Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα Σπουδών *Διοίκηση, Τεχνολογία και Ποιότητα*

Μεταπτυχιακή Διατριβή

Προστασία Από Κακόβουλο Λογισμικό : Περίπτωση Πιστωτικού Ιδρύματος, Ασφάλεια e Banking και Εκπαίδευση Προσωπικού.

Μαντζαρίνης Ιωάννης

Επιβλέπουσα Καθηγήτρια

Γεωργίου Ιφιγένεια

Δεκέμβριος 2017

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα Σπουδών *Διοίκηση, Τεχνολογία και Ποιότητα*

Μεταπτυχιακή Διατριβή

Προστασία Από Κακόβουλο Λογισμικό : Περίπτωση Πιστωτικού Ιδρύματος, Ασφάλεια e Banking και Εκπαίδευση Προσωπικού.

Μαντζαρίνης Ιωάννης

Επιβλέπουσα Καθηγήτρια

Γεωργίου Ιφιγένεια

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Διοίκηση, Τεχνολογία και Ποιότητα από τη Σχολή Οικονομικών Επιστημών και Διοίκησης του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβριος 2017

Περίληψη

Με την παρούσα διατριβή επιχειρείται μια προσπάθεια για την ανάδειξη της σημαντικότητας για την εκπαίδευση του προσωπικού στον τραπεζικό κλάδο αναφορικά σε θέματα ασφάλειας και προστασίας από κακόβουλα λογισμικά. Η έρευνα έχει διεξαχθεί σε μία από τις τέσσερις συστημικές Τράπεζες τις Ελλάδας και σκοπός είναι να παρουσιάσουμε για το αν πράγματι γνωρίζουν οι εργαζόμενοι τους βασικούς κινδύνους που κρύβει το διαδίκτυο και κατ' επέκταση πως μπορούν αυτοί οι κίνδυνοι να πλήξουν το e banking αλλά και τα συμφέροντα της Τράπεζας (πέραν των ίδιων). Επιπροσθέτως, θα αναδείξουμε την στάση των εργαζομένων απέναντι στην πολιτική ασφαλείας που διέπει την Τράπεζα, τους τρόπους πρόληψης και αντιμετώπισης αλλά κυρίως την ανάγκη για συνεχή επιμόρφωση και ευαισθητοποίηση σε θέματα ασφάλειας.

Στο πρώτο κεφάλαιο, θα δοθεί ο ορισμός του κακόβουλου λογισμικού και στη συνέχεια θα αποτυπωθεί η ιστορική αναδρομή. Εν συνεχεία, θα αναφερθούμε στα είδη των κακόβουλων λογισμικών, τους τρόπους που μολύνουν τα συστήματα αλλά και τους γενικότερους κινδύνους της ηλεκτρονικής τραπεζικής. Πέραν αυτών, θα γίνει αναφορά και ανάλυση στις πολιτικές ασφαλείας των πιστωτικών ιδρυμάτων, στην ασφάλεια των συναλλαγών μέσω e banking αλλά και τους τρόπους αντιμετώπισης και πρόληψης πιθανόν κινδύνων ή επιθέσεων.

Στο δεύτερο κεφάλαιο, θα γίνει εισαγωγή στις έννοιες της εκπαίδευσης αναδεικνύοντας ότι ο ανθρώπινος παράγοντας αποτελεί το πλέον σοβαρό κίνδυνο για έναν οργανισμό. Στη συνέχεια, θα καταγράψουμε τον τρόπο που ενημερώνεται ο εργαζόμενος σήμερα για θέματα ασφάλειας ώστε να υπεισέλθουμε στην πορεία στα μοντέλα εκπαίδευσης που βασίζονται στην συμπεριφορά, στην οργάνωση των τραπεζών, στην θεωρία και στην κοινωνική ψυχολογία.

Στο τρίτο και τελευταίο κεφάλαιο, θα ακολουθήσει η εμπειρική έρευνα με τους στόχους, την μεθοδολογία (συνέντευξη με ερωτήσεις ανοιχτού τύπου) και τα συμπεράσματα. Η συνέντευξη έγινε σε δείγμα 14 εργαζομένων από τέσσερις διαφορετικούς τομείς και ο κάθε εργαζόμενος έχει διαφορετικό ρόλο στην οργανωτική δομή της Τράπεζας. Όλοι οι συμμετέχοντες συμφώνησαν ότι ο ανθρώπινος παράγοντας αποτελεί τον βασικό κίνδυνο και απειλή για θέματα ασφάλειας και θεώρησαν ότι η εκπαίδευση θα πρέπει να συνδυαστεί με θεωρητική προσέγγιση αλλά και πρακτική.

Summary

This graduate thesis attempts to raise awareness of the training of staff in the banking sector with regard to security and malware protection. The survey has been conducted in one of the four Systemic Banks in Greece and the aim is to present whether they are really aware of the main risks of the Internet and consequently that these risks can affect both e banking and the interests of the Bank beyond themselves). In addition, we will highlight the attitude of employees towards the security policy that governs the Bank, the ways of prevention and coping, but also the need for continuous training and awareness on security issues.

In the first chapter, the definition of malware will be defined and then the historical review will be captured. Next, we will discuss the kinds of malware, the ways that infect the systems and the more general risks of e-banking. In addition, reference will be made to the security policies of credit institutions, the security of transactions through e banking, as well as ways of dealing with and preventing possible risks or attacks.

In the second chapter, we will introduce the concepts of education by pointing out that the human factor is the most serious threat to an organism. We will then describe how the employee is now informed about security issues in order to get into the path of behavioral, banking, theory, and social psychology education models.

In the third and final chapter, empirical research will follow with the objectives, the methodology (interview with open-ended questions) and the conclusions. The interview was conducted on a sample of 14 employees from four different sectors and each employee has a different role in the Bank's organizational structure. All participants agreed that human factor is the main threat and threat to security issues and felt that education should be combined with a theoretical approach and practice.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτρια κα Γεωργίου Ιφιγένεια, για την βοήθεια, την καθοδήγηση και νουθεσία της καθ' όλη την διάρκεια εκπόνησης της παρούσας εργασίας.

Επιπροσθέτως, θα ήθελα να ευχαριστήσω την οικογένειά μου για την στήριξη που μου παρέχει σε όλα τα βήματα της ζωής μου, και τον φίλο και αδερφό Μάριο Τσαμούρη για την ηθική στήριξη σε όλη την προσπάθεια.

Τέλος, θα ήθελα να ευχαριστήσω και τους συμμετέχοντες στην έρευνα για την συνεργασία τους, την προθυμία τους και την ειλικρίνειά τους.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Ένα από τα πολύ σημαντικά χαρακτηριστικά της σύγχρονης εποχής – και σύμφωνα με το γενικότερο πλαίσιο της παγκοσμιοποίησης – είναι ο ανταγωνισμός των επιχειρήσεων ο οποίος έχει προχωρήσει και έχει αλλάξει ο τρόπος με τον οποίο συμβαίνει αυτό. Δεδομένου ότι η κοινωνία και τα οικονομικά της πρότυπα έχουν εξελιχθεί από τη βαριά βιομηχανική εποχή στην εποχή της ηλεκτρονικής πληροφόρησης, όσον αφορά την παροχή νέων προϊόντων και υπηρεσιών για την ικανοποίηση των αναγκών των ανθρώπων, οι επιχειρήσεις κλήθηκαν να διαμορφώσουν ανάλογα την οργανωτική δομή τους αλλά κα τις στρατηγικές που τις διέπουν. Πέραν αυτού, οι επιχειρήσεις άλλαξαν και τα πρότυπα εργασίας, προκειμένου να αξιοποιηθούν οι τεχνολογικές εξελίξεις. Το γενικότερο κλίμα των αλλαγών, ακολούθησε και ο Τραπεζικός κλάδος ο οποίος αντιλαμβανόμενος τις ταχύτατες εξελίξεις στην παγκόσμια αγορά και στο ηλεκτρονικό επιχειρήν, προχώρησε σε νέες αναπτύξεις στα πληροφοριακά συστήματα δημιουργώντας ηλεκτρονικές πλατφόρμες για την διεκπεραίωση των συναλλαγών για κάθε πελάτη. Η ηλεκτρονική τραπεζική ή αλλιώς e banking, προβλέπει για όλους τους καταναλωτές που το χρησιμοποιούν να μπορούν συναλλάσσονται ηλεκτρονικά όποτε εκείνοι το επιθυμούν (ανεξάρτητα από τόπο και χρόνο) εξοικονομώντας χρόνο και αυξάνοντας την ικανοποίηση τους από την παροχή υπηρεσιών. Με τον όρο e banking εννοούμε όλες εκείνες τις υπηρεσίες που παρέχονται από την Τράπεζα χωρίς να είναι υποχρεωτική η παρουσία του πελάτη (με φυσικά παραστατικά, λήψη υπογραφών κλπ). Σύμφωνα με την Ένωση Ελληνικών Τραπεζών ως ηλεκτρονική Τραπεζική νοείται οποιαδήποτε εμπορική συναλλαγή που διεξάγεται μεταξύ της Τράπεζας και των πελατών της διαμέσου ηλεκτρονικών δικτύων και βοηθάει ή οδηγεί στην πώληση τραπεζικών προϊόντων ή υπηρεσιών. Όταν λοιπόν αυτές οι εμπορικές συναλλαγές πραγματοποιούνται μέσω του internet, τότε γίνεται λόγος για Διεξαγωγή Τραπεζικών Συναλλαγών μέσω Διαδικτύου (Ένωση Ελληνικών Τραπεζών, 2000).

Σύμφωνα με τον ευρύ ορισμό, η ηλεκτρονική τραπεζική είναι εδώ και αρκετό καιρό με τη μορφή των ATMs και μέσω τηλεφωνικών συναλλαγών (Aggelopoulos, Michiotis, 2011 ; Morten Hertzum, Niels Jørgensen, Mie Nørgaard, 2004). Πιο πρόσφατα, έχει μεταμορφωθεί και

εξελιχθεί μέσω του Διαδικτύου, ένα κανάλι που προσφέρει τραπεζικές υπηρεσίες που ωφελεί και τα δύο μέρη, πελάτες και τράπεζες. Η πρόσβαση είναι γρήγορη, βολική και διαθέσιμη όλο το εικοσιτετράωρο, ανεξάρτητα από την τοποθεσία του πελάτη. Επιπλέον, οι τράπεζες μπορούν να παρέχουν περισσότερες υπηρεσίες αποτελεσματικά και με σημαντικά χαμηλότερο κόστος. Αν και η ηλεκτρονική τραπεζική μπορεί να προσφέρει πολλά οφέλη για τους πελάτες αλλά και νέες επιχειρηματικές ευκαιρίες για τις τράπεζες, ελλοχεύει σοβαρούς κινδύνους που μπορεί να συνοψιστούν ως επιχειρησιακοί κίνδυνοι, κίνδυνοι φήμης, νομικοί κίνδυνοι. Παρόλο που έχουν γίνει σημαντικές εργασίες σε ορισμένες τράπεζες του υιοθετώντας μέτρα ασφαλείας και κανονισμούς ηλεκτρονικής τραπεζικής, η συνεχής επαγρύπνηση πρέπει να είναι ουσιαστικής σημασίας καθώς το εύρος της ηλεκτρονικής τραπεζικής αυξάνεται κι έτσι εξακολουθεί να υπάρχει ανάγκη για μεγαλύτερη εναρμόνιση και συντονισμό σε ό,τι αφορά την ασφάλεια (Koskosas, 2011).

Η αλματώδης ανάπτυξη της τεχνολογίας έχει ανοίξει νέους ορίζοντες και προσφέρει ποικίλες δυνατότητες. Ο παγκόσμιος ιστός έχει εκμηδενίσει τις αποστάσεις, προσφέρει νέες μεθόδους επικοινωνίας και αποτελεί μια ανεξάντλητη πηγή πληροφοριών. Ωστόσο, τα τεράστια οφέλη που προσφέρει η έκρηξη του Τομέα της πληροφορικής με αναπτύξεις συστημάτων, πλατφορμών αλλά και η ταυτόχρονη χρήση του Διαδικτύου, εκτός από σημαντικά οφέλη τόσο στην καθημερινότητα του καταναλωτή όσο και στην ανάπτυξη των ίδιων των επιχειρήσεων/ομίλων/Τραπεζών, ελλοχεύει και σημαντικούς κινδύνους και απειλές. Μία από τις σοβαρότερες απειλές είναι τα κακόβουλα λογισμικά. Το «κακόβουλο λογισμικό» (malicious software / malware ή badware) αποτελεί μείζον πρόβλημα για την ασφάλεια των Πληροφοριακών Συστημάτων. Το λογισμικό χαρακτηρίζεται ως κακόβουλο όταν βάσει των προθέσεων του προγραμματιστή το λογισμικό που προκύπτει διαθέτει τις απαιτούμενες εντολές προκειμένου να βλάψει ένα υπολογιστικό σύστημα. Το κακόβουλο λογισμικό μπορεί να χωριστεί σε δύο κατηγορίες. Σε αυτό που χρειάζεται ένα πρόγραμμα «ξενιστή» και σε αυτό που δεν χρειάζεται «ξενιστή» και μπορεί να εκτελεστεί από μόνο του όπως κάθε άλλο πρόγραμμα. Επιπλέον το κακόβουλο λογισμικό μπορεί να διαχωριστεί και με διαφορετικό τρόπο σε δύο άλλες κατηγορίες. Το ιομορφικό λογισμικό και το μη ιομορφικό λογισμικό. Στο ιομορφικό λογισμικό ανήκουν τα προγράμματα που μπορούν και αναπαράγονται από μόνα τους και στο μη ιομορφικό λογισμικό τα προγράμματα που δεν αναπαράγονται χωρίς την ανάμειξη του ανθρώπινου παράγοντα (Microsoft, 2003).

1.1 Ιστορικότητα

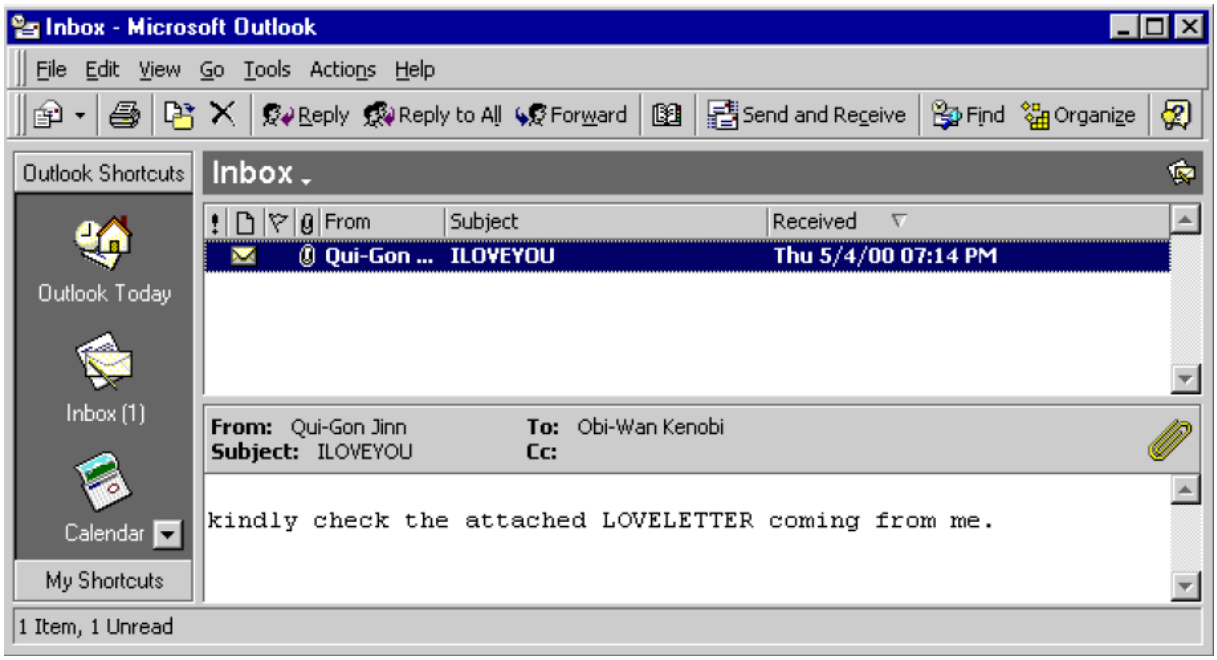
Εύλογα μπορείς να αναλογιστεί κανείς ότι οι γρήγορες τεχνολογικές εξελίξεις δεν θα μπορούσαν να μην επηρεάσουν και τα malwares (εφεξής κακόβουλο λογισμικό) γενικότερα καθώς τα πρώτα δείγματα τέτοιων λογισμικών διαφέρουν από αυτά που υπάρχουν σήμερα. Εξελικτικά, οι τρόποι μετάδοσης είναι τελείως διαφορετικοί και μάλιστα μπορούν να διαχωριστούν σε 3 φάσεις ήτοι μέσα της δεκαετίας 90, τέλη της δεκαετίας 90 και ερχόμενοι στο σήμερα (Steven Furnell, Jeremy Ward, 2004). Στην αρχή τους, οι άνθρωποι που δημιουργούσαν τέτοια προγράμματα, είχαν σκοπό περισσότερο την εκδίκηση για προσωπικούς λόγους (άρα το κακόβουλο λογισμικό απευθυνόταν καθαρά σε προσωπικό επίπεδο) ή την φάρσα (Kruegel 2012). Τα πρώτα χρόνια που συναντάμε κακόβουλο λογισμικό είναι το διάστημα 1986-1990 όπου τα ιογενή προγράμματα μεταδίδονταν από έναν ξενιστή – και συγκεκριμένα την χρησιμοποιούμενη δισκέτα της εποχής – μέσω της περιοχής εκκίνησης των δισκετών. Στη συνέχεια και μεταξύ 1990-1995 οι ιοί μεταδίδονταν μέσω αρχείων ενώ από το 1995-1998 κάνουν την εμφάνιση τους οι πρώτοι ιοί μακρο-εντολών που μεταδίδονταν με τα έγγραφα κειμένου. Την επόμενη τριετία που ακολούθησε η μετάδοση των ιών αλλάζει μορφή και εμφανίζονται ιοί τύπου worms οι οποίοι μεταδίδονταν μέσω ηλεκτρονικής αλληλογραφίας. Ενώ, από το 2001 και μετά οι είναι χιλιάδες που συνεχώς μεταλλάσσονται και εξελίσσονται. Αυτό πρακτικά σημαίνει ότι τα νέα κακόβουλα λογισμικά των ημερών μας είναι πολύ πιο δύσκολο να εντοπιστούν αλλά και να αφαιρεθούν δημιουργώντας μεγαλύτερης έκτασης ζημιές (Furnell & Ward 2004). Άλλωστε από το 2010 και μετά, ήρθε κακόβουλο λογισμικό που δημιουργήθηκε με σκοπό την εικονική κατασκοπεία και σαμποτάζ. Αυτά τα κακόβουλα προγράμματα δημιουργήθηκαν από μυστικές υπηρεσίες ορισμένων χωρών, και αυτή είναι η τελευταία φάση της εξέλιξης κακόβουλου λογισμικού που αντιμετωπίζουμε τώρα (Milosevic 2013).

