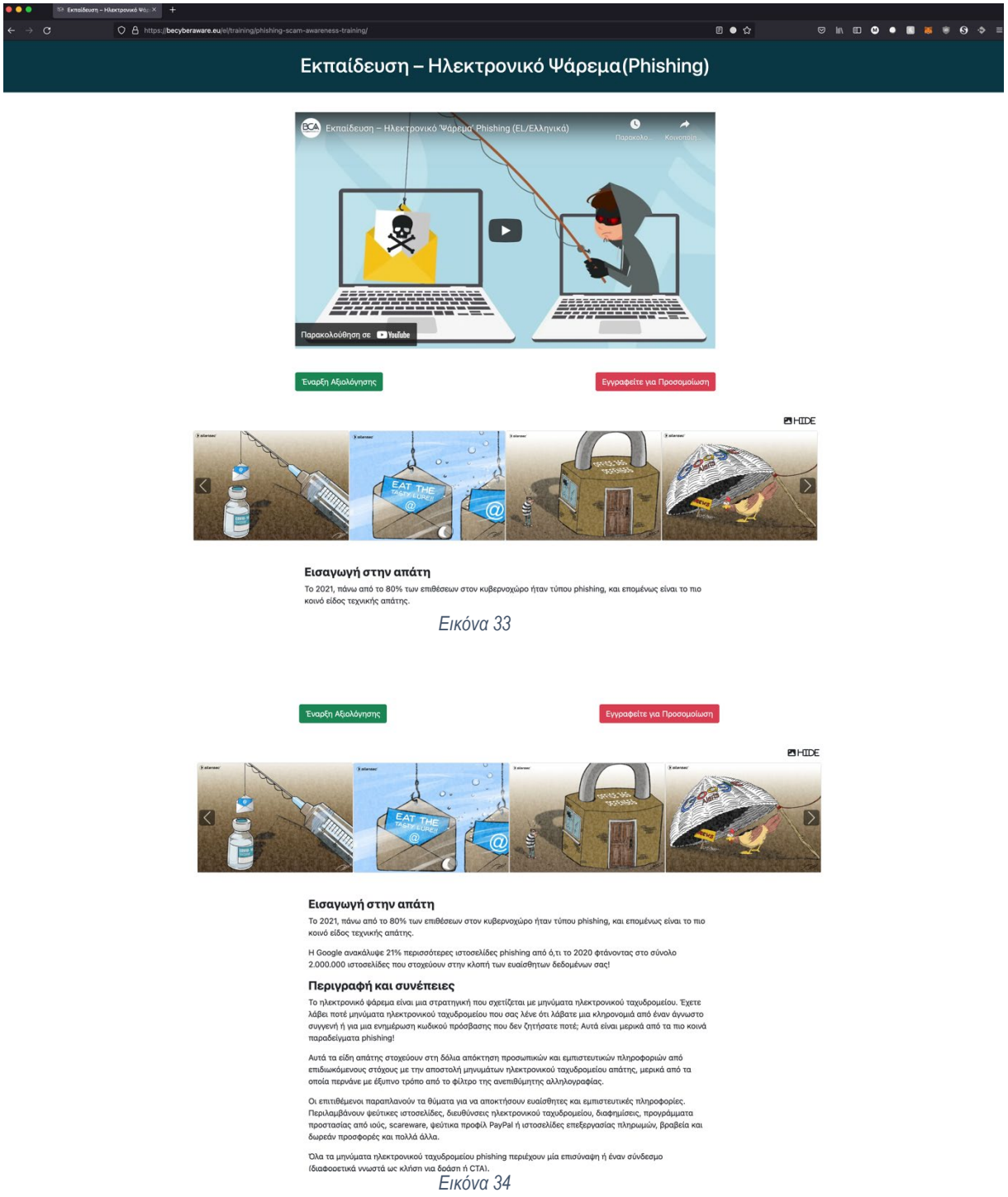
Αρχική

Στην αρχική σελίδα απεικονίζονται οι εκπαιδεύσεις για τις 6 κύριες απειλές που μπορεί να πέσουν θύματα οι καταναλωτές του ψηφιακού εμπορίου.



Εικόνα 32

Πατώντας στο κουμπί Έναρξη Εκπαίδευσης σε μία από τις προσφερόμενες εκπαιδεύσεις ο χρήστης μεταφέρεται σε μία νέα οθόνη στην πλατφόρμα όπου μπορεί να παρακολουθήσει το επιμορφωτικό βίντεο. Ακόμη στην νέα οθόνη υπάρχουν διάφορα posters σε διαμόρφωση γκαλερί καθώς επίσης και το κείμενο της εκπαίδευσης για υποστήριξη στα άτομα που έχουν θέματα ακοής.



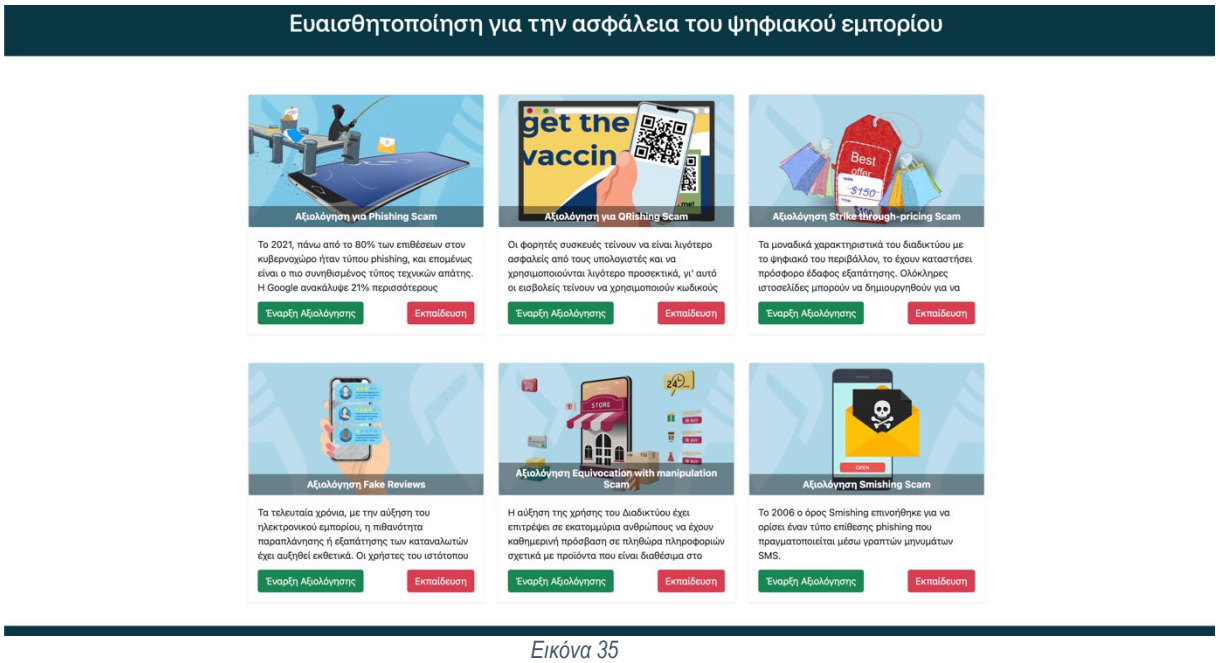
Εικόνα 33

Εικόνα 34

Μετά το τέλος του επιμορφωτικού βίντεο ο χρήστης μπορεί να πατήσει στο κουμπί Έναρξη Αξιολόγησης όπου θα οδηγηθεί στην αντίστοιχη οθόνη για αξιολόγηση στην συγκεκριμένη επίθεση/απειλή ή πατώντας στο κουμπί Εγγραφείτε για Προσομοίωση να οδηγηθεί στην οθόνη εγγραφής.

Αξιολογήσεις

Στην σελίδα αξιολογήσεις απεικονίζονται οι αξιολογήσεις για τις 6 κύριες απειλές που μπορεί να πέσουν θύματα οι καταναλωτές του ψηφιακού εμπορίου.

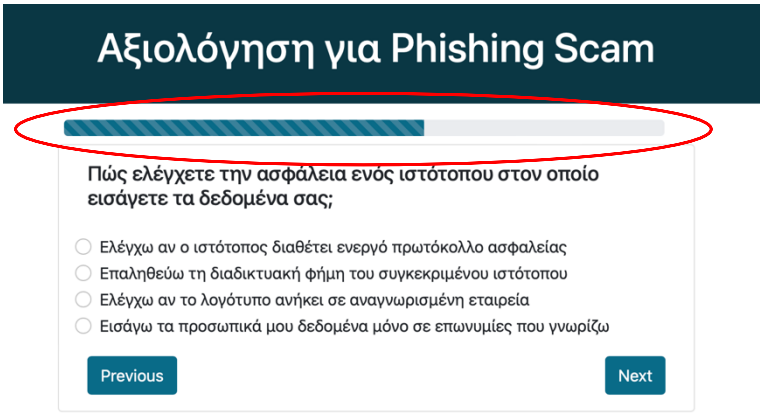


Εικόνα 35

Πατώντας στο κουμπί Έναρξη Αξιολόγησης σε μία από τις προσφερόμενες αξιολόγησης ο χρήστης μεταφέρεται σε μία νέα οθόνη στην πλατφόρμα όπου μπορεί να απαντήσει σε 5 ερωτήσεις κλειστού τύπου πολλαπλής επιλογής.

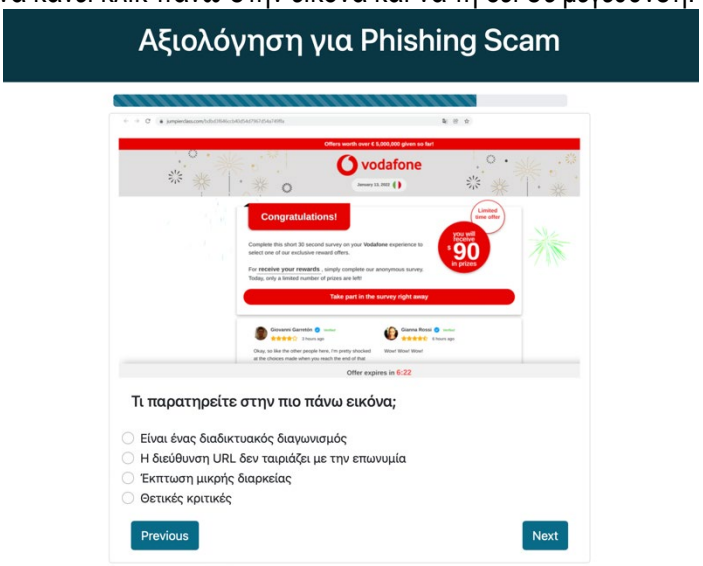
Εικόνα 36

Ο χρήστης μπορεί να διαπίστωση το υπόλοιπο που του απτομένη για να ολοκλήρωση την αξιολόγηση του από την γραμμή προόδου που βρίσκεται πάνω από κάθε ερώτηση.

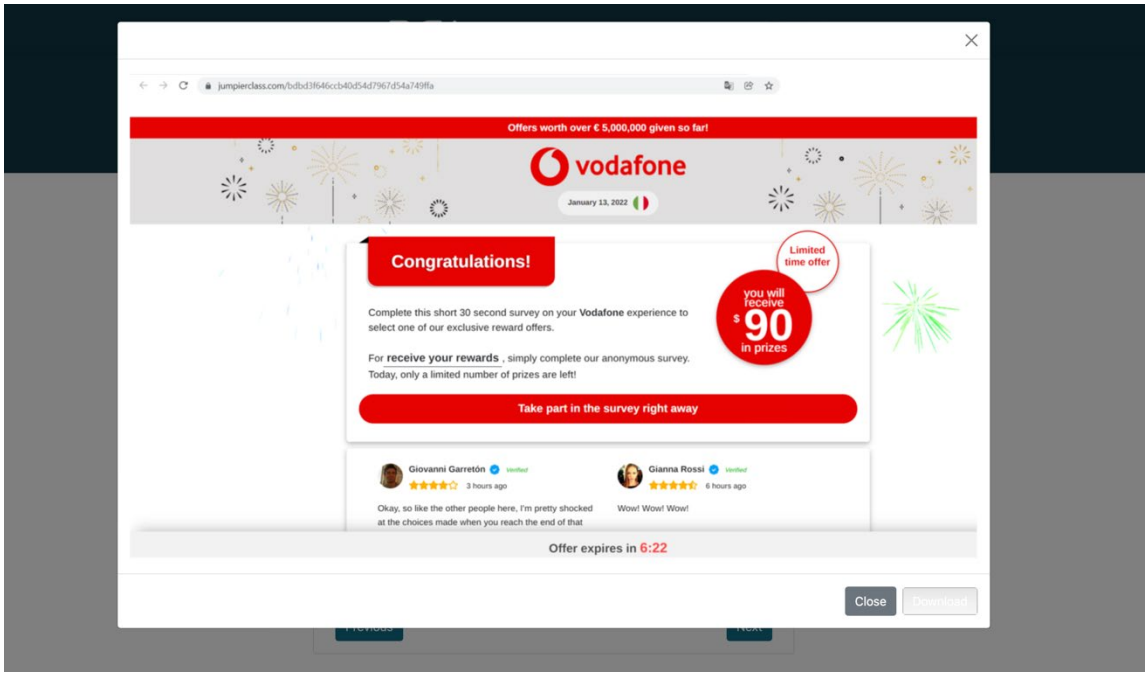


Εικόνα 37

Ακόμη σε ερωτήσεις όπου ο χρήστης καλείται να εξετάσει μια εικόνα και να απαντήσει με βάσει την εικόνα μπορεί να κάνει κλικ πάνω στην εικόνα και να τη δει σε μεγέθυνση.

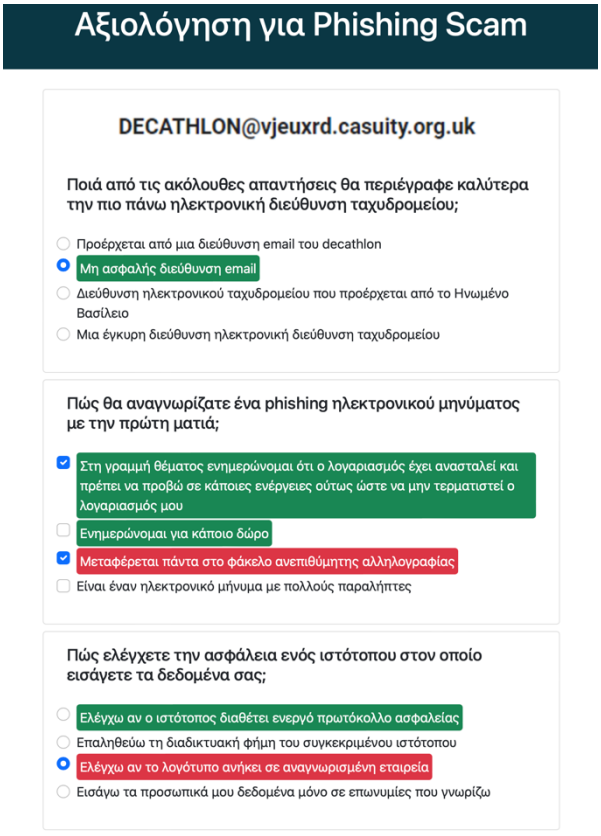


Εικόνα 38



Εικόνα 39

Με το τέλος της αξιολόγηση ο χρήστης μπορεί να δει τις απαντήσεις που έδωσε καθώς και τη/ις σωστη/ες απαντίση/εις σε κάθε ερώτηση.



Εικόνα 40

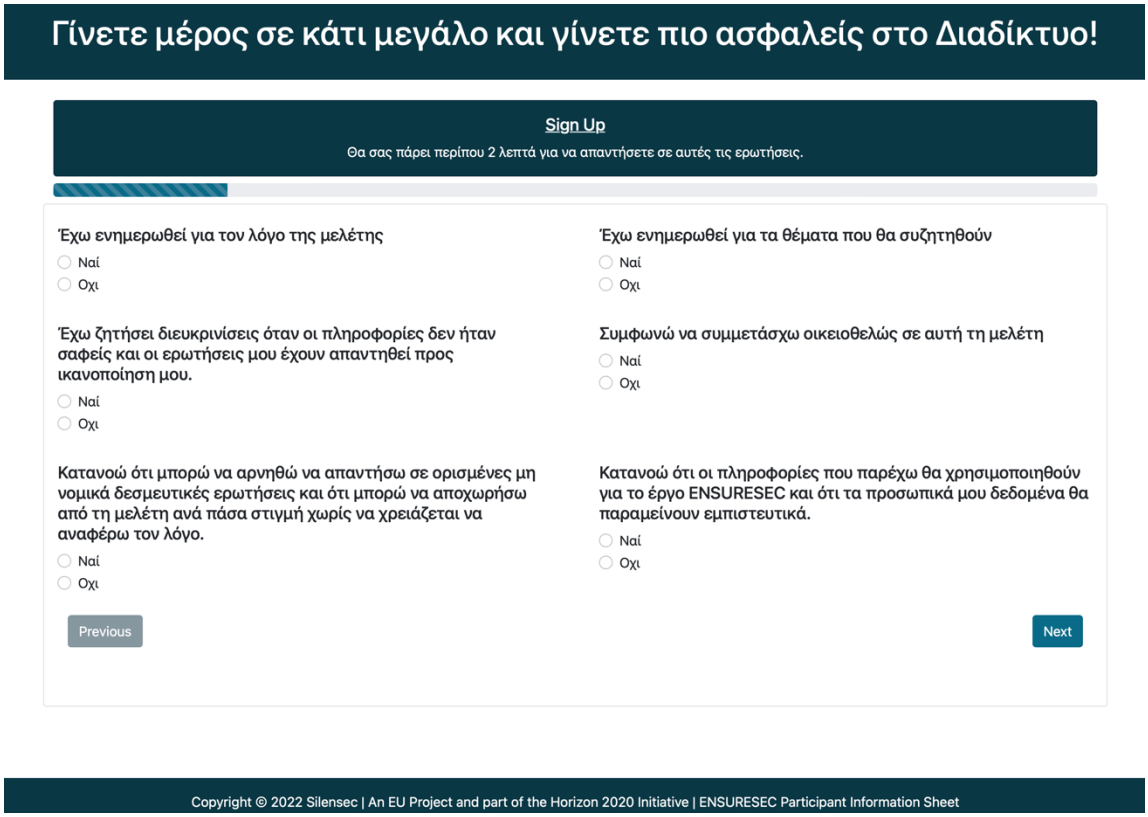
Εγγραφή για Προσομοίωση

Σε αυτή την οθόνη καλείται ο χρήστης να εγγραφή για να λάβει μέρος σε μία προσομοίωση επίθεσης κοινωνικής μηχανικής και να μας εξουσιοδότηση για την αποστολή ηλεκτρονικού μνήματος προσομοίωση επίθεσης κοινωνικής μηχανικής.