Η ιστορία του κακόβουλου λογισμικού μπορεί να διαχωριστεί σε πολλές διάφορες κατηγορίες οι οποίες αντιπροσωπεύουν τις παραπάνω χρονικές περιόδους-σταθμούς. Ο πρώτος ιός που αφορούσε σε PC είναι ο ιός "Brain.A" ο οποίος δημιουργήθηκε από δύο αδέρφια στο Πακιστάν, και τα οποία είχαν σκοπό να αποδείξουν στην τεχνολογική κοινωνία της εποχής ότι τα personal computers σαν πλατφόρμες δεν είναι και τόσο ασφαλή όσο πίστευαν. Ο τρόπος που είχαν δημιουργήσει τον ιό αφορούσε την μόλυνση του τομέα εκκίνησης της δισκέτας και τον τομέα εκκίνησης κάθε εισαγόμενης δισκέτας. Έτσι, κάθε φορά που μια μολυσμένη δισκέτα εισαγόταν στον υπολογιστή, τότε αυτόματα θα μολυνόταν και ο δίσκος του (drive), οπότε ο δίσκος με τη σειρά του θα μπορούσε εν δυνάμει να μολύνει κάθε καθαρή δισκέτα που θα εισερχόταν. Μετά τον ιό "Brain" όπως είναι φυσικό υπήρξαν και άλλοι ιοί με πιο αξιομνημόνευτο τον ιό "Omega".

Ονομάστηκε έτσι, λόγω του σημείου ωμέγα που αποτυπωνόταν σε κάποιες συνθήκες στην κονσόλα. Ήταν ένας μολυσματικός τομέας εκκίνησης, αλλά δεν έκανε μεγάλες ζημιές αν η ημερομηνία δεν ήταν Παρασκευή και 13. Την ημέρα εκείνη ο υπολογιστής απλά δεν μπόρεσε να εκκινήσει (Milosevic 2013).

Αργότερα, όταν βγήκε στην παραγωγή το λειτουργικό των windows, πολλοί χρήστες πίστευαν ότι η ασφάλεια από βλαβερούς ιούς θα ήταν υψηλή συν το γεγονός ότι η απλότητα χρήσης των windows προσέλκυσε πληθώρα χρηστών. Αυτό αποτέλεσε και τον λόγο που κέντρισε των ενδιαφέρον των ανθρώπων που δημιουργούσαν τους ιούς. Έτσι ο πρώτος ιός που κατασκευάστηκε για τα windows ήταν ο WinVir. Η ζημιά που προκαλούσε επί τοις πράγμασι δεν ήταν πολύ μεγάλη καθώς το κύριο χαρακτηριστικό του ήταν η αναπαραγωγή και ήταν ο πρώτος ιός που είχε την ικανότητα να μολύνει τα windows files "Portable Executable". Ακολούθησαν κι άλλοι ιοί όπως για παράδειγμα ο Monkey, Slovak Bomber κλπ. Ο πρώτος χρονικά ιός που αφορούσε σε μάκρο-εντολή ήταν ο Concept (WM.Concept). Καταγράφηκε σε γλώσσα μακροεντολών του Microsoft Word και εξαπλώθηκε με την κοινή χρήση εγγράφων. Έτσι λοιπόν όταν ένα έγγραφο που είχε μολυνθεί με τον ιό Concept άνοιγε σε κάποιο υπολογιστή, ο ιός θα αντιγράφε το κακόβουλο πρότυπο του πάνω από το πρότυπο, οπότε κάθε νέο έγγραφο που δημιουργούνταν σε αυτόν τον υπολογιστή μολυνόταν. Ο Laroyx ήταν αντίστοιχα ο πρώτος ιός για το Microsoft Excel ο οποίος είχε γραφτεί σε Visual Basic μορφή (Milosevic 2013).

Στην ιστορία των κακόβουλων λογισμικών εντύπωση έχει προκαλέσει ο πρώτος ιός που εξαπλώθηκε μέσω ηλεκτρονικής αλληλογραφίας και σαν συνημμένο αρχείο. Αυτός ήταν ο Happy 99 ο οποίος εξαπλωνόταν μέσω του συνημμένου την εποχή μάλιστα με τα ειδικά φίλτρα εκείνη την εποχή να μην έχουν κάνει ακόμα την εμφάνισή τους (Milosevic 2013). Στην πραγματικότητα όμως κινδύνευαν οι χρήστες που έμπαιναν στην διαδικασία που άνοιγαν το συγκεκριμένο συνημμένο. Σε διαφορετική περίπτωση δεν απειλούνταν από το μολυσμένο επισυναπτόμενο αρχείο (Cranor, Greenstein 2001). Αντίθετα ο ιός Loveletter ήταν ένας από τους πλέον επιτυχημένους «κοινωνικούς» ιούς αφού χρησιμοποιούσε λεκτικά και φράσεις αγάπης προσελκύοντας να το ανοίξει ο χρήστης. Παρακάτω απεικονίζεται μια τέτοια κατάσταση (IBM 2007)



Επτά χρόνια αργότερα δημιουργήθηκε το σκουλήκι StormWorm το οποίο σε αντίθεση με τον LoveLetter χρησιμοποίησε τον φόβο και τον τρόμο σαν παγίδα και όχι την αγάπη (Milosevic 2013).

Στα τέλη του 1980 κατά λάθος δημιουργήθηκε και το πρώτο σκουλήκι σε PC. Για την ακρίβεια το 1988 ο Robert Tappan Moris, ο οποίος ήταν τότε φοιτητής του MIT έγραψε ένα πρόγραμμα το οποίο έμελε να αλλάξει την ιστορία των κακόβουλων λογισμικών. Στο πλαίσιο του έργου του, ο Morris ήθελε να υπολογίσει τους υπολογιστές που συνδέονται με το Διαδίκτυο. Έτσι έγραψε ένα μικρό πρόγραμμα το οποίο θα αναπαραχθεί από έναν συνδεδεμένο υπολογιστή σε άλλο και θα προβεί στις σχετικές μετρήσεις. Όμως, ο Morris έκανε ένα σφάλμα, και το σκουλήκι επισκέφθηκε επίσης υπολογιστές που έχει ήδη επισκεφθεί σε παρελθόντα χρόνο. Στην πραγματικότητα, ο ιός τύπου worm αναπαράγεται συνεχώς από τον μολυσμένο υπολογιστή σε όλους τους άλλους συνδεδεμένους υπολογιστές. Αυτό δημιούργησε πολλή μεγάλη κίνηση στο δίκτυο και σχεδόν συνθλίβει το διαδίκτυο. Έτσι λοιπόν, ο Code Red ήταν το πρώτο διαδικτυακό σκουλήκι το οποίο διαδόθηκε στις αρχές του 2000 μέσα σε ελάχιστες ώρες. Αντίθετα, ο ιός Nimda ανακαλύφθηκε το 2001 όπου με έναν απλό αναγραμματισμό σχηματιζόταν η λέξη Admin. Ο ιός αυτός έμοιαζε κατά πολύ με τον Code Red με την μόνη διαφορά ότι ο Nimda σάρωνε όλες τις ip διευθύνσεις σε αντίθεση με τον Code Red που σάρωνε ένα απλό δημόσιο φάσμα IP (Milosevic 2013).

Λίγα χρόνια αργότερα, το 2003, ακολούθησε μια νέα μορφή ιού με απώτερο σκοπό την κερδοσκοπία εις βάρος άλλων. Ο ιός με την ονομασία Fizzer διαδόθηκε με την μορφή

συνημμένου μέσα από ηλεκτρονική αλληλογραφία. Είναι ακριβώς αυτό το χρονικό σημείο όπου όλοι όσοι δημιουργούσαν κακόβουλα λογισμικά έστρεψαν το ενδιαφέρον τους στο κέρδος. Άρα όσα ακολούθησαν χρονικά από το Fizzer είχαν αυτό τον σκοπό. Το 2003 δημιουργήθηκε ο ιός Slammer και θεωρήθηκε πρωτοπόρος καθώς παρά το γεγονός ότι ήταν ένα διαδικτυακό σκουλήκι, χρησιμοποίησε την ευπάθεια στο OpenSSL και είναι ένα από τα πρώτα κακόβουλα προγράμματα που επιτέθηκαν σε μηχανές Linux και διακομιστές Apache. Είχε επίσης ένα «παράθυρο», οπότε ο επιτιθέμενος θα μπορούσε να χρησιμοποιήσει μολυσμένο μηχάνημα, να φορτώσει σε αυτό κάποια πρόσθετα εργαλεία ή κακόβουλα προγράμματα. Απόρροια αυτών ήταν η δολιοφθορά σε διάφορες υπηρεσίες και δημιουργία δυσλειτουργίας στα κεντρικά συστήματα. Με την ίδια λογική λειτούργησαν και οι ιοί Blaster και Sasser το 2004 (Milosevic 2013).

Το 2005 υπεισήλθε μια νέα κατηγορία κακόβουλου λογισμικού με την ονομασία Rootkits. Τα RootKits είναι εργαλεία κακόβουλου λογισμικού που τροποποιούν το υπάρχον λογισμικό λειτουργικού συστήματος έτσι ώστε ο εισβολέας να μπορεί να διατηρεί πρόσβαση και να κρύβεται σε ένα μηχάνημα. Τα RootKits μπορούν να λειτουργούν σε δύο διαφορετικά επίπεδα, ανάλογα με το λογισμικό που αντικαθιστούν ή αλλάζουν στο σύστημα προορισμού. Θα μπορούσαν να μεταβάλουν τα υπάρχοντα δυαδικά εκτελέσιμα αρχεία ή βιβλιοθήκες στο σύστημα. Με άλλα λόγια, ένα RootKit θα μπορούσε να αλλάξει τα ίδια τα προγράμματα που τρέχουν οι χρήστες και οι διαχειριστές. Το πρώτο RootKit έγινε από την SONY Entertainment και είχε πολύ αρνητικό αντίκτυπο στη φήμη της SONY. Η SONY BMG RootKit γεννήθηκε το 2005, ως ιδέα της SONY για την προστασία των πνευματικών δικαιωμάτων των εκδόσεών τους (Milosevic 2013).

Κομβική χρονιά για την εξέλιξη των κακόβουλων λογισμικών υπήρξε το 2008 όπου με τον ιό Mebroot, το θύμα θα μπορούσε να μολυνθεί μόνο με την πλοήγηση στο διαδίκτυο από το πρόγραμμα περιήγησης. Όταν ο Mebroot αποκτούσε πρόσβαση στα τερματικά των χρηστών, εγκαθιστούσε το rootkit που μπορούσε να τον κρύψει από τους ανιχνευτές RootKit, οι οποίοι γίνονται μέρος πολλών λύσεων προστασίας από ιούς. Ο Mebroot στην πραγματικότητα κατασκοπεύει τι πληκτρολογεί ο χρήστης και στέλνει τα δεδομένα αυτά στον εισβολέα. Επίσης, αυτό το κακόβουλο λογισμικό ήταν πολύ καλό στον εντοπισμό σφαλμάτων, οπότε σχεδόν ποτέ δεν προκάλεσε «συντριβές» του συστήματος. Ακόμα κι αν προκαλούσε συντριβή, θα μπορούσε να συλλέξει και να στείλει ίχνη στον επιτιθέμενο ώστε να μπορέσει να εντοπίσει σφάλματα και να διορθώσει το πρόβλημα. Κάνοντας αυτό ήταν το πιο προηγμένο κακόβουλο λογισμικό εκείνη την εποχή. Αργότερα, δημιουργήθηκε το Conficer όπου αποτελεί ένα από τα μεγαλύτερα

μυστήρια στην ιστορία κακόβουλων λογισμικών, και αυτό διότι δεν βρέθηκε ποτέ η πρόθεση του δημιουργού του κακόβουλου λογισμικού (Milosevic 2013).

Το 2010 το κακόβουλο λογισμικό αλλάζει μορφή και στόχο. Στόχος πλέον δεν φέρονται οι επιχειρήσεις ή τα προσωπικά και οικονομικά στοιχεία. Αντίθετα, στρατιωτικές και παραστρατιωτικές οργανώσεις, αστυνομικές δυνάμεις και μυστικές υπηρεσίες πολλών χωρών έχουν εμπλακεί στη δημιουργία κακόβουλου λογισμικού. Απόδειξη αυτών αποτελεί και η τοποθέτηση της αμερικανικής κυβέρνησης η οποία δήλωσε ότι ο στρατός εξακολουθεί να έχει δικαίωμα αντίδρασης σε επιθέσεις στον κυβερνοχώρο με φυσική επίθεση. Επίσης, το κακόβουλο λογισμικό μπορεί να κάνει σχεδόν ίδιες ζημίες με τη βόμβα, αλλά χωρίς να διακινδυνεύει ανθρώπινες ζωές. Το καλύτερο παράδειγμα για αυτό, είναι το κακόβουλο λογισμικό που ονομάζεται Stuxnet, το οποίο ανακαλύφθηκε το καλοκαίρι του 2010. Πιστεύεται ότι το Stuxnet δημιουργήθηκε για να καταστρέψει ή τουλάχιστον να επιβραδύνει το ιρανικό πυρηνικό πρόγραμμα. Το DoQu είναι κακόβουλο λογισμικό που έχει παρόμοια βάση δεδομένων με το Stuxnet. Πιστεύεται ότι το Stuxnet και το DoQu έχουν την ίδια προέλευση και τους ίδιους συγγραφείς (Milosevic 2013).

Το 2012 δημιουργήθηκε το κακόβουλο λογισμικό Flame και αποτελεί ένα από τα πιο πολύπλοκα λογισμικά που έχει δημιουργηθεί. Θεωρείται ότι δημιουργήθηκε από το Ισραήλ και τις μυστικές υπηρεσίες και στρατιωτικές υπηρεσίες των ΗΠΑ. Αυτό είναι αρθρωτό κακόβουλο λογισμικό, το οποίο μπορεί να ελεγχθεί από τον εισβολέα και μπορεί να προσθέσει νέες μονάδες από απόσταση. Με όλες τις μονάδες μπορεί να είναι 20MB μεγάλο. Η φλόγα θα μπορούσε να εξαπλωθεί μέσω της θύρας USB ή μέσω δικτύου. Χρησιμοποίησε την δυνατότητα rootkit για να κρυφτεί σε μολυσμένο σύστημα. Είχε την ικανότητα να καταγράφει ήχο, βίντεο, skype κλήσεις, δραστηριότητα δικτύου, για να κλέψει τα αρχεία από τον σκληρό δίσκο και να στείλει στον εισβολέα (Milosevic 2013).

Ερχόμενοι στις μέρες μας, τα κακόβουλα λογισμικά ολοένα και αυξάνουν την δυναμική τους και την ζημιά που προκαλούν. Περιπτώσεις όπως ο εκβιασμός είναι κάτι το οποίο συναντάει κανείς συχνά. Ένα τέτοιο εξαιρετικά επικίνδυνο κακόβουλο λογισμικό είναι και το «Crypto-Wall» το οποίο κατάφερε να απειλήσει χιλιάδες υπολογιστές, κυρίως επιχειρήσεων αλλά και ιδιωτών. Το εν λόγω κακόβουλο λογισμικό στοχεύει στην καταβολή χρηματικών ποσών ως «λύτρα», με ψηφιακό νόμισμα «bitcoin» , προκειμένου να «ξεκλειδωθούν» – αποκρυπτογραφηθούν ψηφιακά αρχεία και δεδομένα στους ηλεκτρονικούς υπολογιστές απλών χρηστών ή εταιρικών δικτύων. Τα κακόβουλα λογισμικά της οικογένειας «crypto-malware» μπορούν να επηρεάσουν όλες τις

εκδόσεις λειτουργικών συστημάτων και εξαπλώνονται, κυρίως, μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Σαν γενικό συμπέρασμα αντιλαμβανόμαστε ότι τα κακόβουλα λογισμικά με το πέρασμα των χρόνων έχουν αλλάξει κατά πολύ στον τρόπο μετάδοσης αλλά κυρίως τους σκοπούς για τους οποίους δημιουργούνται. Ενώ στην αρχή τους οι σκοποί ήταν η εκδίκηση ή φάρσες εξελίχθηκαν σε σαμποτάζ, κερδοσκοπία, κατασκοπεία. Κυβερνήσεις χωρών εμπλέκονται σε έναν cyber πόλεμο διοχετεύοντας ιούς για απόσπαση πληροφοριών ή ακόμα με σκοπό να προκαλέσουν ζημιές και απώλειες όπως ένας πραγματικός πόλεμος.

1.2 Είδη κακόβολων λογισμικών

Ο κακόβουλος κώδικας ή κακόβουλο λογισμικό συνήθως χωρίζεται σε διαφορετικές κατηγορίες, τα όρια μεταξύ των οποίων δεν είναι σαφώς καθορισμένα. Πολλές φορές μάλιστα κακόβουλα προγράμματα παρουσιάζουν χαρακτηριστικά από συνδυασμό κατηγοριών. Κάποιος κώδικας σχεδιάζεται για να εκμεταλλευτεί τρωτά σημεία λογισμικού στο σύστημα, το πρόγραμμα περιήγησης, τις εφαρμογές ή άλλο λογισμικό υπολογιστή. Παλαιότερα, το κακόβουλο λογισμικό αποσκοπούσε στο να φθείρει απλώς έναν ηλεκτρονικό υπολογιστή αλλά όπως προαναφέρθηκε, σταδιακά άλλαξαν οι σκοποί : κλοπή emails, κωδικών σύνδεσης σε εφαρμογές και πλατφόρμες οποιασδήποτε χρήσης, προσωπικά και οικονομικά δεδομένα (K. C. Laudon, C. G. Traver, Επιμέλεια Γ. Γκαντζιάς, 2014). Παρακάτω παρατίθενται οι πιο συνηθισμένες κατηγορίες.

Ιός (virus) : είναι ένα πρόγραμμα υπολογιστή το οποίο έχει την δυνατότητα να αντιγράφει ή να δημιουργεί αντίτυπα του εαυτού του και κα να εξαπλώνεται σε άλλα αρχεία. Είναι κατά κάποιο τρόπο αυτοαναπαραγόμενο (self-replicating) λογισμικό, του οποίου η λειτουργία μοιάζει πολύ με αυτή των βιολογικών ιών. Εκτός από την δυνατότητα τους για αναπαραγωγή, οι περισσότεροι ιοί μεταφέρουν ένα ωφέλιμο φορτίο που μπορεί να σχετικά καλοήθες (πχ μια εικόνα ή μήνυμα) ή κακοήθες που μπορεί να καταστρέψει φακέλους ή να σβήσει αρχεία στον σκληρό δίσκο. Συνήθως
για να εκτελεστούν χρειάζονται την ύπαρξη κάποιου αρχείου ξενιστή, το οποίο μολύνουν προσθέτοντας σε αυτό τον εαυτό τους. Για να εκτελεστούν και για να εξαπλωθούν χρειάζεται ανθρώπινη παρέμβαση, ώστε να εκτελεστεί το πρόγραμμα-ξενιστής και μαζί του και ο ιός.

Σκουλήκι (worm) : Τα σκουλήκια είναι σχεδιασμένα για να εξαπλώνονται από υπολογιστή σε υπολογιστή ενώ δεν είναι απαραίτητο να ενεργοποιηθεί από κάποιον χρήστη ή πρόγραμμα για να αντιγραφεί. Εξαπλώνονται χρησιμοποιώντας το δίκτυο για να μολύνουν άλλα συστήματα εκμεταλλευόμενα διάφορα κενά ασφαλείας.

Ransomware (Scareware) : είναι ένας τύπος κακόβολου λογισμικού (συχνά ένα σκουλήκι) το οποίο κλειδώνει συνήθως τον υπολογιστή ή τα αρχεία και δεν είναι πλέον προσπελάσιμα. Αυτός ο τύπος απειλής εμφανίζεται συχνά ως προειδοποίηση από μια δημόσια αρχή (πχ Αστυνομία) που ενημερώνει ότι διαπίστωσε παράνομη δραστηριότητα στον υπολογιστή και απαιτεί από μέρους τους χρήστη καταβολή προστίμου.

Δούρειος ίππος (trojan horse) : Ο δούρειος ίππος δεν είναι ιός καθώς δεν αναπαράγεται αλλά αποτελεί το μέσο με το οποίο άλλοι ιοί ή κακόβουλοι κώδικες εισβάλλουν σε άλλα προγράμματα.

Το bot είναι κακόβουλο λογισμικό το οποίο εγκαθίσταται λαθραία όταν ο χρήστης συνδέεται στο internet. Όταν εγκατασταθεί το bot ανταποκρίνεται σε εξωτερικές εντολές που στέλνει ο επιτιθέμενος ενώ ο υπολογιστής μετατρέπεται σε ζόμπι.

Το **botnet** είναι δίκτυο ελεγχόμενων υπολογιστών που χρησιμοποιούνται για κακόβουλες ενέργειες όπως η αποστολή ανεπιθύμητης αλληλογραφίας, η συμμετοχή σε επίθεση τύπου κατανεμημένης άρνησης υπηρεσίας, κλοπή πληροφοριών από υπολογιστές και αποθήκευση πληροφορίας στο internet για μετέπειτα ανάλυση.

Κερκόπορτα (backdoor) : είναι ένα χαρακτηριστικό ιών, σκουληκιών, και Δούρειων ίππων που επιτρέπουν στους επιτιθέμενους να προσπελάσουν εξ αποστάσεως έναν εκτεθειμένο υπολογιστή. Παρουσιάζει ομοιότητες με το bot όσον αφορά την απομακρυσμένη πρόσβαση, η διαφορά τους όμως έγκειται στο ότι τα bots αποτελούν πάντα τμήμα ενός μεγαλύτερου botnet.

Εκτός από τα παραπάνω που αποτελούν κακόβουλο λογισμικό, υπάρχουν και τα κακόβουλα προγράμματα, όπως adware και spyware που εγκαθίστανται στους υπολογιστές χωρίς την συναίνεση του χρήστη.

Adware : χρησιμοποιείται συνήθως για αναδυόμενες διαφημίσεις που εμφανίζονται όταν ο χρήστης επισκέπτεται κάποια συγκεκριμένα sites, ενώ δεν χρησιμοποιείται συνήθως για παράνομες δραστηριότητες.

Παράσιτο προγράμματος περιήγησης : Είναι ένα πρόγραμμα που μπορεί να αλλάζει και να παρακολουθεί τις ρυθμίσεις προγράμματος περιήγησης του χρήστη ενώ αποτελούν συχνά συστατικά στοιχεία των προγραμμάτων adware.

Λογισμικό κατασκοπείας (spyware) : Έτσι ονομάζεται κάθε πρόγραμμα, που μπορεί να χρησιμοποιηθεί για άντληση πληροφοριών και ευαίσθητων δεδομένων και τα οποία

προωθούνται στον επιτιθέμενο. Συνήθως το ενδιαφέρον των επιτιθεμένων εστιάζεται σε κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών και στο περιεχόμενο διαφόρων emails.

1.3 Μέθοδοι Μόλυνσης

Το κακόβουλο λογισμικό χρησιμοποιεί διάφορες τεχνικές για να εξαπλωθεί και να μολύνει καινούργια συστήματα. Το κοινό τους σημείο είναι ότι εκμεταλλεύονται κάποια αδυναμία είτε του συστήματος είτε του χρήστη του. Παρακάτω παρουσιάζονται συνοπτικά κάποιοι τρόποι μετάδοσης :

- Μέσω Ηλεκτρονικής Αλληλογραφίας. Το κακόβουλο λογισμικό βρίσκεται συνημμένο σε ένα μήνυμα ηλεκτρονικής αλληλογραφίας. Η αποστολή του μηνύματος μπορεί να είναι είτε ηθελημένη από κάποιον τρίτο, είτε ως αποτέλεσμα αυτόματης μετάδοσης (π.χ. mail Worm).
- Μέσω αφαιρούμενων αποθηκευτικών μέσων (floppy, CD, DVD, USB disks,).
- Μέσω Web (εκτελέσιμος κώδικας ενσωματωμένος σε σελίδες html).
- Μέσω άλλων υπηρεσιών διαδικτυακής επικοινωνίας. Υπηρεσίες συνομιλίας σε πραγματικό χρόνο.
- Μέσω Δικτύων (LAN, WAN). Το κακόβουλο λογισμικό (π.χ. τύπου Worm) εκμεταλλεύεται ευπάθειες δικτυακών πρωτοκόλλων, υπηρεσιών, εφαρμογών και δικτυακών λειτουργικών συστημάτων ώστε να μεταδίδεται αυτόματα μέσω τοπικών δικτύων ή δικτύων Ευρείας Περιοχής που εκτελούν την οικογένεια πρωτοκόλλων TCP/IP.
- Ενοχλητικά μηνύματα, διαφημίσεις κλπ
- Επιθέσεις υποκλοπής δεδομένων και πληροφοριών, ή κλήσης (dialers) με υπεραστική χρέωση (σχετική κατηγορία: trojans, spyware)
- Δημιουργία «κερκόπορτας» (back door) με σκοπό την (μετέπειτα) παραβίαση της ασφάλειας του συστήματος (σχετικές κατηγορίες: trojans, rootikits, zombies)
- Επιθέσεις εναντίον της διαθεσιμότητας συστημάτων με κατανάλωση υπολογιστικών πόρων (κύρια μνήμη, αποθηκευτικός χώρος), κατανάλωση της χωρητικότητας (bandwidth) του δικτύου, χρήση των ξενιστών για συγχρονισμένη επίθεση σε κάποιον τρίτο, στα πλαίσια μιας επίθεσης DDOS (Distributed DOS).

1.4 Κίνδυνοι της γενικότερης ηλεκτρονικής τραπεζικής και του e banking

Οι ηλεκτρονικές υπηρεσίες απλοποιούν τις ζωές μας. Μας επιτρέπουν να έχουμε πρόσβαση σε πληροφορίες παντού και είναι επίσης χρήσιμες για τους παρόχους υπηρεσιών, επειδή μειώνουν το λειτουργικό κόστος. Για παράδειγμα, η ηλεκτρονική τραπεζική έχει καταστεί απαραίτητη για τους πελάτες αλλά και για τις ίδιες τις Τράπεζες. Δυστυχώς, η αλληλεπίδραση με μια ηλεκτρονική υπηρεσία όπως μια τραπεζική πλατφόρμα στον ιστό, απαιτεί συχνά και μια καλή εξοικείωση σε ό,τι αφορά την γνώση σε τεχνολογικά θέματα που δεν διαθέτουν όλοι οι χρήστες του Διαδικτύου. Σύμφωνα με σχετικές πανεπιστημιακές έρευνες, την τελευταία δεκαετία, τέτοιας κατηγορίας χρήστες στοχεύονται ολοένα και περισσότερο για επιθέσεις από κακοποιούς που έχουν σκοπό το εύκολο κέρδος (Aburrous, Maher, Hossain, Alamgir, Dahal, Keshav and Thabtah, Fadi, 2010).

1.4.1 Phishing ή κοινωνική μηχανική

Η κοινωνική μηχανική βασίζεται στην ανθρώπινη περιέργεια, την απληστία και την ευπιστία προκειμένου να εξαπατήσει του ανθρώπους να πράξουν κάτι που θα τους οδηγήσει στην λήψη εν αγνοία τους κακόβουλου λογισμικού (K. C. Laudon, C. G. Traver, Επιμέλεια Γ. Γκαντζιάς, 2014 ; Antonio San Martino, Xavier Perramon, 2009). Το ηλεκτρονικό "ψάρεμα" είναι ένα σχετικά νέο έγκλημα στο διαδίκτυο σε σύγκριση με άλλες μορφές, π.χ. ιοί και hacking. Όλο και περισσότερες ιστοσελίδες ηλεκτρονικού "ψαρέματος" έχουν βρεθεί τα τελευταία χρόνια σε ιστότοπους του e banking. Το phishing είναι μια ευρέως διαδεδομένη τεχνική κοινωνικής μηχανικής επίθεσης που προσπαθεί να εξαπατήσει τους ανθρώπους αποσπώντας τις προσωπικές τους πληροφορίες, συμπεριλαμβανομένου του αριθμού της πιστωτικής κάρτας, τις πληροφορίες τραπεζικού λογαριασμού, τον αριθμό κοινωνικής ασφάλισης και τα προσωπικά διαπιστευτήριά τους για να τα χρησιμοποιήσουν λεπτομέρειες με δόλο εναντίον τους. Το ηλεκτρονικό "ψάρεμα" έχει τεράστιο αρνητικό αντίκτυπο τα έσοδα των Τραπεζών, τις σχέσεις με τους πελάτες, τις προσπάθειες μάρκετινγκ και τη συνολική εταιρική εικόνα (Aburrous, Maher, Hossain, Alamgir, Dahal, Keshav and Thabtah, Fadi, 2010).

Μία επιτυχημένη επίθεση phishing στηρίζεται σε τρεις βασικούς παράγοντες: την έλλειψη γνώσεων του θύματος, την έλλειψη προσοχής του θύματος και την οπτική εξαπάτηση. Ο μέσος άνθρωπος ξέρει να χειρίζεται τις βασικές λειτουργίες του υπολογιστή και του διαδικτύου χωρίς να γνωρίζει την διαδικασία με την οποία αυτό λειτουργεί. Έτσι δεν μπορεί να αναγνωρίσει τα ίχνη του phishing, όπως είναι παραλλαγμένη διεύθυνση e-mail, ή το διαφορετικό URL. Ταυτόχρονα, λόγω της άγνοιας του κινδύνου, αμελεί τη χρήση προγραμμάτων anti-phishing.

Οι τρόποι που μπορεί ένας εισβολέας να παραπλανήσει ένα θύμα μπορεί να είναι με τους εξής τρόπους :

- Μέσω πλαστής ιστοσελίδας. Πολλοί χρήστες δεν έχουν την ικανότητα ή την εμπειρία να μπορούν να διακρίνουν όλες εκείνες τις μικρές λεπτομέρειες που καθιστούν μία ιστοσελίδα πλαστή. Έτσι κάνοντας περιήγηση στο διαδίκτυο μπορεί να παρασυρθούν. Οι δύο πιο κοινές μέθοδοι για να προσελκύσουν έναν χρήστη να κάνει κλικ ένα κουμπί μέσα σε ένα παράθυρο διαλόγου είναι η εμφάνιση παραθύρου που προειδοποιεί για ένα πρόβλημα, η εμφάνιση μιας ρεαλιστικής λειτουργίας μηνύματος σφάλματος συστήματος ή εφαρμογής ή προσφέροντας πρόσθετες υπηρεσίες. Άλλωστε, η τεχνική του phishing χαρακτηρίζεται από :
  - ένα τέλειο παραπλανητικό κείμενο. Το κείμενο αυτό, που συνήθως είναι οι παραπλανητικοί σύνδεσμοι, μπορεί να χρησιμοποιεί λάθος σύνταξη ή ορθογραφία ή να αντικαθιστά παρόμοια γράμματα όπως το αγγλικό μικρό l (L) με το κεφαλαίο I (i), κλπ.
  - Παραπλανητικές εικόνες. Οι εικόνες αυτές, μπορεί να είναι οι ίδιες οπτικά με τις εικόνες που χρησιμοποιεί κάποια ιστοσελίδα, Μία εξίσου κοινή μέθοδος είναι εικόνες που μιμούνται το λειτουργικό σύστημα του υπολογιστή.
  - Παραπλανητικό design. Με τη βοήθεια του παραπλανητικού κειμένου και εικόνων, αλλά και την επεξεργασία του κώδικα της αυθεντικής ιστοσελίδας, ο hacker μπορεί να φτιάξει μία ολόκληρη ιστοσελίδα με το ίδιο ακριβώς design που έχει η αυθεντική.