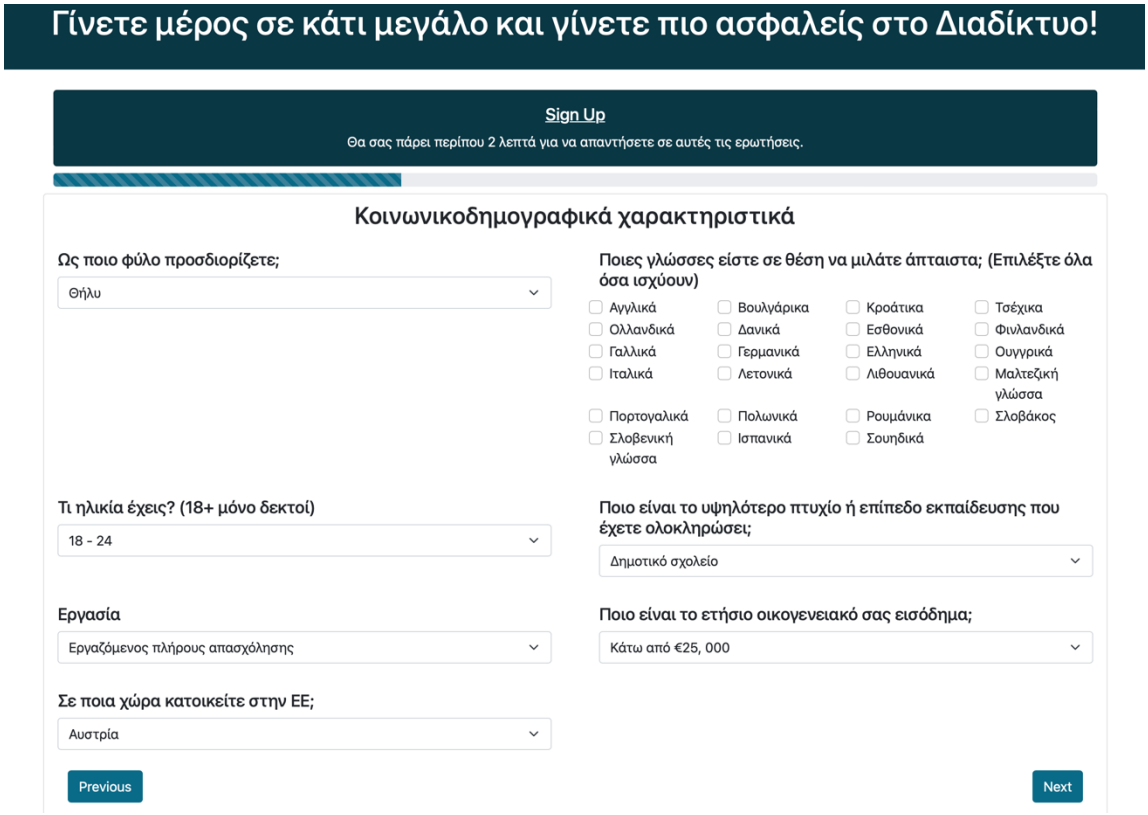
Εικόνα 41

Εικόνα 42

Ο χρήστης πατώντας στο κουμπί Εγράφητε τώρα οδηγείται σε νέα οθόνη όπου πρέπει να απαντήσει σε μερικές ερωτήσεις καθώς επίσης να μας εξουσιοδοτήσει για τις προσομοιώσεις επίθεσης κοινωνικής μηχανικής.

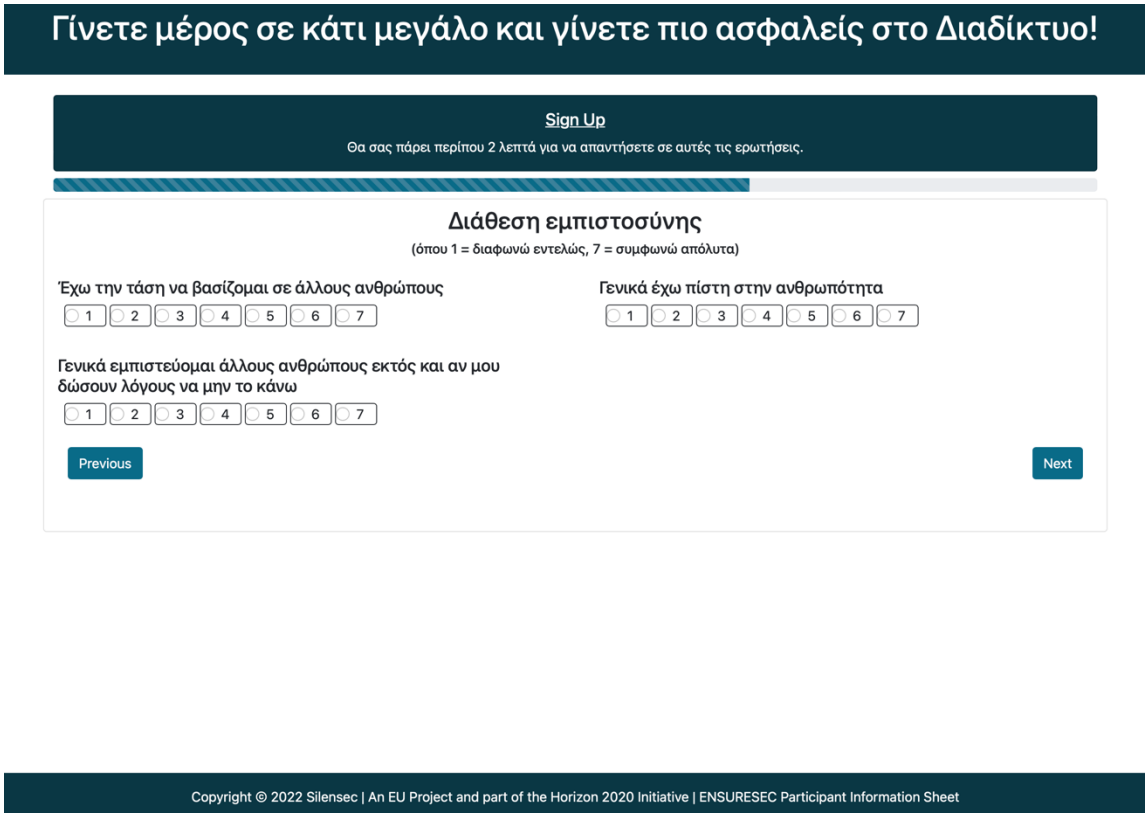


Εικόνα 43

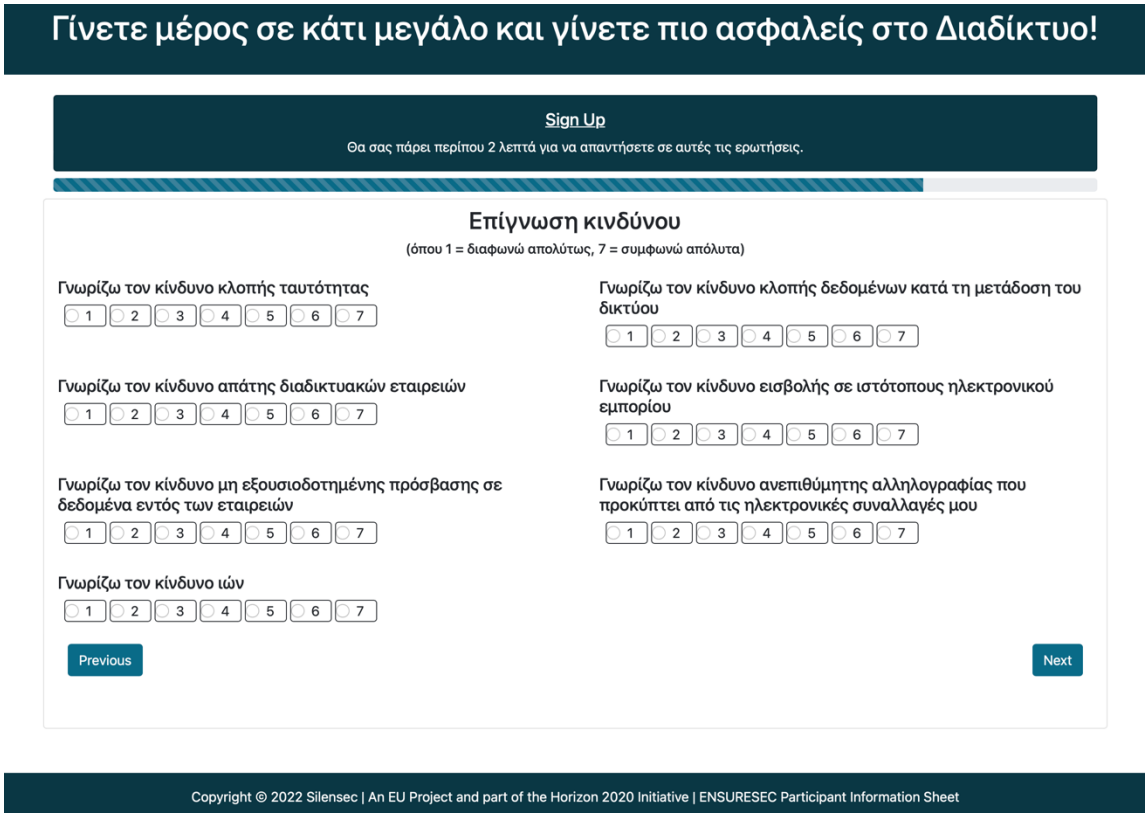


Εικόνα 44

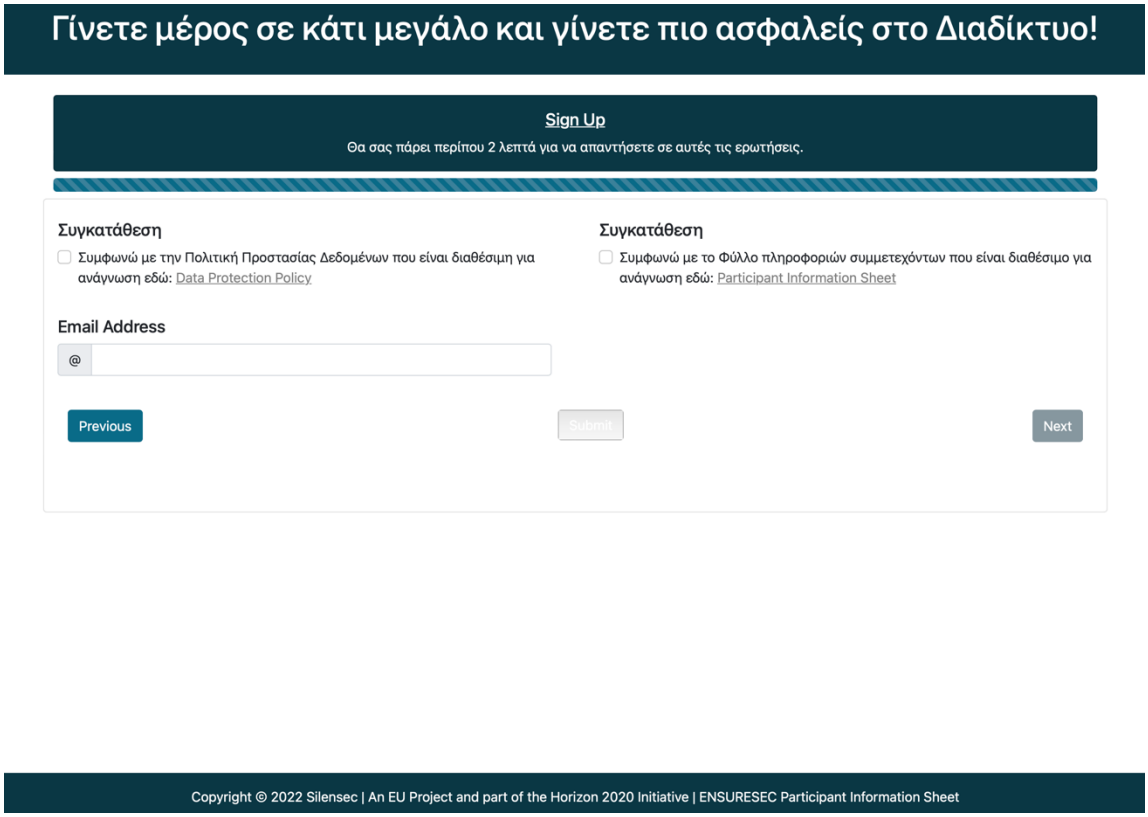
Εικόνα 45



Εικόνα 46



Εικόνα 47



Εικόνα 48

4.3 Υπηρεσία ανάλυσης επισκεψιμότητας

Για την καταγραφή και την ανάλυση των επισκεπτών της πλατφόρμας εκπαίδευσης έγινε χρήση του λογισμικού Open Web Analytics. Το Open Web Analytics είναι ένα δωρεάν και ανοιχτού κώδικα πλαίσιο αναλυτικών στοιχείων ιστού που μας επιτρέπει να διατηρείτε ο έλεγχος του τρόπου με τον οποίο οργανώνουμε και αναλύουμε τη χρήση των ιστότοπων και της εφαρμογής μας.
Οι λόγοι που οδήγησαν στην χρήση του OWA είναι:

Έλεγχος

Η δυνατότητα ανάπτυξης του σε ιδιωτικό διακομιστή εντός της Ευρωπαϊκής ένωσης και η διασφάλιση των δεδομένων των επισκεπτών να μην πέσουν σε με εξουσιοδοτημένες οντότητες.

Προσαρμογή

Το OWA είναι ένα προσαρμόσιμο πλαίσιο αναλυτικών στοιχείων ιστού που μπορεί να επεκταθεί για να καλύψει τις ανάγκες μας.

Μετρήσεις, Διαστάσεις, Αναφορές

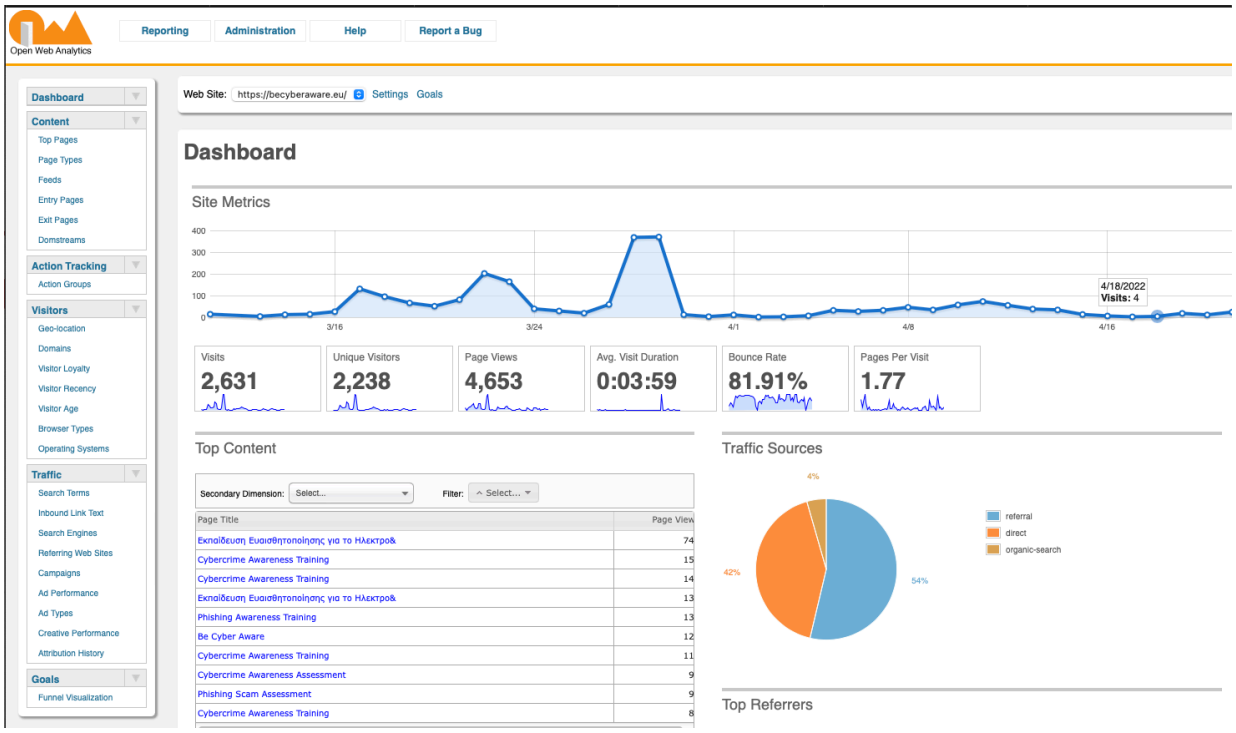
Το OWS μάς παρέχει δεκάδες τυπικές μετρήσεις, διαστάσεις και αναφορές.