1.4.2 Spoofing

Το spoofing (παραπλάνηση), περιλαμβάνει απόπειρες απόκρυψης μιας πραγματικής ταυτότητας χρησιμοποιώντας το email ή την IP κάποιου άλλου. Ένα τέτοιο email έχει μια πλαστογραφημένη διεύθυνση αποστολέα η οποία έχει σχεδιαστεί ώστε να παραπλανήσει τον παραλήπτη σχετικά με το ποιός στέλνει το μήνυμα (K. C. Laudon, C. G. Traver, Επιμέλεια Γ. Γκαντζιάς, 2014). Χρήσεις και τεχνικές του spoofing είναι Χρήσεις του Spoofing : man-in-the-middle , routing redirect, source routing, blind spoofing, flooding, E-mail Spoofing, Spoofing GPS (K. C. Laudon, C. G. Traver, Επιμέλεια Γ. Γκαντζιάς, 2014).

1.4.3 Pharming

Το pharming είναι αυτόματη ανακατεύθυνση ενός συνδέσμου σε μια διεύθυνση διαφορετική από την αρχική του συνδέσμου με ένα άλλο site το οποίο προσποιείται ότι είναι ο σωστός προορισμός που επιθυμεί ο χρήστης. Έτσι ο εισβολέας, μπορεί να μην έχει σαν σκοπό να

καταστρέψει αρχεία κλπ αλλά μέσω ένα ψεύτικου website πιστό αντίγραφο του πρωτότυπου να καταφέρει να αποσπάσει σοβαρές πληροφορίες. Ειδικότερα όταν πρόκειται για ιστοσελίδα Τράπεζας και συγκεκριμένα του e banking, η προσπάθεια του θύματος να μπορέσει να ολοκληρώσει τις τυχόν συναλλαγές πιθανόν να οδηγήσει σε μεταφορά εμβασμάτων στον hacker (Ηλεκτρονικό εμπόριο - Επιχειρήσεις, Τεχνολογία, Κοινωνία, K. C. Laudon, C. G. Traver, Επιμέλεια Γ. Γκαντζιάς, 2014).

1.4.4 Hijacking

Το hijacking είναι ένας τύπος επίθεσης ασφάλειας δικτύων στον οποίο ο επιτιθέμενος παίρνει τον έλεγχο μιας επικοινωνίας ανάμεσα σε δύο οντότητες και προσποιείται ως ένα από αυτά. Σε έναν τύπο πειρατείας (γνωστό και ως man in the middle), ο δράστης παίρνει τον έλεγχο μιας σύνδεσης ενώ βρίσκεται σε εξέλιξη. Ο εισβολέας παρακολουθεί τα μηνύματα σε μια ανταλλαγή δημόσιου κλειδιού και στη συνέχεια τα αναμεταδίδει, υποκαθιστώντας το δημόσιο κλειδί του για το ζητούμενο, έτσι ώστε τα δύο αρχικά μέρη να φαίνεται ότι επικοινωνούν μεταξύ τους άμεσα. Ο εισβολέας χρησιμοποιεί ένα πρόγραμμα που φαίνεται να είναι ο διακομιστής στον πελάτη. Αυτή η επίθεση μπορεί να χρησιμοποιηθεί απλώς για να αποκτήσει πρόσβαση στα μηνύματα ή για να επιτρέψει στον εισβολέα να τα τροποποιήσει πριν τα μεταδώσει ξανά (K. C. Laudon, C. G. Traver, Επιμέλεια Γ. Γκαντζιάς, 2014).

1.4.5 Υποκλοπέας Sniffer

Ο υποκλοπέας sniffer είναι ένα είδος προγράμματος ιχνηλάτη που παρακολουθεί τις πληροφορίες που κυκλοφορούν στο διαδίκτυο. Ο κίνδυνος από μια τέτοια υποκλοπή είναι η κλοπή ή δημοσίευση απόρρητων ή προσωπικών πληροφοριών όπως για παράδειγμα στοιχεία ταυτότητας, τραπεζικών λογαριασμών και κωδικών πρόσβασης. Παρόμοια λογική έχουν και τα προγράμματα υποκλοπής μηνυμάτων τα οποία συνήθως περιέχουν κρυφό κώδικα σε ένα μήνυμα email που επιτρέπει την παρακολούθηση όλων των διαδοχικών μηνυμάτων που προωθούνται με το αρχικό μήνυμα (K. C. Laudon, C. G. Traver, Επιμέλεια Γ. Γκαντζιάς, 2014).

1.4.6 Επιθέσεις άρνησης υπηρεσίας

Στην επίθεση άρνηση υπηρεσίας (DoS) οι εισβολείς υπερφορτώνουν ένα site με αχρείαστες αιτήσεις σελίδων που κατακλύζουν και υπερχειλίζουν τους διακομιστές του site. Το αποτέλεσμα μιας τέτοιας επίθεσης είναι το κλείσιμο του site καθιστώντας αδύνατη την πρόσβαση των χρηστών κι έτσι οι εισβολείς ζητούν «λύτρα» από τον πάροχο της υπηρεσίας προκειμένου να σταματήσουν την επίθεση. Αντίστοιχα, η επίθεση τύπου κατανεμημένης άρνησης υπηρεσίας

(DDoS) χρησιμοποιεί πολλούς υπολογιστές ταυτόχρονα προκειμένου να σημειωθεί σε ένα δίκτυο από αμέτρητα σημεία (K. C. Laudon, C. G. Traver, Επιμέλεια Γ. Γκαντζιάς, 2014).

Σύμφωνα με σχετική έρευνα, το πρώτο τρίμηνο του 2017 επιβεβαιώθηκαν οι προβλέψεις για την εξέλιξη των επιθέσεων DDoS που έγιναν από τους ειδικούς της Kaspersky Lab μετά τα αποτελέσματα του 2016. Παρά την αυξανόμενη δημοτικότητα των σύνθετων επιθέσεων DDoS που συνεχίζονται στο πρώτο τρίμηνο, παρατηρήθηκε αισθητή μείωση του αριθμού των συνολικών επιθέσεων και της αλλαγής του τρόπου με τον οποίο διασκορπίστηκαν ανά χώρα. το πρώτο τρίμηνο του 2017, το σύστημα Kaspersky DDoS Intelligence κατέγραψε επιθέσεις DDoS σε πόρους σε 72 χώρες, οι οποίες είναι οκτώ λιγότερες σε σχέση με το τέταρτο τρίμηνο του 2016. Η Ολλανδία και το Ηνωμένο Βασίλειο αντικατέστησαν την Ιαπωνία και τη Γαλλία μεταξύ των 10 πρώτων χωρών με τις περισσότερες επιθέσεις DDoS. Η Νότια Κορέα παρέμεινε ηγέτης όσον αφορά τον αριθμό των ανιχνευθέντων διακομιστών C & C. Οι ΗΠΑ έρχονται δεύτερες από αυτή την άποψη, ακολουθούμενες από την Ολλανδία, οι οποίες απομάκρυναν την Κίνα από τα τρεις πρώτες θέσεις για πρώτη φορά από τότε που ξεκίνησε η παρακολούθηση. Η κατανομή ανά λειτουργικό σύστημα άλλαξε και το 1ο τρίμηνο του 2017. Το προηγούμενο τρίμηνο, τα botnets IoT που βασίζονται στο Linux ήταν τα πιο δημοφιλή, αλλά εξαφανίστηκαν από botnets που βασίζονται στα Windows, των οποίων το μερίδιο αυξήθηκε από 25% σε 60% τέταρτο. Ο αριθμός των επιθέσεων TCP, UDP και ICMP αυξήθηκε σημαντικά, ενώ το μερίδιο των επιθέσεων SYN DDoS και HTTP μειώθηκε από 75% το τέταρτο τρίμηνο του 2016 σε 48% το πρώτο τρίμηνο. Συνολικά, το τρίμηνο ήταν σχετικά ήσυχο: ο μεγαλύτερος αριθμός επιθέσεων (994) παρατηρήθηκε στις 18 Φεβρουαρίου. Η μεγαλύτερη επίθεση DDoS στο πρώτο τρίμηνο του 2017 διήρκεσε μόνο 120 ώρες, γεγονός που είναι σημαντικά χαμηλότερο από το μέγιστο των 292 ωρών του προηγούμενου τριμήνου (Kaspersky Lab, 2017).

1.4.7 Επιθέσεις εκ των έσω

Εκτός από τις απειλές και τις επιθέσεις από εξωτερικούς εισβολείς, θα πρέπει να ληφθεί σοβαρά υπόψη ότι ελλοχεύει ο εσωτερικός κίνδυνος, εντός μιας επιχείρησης και ιδιαίτερα σε μια Τράπεζα. Ειδικά τμήματα που αποτελούν θεματοφύλακες της πληροφορίας, έχοντας πρόσβαση στις βάσεις δεδομένων των συστημάτων και σε ευαίσθητες πληροφορίες (στην περίπτωση χαλαρών μέτρων ασφαλείας), αποκτούν στοιχεία τέτοια που τους καθιστά υπεύθυνους για κλοπές καρτών, στοιχείων από τραπεζικούς λογαριασμούς, προσωπικά δεδομένα χρηστών κλπ. (K. C. Laudon, C. G. Traver, Επιμέλεια Γ. Γκαντζιάς, 2014).

1.4.8 Θέματα ασφαλείας κινητής πλατφόρμας

Η έκρηξη τις τεχνολογίας σε ό,τι αφορά τις κινητές συσκευές διεύρυνε τις ευκαιρίες για τους εισβολείς. Έτσι, τους ίδιους κινδύνους που αντιμετωπίζει οποιαδήποτε άλλη συσκευή που συνδέεται στο διαδίκτυο, την ίδια ακριβώς επικινδυνότητα αντιμετωπίζει και μια κινητή συσκευή τηλεφώνου. Τα δημόσια ασύρματα δίκτυα είναι αρκετά ευάλωτα σε ό,τι αφορά την ασφάλεια τους. Οι χάκερ από την άλλη στοχεύουν σε εύπιστα θύματα που μέσα από μια σειρά μηνυμάτων. Το *vishing* στοχεύει σε χρήστες οι οποίοι θα δραστηριοποιηθούν και θα ανταποκριθούν σε φωνητικά μηνύματα που προτρέπουν να καλέσει ο χρήστης σε έναν συγκεκριμένο αριθμό με σκοπό να προβούνς σε κάποια δωρεά σε ένα κοινωφελές ίδρυμα. Οι επιθέσεις *smishing* εκμεταλλεύονται τα SMS που περιέχουν διευθύνσεις και sites τα οποία οδηγούν τον χρήστη σε κακόβουλα sites. Τα μηνύματα αυτά φαίνεται ότι προέρχονται από νόμιμο οργανισμό (K. C. Laudon, C. G. Traver, Επιμέλεια Γ. Γκαντζιάς, 2014). Επιπροσθέτως, διάφοροι ιοί που μπορεί να κρύβονται στα SMS μοιάζει λίγο δύσκολο αλλά κάτι τέτοιο μπορεί να συμβεί χάρη στις φορητές συσκευές που μοιάζουν με υπολογιστές όπως οι κινητές συσκευές iPhone, iPad και Android. Το πιο σημαντικό είναι ότι τα εργαλεία εφαρμογής της SIM έχουν τη δυνατότητα να επιτρέπουν στις υπόλοιπες εφαρμογές να έχουν πρόσβαση στις λειτουργίες κλήσης και τις καταχωρίσεις του τηλεφωνικού καταλόγου, ώστε να μεταδίδουν τους ιούς με αποστολή μηνυμάτων (Sam Johnson, Nick Twilley, Tianyi Zhang, Zhanni Zhou, & Suijun Wu, 2014).

Σύμφωνα με σχετική έρευνα, το 2013 σηματοδοτήθηκε από την ταχεία αύξηση των κακόβουλων λογισμικών σε λειτουργικά Android και σε σχέση με applications που αφορούν τράπεζες. Η «βιομηχανία» κακόβουλου λογισμικού για κινητά γίνεται όλο και περισσότερο επικεντρωμένη στην αποτελεσματικότερη συσσώρευση κερδών, δηλαδή το κινητό ηλεκτρονικό ψάρεμα (phishing), την κλοπή των πληροφοριών πιστωτικών καρτών, τις μεταφορές χρημάτων από τραπεζικές κάρτες σε κινητά τηλέφωνα και από τηλέφωνα στα ηλεκτρονικά πορτοφόλια των εγκληματιών (electronic wallets). Οι εγκληματίες του κυβερνοχώρου έχουν μοιραστεί με αυτή τη μέθοδο παράνομων κερδών: στις αρχές του έτους γνωρίζαμε μόνο 67 τραπεζικούς Trojans, αλλά μέχρι το τέλος του έτους υπήρχαν ήδη 1321 μοναδικά δείγματα. (Kaspersky Lab, 2013).

1.5 Πολιτική Ασφαλείας

Η Πολιτική Ασφάλειας των Πληροφοριακών Συστημάτων, αν και μπορεί να διαφέρει σημαντικά από οργανισμό σε οργανισμό, περιλαμβάνει γενικά το σκοπό και τους στόχους της ασφάλειας,

οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν την προστασία των πληροφοριακών συστημάτων του οργανισμού. Οι οδηγίες και οι διαδικασίες που περιλαμβάνονται στην πολιτική ασφάλειας υλοποιούνται με την εφαρμογή των μέτρων προστασίας για την ασφάλεια των πληροφοριακών συστημάτων. Η πολιτική ασφάλειας διατυπώνεται σε ένα έγγραφο, το οποίο θα πρέπει να γνωρίζουν και να ακολουθούν όλα τα μέλη του οργανισμού, στις δραστηριότητές τους που έχουν σχέση με τα πληροφοριακά συστήματα που καλύπτει η πολιτική.

Στην πολιτική ασφάλειας, δηλαδή, καθορίζονται οι στόχοι της ασφάλειας, καθώς και ο τρόπος με τον οποίο οι στόχοι αυτοί θα υλοποιηθούν. Βασικό συστατικό στοιχείο, επομένως, κάθε πολιτικής ασφάλειας πληροφοριακών συστημάτων είναι η περιγραφή των κανόνων και των διαδικασιών που πρέπει να ακολουθούνται για την προστασία των πληροφοριακών συστημάτων, καθώς και ο καθορισμός των συγκεκριμένων ρόλων και αρμοδιοτήτων που απαιτούνται για την υλοποίηση της πολιτικής ασφάλειας (Κάτσικας, Γκριτζάλης, 2004 ; Thomas Thostheim, 2004). Με τον γενικότερο όρο ασφάλεια πληροφοριακών συστημάτων εννοούμε ένα γνωστικό πεδίο της επιστήμης της πληροφορικής, και ειδικότερα του κλάδου των υπολογιστικών συστημάτων, που ασχολείται με την προστασία των υπολογιστών, των δικτύων που τους διασυνδέουν και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους.

Έτσι, μια πολιτική ασφάλειας διέπεται από τρεις βασικές αρχές (Παπασωτηρίου, 2003):

- ✓ **διαθεσιμότητα** δλδ εξουσιοδοτήσεις σε συγκεκριμένους χρήστες που μπορούν να επηρεάσουν κόμβους μέσα σε ένα πληροφοριακό σύστημα,
- ✓ **εμπιστευτικότητα** που σημαίνει ότι έχει γίνει απαγόρευση διαχείρισης ευαίσθητων πληροφοριών από μη εξουσιοδοτημένους χρήστες και
- ✓ **ακεραιότητα** ότι το πληροφοριακό σύστημα και κατ' επέκταση η πολιτική ασφάλειας παραμένει σταθερή χωρίς μη εξουσιοδοτημένες αλλαγές.

Οι οδηγίες και οι διαδικασίες που περιλαμβάνονται στην πολιτική ασφάλειας υλοποιούνται με την εφαρμογή των μέτρων προστασίας για την ασφάλεια των πληροφοριακών συστημάτων. Η εφαρμογή μιας πολιτικής ασφάλειας σε έναν οργανισμό έχει δεσμευτικό χαρακτήρα για όλα τα μέλη του οργανισμού. Αυτό σημαίνει ότι η τήρηση των διαδικασιών και οδηγιών που προβλέπει η πολιτική ασφάλειας, και η εφαρμογή των μέτρων ασφάλειας που προδιαγράφονται σε αυτήν, είναι υποχρεωτική για όλους τους χρήστες των πληροφοριακών συστημάτων (Κάτσικας, Γκρίτζαλης, 2004).