API πρόσβασης δεδομένων

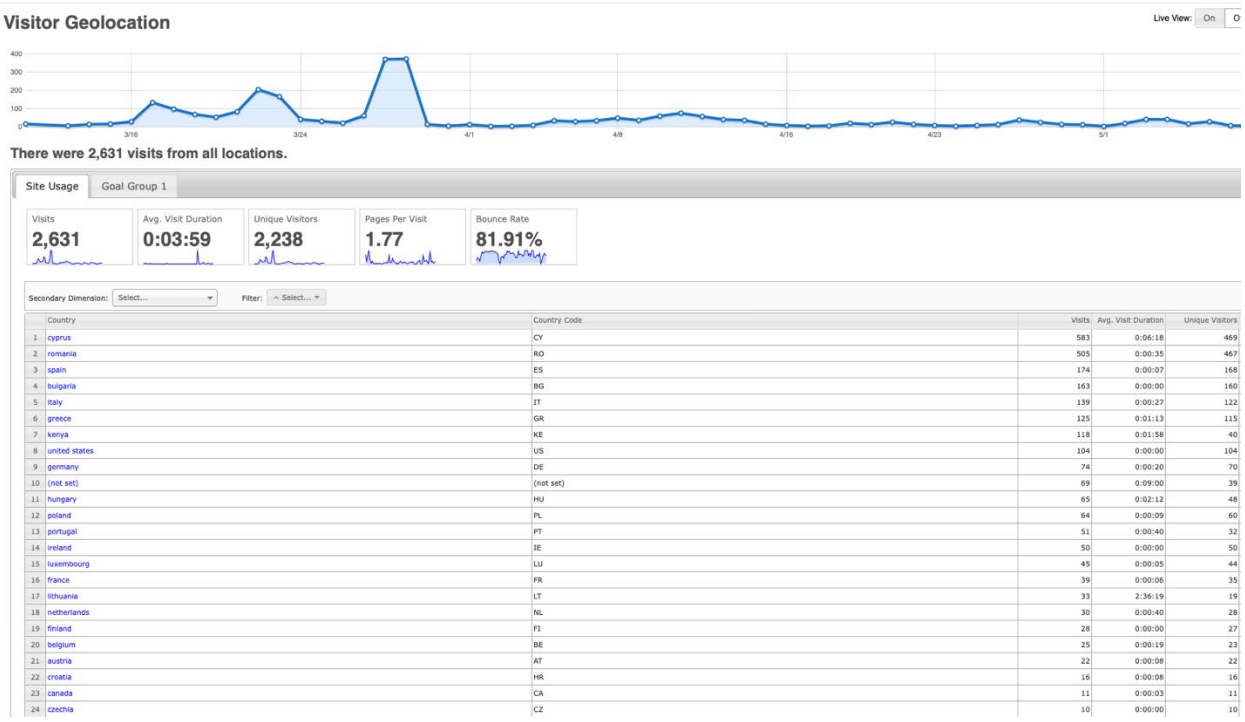
Το API εκτεταμένης πρόσβασης δεδομένων επιτρέπει την ενοποίηση και την πρόσβαση σε μη επεξεργασμένα δεδομένα.

Έλεγχος απορρήτου

Σέβεται το GDRP και άλλα πλαίσια απορρήτου.



Εικόνα 49



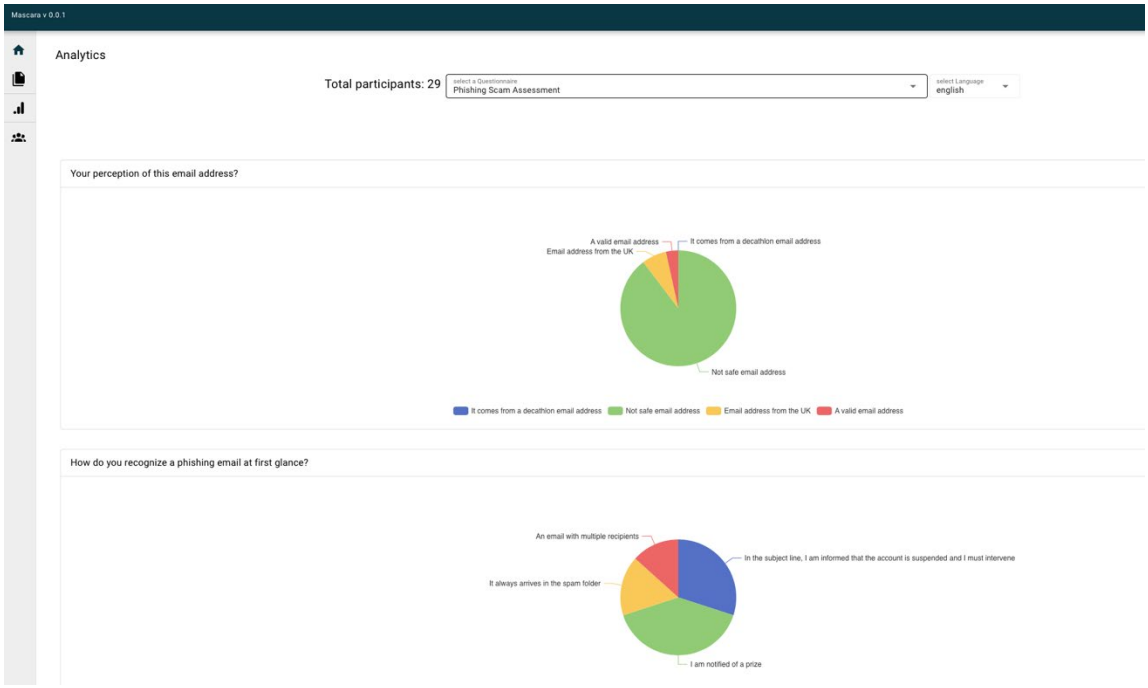
	Country	Country Code	Visits	Avg. Visit Duration	Unique Visitors
1	cyprus	CY	583	0:06:18	469
2	romania	RO	505	0:00:35	467
3	spain	ES	174	0:00:07	168
4	bulgaria	BG	163	0:00:00	160
5	italy	IT	139	0:00:27	122
6	greece	GR	125	0:01:13	115
7	kenya	KE	118	0:01:58	40
8	united states	US	104	0:00:00	104
9	germany	DE	74	0:00:20	70
10	(not set)	(not set)	69	0:09:00	39
11	hungary	HU	65	0:02:12	48
12	poland	PL	64	0:00:09	60
13	portugal	PT	51	0:00:40	32
14	ireland	IE	50	0:00:00	50
15	luxembourg	LU	45	0:00:05	44
16	france	FR	39	0:00:06	35
17	lithuania	LT	33	2:36:19	19
18	netherlands	NL	30	0:00:40	28
19	finland	FI	28	0:00:00	27
20	belgium	BE	25	0:00:19	23
21	austria	AT	22	0:00:08	22
22	croatia	HR	16	0:00:08	16
23	canada	CA	11	0:00:03	11
24	czechia	CZ	10	0:00:00	10