Άρα γίνεται άμεσα αντιληπτό ότι οφείλουμε να εφαρμόζουμε τέτοιου είδους πολιτικές στα πληροφοριακά συστήματα διότι με αυτόν τον τρόπο υλοποιείται ένα ολοκληρωμένο πλαίσιο που συμβάλλει στην εγκαθίδρυση μέτρων ασφαλείας, μεγιστοποιείται η σημασία της ασφάλειας του πληροφοριακού συστήματος για κάθε έναν εργαζόμενο γαλουχώντας ταυτόχρονα την ανάλογη κουλτούρα και τέλος είναι νομικό προαπαιτούμενο ειδικά όταν στο πληροφοριακό σύστημα λαμβάνουν χώρα χρηματικές συναλλαγές και όχι μόνο.

Ένα μείζον θέμα για τα πιστωτικά ιδρύματα είναι η ασφάλεια της πληροφορίας και των συναλλαγών που λαμβάνουν χώρα διαδικτυακά. Η ασφάλεια της πληροφορίας καθώς και η προστασία των πληροφοριακών συστημάτων και συναλλαγών από τις συνεχώς αυξανόμενες απειλές στον κυβερνοχώρο, αποτελεί κύρια προτεραιότητα για της Τράπεζας. Ως πληροφορία νοείται κάθε έντυπη, ηλεκτρονική ή προφορική πληροφορία που παράγεται ή/ και χρησιμοποιείται από την Τράπεζα για την εκτέλεση των επιχειρηματικών της δραστηριοτήτων και περιλαμβάνει ενδεικτικά και όχι περιοριστικά τα ακόλουθα: ηλεκτρονικά δεδομένα, προσωπικά δεδομένα (ευαίσθητα και μη), οικονομικά δεδομένα, βάσεις δεδομένων, αρχεία, επιχειρηματικά σχέδια, εκθέσεις, ανακοινώσεις, προγράμματα λογισμικού, αποτελέσματα ελέγχων, μελέτες, υποδείγματα, σχέδια, προδιαγραφές, τεχνογνωσία, εγχειρίδια, πολιτικές, διαδικασίες κλπ. Έτσι η Τράπεζα καταρτίζει ειδικά έγγραφα προς ενημέρωση του προσωπικού με τους βασικούς κανόνες που πρέπει να τηρεί πιστά κατά την χρήση των πληροφοριακών μέσων της Τράπεζας, προκειμένου να υπάρχει ασφάλεια κατά την διενέργεια των τραπεζικών εργασιών και προστασία αυτών έναντι προσπαθειών ηλεκτρονικής εξαπάτησης.

1.5.1 Emails

Βασικοί κανόνες ασφαλείας που πρέπει να τηρούνται από το προσωπικό της Τράπεζας κατά την χρήση του εταιρικού e-mail :

- ✓ Αποφυγή να ανοίγουν ή να απαντούν σε e-mails από άγνωστους αποστολείς ή/ και με δελεαστικό θέμα/ περιεχόμενο ή να επιλέγουν τα links που τυχόν περιλαμβάνονται σε αυτά. Αυτού του τύπου τα e-mails είναι συνήθως κακόβουλα και ενδέχεται να περιλαμβάνουν επισυναπτόμενα αρχεία ή/ και συνδέσμους (links) προς ιστοσελίδες που αποσκοπούν είτε να μεταδώσουν ιούς είτε να υποκλέψουν ευαίσθητες πληροφορίες.
- ✓ Αποφυγή να επιλέγουν τα links που λαμβάνετε μέσω e-mails, έστω και εάν είναι γνωστός ο φερόμενος ως αποστολέας. Προτιμότερο είναι να πληκτρολογούν οι ίδιοι τη διεύθυνση στον Internet browser και μόνο εφόσον πρόκειται για γνωστή ιστοσελίδα.
- ✓ Αποφυγή απάντησης σε e-mail τρίτων, μέσω των οποίων ζητείται η παροχή ή επιβεβαίωση προσωπικών, εργασιακών ή οικονομικών δεδομένων.

- ✓ Έλεγχος της εγκυρότητας των στοιχείων του αποστολέα πριν προβούν σε οποιαδήποτε απάντηση μέσω e-mail και πριν αποσταλούν τυχόν πληροφορίες που έχουν ζητηθεί.
- ✓ Προώθηση για έλεγχο στον e-mail administrator ύποπτα ή αμφίβολης προέλευσης ή/και περιεχομένου e-mail,
- ✓ Μη προώθηση εταιρικών e-mails και αρχείων σε τρίτα μη εξουσιοδοτημένα άτομα ή σε προσωπικούς λογαριασμούς e-mail (π.χ. hotmail, gmail, yahoo) καθώς επίσης αποφυγή χρήσης υπηρεσιών cloud storage ή online back-up (π.χ. SkyDrive, iCloud, Google Drive) για την αποθήκευση των εταιρικών e-mail και αρχείων.
- ✓ Ενσωμάτωση κωδικών (passwords) σε αρχεία με ευαίσθητα δεδομένα

1.5.2 Χρήση Διαδικτύου

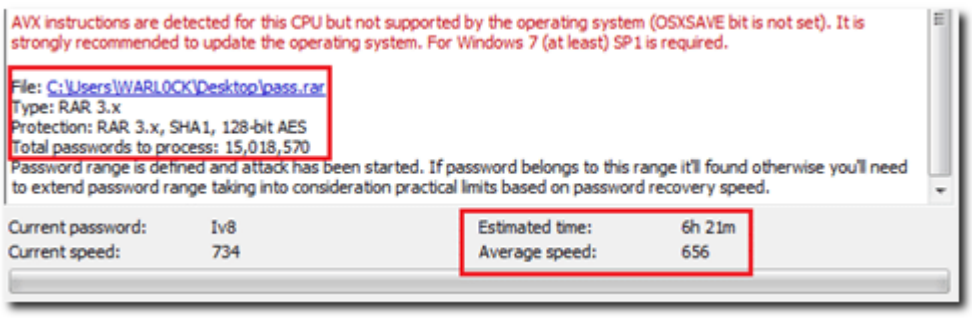
Βασικοί κανόνες ασφαλείας που πρέπει να τηρούνται από το προσωπικό της Τράπεζας κατά την χρήση του Διαδικτύου:

- ✓ Η πρόσβαση στο Διαδίκτυο (Internet) επιτρέπεται μόνο μέσω ειδικού διακομιστή (web proxy server). Η απ' ευθείας πρόσβαση μπλοκάρεται από τα συστήματα της Τράπεζας. Ο συγκεκριμένος διακομιστής – με τη χρήση κατάλληλου λογισμικού – προστατεύει σε πραγματικό χρόνο από κακόβουλο λογισμικό (virus, Trojans) που ενδεχομένως έχει μολύνει κάποιες ιστοσελίδες και ταυτόχρονα επιτρέπει την πρόσβαση σε συγκεκριμένες κατηγορίες ιστοσελίδων (internet websites) που είναι ασφαλείς και το περιέχομενο τους συνάδει με την επαγγελματική χρήση του Διαδικτύου.
- ✓ Ιδιαίτερη προσοχή κατά την πλοήγηση στο διαδίκτυο και αποφυγή εισόδου σε άγνωστες ιστοσελίδες, οι οποίες μπορεί να περιέχουν ιούς. Εφαρμογή της πρακτικής "Think before you click".
- ✓ Αποφυγή λήψης δεδομένων από το διαδίκτυο (downloading) που δεν προορίζονται για υπηρεσιακή χρήση.
- ✓ Προσοχή στις σχετικές αναρτήσεις και τις πληροφορίες που δημοσιοποιεί το προσωπικό στο διαδίκτυο και ιδιαίτερα στις ιστοσελίδες κοινωνικής/ επαγγελματικής δικτύωσης (facebook, twitter, linkedin κλπ.), καθώς ελλοχεύει ο κίνδυνος να γίνουν αντικείμενο εκμετάλλευσης από τρίτους.
- ✓ Μη παροχή της διεύθυνση του εταιρικού email κατά την εγγραφή σε ιστοσελίδες μη σχετιζόμενες με την επαγγελματική δραστηριότητα ή σε ιστοσελίδες παροχής μιας προσωρινής ή πολύ μικρής υπηρεσίας (π.χ. «κατέβασμα» δωρεάν ενός αρχείου).

1.5.3 Κωδικοί Πρόσβασης (Passwords)

Βασικοί κανόνες ασφαλείας που πρέπει να τηρούνται από το προσωπικό της Τράπεζας αναφορικά με την χρήση των κωδικών πρόσβασης (passwords):

- ✓ Οι κωδικοί πρόσβασης που χρησιμοποιούνται πρέπει να συμμορφώνονται με τους αντίστοιχους σχετικούς κανόνες πολυπλοκότητας των συνθηματικών της Τράπεζας πχ θα πρέπει να αποτελούνται από 12 αλφαριθμητικούς χαρακτήρες , να περιέχουν κεφαλαία και πεζά γράμματα, να περιέχουν έναν τουλάχιστον αριθμό (0-9) και να περιέχει τουλάχιστον έναν ειδικό χαρακτήρα (πχ !@#$%^). Ο συνδυασμός αυτών των στοιχείων κατατάσσει τον κωδικό στους κοινώς λεγόμενους ισχυρούς. Έτσι λοιπόν η Τράπεζα μέσω του των διαχειριστών του IT επιβάλλει τους παραπάνω όρους μέσω των σχετικών ρυθμίσεων και παραμέτρων. Οι λόγοι που συνίστανται αυτές οι προδιαγραφές είναι ότι όσο πιο σύνθετοι και ισχυροί είναι οι κωδικοί τόσο πιο δύσκολα σπάνε από τους επίδοξους απατεώνες, Γενικά, οι επιχειρήσεις εφιστούν την προσοχή στους χρήστες ώστε να μην χρησιμοποιούνται κωδικοί πρόσβασης οι οποίοι να χαρακτηρίζονται από γενέθλια, διευθύνσεις, προσωπικά στοιχεία, ονόματα κλπ διότι είναι από τα πλέον εύκολα και τα πιο χαρακτηριστικά που ο κάθε απατεώνας μπορεί να μαντέψει και να σπάσει εκθέτοντάς μας σε κίνδυνο. Είναι τρομερά προβλέψιμοι οι συγκεκριμένοι κωδικοί και γι αυτό συστήνεται να τους αποφεύγουμε. Μπορούμε εύκολα να συναντήσουμε κωδικούς που δημιουργούνται από μια συνεχόμενη γραμμή του πληκτρολογίου πχ qwerty ή κωδικούς που αποτελούνται από το όνομά μας και το έτος γέννησης πχ giannis81. Ένα ακόμη πολύ σημαντικό πρόβλημα είναι ότι πολλοί χρήστες δημιουργούν κωδικούς πρόσβασης με βάση την ημερομηνία γέννησης ή διευθύνσεις επειδή είναι κάτι εύκολο να θυμούνται και μοναδικό. Ακόμα και οι απλές και ασυνήθιστες λέξεις από ένα λεξικό θεωρούνται επικίνδυνες καθώς υπάρχουν ειδικά προγράμματα τα οποία μέσα σε λίγες ώρες μπορούν να βρουν όλους τους πιθανούς συνδυασμούς ακόμα και αν γίνει αντικατάσταση των λέξεων με αριθμούς και σύμβολα αφού οι hackers έχουν ήδη πρωτοπορήσει σ' αυτό το κομμάτι έχοντας προβλέψει στα προγράμματά τους τέτοιου είδους περιπτώσεις



(Πηγή https://www.pcsteps.gr/category/software/hlektroniki-asfaleia/)

Ως εκ τούτου γίνεται άμεσα κατανοητό ότι θα πρέπει να αποφεύγονται όλα εκείνα τα Password που εύκολα μπορεί κάποιος να μαντέψει όπως 12345 ή @qaz ή passw0rd διότι ο κίνδυνος είναι τεράστιος και οι ζημιές που μπορούν να προκληθούν είναι ανυπολόγιστες τόσο στο τερματικό της εταιρίας και στον υπολογιστή μας όσο και στα προσωπικά μας δεδομένα, τα δεδομένα τις εταιρίας. Παρατίθεται μία μικρή λίστα με τα πλέον επικίνδυνα Passwords που πρέπει οπωσδήποτε να αποφεύγουμε γενικότερα : 123456, password, 12345678, qwerty, abc1234 (Πηγή : http://www.cnn.gr/tech/story/55871/prosoxi-ayta-einai-ta-25-xeirotera-passwords-toy-kosmoy)

- ✓ Θα πρέπει να διαφυλάσσεται η μυστικότητα των κωδικών πρόσβασης.
- ✓ Να μην αναγράφονται σε σημεία μη ασφαλή, ειδικά πλησίον του χώρου εργασίας ούτε να αποστέλλονται μέσω e-mail.
- ✓ Να αλλάζονται οι κωδικοί σε περίπτωση που πιθανολογείται ότι μπορεί να έχουν διαρρεύσει ή προβλεφθεί από τρίτους καθώς επίσης οι κωδικοί προορίζονται για ίδια χρήση
- ✓ Αποφυγή χρήσης των ίδιων κωδικών πρόσβασης σε όλα τα συστήματα του Τράπεζας με αυτούς που χρησιμοποιούνται σε άλλες υπηρεσίες του διαδικτύου, όπως κοινωνικά δίκτυα, υπηρεσίες e-mail, online storage κλπ.

1.5.4 Ασφαλής Χρήση Κινητών Συσκευών (smartphones / tablets)

Οι κανόνες που ακολουθούν αφορούν κινητές συσκευές με πρόσβαση στο εταιρικό e-mail και δεδομένα της Τράπεζας:

- ✓ Να φυλάσσονται οι συσκευές από κλοπή ή προσωρινή αφαίρεση.
- ✓ Να ορίζονται PINs και κωδικοί πρόσβασης στις συσκευές
- ✓ Εγκατάσταση λογισμικού anti-virus, εφόσον υποστηρίζεται από την συσκευή.
- ✓ Ενεργοποίηση της δυνατότητας για απομακρυσμένη διαγραφή δεδομένων σε περίπτωση απώλειας της συσκευής.
- ✓ Εγκατάσταση ενημερώσεων / αναβαθμίσεων του λειτουργικού συστήματος και των εφαρμογών της συσκευής.
- ✓ Αποφυγή σύνδεσης σε links που περιέχονται σε SMS από άγνωστους ή μη αξιόπιστους αποστολείς.
- ✓ Αποφυγή σύνδεσης σε ελεύθερα ασύρματα τοπικά δίκτυα (free public WiFi hotspots).

- ✓ Έλεγχος πριν την εγκατάσταση μιας εφαρμογής, τα δικαιώματα πρόσβασης που απαιτεί για να εκτελεστεί.
- ✓ Διαγραφή όλων τα εταιρικών δεδομένων / πληροφοριών και επαναφορά της συσκευής στις εργοστασιακές της ρυθμίσεις πριν την διάθεση προς πώληση ή προς επισκευή.

Αξίζει να σημειωθεί ότι, η διαχείριση της ασφάλειας των πληροφοριακών συστημάτων είναι μια διαδικασία στην οποία εμπλέκονται πολλοί φορείς, οι οποίοι μπορεί να βρίσκονται τόσο εντός όσο και εκτός του οργανισμού. Οι ρόλοι εντός του οργανισμού που έχουν σημαντική εμπλοκή στην ασφάλεια των πληροφοριακών συστημάτων περιλαμβάνουν, μεταξύ άλλων, τους χρήστες και τους διαχειριστές των συστημάτων αυτών, τους υπεύθυνους για την ασφάλεια, και τα διοικητικά στελέχη του οργανισμού. Η καλή επικοινωνία και συνεργασία όλων των εμπλεκόμενων (stakeholders) είναι βασική προϋπόθεση για την αποτελεσματική διαχείριση της ασφάλειας των πληροφοριακών συστημάτων. Η πολιτική ασφάλειας, που αποτελεί το έγγραφο στο οποίο δηλώνονται τόσο οι στόχοι όσο και τα γενικά μέτρα για την ασφάλεια των πληροφοριακών συστημάτων, μπορεί να αποτελέσει ένα σημαντικό σημείο αναφοράς για την επικοινωνία και διαπραγμάτευση μεταξύ των εμπλεκόμενων φορέων, ώστε να δημιουργηθεί μια κοινή αντίληψη για την αναγκαιότητα της ασφάλειας (Κάτσικας, Γκριτζάλης, 2004).

1.6 Ασφάλεια Συναλλαγών e Banking

Οι Τράπεζες συνολικά έχουν επενδύσει πολλά στον τομέα της ασφάλειας των συναλλαγών και των υπηρεσιών πληρωμών μέσω e banking προκειμένου να εξασφαλίσει την προστασία των χρηστών. Και αυτό γιατί ο αριθμός των κακόβουλων λογισμικών και των εν γένει εκμεταλλεύσεων που επικεντρώνονται στα τρωτά σημεία των ηλεκτρονικών τραπεζικών συστημάτων και συναλλαγών, ολοένα και αυξάνεται (Laerte Peotta, Marcelo D. Holtz, Bernardo M. David, Flavio G. Deus, Rafael Timóteo de Sousa Jr, 2011). Ταυτόχρονα, προσβλέπουν και επενδύουν στην ανάπτυξη ενός υγιούς και αξιόπιστου περιβάλλοντος για τις υπηρεσίες πληρωμών. Ως ηλεκτρονικές πληρωμές κατατάσσονται τα εξής :

- Η εκτέλεση των πληρωμών με κάρτα στο διαδίκτυο, συμπεριλαμβανομένης της εικονικής κάρτας πληρωμών
- Η εκτέλεση των μεταφορών πίστωσης (CTs) στο διαδίκτυο.
- Την έκδοση και την τροποποίηση της άμεσης χρέωσης ηλεκτρονικές εντολές.
- Μεταφορές χρήματος μεταξύ δύο λογαριασμών μέσω του Διαδικτύου.

Οι εκάστοτε ομάδες / τμήματα Εταιρικής Ασφάλειας, είναι υπεύθυνες για τον συντονισμό και την παρακολούθηση δραστηριοτήτων που άπτονται της ασφάλειας των πληρωμών στο διαδίκτυο αλλά ταυτόχρονα επιφορτίζονται με τον συντονισμό νέων αναπτύξεων και την ενημέρωση των συμπληρωματικών σχετικών πολιτικών. Έτσι, οι Τράπεζες φροντίζουν να διενεργούν σχετικές αξιολογήσεις κινδύνου όσον αφορά την ασφάλεια των συναλλαγών / πληρωμών στο internet αλλά και για συναφείς υπηρεσίες όπως αναθεώρηση πολιτικών ασφαλείας, έλεγχος των υπηρεσιών πριν το rollout σε παραγωγικό περιβάλλον, σχετική αξιολόγηση πριν από την εγκατάσταση των εφαρμογών.

Οι Τράπεζες σε γενικότερο πλαίσιο βρίσκονται σε εγρήγορση ελέγχοντας και αξιολογώντας όλα εκείνα τα αποτελέσματα από το σύνολο αναφοράς των απειλών για την ασφάλεια των συναλλαγών. Ταυτόχρονα, αξιολογούν και τις συναφείς περιπτώσεις απάτης που σχετίζονται με τις υπηρεσίες πληρωμών διαδικτύου λαμβάνοντας υπόψη: i) τις τεχνικές λύσεις που χρησιμοποιήθηκαν, ii) αν οι υπηρεσίες έχουν ανατεθεί σε εξωτερικούς προμηθευτές και iii) το τεχνικό περιβάλλον των πελατών. Επιπλέον, οι Τράπεζες εξετάζουν τους κινδύνους ασφαλείας που σχετίζονται με τις ηλεκτρονικές πλατφόρμες e banking, την αρχιτεκτονική που τις διέπουν, τις τεχνικές προγραμματισμού και τις ρουτίνες τόσο από την πλευρά της ως παροχέα υπηρεσίας όπως για παράδειγμα την ανταπόκριση του συστήματος σε περίπτωση hijacking, επιθέσεις έγχυσης SQL, cross-site scripting, υπερχείλιση buffer από επίθεση DoS. Από την άλλη πλευρά, αυτή των πελατών της, εξετάζει τους κινδύνους που συνδέονται με τη χρήση εφαρμογών πολυμέσων, plugins του προγράμματος περιήγησης, πλαισίων, εξωτερικών συνδέσεων κ.λπ., καθώς και τα αποτελέσματα της διαδικασίας παρακολούθησης των συμβάντων ασφαλείας. Σε αυτή τη βάση, οι Τράπεζες καθορίζουν εάν και σε ποιο βαθμό ενδέχεται να χρειαστούν αλλαγές στις υπάρχουσες πολιτικές και διαδικασίες αναφορικά με τα μέτρα ασφαλείας, τις χρησιμοποιούμενες τεχνολογίες και τις προσφερόμενες διαδικασίες ή υπηρεσίες. Γι αυτό και στις προαναφερόμενες αλλαγές λαμβάνεται υπόψη και ο χρόνος που απαιτείται για τις σχετικές υλοποιήσεις που απαιτούνται για την καλύτερη ανταπόκριση της πλατφόρμας του e banking αλλά και της ανάλογης ασφάλειας των συναλλαγών και θεσπίζει εκ νέου ή επικαιροποιεί τα κατάλληλα μέτρα για την ελαχιστοποίηση των κινδύνων σε σχέση με την ασφάλεια των διαδικτυακών συναλλαγών αλλά και των περιπτώσεων απάτης (fraud). Μέσα στα πλαίσια αυτά, οι Τράπεζες αναλαμβάνουν την επανεξέταση των σεναρίων κινδύνου και των υφιστάμενων μέτρων ασφαλείας μετά από σοβαρά περιστατικά επηρεάζοντας και τροποποιώντας αναλόγως τις υπηρεσίες τους.

1.7 Αντιμετώπιση και πρόληψη

Σε αυτή την ενότητα θα αναλύσουμε τους τρόπους αντιμετώπισης που χρησιμοποιούν οι Τράπεζες αλλά και τις σχετικές μεθόδους πρόληψης.

1.7.1 Έλεγχοι και αναφορές

Βασικό και σημαντικό βήμα για τις Τράπεζες προκειμένου να καταστήσουν την διαδικτυακή προσφερόμενη υπηρεσία μέσω του e banking ασφαλή και να κρατήσουν την ικανοποίηση του χρήστη σε υψηλά επίπεδα, είναι η γενικότερη παρακολούθηση όλων των περιστατικών που μπορούν να συμβούν, η αναφορά τους και η αντιμετώπιση. Για το σκοπό αυτό, έχουν θεσπίσει διαδικασίες για την αναφορά τέτοιων στοιχείων. Σε περίπτωση σημαντικού συμβάντος σχετικά με την ασφάλεια συναλλαγών στο e banking, συμπεριλαμβανομένων των παραβιάσεων δεδομένων, υποκλοπή κωδικών κλπ η Τράπεζα αναφέρει το περιστατικό στις αρμόδιες αρχές (π.χ. Τράπεζα της Ελλάδος, Αρχή Προστασίας Δεδομένων). Την ίδια λογική ακολουθεί και με τους συνεργαζόμενους ηλεκτρονικού εμπόρους όπου για τις υπηρεσίες απόκτησης καρτών, οι Τράπεζες απαιτεί από τους συνεργαζόμενους ηλεκτρονικούς εμπόρους που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν ευαίσθητες πληροφορίες και δεδομένα να συνεργάζονται για τέτοια σημαντικά περιστατικά ασφάλειας πληρωμών, συμπεριλαμβανομένων παραβιάσεων δεδομένων, τόσο με την Τράπεζα όσο και με τις αρμόδιες αρχές.

Οι Τράπεζες εφαρμόζουν μέτρα ασφαλείας που συμβαδίζουν με τις ισχύουσες πρακτικές ασφαλείας της και ενσωματώνουν πολλαπλά στρώματα «άμυνας» όπου η αποτυχία μιας γραμμής άμυνας εμπίπτει στην επόμενη γραμμή υπεράσπισης (“defense in depth”). Η άμυνα σε βάθος (γνωστή και ως προσέγγιση του Κάστρου) είναι μια έννοια διασφάλισης πληροφοριών, στην οποία τοποθετούνται πολλαπλά στρώματα ελέγχων ασφαλείας (άμυνας) σε όλο το σύστημα πληροφορικής (IT). Η πρόθεσή της είναι να παρέχει πλεονασμό σε περίπτωση που αποτύχει ο πρώτος έλεγχος ασφαλείας ή εκμεταλλευτεί ο εισβολέας μια ευπάθεια που μπορεί να καλύψει πτυχές προσωπικού, διαδικαστικής, τεχνικής και φυσικής ασφάλειας για τη διάρκεια του κύκλου ζωής του συστήματος. Έτσι, κατά το σχεδιασμό, την ανάπτυξη και τη συντήρηση των υπηρεσιών μέσω Διαδικτύου, η Τράπεζα δίνει ιδιαίτερη προσοχή στον επαρκή έλεγχο από τα τμήματα του IT στις τεχνικές προδιαγραφές (π.χ. ανάπτυξη, δοκιμή και περιβάλλον παραγωγής) και την ορθή εφαρμογή της αρχής των «λιγότερο προνομιούχων» (principle of least privilege). Στην ασφάλεια των πληροφοριών, την επιστήμη των υπολογιστών και σε άλλους τομείς, η αρχή του ελάχιστου προνομίου (γνωστή και ως αρχή ελάχιστου προνομίου ή αρχή της

ελάχιστης εξουσίας) απαιτεί ότι σε ένα συγκεκριμένο επίπεδο αφαίρεσης ενός υπολογιστικού περιβάλλοντος, κάθε ενότητα διαδικασία, χρήστης ή πρόγραμμα, ανάλογα με το θέμα) πρέπει να έχει πρόσβαση μόνο στις πληροφορίες και τους πόρους που είναι απαραίτητες για τον νόμιμο σκοπό του. Η αρχή σημαίνει ότι δίνεται σε έναν χρήστη μόνο εκείνα τα δικαιώματα που είναι απαραίτητα για την εκτέλεση της προβλεπόμενης εργασίας του. Για παράδειγμα, ένας λογαριασμός χρήστη με μοναδικό σκοπό τη δημιουργία αντιγράφων ασφαλείας δεν χρειάζεται να εγκαταστήσει λογισμικό: συνεπώς, έχει δικαιώματα μόνο για την εκτέλεση εφαρμογών δημιουργίας αντιγράφων ασφαλείας. Οποιαδήποτε άλλα δικαιώματα, όπως η εγκατάσταση νέου λογισμικού, αποκλείονται.

Οι Τράπεζες επίσης διαθέτουν λύσεις ασφάλειας για την προστασία των δικτύων, των ιστότοπων, των διακομιστών (servers) από επιθέσεις. Οι διακομιστές απαλλάσσονται από όλες τις περιττές λειτουργίες προκειμένου να προστατευτούν και να εξαλειφθούν (ή μειωθούν) οι τυχόν ευπάθειες των εφαρμογών σε υπάρχοντα κίνδυνο. Ακολουθείται κι εδώ η λογική principle of least privilege ώστε να περιοριστεί η χρήση των «ψεύτικων» ιστότοπων (που μιμούνται νόμιμους ιστότοπους της Τράπεζας), οι ιστοσελίδες συναλλαγών που προσφέρουν υπηρεσίες πληρωμών μέσω διαδικτύου είναι που προσδιορίζονται από εκτεταμένα πιστοποιητικά επικύρωσης που καταρτίζονται στο όνομα της Τράπεζας ή από άλλη παρόμοια πιστοποίηση. Κατά το σχεδιασμό λοιπόν, την ανάπτυξη και τη συντήρηση υπηρεσιών πληρωμών μέσω Διαδικτύου, η Τράπεζα διασφαλίζει ότι η ελαχιστοποίηση των δεδομένων, δηλαδή η συλλογή του ελάχιστου αριθμού προσωπικών πληροφοριών που είναι απαραίτητες για την εκτέλεση μιας συγκεκριμένης λειτουργίας, είναι το βασικό στοιχείο της κύριας λειτουργικότητας (προστασία της ιδιωτικότητας κατά τον σχεδιασμό) και επομένως η συλλογή, η επεξεργασία, η αποθήκευση και η αρχειοθέτηση των ευαίσθητων δεδομένων διατηρούνται στο απολύτως ελάχιστο επίπεδο (βάσει ισχύουσας νομοθεσίας). Όλα τα απαιτούμενα μέτρα ασφαλείας της Τράπεζας για τις υπηρεσίες πληρωμών διαδικτύου ελέγχονται από συγκεκριμένα τμήματα που έχουν επιφορτιστεί με αυτό τον σκοπό και όλες οι κατά περίπτωση διαδικαστικές και συστημικές αλλαγές υπόκεινται στην επίσημη διαδικασία διαχείρισης αλλαγών (προδιαγραφές, έλεγχος, τεκμηρίωση, παραγωγή). Και επειδή η πρόληψη είναι ύψιστης σημασίας, οι Τράπεζες προβαίνουν σε τακτικές δοκιμές που περιλαμβάνουν σενάρια επιθέσεων και απειλών που έχουν γίνει κατά το παρελθόν. Αντίστοιχα και τα μέτρα ασφάλειας για τις υπηρεσίες πληρωμών μέσω Διαδικτύου ελέγχονται περιοδικά για να εξασφαλίζεται η ακεραιότητά τους και η αποτελεσματικότητά τους. Ωστόσο στην συχνότητα αυτών των ελέγχων λαμβάνεται υπόψη και είναι ανάλογη με τους κινδύνους ασφαλείας που συνεπάγεται.

Οι Τράπεζες επίσης, προκειμένου να παρέχουν όσο το δυνατόν μεγαλύτερη ασφάλεια στις συναλλαγές και για να προλάβουν τυχόν δυσλειτουργίες έχουν ενεργοποιήσει ειδικούς μηχανισμούς ασφαλείας για την λεπτομερή καταγραφή των συναλλαγών συμπεριλαμβανομένου του διαδοχικού αριθμού συναλλαγής (αύξων αριθμός), timestamps για δεδομένα συναλλαγής, παραμετροποίηση καθώς και πρόσβαση σε δεδομένα της ηλεκτρονικής εντολής (πχ έμβασμα, πάγια εντολή κλπ). Εξουσιοδοτημένοι χρήστες από ειδικά τμήματα έχουν την πρόσβαση που επιτρέπει την προσθήκη, αλλαγή ή διαγραφή δεδομένων συναλλαγής και ηλεκτρονικής εντολής. Στη συνέχεια, όλα τα στοιχεία διερευνώνται και αναλύονται για να διασφαλίζεται η ασφάλεια της συναλλαγής.

Από την πλευρά του χρήστη, οι Τράπεζες φροντίζουν να διασφαλίζουν την εγκυρότητα στην πρόσβαση των υπηρεσιών παρέχοντας όλες τις απαραίτητες πληροφορίες σχετικά με τις απαιτήσεις για την πραγματοποίηση ασφαλών συναλλαγών πληρωμών στο διαδίκτυο και τους εγγενείς κινδύνους. Γι αυτό φροντίζουν να ενημερώνουν τον χρήστη πριν από τη σύναψη σύμβασης παροχής των υπηρεσιών συναλλαγών μέσω διαδικτύου, εκτός από τις πληροφορίες που ορίζονται σε οποιαδήποτε ισχύουσα νομοθεσία περί των σχετικών υπηρεσιών. Αυτά περιλαμβάνουν, κατά περίπτωση:

- Σαφή πληροφόρηση σχετικά με τυχόν απαιτήσεις από πλευράς εξοπλισμού πελατών, λογισμικού ή άλλων απαραίτητων εργαλείων (π.χ. λογισμικό προστασίας από ιούς, firewalls).
- Κατευθυντήριες γραμμές για τη σωστή και ασφαλή χρήση των στοιχείων εισόδου στο e banking
- Περιγραφή της διαδικασίας προς τον χρήστη για προβεί και να εγκρίνει μια συναλλαγή πληρωμής και / ή τη λήψη πληροφοριών, συμπεριλαμβανομένων των συνεπειών κάθε ενέργειας
- Οδηγίες για την σωστή και ασφαλή χρήση του υλικού και του λογισμικού που παρέχονται στον πελάτη.
- Τις διαδικασίες που πρέπει να ακολουθούνται σε περίπτωση απώλειας ή κλοπής των στοιχείων εισόδου στο e banking
- Τις διαδικασίες που πρέπει να τηρούνται σε περίπτωση ανίχνευσης ή ύποπτης κατάχρησης.
- Περιγραφή των ευθυνών και των υποχρεώσεων της Τράπεζας και του πελάτη αντίστοιχα όσον αφορά την χρήση της υπηρεσίας του e banking.

Πέραν των άλλων η Τράπεζα διασφαλίζει ότι η σύμβαση με τον πελάτη ορίζει ότι μπορεί να αποκλείσει συγκεκριμένη συναλλαγή, λαμβάνοντας υπόψη τυχόν εφαρμοστέες νομοθετικές απαιτήσεις σχετικά με τα όρια χρήσης μέσων πληρωμών βάσει σχετικών ανησυχητικών ή ύποπτων ενδείξεων. Ταυτόχρονα η σύμβαση καθορίζει τη μέθοδο και τους όρους της ειδοποίησης του πελάτη και τον τρόπο με τον οποίο ο πελάτης μπορεί να επικοινωνήσει με την Τράπεζα.