Εικόνα 50

Κεφάλαιο 5

Αποτελέσματα

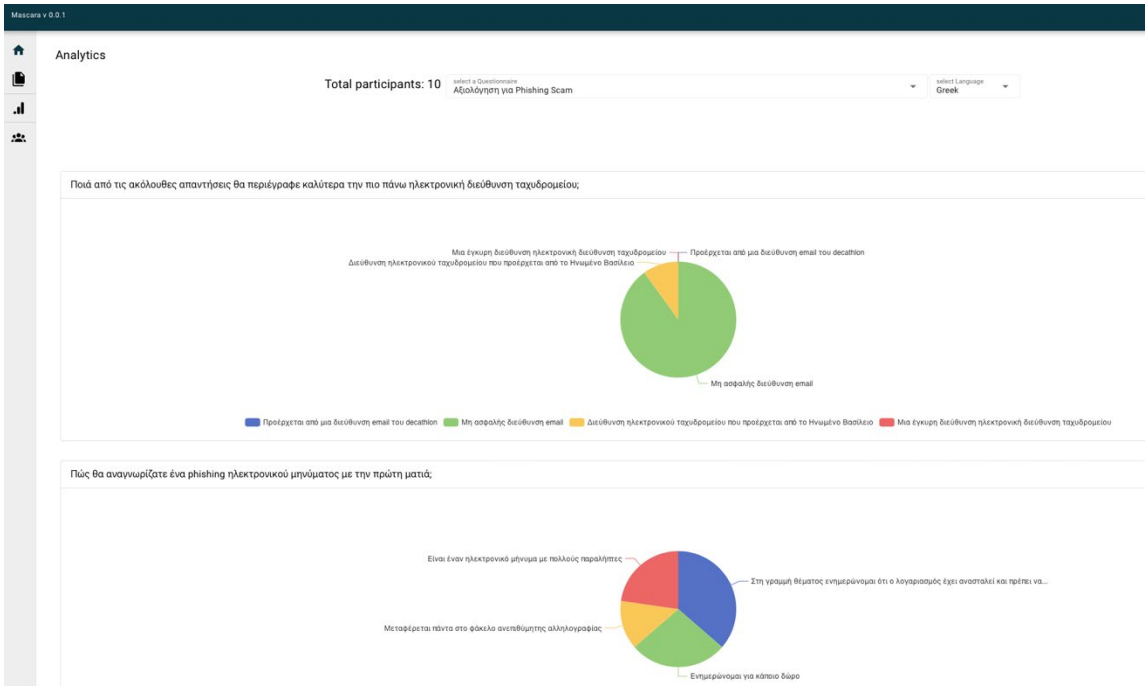
Αξιολόγηση επίθεσης τύπου Phishing



Εικόνα 51

Γλώσσα	Συμμετέχοντες
Αγγλικά	29
Ποια από τις ακόλουθες απαντήσεις θα περιέγραφε καλύτερα την πιο πάνω ηλεκτρονική διεύθυνση ταχυδρομείου;	
Προέρχεται από μια διεύθυνση email του decathlon	0
Μη ασφαλής διεύθυνση email	26
Διεύθυνση ηλεκτρονικού ταχυδρομείου που προέρχεται από το Ηνωμένο Βασίλειο	2
Μια έγκυρη διεύθυνση ηλεκτρονική διεύθυνση ταχυδρομείου	1
Πώς θα αναγνωρίζατε ένα phishing ηλεκτρονικού μηνύματος με την πρώτη ματιά;	
Στη γραμμή θέματος ενημερώνομαι ότι ο λογαριασμός έχει ανασταλεί και πρέπει να προβώ σε κάποιες ενέργειες ούτως ώστε να μην τερματιστεί ο λογαριασμός μου	18
Ενημερώνομαι για κάποιο δώρο	24

Μεταφέρεται πάντα στο φάκελο ανεπιθύμητης αλληλογραφίας	10
Είναι έναν ηλεκτρονικό μήνυμα με πολλούς παραλήπτες	8
Πώς ελέγχετε την ασφάλεια ενός ιστότοπου στον οποίο εισάγετε τα δεδομένα σας;	
Ελέγχω αν ο ιστότοπος διαθέτει ενεργό πρωτόκολλο ασφαλείας	16
Επαληθεύω τη διαδικτυακή φήμη του συγκεκριμένου ιστότοπου	4
Ελέγχω αν το λογότυπο ανήκει σε αναγνωρισμένη εταιρεία	2
Εισάγω τα προσωπικά μου δεδομένα μόνο σε επωνυμίες που γνωρίζω	7
Τι παρατηρείτε στην πιο πάνω εικόνα;	
Είναι ένας διαδικτυακός διαγωνισμός	0
Η διεύθυνση URL δεν ταιριάζει με την επωνυμία	28
Έκπτωση μικρής διαρκείας	0
Θετικές κριτικές	1
Πώς αναγνωρίζετε ότι οι σύνδεσμοι που εμπεριέχονται στα ηλεκτρονικά μηνύματα αναφέρονται στον ιστότοπο του αποστολέα;	
Ανοίγω τον υπερσύνδεσμο	1
Τοποθετώ τον κέρσορα και επαληθεύω ότι είναι αξιόπιστος σύνδεσμος	22
Ελέγχω τη συνοχή στο κύριο μέρος του ηλεκτρονικού μηνύματος	5
Εξαρτάται από την ενέργεια που σε παροτρύνει το συγκεκριμένο κουμπί να κάνεις	1

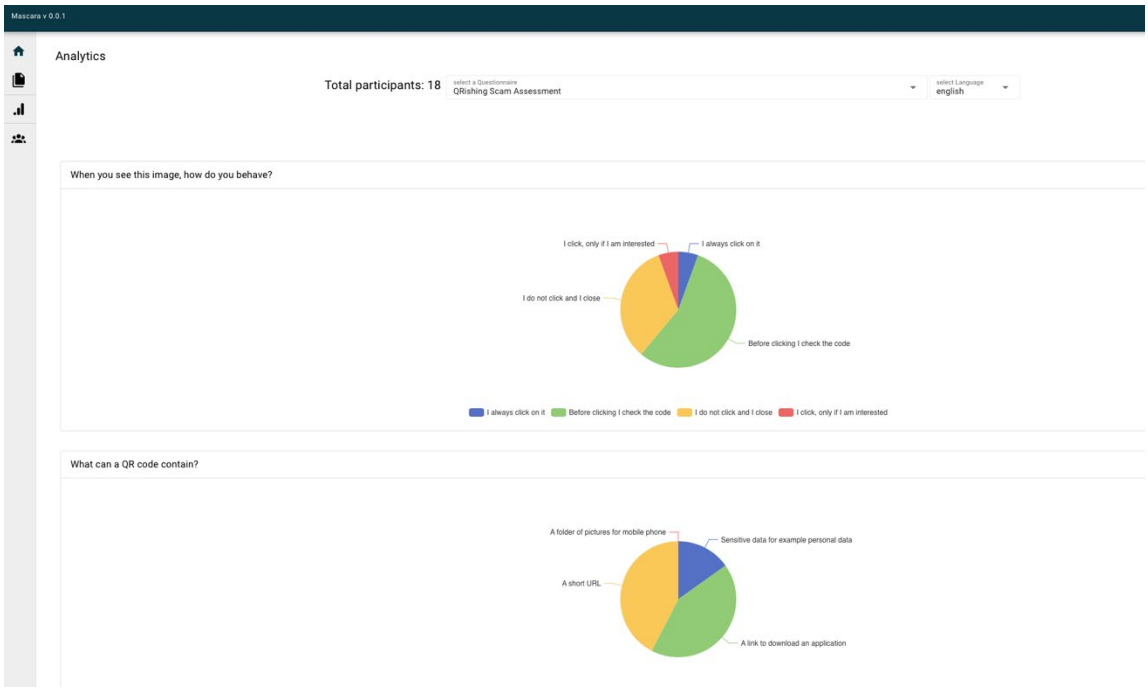

Mascara v 0.0.1
Analytics
Total participants: 10
select a Questionnaire
Αξιολόγηση για Phishing Scam
select Language
Greek
Ποιά από τις ακόλουθες απαντήσεις θα περιέγραφε καλύτερα την πιο πάνω ηλεκτρονική διεύθυνση ταχυδρομείου;
Μια έγκυρη διεύθυνση ηλεκτρονική διεύθυνση ταχυδρομείου
Προέρχεται από μια διεύθυνση email του decathlon
Διεύθυνση ηλεκτρονικού ταχυδρομείου που προέρχεται από το Ηνωμένο Βασίλειο
Μη ασφαλής διεύθυνση email
Προέρχεται από μια διεύθυνση email του decathlon
Μη ασφαλής διεύθυνση email
Διεύθυνση ηλεκτρονικού ταχυδρομείου που προέρχεται από το Ηνωμένο Βασίλειο
Μια έγκυρη διεύθυνση ηλεκτρονική διεύθυνση ταχυδρομείου
Πώς θα αναγνωρίζατε ένα phishing ηλεκτρονικού μηνύματος με την πρώτη ματιά;
Είναι έναν ηλεκτρονικό μήνυμα με πολλούς παραλήπτες
Στη γραμμή θέματος ενημερώνομαι ότι ο λογαριασμός έχει ανασταλεί και πρέπει να...
Μεταφέρεται πάντα στο φάκελο ανεπιθύμητης αλληλογραφίας
Ενημερώνομαι για κάποιο δώρο

Εικόνα 52

Γλώσσα	Συμμετέχοντες
Ελληνικά	11
Ποιά από τις ακόλουθες απαντήσεις θα περιέγραφε καλύτερα την πιο πάνω ηλεκτρονική διεύθυνση ταχυδρομείου;	
Προέρχεται από μια διεύθυνση email του decathlon	0
Μη ασφαλής διεύθυνση email	10
Διεύθυνση ηλεκτρονικού ταχυδρομείου που προέρχεται από το Ηνωμένο Βασίλειο	1
Μια έγκυρη διεύθυνση ηλεκτρονική διεύθυνση ταχυδρομείου	0
Πώς θα αναγνωρίζατε ένα phishing ηλεκτρονικού μηνύματος με την πρώτη ματιά;	
Στη γραμμή θέματος ενημερώνομαι ότι ο λογαριασμός έχει ανασταλεί και πρέπει να προβώ σε κάποιες ενέργειες ούτως ώστε να μην τερματιστεί ο λογαριασμός μου	9
Ενημερώνομαι για κάποιο δώρο	7
Μεταφέρεται πάντα στο φάκελο ανεπιθύμητης αλληλογραφίας	3
Είναι έναν ηλεκτρονικό μήνυμα με πολλούς παραλήπτες	5
Πώς ελέγχετε την ασφάλεια ενός ιστότοπου στον οποίο εισάγετε τα δεδομένα σας;	
Ελέγχω αν ο ιστότοπος διαθέτει ενεργό πρωτόκολλο ασφαλείας	6
Επαληθεύω τη διαδικτυακή φήμη του συγκεκριμένου ιστότοπου	2
Ελέγχω αν το λογότυπο ανήκει σε αναγνωρισμένη εταιρεία	3
Εισάγω τα προσωπικά μου δεδομένα μόνο σε επωνυμίες που γνωρίζω	0
Τι παρατηρείτε στην πιο πάνω εικόνα;	
Είναι ένας διαδικτυακός διαγωνισμός	0
Η διεύθυνση URL δεν ταιριάζει με την επωνυμία	10
Έκπτωση μικρής διαρκείας	1
Θετικές κριτικές	0
Πώς αναγνωρίζετε ότι οι σύνδεσμοι που εμπεριέχονται στα ηλεκτρονικά μηνύματα αναφέρονται στον ιστότοπο του αποστολέα;	