Δεν θα πρέπει να παραβλέψουμε και το πολύ σημαντικό κομμάτι της ισχυρής πιστοποίησης του χρήστη στην υπηρεσία και στην πλατφόρμα του e banking. Οι Τράπεζες διενεργούν ελέγχους ταυτότητας χρήστη για την εξουσιοδότηση συναλλαγής μέσω διαδικτύου και την έκδοση ή τροποποίηση εντολών ηλεκτρονικής άμεσης χρέωσης (πάγιες εντολές). Ωστόσο, ανάλογα με τους κινδύνους που ενέχει κάθε συναλλαγή ή κίνηση, η Τράπεζα θα μπορούσε να εξετάσει το ενδεχόμενο υιοθέτησης εναλλακτικών μέτρων ταυτοποίησης όπως για παράδειγμα :

- Τις εξερχόμενες πληρωμές σε αξιόπιστους δικαιούχους που περιλαμβάνονται σε «λευκές και καθαρές λίστες» που είχαν καταρτιστεί προηγουμένως για αυτόν τον χρήστη
- Συναλλαγές μεταξύ δύο λογαριασμών του ίδιου πελάτη που τηρούνται στην Τράπεζα,
- Μεταφορές εντός της Τράπεζας που δικαιολογούνται βάσει της σχετικού risk analysis.
- πληρωμές χαμηλής αξίας, όπως αναφέρεται σε οποιαδήποτε σχετική νομοθεσία περί υπηρεσιών πληρωμών.

Για συναλλαγές έκδοσης καρτών, οι Τράπεζες υποστηρίζουν επίσης τον ισχυρό έλεγχο ταυτότητας του κατόχου της κάρτας, όπως αυτό προβλέπεται από τα συστήματα πληρωμών με κάρτα. Όταν οι Τράπεζες προσφέρουν υπηρεσίες απόκτησης καρτών, υποστηρίζουν τέτοιες τεχνολογίες που επιτρέπουν στον εκδότη να επιτελέσει ισχυρή επικύρωση του κατόχου της κάρτας για τα συστήματα πληρωμών με κάρτα στα οποία συμμετέχει ο αγοραστής. Η χρήση εναλλακτικών μέτρων εξακρίβωσης της γνησιότητας θεωρούνται για προκαθορισμένες κατηγορίες συναλλαγών χαμηλού κινδύνου, π.χ. με βάση την ανάλυση κινδύνου συναλλαγών (risk analysis) ή τις εντολές πληρωμών με prepaid cards ή με πληρωμές μικρής αξίας, όπως αναφέρεται σε οποιαδήποτε ισχύουσα νομοθεσία περί υπηρεσιών πληρωμών. Τέλος, για τις εικονικές κάρτες, η αρχική εγγραφή λαμβάνει χώρα σε ένα ασφαλές και αξιόπιστο περιβάλλον.

1.7.2 Προστασία ευαίσθητων δεδομένων

Όλα τα δεδομένα που χρησιμοποιούνται για τον εντοπισμό και τον έλεγχο ταυτότητας των πελατών (π.χ. κατά την σύνδεση, κατά την έναρξη των συναλλαγών μέσω e banking, την έκδοση, την τροποποίηση ή την ακύρωση ηλεκτρονικών εντολών), προστατεύονται κατάλληλα κατά της κλοπής και της μη εξουσιοδοτημένης πρόσβασης ή τροποποίησης από εισβολείς. Οι

Τράπεζες διασφαλίζουν ότι όταν ανταλλάσσει ευαίσθητα δεδομένα συναλλαγών μέσω e banking, η ασφάλεια ως προς την κρυπτογράφηση είναι τέτοια ώστε κατά την διάρκεια της επικοινωνίας μεταξύ των δύο μερών να διασφαλιστεί η εμπιστευτικότητα και η ακεραιότητα των δεδομένων, χρησιμοποιώντας ισχυρές και ευρέως αναγνωρισμένες τεχνικές κρυπτογράφησης. Για να παραμένουν απόρρητα τα δεδομένα που μεταφέρονται κατά τη διάρκεια της σύνδεσης του χρήστη με το e banking, χρησιμοποιείται αναλόγως το πρωτόκολλο κρυπτογράφησης SSL-128bit. Η κρυπτογράφηση με 128bit σημαίνει ότι υπάρχουν 2128 πιθανά κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των μηνυμάτων από τον Internet Explorer στον server της τράπεζας. Για αυτόν τον λόγο, η κρυπτογράφηση στα 128bit θεωρείται πρακτικά αδύνατο να παραβιαστεί. Η σελίδα μπορεί να αναγνωριστεί ότι είναι αυθεντική, καθώς το πρωτόκολλο που εμφανίζεται με την διεύθυνση της τράπεζας μετατρέπεται από «http» σε «https» και εμφανίζεται παράλληλα και το χαρακτηριστικό εικονίδιο με το λουκέτο. Το κλειδί αυτό έχει υλοποιηθεί σε συνεργασία με την πιο αναγνωρισμένη εταιρεία έκδοσης κρυπτογραφικών κλειδιών για τραπεζικές υπηρεσίες, που ειδικεύεται σε θέματα ασφάλειας συναλλαγών.

1.7.3 Παρακολούθηση συναλλαγών

Οι Τράπεζες χρησιμοποιούν συστήματα ανίχνευσης και πρόληψης της απάτης για τον εντοπισμό ύποπτων συναλλαγών. Τέτοια συστήματα βασίζονται, για παράδειγμα, σε παραμετροποιημένους κανόνες (όπως π.χ. Black list δεδομένων από κλοπή καρτών) και την παρακολούθηση μη φυσιολογικών συμπεριφορών του πελάτη ή την πρόσβαση του χρήστη (όπως αλλαγή διεύθυνσης πρωτοκόλλου Internet ή IP, μερικές φορές προσδιορίζεται από ελέγχους IP γεωγραφικής θέσης και κατανομής κ.λπ.). Τέτοια συστήματα είναι επίσης σε θέση να ανιχνεύσουν σημάδια κακόβουλου λογισμικού (π.χ. μέσω script) και γνωστών σεναρίων απάτης. Η έκταση, η πολυπλοκότητα, και η προσαρμοστικότητα των λύσεων παρακολούθησης, τηρώντας παράλληλα τη σχετική νομοθεσία για την προστασία των δεδομένων, είναι ανάλογα με το αποτέλεσμα της αξιολόγησης του κινδύνου ασφαλείας. Για τις συναλλαγές απόκτησης κάρτας, υπάρχουν συστήματα ανίχνευσης και πρόληψης της απάτης για την παρακολούθηση του ηλεκτρονικού εμπόρου. Η Τράπεζα διενεργεί όλες τις διαδικασίες ελέγχου και αξιολόγησης των συναλλαγών εντός κατάλληλης χρονικής περιόδου, ώστε να μην καθυστερήσει αδικαιολόγητα την έναρξη ή / και την εκτέλεση της σχετικής υπηρεσίας. Σε περίπτωση που η Τράπεζα αποφασίσει να αποκλείσει μια συναλλαγή πληρωμής που έχει προσδιοριστεί ως δυνητικά δόλια, διατηρεί την σχετική φραγή των συναλλαγών για όσο το δυνατόν πιο σύντομο χρονικό διάστημα μέχρι να επιλυθούν τα ζητήματα ασφάλειας.

Κεφάλαιο 2

Εκπαίδευση

Όπως έχουμε ήδη δει, η χρήση του διαδικτύου και συγκεκριμένα η ηλεκτρονική τραπεζική εγκυμονεί πολλούς κινδύνους από εισβολείς και απατεώνες που έχουν σκοπό συνήθως το κέρδος. Εκτός λοιπόν από την ασφαλή και εύκολη χρήση της εφαρμογής απαιτείται και η σωστή εκπαίδευση των χρηστών. Συμφωνούμε μέχρι στιγμής ότι η μεγάλη απειλή για την ασφάλεια της πλατφόρμες του e banking δεν είναι άλλη παρά από τα κακόβουλα λογισμικά και γενικότερες επιθέσεις. Ωστόσο, δεν θα πρέπει να παραβλέψουμε το γεγονός ότι σε ένα οργανισμό όπως η Τράπεζα, υπάρχει και η μερίδα εκείνων των εργαζομένων που θεωρούνται ως οι απρόσεκτοι που δεν συμμορφώνονται με τις πολιτικές ασφαλείας που έχουν θεσπιστεί με σκοπό την ασφάλεια των πληροφοριών και τις διαδικασίες. Παράγοντες της γενικότερης μη συμμόρφωσης είναι η γενικότερη νοοτροπία των εργαζομένων, η έλλειψη σχετικής ευαισθητοποίησης σε θέματα ασφάλειας, οι πεποιθήσεις και οι συνήθειες, η άγνοια και εν γένει έλλειψη εκπαίδευσης σε θέματα ασφάλειας (Seppo Pahnila, Mikko Siponen and Adam Mahmoodb 2007).

2.1 Εκπαίδευση και ενημέρωση εργαζομένων σήμερα

Οι Τράπεζες παρέχουν βοήθεια και καθοδήγηση στους χρήστες, όπου χρειάζεται, σε σχέση με την ασφαλή χρήση του e banking. Στο πλαίσιο αυτής της διαδικασίας :

- Η Τράπεζα παρέχει τουλάχιστον ένα ασφαλές κανάλι (π.χ. ιστότοπο Internet, τηλεφωνική υπηρεσία) για συνεχή χρήση επικοινωνία με τους πελάτες σχετικά με τη σωστή και ασφαλή χρήση της υπηρεσίας και της πλατφόρμας του e banking.
- Η Τράπεζα ενημερώνει τους πελάτες ότι αυτό το κανάλι δεν είναι αξιόπιστο και εξηγεί ότι οποιοδήποτε μήνυμα εξ ονόματος της Τράπεζας μέσω οποιασδήποτε άλλης όπως το ηλεκτρονικό ταχυδρομείο, στο οποίο μπορεί να έχει μηνύματα που αφορούν τη σωστή και ασφαλή χρήση της υπηρεσίας, να μην λαμβάνονται υπόψη (think before you click)

- Εξηγεί την διαδικασία για την υποβολή σχετικών παραπόνων για ύποπτες και δόλιες πληρωμές, ύποπτα περιστατικά ή ανωμαλίες κατά τη διάρκεια που είναι συνδεδεμένοι οι χρήστες στην πλατφόρμα (πιθανές προσπάθειες κοινωνικής μηχανικής). Ταυτόχρονα αναφέρει :
    - τα επόμενα βήματα και το πώς θα ανταποκριθεί
    - τον τρόπο με τον οποίο η Τράπεζα θα ειδοποιήσει τον πελάτη σχετικά με (δυνητικές) δόλιες συναλλαγές ή θα προειδοποιήσει τον πελάτη για την εμφάνιση επιθέσεων (π.χ. phishing e-mails).
- Μέσω του ασφαλούς ιστότοπου, η Τράπεζα ενημερώνει τους πελάτες για σχετικά updates στις διαδικασίες ασφαλείας και σχετικά με τις υπηρεσίες πληρωμών μέσω Διαδικτύου. Η ίδια λογική ακολουθείται και για όλες τις ειδοποιήσεις σχετικά με σημαντικούς κινδύνους που αφορούν την κοινωνική μηχανική.
- Παρέχεται βοήθεια από την Τράπεζα για όλες τις ερωτήσεις, τις καταγγελίες, τα αιτήματα υποστήριξης και την υποστήριξη πελατών/χρηστών. Τέτοια αιτήματα μπορεί να είναι ειδοποιήσεις ύποπτων συμβάντων σχετικά με τις συναλλαγές μέσω Διαδικτύου και συναφείς υπηρεσίες.
- Η Τράπεζα προωθεί προγράμματα εκπαίδευσης και ευαισθητοποίησης πελατών, με σκοπό να διασφαλίσει ότι οι πελάτες θα κατανοήσουν, στο ελάχιστο την ανάγκη :
    - να προστατεύουν τους κωδικούς τους, τα προσωπικά τους στοιχεία και άλλα εμπιστευτικά δεδομένα
    - να διαχειρίζεται σωστά την ασφάλεια της προσωπικής συσκευής (π.χ. υπολογιστή, κινητό, tablet), μέσω της εγκατάστασης και της ενημέρωσης (update) προγραμμάτων ασφαλείας (antivirus, firewalls).
    - να εξετάσει τις σημαντικές απειλές και τους κινδύνους που σχετίζονται με τη λήψη λογισμικού μέσω του διαδικτύου εάν δεν μπορεί να είναι αρκετά σίγουρος ότι το λογισμικό είναι αυθεντικό και δεν έχει αλλοιωθεί.
    - να χρησιμοποιήσει τον ιστότοπο του e banking μέσω της επίσημης ιστοσελίδας της Τράπεζας.

Γενικότερα η Τράπεζα, σύμφωνα με την ισχύουσα νομοθεσία περί υπηρεσιών πληρωμών και συναλλαγών, θα μπορούσε να συμφωνήσει με τους πελάτες της σχετικά με τα όρια του χρήσης του e banking ειδικά για τις υπηρεσίες πληρωμών και θα μπορούσε να παρέχει στους χρήστες, δυνατότητες για περαιτέρω περιορισμό των κινδύνων εντός αυτών των ορίων. Μπορεί επίσης να παρέχει υπηρεσίες διαχείρισης ειδοποιήσεων στο προφίλ των χρηστών εντός της πλατφόρμας. Πριν από την παροχή στον πελάτη αυτών των υπηρεσιών, η Τράπεζα θέτει όρια, τα οποία

μπορεί να ισχύουν είτε ατομικά είτε παγκοσμίως δηλαδή σε όλα τα μέσα πληρωμών που επιτρέπουν τις συναλλαγές στο διαδίκτυο (π.χ. μέγιστο ποσό για κάθε πληρωμή ή ένα σωρευτικό ποσό για ένα συγκεκριμένο χρονικό διάστημα) και να ενημερώνει αναλόγως. Τέλος, παρέχεται η δυνατότητα για σχετική πρόσβαση των χρηστών σε πληροφορίες σχετικά με την κατάσταση της έναρξης και εκτέλεσης των πληρωμών, εμβασμάτων, πάγιων εντολών.

2.2 Μη συμμόρφωση εργαζομένων και κατευθυντήριες γραμμές

Στις μέρες μας, για τα ευαίσθητα θέματα της ασφάλειας, οι Τράπεζες ενημερώνουν τους εργαζόμενους με σχετικές ηλεκτρονικές αλληλογραφίες ή αντίστοιχα υπηρεσιακά σημειώματα. Παρόλα αυτά, σε σχετική έκθεση από την ερευνητική εταιρία Haystax (Πηγή:http://www.real.gr/DefaultArthro.aspx?page=arthro&id=621806&catID=22&mode=tab) , έχουν εντοπιστεί τρία είδη εργαζομένων που μπορούν να αποτελέσουν απειλή για τα συστήματα και τα δεδομένα κάποιας εταιρείας: οι εργαζόμενοι που ενώ έχουν αθώες προθέσεις εντούτοις καταφέρνουν να προκαλέσουν ζημιά, αυτοί που είναι απρόσεκτοι και αυτοί που έχουν κάποια σκοπιμότητα. Όταν πρόκειται για παραβίαση δεδομένων, οι «αθώοι» εργαζόμενοι μπορούν να προκαλέσουν τόση ζημιά όσο και κυβερνοεγκληματίες. Σύμφωνα με την έρευνα, οι τοπικές αρχές συγκεκριμένων περιοχών του Ηνωμένου Βασιλείου, κατέγραψαν 160 παραβιάσεις στα συστήματά τους την περίοδο 2014-2015. Η πλειονότητα αυτών οφειλόταν σε ανθρώπινο λάθος. Ένας ακόμα παράγοντας είναι η αμέλεια. Από έρευνα που είχε διεξάγει η Google το 2013 προέκυψε το συμπέρασμα ότι περίπου το 70% των προειδοποιήσεων ασφαλείας που εμφανίζονται σε αναδυόμενα παράθυρα του Chrome, αγνοούνται συστηματικά από τους χρήστες. Αυτό σημαίνει ότι το πρόγραμμα περιήγησης στο Διαδίκτυο δεν ενημερώνεται με τις τελευταίες εκδόσεις ασφαλείας, κάτι που αφήνει τα συστήματα ευάλωτα σε εξωτερικές επιθέσεις. Τέλος, όπως και το ανθρώπινο λάθος, έτσι και οι κακόβουλες ενέργειες εργαζομένων παίζουν επίσης ρόλο στις παραβιάσεις προσωπικών στοιχείων. Η περίπτωση αυτή συμβαίνει συνήθως όταν κάποιος δυσαρεστημένος υπάλληλος επιδιώκει να «εκδικηθεί» την εταιρεία στην οποία εργάζεται. Σύμφωνα με έρευνα που είχε διεξάγει η εταιρεία Nuix το 2016, το 93% των ερωτηθέντων απάντησαν ότι η ανθρώπινη συμπεριφορά αποτελεί τον μεγαλύτερο κίνδυνο στην προστασία των δεδομένων. Όπως αναφέρει στην έκθεσή της η Haystax, ίσως το πιο λογικό βήμα που θα μπορούσαν να κάνουν οι εργοδότες είναι να διασφαλίσουν ότι όλοι ανεξαιρέτως οι εργαζόμενοί τους είναι ενημερωμένοι σχετικά με τον πιθανό αντίκτυπο των ενεργειών τους καθώς και πώς μπορούν να αποφύγουν την ακούσια απώλεια δεδομένων.