Ανοίγω τον υπερσύνδεσμο	1
Τοποθετώ τον κέρσορα και επαληθεύω ότι είναι αξιόπιστος σύνδεσμος	6
Ελέγχω τη συνοχή στο κύριο μέρος του ηλεκτρονικού μηνύματος	0
Εξαρτάται από την ενέργεια που σε παροτρύνει το συγκεκριμένο κουμπί να κάνεις	4

Αξιολόγηση επίθεσης τύπου QRishing



Εικόνα 53

Γλώσσα	Συμμετέχοντες
Αγγλικά	18
Ποιά θα είναι η ενέργεια σας με βάση την πιο πάνω εικόνα.	
Πάντα κάνω κλικ	1
Πριν κάνω κλικ, ελέγχω τον QR κωδικό	10
Δεν κάνω κλικ και κλείνω	0
Κάνω κλικ, μόνο αν με ενδιαφέρει	1
Τι μπορεί να περιέχει ένας QR κωδικός;	
Ευαίσθητα δεδομένα , για παράδειγμα προσωπικά δεδομένα	5
Έναν υπερσύνδεσμο για τη λήψη μιας εφαρμογής	14
Ένα σύντομο υπερσύνδεσμο	14

Ένα φάκελο με φωτογραφίες	0
Ποια εργαλείο μπορείτε να χρησιμοποιήσετε για να σαρώσετε τον κωδικό QR;	
Με χρήση κάμερας κινητού τηλεφώνου	8
Με χρήση ηλεκτρονικού υπολογιστή	2
Με χρήση εφαρμογής σάρωσης κωδικού QR	8
Με χρήση ηλεκτρονικής ταμπλέτας (Tablet)	0
Μέσω ποιων καναλιών μπορεί να λάβεις κάποιο κωδικό QR;	
Μέσω ηλεκτρονικού μηνύματος	14
Μέσω των Κοινωνικών δικτύων (π.χ Facebook/ Instagram)	13
Μέσω διαφημιστικών πινακίδων	12
Μέσω της τηλεόρασης	6
Ποιες θα είναι οι συνέπειες μίας σάρωσης ενός κακόβουλου κωδικού QR;	
Λήψη κακόβουλου λογισμικού	14
Μετάβαση σε κακόβουλη ιστοσελίδα	14
Πρόκληση ζημιάς στη συσκευή σάρωσης (π.χ στο κινητό τηλέφωνο, στο tablet	10
Απώλεια αριθμών τηλεφωνικού καταλόγου	7

Ανάλυση αποτελεσμάτων

Στην αξιολόγηση Phishing 77% του κοινού που έλαβε μέρος στην αγγλική έκδοση του ερωτηματολογίου απάντησαν σωστά. Κοντά στο ίδιο ποσοστό βρίσκεται και το κοινό που έλαβε μέρος στην ελληνική έκδοση με ποσοστό 72%.

Η ερώτηση με το χαμηλότερο ποσοστό επιτυχίας ήταν «Πώς ελέγχετε την ασφάλεια ενός ιστότοπου στον οποίο εισάγετε τα δεδομένα σας;» με ποσοστό 55%.

Στην αξιολόγηση QRishing 64.7% του κοινού που έλαβε μέρος στην αγγλική έκδοση του ερωτηματολογίου απάντησαν σωστά.

Η ερώτηση με το χαμηλότερο ποσοστό επιτυχίας ήταν «Τι μπορεί να περιέχει ένας QR κωδικός;» με ποσοστό 61%.

Κεφάλαιο 6

Επίλογος και Συμπεράσματα

Στην παρούσα μεταπτυχιακή διατριβή αναλύθηκαν οι τεχνικές και οι πρακτικές κοινωνική μηχανικής καθώς επίσης οι τεχνικές και οι πρακτικές παραπλάνησης στο marketing. Ακόμη παρουσιάστηκαν οι απειλές και τεχνικές της κοινωνικής μηχανικής στο ψηφιακό εμπόριο καθώς επίσης η ανάπτυξη διαδικτυακής πλατφόρμας “Be Cyber Aware” εκπαίδευσης και αξιολόγησης των καταναλωτών. Επιπλέων αναπτύχθηκε το εργαλείο “MASCARA” για την προσομοίωση τον επιθέσεων της κοινωνικής μηχανικής.

Επιπλέον, ένα κεφάλαιο αναφέρθηκε στην κοινωνική μηχανική και στις πρακτικές παραπλάνησης το marketing αποδίδοντας ορισμούς, ώστε να γίνει αντιληπτό τι ακριβώς είναι και πως λειτουργεί. Επίσης ακολούθησε μια κατηγοριοποίηση των ανθρώπων που μπορεί να πέσουν θύματα των πιο πάνω.

Ακολούθησες η ανάλυση της ανάπτυξης του εργαλείου MASCARA που μας βοηθά να δημιουργήσουμε και να αναπτύξουμε εύκολα εφαρμογές ιστού, από απλούς ιστότοπους, ιστότοπους WordPress ή εφαρμογές Django έως πιο περίπλοκες υπηρεσίες όπως διακομιστές αλληλογραφίας ή διαδικασίες όπως η αποστολή αυτοματοποιημένων μηνυμάτων ηλεκτρονικού ταχυδρομείου σε συγκεκριμένες ομάδες-στόχους χωρίς υπερβολικά περίπλοκες διαμορφώσεις που απαιτούνται από χειροκίνητη εγκατάσταση τέτοιων συστημάτων.

Στην συνέχεια αναλύεται η δημιουργία της διαδικτυακής πλατφόρμας Be Cyber Aware που έχει ως στόχο την εκπαίδευση και ευαισθητοποίησης για την ασφάλεια του ψηφιακού εμπορίου. Παρέχοντας δωρεάν εκπαιδευτικό περιεχόμενο για την ευαισθητοποίηση στον κυβερνοχώρο (βίντεο και κείμενο).

Τέλος γίνεται αναφορά στις αξιολογήσεις σχετικά με τη επίγνωση στην κυβερνοασφάλεια και τα αποτελέσματα από τα ερωτηματολόγια.

Κεφάλαιο 7

Μελλοντική δουλέια

7.1 Αυτοματοποίηση του διακομιστή αλληλογραφίας

Κατά τη δημιουργία ενός ιστότοπου ή μιας εφαρμογής, είναι πιθανό να θέλουμε επίσης έναν διακομιστή αλληλογραφίας για να χειρίζεται τα εισερχόμενα και εξερχόμενα email. Κάνοντας αυτή τη ροή εργασίας χειροκίνητα, κάθε φορά είναι χρονοβόρα. Επίσης, ένα άλλο μειονέκτημα του να το κάνεις χειροκίνητα είναι το γεγονός ότι είναι ευάλωτο σε λανθασμένη διαμόρφωση και αυτό θα οδηγήσει και πάλι σε χρονοβόρα διαδικασίας λόγω σφάλματος.
Η αυτοματοποίηση της διαμόρφωσης του διακομιστή αλληλογραφίας και η δημιουργία μιας νέας βάσης διεύθυνσης email στον τομέα του σεναρίου θα επιταχύνει τη διαδικασία δημιουργίας νέων σεναρίων με δυνατότητα αποστολής email και ελαχιστοποίηση των εσφαλμένων διαμορφώσεων και σφαλμάτων.
Αυτό μπορεί να επιτευχθεί με τη δημιουργία και την προρύθμιση μιας εικόνας docker με τις απαραίτητες διαμορφώσεις και τη χρήση της όποτε χρειάζεται, αλλάζοντας μερικές παραμέτρους κάθε φορά.

7.2 Αυτοματοποίηση της δημιουργίας μιας φόρμας εισαγωγής παραμέτρων του widget με βάση το «σχήμα» json της προσθήκης παραμέτρων.

Αυτήν τη στιγμή, η διαμόρφωση του widget μέσα στη φόρμα δημιουργίας είναι απλώς ένα πεδίο περιοχής κειμένου που λαμβάνει ολόκληρη τη διαμόρφωση. Η διαμόρφωση προετοιμάζεται χειροκίνητα στο πεδίο εισαγωγής ή χρησιμοποιώντας μια διαμόρφωση προεπισκοπήσεων και αλλάζοντας τις απαραίτητες τιμές. Αυτή η ενέργεια μπορεί να προκαλέσει σύγχυση στους νεότερους χρήστες και επίσης να οδηγήσει σε εσφαλμένη διαμόρφωση λόγω έλλειψης καθοδήγησης. Η ιδέα είναι η δημιουργία των απαραίτητων πεδίων με βάση το σχήμα json κάθε πρόσθετου που υποστηρίζει το MASCARA για τη διαμόρφωση, ώστε ο χρήστης να μπορεί να εισάγει εύκολα τις παραμέτρους.
Το κύριο πλεονέκτημα αυτού είναι η ελαχιστοποίηση των παραμέτρων που λείπουν ή η εσφαλμένη διαμόρφωση στο πεδίο διαμόρφωσης ενός widget.

7.3 Αυτοματοποίηση και προγραμματισμός της εκτέλεση μιας καμπάνιας

Προς το παρόν υποστηρίζεται μόνο η μη αυτόματη εκτέλεση για μια καμπάνια, αυτό σημαίνει ότι κάθε φορά που χρειάζεται να ξεκινήσει μια νέα καμπάνια π.χ. στης 02:00 π.μ. πρέπει να γίνει χειροκίνητα. Φυσικά αυτό δεν είναι ιδανικό γιατί εξαρτάται από μια ανθρώπινη πράξη και μερικές φορές ο άνθρωπος ξεχνά να κάνει τη δουλειά του. Ένα χαρακτηριστικό του προγραμματισμού της εκτέλεσης της καμπάνιας θα δώσει την ευκαιρία για τη δημιουργία πιο περίπλοκων σεναρίων και χωρίς να ανησυχούμε όταν έρθει η ώρα για την εκτέλεσή της.
Αυτό θα το επιτευχθεί εφαρμόζοντας έναν μηχανισμό χρονοδιαγράμματος, με αποτέλεσμα η καμπάνια να παίρνει ως είσοδο την ημερομηνία και την ώρα που χρειάζεται να εκτελεστεί και στη συνέχεια ο μηχανισμό θα ελέγχει και θα εκτελεί κάθε καμπάνια.

7.4 Εξαγωγή δεδομένων

Σε ένα τέτοιο έργο κύριος στόχος είναι η συλλογή δεδομένων σχετικά με τη συμπεριφορά της ομάδας στόχου των χρηστών και στο τέλος να αναλυθούν από τους ειδικούς. Αυτήν τη στιγμή τα δεδομένα αποθηκεύονται σε μια βάση δεδομένων και μπορούν να προσπελαστούν μόνο από την πλατφόρμα MASCARA χωρίς καμία υποστήριξη εξαγωγής των δεδομένων. Αυτό έχει ως αποτέλεσμα ελάχιστα συμπεράσματα και εγκλωβίζεται στα γραφήματα που ήδη εφαρμόστηκαν. Με την εξαγωγή των ακατέργαστων δεδομένων θα δοθεί η ευκαιρία για πιο εις βάθος ανάλυση χρησιμοποιώντας περισσότερα εργαλεία και εύρεση συσχετίσεων.
Τα δεδομένα μπορούν να εξαχθούν για κάθε καμπάνια σε μορφή csv.

7.5 Ενσωμάτωση με το Facebook και το Google

Πολλές από τις επιθέσεις κοινωνικής μηχανικής λαμβάνουν χώρα στις πλατφόρμες μέσων κοινωνικής δικτύωσης και από ψευδείς διαφημίσεις στο google. Ο χρόνος που χρειάζεται για να επενδύσεις για τη δημιουργία σελίδας και αναρτήσεων καθημερινά στα social media είναι πολύς. Επίσης ένα άλλο πρόβλημα είναι ο μηχανισμός ασφαλείας που έχει αυτή η πλατφόρμα και μπορεί εύκολα να μπλοκάρει την ανάρτηση και να απενεργοποιήσει την σελίδα. Και αυτός είναι ο λόγος που τα πειράματα χρειάζονται πολύ χρόνο και στο τέλος τα αποτελέσματα μερικές φορές δεν είναι έγκυρα μετά από τόσο μεγάλο χρονικό διάστημα.
Με την ενσωμάτωση με τις πλατφόρμες μέσων κοινωνικής δικτύωσης και το Google Ads, αυτό θα δώσει την ευκαιρία για τη δημιουργία πιο περίπλοκων επιθέσεων αυτοματοποιώντας τη δημοσίευση μιας διαφήμισης στα μέσα κοινωνικής δικτύωσης ή στο google σε λιγότερο χρόνο. Επιπλέον, μπορούμε να εξαγάγουμε δεδομένα από αυτές τις πλατφόρμες, όπως η αλληλεπίδραση των χρηστών και η ηλικία της ομάδας ατόμων που αλληλεπιδρούν με τη διαφήμιση.

Bibliography

[1] K. R. R. B. R. C. Venkatesha Sushruth, Social Engineering Attacks During the COVID-19 Pandemic, 2021.

[2] P. W. Christopher Hadnagy, Social Engineering, John Wiley &Sons; 1st edition, 2010.

[3] Y.-C. CHIANG, Social Engineering and the Social Sciences in China, 1919-1949, Cambridge University Press, 2001.

[4] "What Is Social Engineering," [Online]. Available: https://www.comptia.org/content/articles/what-is-social-engineering.

[5] "Δούρειος Ίππος," [Online]. Available: https://el.wikipedia.org/wiki/Δούρειος_Ίππος.

[6] N. K. Fatima Salahdine, Social Engineering Attacks: A Survey, 2019.

[7] R. E. Aditya K Sood, Malvertising - Exploiting web advertising, 2011.

[8] L. Z. AHMED ALEROUD, Phishing Environments, Techniques, and Countermeasures: A Survey, 2017.

[9] J. G.-C. A. C. R. C. Aritz Arrate, Malvertising in Facebook: Analysis, Quantification and Solution, 2020.

[10] D. V. S.Sibi Chakkaravarthy, A Survey on malware analysis and mitigation techniques, 2018.

[11] T. K. STEPHEN, Control of deceptive advertisements in India, 2018.

[12] R. N. Aditya, The psychology of deception in marketing: A conceptual framework for research and practice, 2001.

[13] M. Eabrasu, Cheating in Business: A Metaethical Perspective, 2020.

[14] R. M. D. M. B. Guang-Xin Xie, Disentangling the Effects of Perceived Deception and Anticipated Harm on Consumer Responses to Deceptive Advertising, 2015.

[15] A. N. N. S. Y. Z. Z. M. S. B.B.Gupta, Recent research in computational intelligence paradigms into security and privacy for online social networks (OSNs), 2018.

[16] V. P. A. T. N. F. S. S. E. A. Y. Pedram Hayati, Definition of spam 2.0: New spamming boom, 2010.

[17] N. L. Rohan Miller, Social media and its implications for viral marketing, 2010.

[18] B. Xiao, Product-related deceptive information practices in B2C e-commerce :formation, outcomes, and detection., Vancouver :University of British Columbia, 2010.

[19] N. K. ,. D. B. Xiao Han, Deception Techniques in Computer Security: A Research Perspective, 2019.

[20] "What is Deceptive Pricing: Basics," [Online]. Available: https://sendpulse.com/support/glossary/deceptive-pricing.

[21] Google, "Google Ads Help," [Online]. Available: https://support.google.com/google-ads/answer/2615875?hl=en.

[22] H. 2. Framework, "General Data Protection Regulation," [Online]. Available: https://gdpr.eu/.

[23] I. Org, "Lawfulness, fairness and transparency," [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/.

[24] I. Org, "Security," [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/.

[25] E. D. P. Supervisor, "Data minimization," [Online]. Available: https://edps.europa.eu/data-protection/data-protection/glossary/d_en.

[26] Iapp, "Third parties under GDPR and CCPA," [Online]. Available: https://iapp.org/news/a/what-you-must-know-about-third-parties-under-the-gdpr-ccpa/.

[27] M. P. Srinivasan Balakrishnan, Information asymmetry, adverse selection and joint-ventures: Theory and evidence, 2002.

[28] Europa, "How digitalised are EU's enterprises," [Online]. Available: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211029-1.

[29] S. Canada, "Intensity of Internet Use in Canada: Understanding Different Types of Users," [Online]. Available: https://www150.statcan.gc.ca/n1/pub/88f0006x/2010002/part-partie1-eng.htm.

[30] B. F. A. Brečko, The Digital Competence Framework for Consumers, 2016.

[31] T. A. S. Jeff Langenderfer, Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion, 2001.

[32] N. Luhmann, Trust and Power, 2017.

[33] N. Moran, Illusion of safety: How consumers underestimate manipulation and deception in online (vs. offline) shopping contexts, 2020.

[34] F. J. J. Y. Y. B. N. Hua Yu Shi, The concept of consumer vulnerability: Scale development and validation, 2017.

[35] M. Sripathi, A Study on Impact of False Advertising on the Consumer Buying Behaviour, 2020.

[36] M. V. HaeranJae, Effects of pictorial product-warnings on low-literate consumers, 2011.

[37] H. S.-F. JINKOOK LEE, Consumer Vulnerability to Fraud: Influencing Factors, 2005.

[38] G. V. Judith fletcher-brown, Vulnerable consumer engagement: How corporate social media can facilitate the replenishment of depleted resources, 2020.

[39] S. K. D. D. S. Swapan Purkait, An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website, 2014.

[40] R. N. Aditya, The psychology of deception in marketing: A conceptual framework for research and practice, 2001.

[41] J. D. T. ,. M. H. Rachna Dhamija, Why phishing works, 2006.

[42] P. Org, "What Is Phishing," [Online]. Available: https://www.phishing.org/what-is-phishing.