Ο άνθρωπος συχνά αποτελεί τον αδύναμο κρίκο σχετικά με την ασφάλεια των πληροφοριών καθώς μπορεί εύκολα να εξαπατηθεί και να χειραγωγηθεί (Francois Mouton, Louise Leenen a, H.S. Venter, 2016). Η γενικότερη μη συμμόρφωση του υπαλλήλου με τις πολιτικές περί ασφάλειας των συστημάτων αποτελεί βασική μέριμνα για τους οργανισμούς και κατ' επέκταση για τις Τράπεζες. Και αυτό γιατί εάν οι χρήστες δεν συμμορφώνονται με τις πολιτικές ασφαλείας, όλες οι πρακτικές και οι λύσεις για την ασφάλεια χάνουν την αποτελεσματικότητά τους. Επομένως, μία από τις πλέον ενδεδειγμένες πρακτικές για την συμμόρφωση του εργαζομένου είναι η εκπαίδευση αλλά και η ευαισθητοποίηση σε θέματα ασφάλειας. Η ευαισθητοποίηση αυτή δείχνει στην πραγματικότητα και τον βαθμό της κατανόησης των χρηστών σχετικά με τη σημασία της ασφάλειας των πληροφοριών, τις ευθύνες αλλά και τις ενέργειες ελέγχων που οφείλουν να ασκούν για την προστασία των δεδομένων και των δικτύων του οργανισμού.

Από τις υπάρχουσες μελέτες σχετικά με την εκπαίδευση των εργαζομένων σε θέματα ασφαλείας σε πληροφοριακά συστήματα και κατ' επέκταση στην ηλεκτρονική τραπεζική, αποτυπώνουν ποιες θα πρέπει να είναι εκείνες οι μαθησιακές αρχές που μπορούν να επηρεάσουν την συμμόρφωση των χρηστών σε θέματα ασφάλειας των πληροφοριών και στις αντίστοιχες πολιτικές που τις διέπουν. Βρισκόμαστε σε μια εποχή όπου ενώ κάποτε οι χρήστες ηλεκτρονικών υπολογιστών ήταν λίγοι αλλά με βαθιές γνώσεις, σήμερα οι χρήστες είναι πολλοί με βασικές και επιφανειακές γνώσεις (M.E. Thomson, R. von Solms, 2009). Ακόμα παρατηρούμε το πόσο επιτακτική είναι η ανάγκη για θέσπιση και οργάνωση προγραμμάτων ανάλογης ευαισθητοποίησης και εκπαίδευσης των εργαζομένων στις επιχειρήσεις (R.S. Shaw, Charlie C. Chen, Albert L. Harris, & Hui-Jou Huang, 2009) . Από την άλλη πλευρά, άλλες μελέτες κάνουν λόγο, για το γεγονός ότι η εκπαίδευση των εργαζομένων έχει μεγαλύτερη επίδραση όταν ακολουθείται από δύο θεωρίες : την καθολική εποικοδομητική διδασκαλία (the universal constructive instructional theory) και το μοντέλο πιθανότητας επεξεργασίας (the elaboration likelihood model) [Petri Puhakainen, Mikko Siponen, 2010]. Πέραν των άλλων, έρευνες βασισμένες σε ψυχολογικά μοντέλα και θεωρίες αξιολογούν με τρόπο αποτελεσματικό τα διάφορα εργαλεία και τεχνικές που ευαισθητοποιούν και κεντρίζουν τον εργαζόμενο σε έναν οργανισμό σε θέματα ασφάλειας (Bilal Khan, Khaled S. Alghathbar, Syed Irfan Nabi1, and Muhammad Khurram, 2011).

Ως εκ τούτου θα προσεγγίσουμε τις παραπάνω θεωρίες και πρακτικές προκειμένου να διεισδύσουμε στις νευραλγικές έννοιες της εκπαίδευσης, ευαισθητοποίησης και της οργάνωσης του προσωπικού.

2.2.1 Συμπεριφορικό μοντέλο

Σύμφωνα με την έρευνα των Bilal Khan, Khaled S. Alghathbar, Syed Irfan Nabi1, and Muhammad Khurram Khan, 2011, η μάθηση για τέτοιου είδους θέματα σχετικά με την ασφάλεια των πληροφοριακών συστημάτων βασίζεται αποτελεσματικότητα των κάτωθι εργαλείων:

1) Εκπαιδευτική παρουσίαση

Η εκπαίδευση συχνά θεωρείται ως το κλειδί για την αλλαγή της συμπεριφοράς απέναντι σε ζητήματα ασφάλειας. Τα διάφορα σεμινάρια και εκπαιδευτικά υλικά βασίζονται σε διαφορετικές ψυχολογικές θεωρίες που επικεντρώνονται σε διαφορετικές πτυχές της ανθρώπινης ψυχολογίας. Πολλοί οργανισμοί επίσης, χρησιμοποιούν την μέθοδο του e learning ως συμπληρωματική μέθοδο (Kirsty Vaughan, Anna McVicar, 2004). Συνήθως αυτές οι εκπαιδευτικές εκστρατείες στοχεύουν αμιγώς στο κομμάτι της γνώσης και της εμπειρίας ενώ αγνοούν το κίνητρο που βρίσκεται πίσω από την ανθρώπινη συμπεριφορά. Σύμφωνα με το εργαλείο αυτό, η γνώση δεν αποτελεί το κίνητρο για την σωστή συμπεριφορά σε θέματα ασφάλειας. Ωστόσο, η έλλειψη γνώσης αποτελεί εμπόδιο στην ανάπτυξη μιας επιθυμητής συμπεριφοράς που διαφυλάττει τα συμφέροντα του οργανισμού. Στα εκπαιδευτικά σεμινάρια παρέχονται όλες οι απαραίτητες και απαιτούμενες πληροφορίες, αλλά δεν παύει να γίνεται μια απλή μεταφορά πληροφοριών και γνώσεων από τον παρουσιαστή στο ακροατήριο. Για παράδειγμα, σε τέτοιες παρουσιάσεις παρατηρούμε ότι δίδονται πληροφορίες και οδηγίες σχετικά την σωστή διαχείριση και δημιουργία ενός κωδικού πρόσβασης, τη σωστή διαχείριση του ηλεκτρονικού ταχυδρομείου, την προστασία από ιούς και τις πολιτικές ασφάλειας των του οργανισμού που όμως στην πράξη δεν οδηγούν σε αλλαγή συμπεριφοράς και ευαισθητοποίησης. Γι αυτό, όταν οι παρουσιάσεις αυτές διέπονται και από τις ανάλογες κοινωνικές διαστάσεις και προδιαγραφές είναι σαφές ότι οι είναι πιο ενημερωτικές και παρέχουν περισσότερες γνώσεις, επομένως μπορούν να αλλάξουν τη στάση και την συμπεριφορά των ανθρώπων απέναντι σε θέματα ασφάλειας.

2) Αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου

Ένας τύπος καμπάνιας για την ενημέρωση σχετικά με την ασφάλεια των πληροφοριών είναι τα μηνύματα ηλεκτρονικού ταχυδρομείου. Αυτά τα μηνύματα διαδίδουν χρήσιμες πληροφορίες σχετικά με το phishing, την κοινωνική μηχανική, τη διαχείριση password και τα περιστατικά ασφάλειας πληροφοριών. Αυτή η μέθοδος είναι αποτελεσματική στην παροχή συναφών πληροφοριών σχετικών με την ασφάλεια και ως εκ τούτου αυξάνει τη γνώση του παραλήπτη. Ωστόσο, η απλή ανάγνωση μηνυμάτων e mail δεν σημαίνει ότι το μήνυμα έχει γίνει κατανοητό και έχει αφομοιωθεί. Επομένως, αυτή η μέθοδος δεν επαρκεί για να αλλάξει η στάση του υπαλλήλου, καθώς αυτή είναι μία επικοινωνία και μπορεί να μην τραβήξει την προσοχή του

παραλήπτη. Καταλήγοντας, η χρήση μηνυμάτων προσελκύει την προσοχή αλλά δεν μπορεί να αλλάξει τη συμπεριφορά.

3) Ομαδικές συζητήσεις

Ένας τύπος ευαισθητοποίησης και μάθησης σχετικά με την ασφάλεια των πληροφοριακών συστημάτων είναι μια άτυπη συνάντηση στην οποία συμμετέχουν περίπου 15-20 άτομα ενός οργανισμού και οι συμμετέχοντες αξιοποιούν πλήρως την ανταλλαγή γνώσεων και εμπειριών (Albrechtsen and Hovden, 2010). Διαφορετικά βασικά ζητήματα ασφάλειας επιλέγονται και συζητούνται ενώ όλοι οι συμμετέχοντες έχουν ίσες ευκαιρίες να εξηγήσουν την άποψή τους. Σε αυτή την μορφή συνάντησης. οι συμμετέχοντες καλούνται να περιγράψουν τυχόν περιστατικά που συνέβησαν και εάν τα περιστατικά αυτά έχουν αναφερθεί και αναδειχθεί καθώς επίσης αναλύονται και οι τυχόν συνέπειες αυτών των περιστατικών. Αυτή η στρατηγική της συζήτησης περιστατικών, προτρέπει και παρακινεί τους συμμετέχοντες καθώς βασίζεται στη θεωρία της αιτιολογημένης δράσης, η οποία αλλάζει την πρόθεση μεταβάλλοντας τη στάση και τους κοινωνικούς κανόνες. Η ομαδική συζήτηση συμβάλλει στο να αυξήσει ο εργαζόμενος την προσοχή του σε θέματα ασφάλειας αφού τέτοιες συναντήσεις είναι περισσότερο διαδραστικού χαρακτήρα και ως εκ τούτου πιο αποτελεσματικές. Αυτή η προσέγγιση έχει αποδειχτεί πολύ χρήσιμη στην αύξηση του επιπέδου ευαισθητοποίησης με τη χρήση της γνώσης, της προσοχής, της αίσθησης, των κοινωνικών κανόνων, των κινήτρων και των στρατηγικών συμπεριφοράς. Άρα η αλληλεπίδραση αυτή επηρεάζει θετικά την κατανόηση του ατόμου για την ασφάλεια των πληροφοριών.

4) Ενημερωτικά δελτία

Τα ενημερωτικά δελτία είναι μια μηνιαία ή τριμηνιαία έκθεση που περιλαμβάνει πληροφορίες σχετικά με θέματα ασφάλειας και μπορεί να είναι σε ηλεκτρονική μορφή ή σε έντυπη μορφή. Διανέμονται μεταξύ των εργαζομένων εντός του οργανισμού και έχουν σχεδιαστεί με στόχο την αύξηση της ενημέρωσης των εργαζομένων σχετικά με την ασφάλεια. Το ενημερωτικό δελτίο ασχολείται με νέες απειλές όπως για παράδειγμα, πρόσφατα ανακαλυφθέντες ιούς, περιστατικά με τρωτά σημεία λογισμικών και χρήσιμες οδηγίες για την αντιμετώπιση τέτοιων περιστατικών. Αυτά τα ενημερωτικά δελτία είναι πολύ χρήσιμα για τη μεταφορά γνώσεων σχετικά με την ασφάλεια και αποτελεί επίσης ένα ενημερωτικό υλικό οι εργαζόμενοι μεταβάλλουν την στάση τους και ευαισθητοποιούνται περαιτέρω. Ωστόσο, οι system administrators δεν είναι σε θέση να γνωρίζουν εάν οι υπάλληλοι έχουν διαβάσει τελικά το ενημερωτικό δελτίο και έχουν καταλάβει και αφομοιώσει τα όσα αναγράφονται σε αυτό και έτσι δεν μπορεί να αλλάξει και να επηρεάσει σε μεγάλο βαθμό την πρόθεση του αναγνώστη και τη συμπεριφορά του.

5) Βιντεοπαιχνίδια

Μέσα στα εργαλεία εκπαίδευσης και μάθησης συμπεριλαμβάνονται και τα βιντεοπαιχνίδια Αυτή η τεχνική χρησιμοποιείται επίσης από ερευνητές σε άλλους τομείς όπως της υγείας και της ευαισθητοποίησης σχετικά με το περιβάλλον. Πολλοί ερευνητές ισχυρίζονται ότι το βιντεοπαιχνίδι είναι μια καλή τεχνική στην παρακίνηση του ατόμου για την προσαρμογή της επιθυμητής συμπεριφοράς, καθώς κεντρίζει την προσοχή πιο ενεργά. Μάλιστα το 2005 η Ναυτική Σχολή της Αμερικής σε συνεργασία με την Αμερικανική Κυβέρνηση, κυκλοφόρησε ένα βίντεο παιχνίδι όπου σύμφωνα με αυτό οι παίκτες κατασκευάζουν και ρυθμίζουν στον υπολογιστή, δίκτυα που είναι απαραίτητα για να μπορούν οι εικονικοί χρήστες να είναι παραγωγικοί και να επιτύχουν στόχους τους. Οι παίκτες που συμμετέχουν υπερασπίζονται τα δίκτυά τους και μπορούν να παρακολουθούν τις συνέπειες των επιλογών τους, ενώ υπόκεινται σε επίθεση από χάκερ (Benjamin D. Cone, Cynthia E. Irvine, Michael F. Thompson, Thuy D. Nguyen, 2007). Ωστόσο, αυτή η μέθοδος δεν έχει το συστατικό στοιχείο της μεταφοράς γνώσης, εκτός εάν πρόκειται για άτομο που εξειδικευμένο και με βαθιά γνώση περί ασφάλειας πληροφοριακών συστημάτων. Επιπλέον, δεν αντικατοπτρίζεται η σχετική πολιτική ασφαλείας. Συμπερασματικά, τα βιντεοπαιχνίδια είναι πιο αλληλεπιδραστικά και διατηρούν τη συμμετοχή του ατόμου παρόλα αυτά δεν είναι πολύ καλή πηγή γνώσης.

6) Εκπαίδευση με βάση υπολογιστή

Η εκπαίδευση βασισμένη στον υπολογιστή έχει πολλά πλεονεκτήματα έναντι των συμβατικών μεθόδων ενημέρωσης για την ασφάλεια των συστημάτων Το τεστ περιβάλλον είναι διαθέσιμο ανά πάσα στιγμή σε όλους τους υπαλλήλους του οργανισμού και είναι μια αποτελεσματική μέθοδος ενημέρωσης και οι εργαζόμενοι του οργανισμού μπορούν να αποκτήσουν την επιθυμητή εκπαίδευση με το δικό τους ρυθμό. Ωστόσο, το CBT (computer based training) απαιτεί περισσότερους πόρους και επιπλέον, αυτή η μέθοδος δεν έχει το πλεονέκτημα της αλληλεπίδρασης μεταξύ του εκπαιδευτή και του κοινού. Επομένως, σε αυτή τη μέθοδο λείπει ένας κοινωνικός κανόνας που είναι ένα από τα πιο χρήσιμα συστατικά του προτεινόμενου μοντέλου.

7) Σημειώματα/πόστερς

Τα σημειώματα λειτουργούν ως απλές και αποτελεσματικές υπενθυμίσεις για θέματα της ασφάλειας που προσελκύουν την προσοχή των τελικών χρηστών και υπενθυμίζουν τους βασικούς κανόνες. Απαιτούν λιγότερους πόρους ενώ τα έξυπνα σλόγκαν σχέδια συμβάλλουν σημαντικά στην αποτελεσματικότητα τους. Εκτός από το σχεδιασμό και το περιεχόμενο των

αφισών, το σημείο εντός τους οργανισμού στο οποίο εμφανίζεται το σημείωμα προσελκύει επίσης την προσοχή του θεατή. Ωστόσο, η χρήση των σημειωμάτων αυτών δεν είναι πρακτική, καθώς δεν είναι δυνατόν να εξηγηθεί κάποια απορία και ως εκ τούτου λείπει ο κοινωνικός παράγοντας της αλληλεπίδρασης. Λόγω έλλειψης της συνιστώσας των κοινωνικών προτύπων, η συμπεριφορά των εργαζομένων δεν μπορεί να αλλάξει και ως εκ τούτου παραμένει αμετάβλητη.

Συμπερασματικά, από τα παραπάνω εργαλεία και μεθόδους αυτά που έχουν την μεγαλύτερη επίδραση είναι οι ομαδικές συζητήσεις αλλά και οι εκπαιδευτικές παρουσιάσεις καθώς και στις δύο περιπτώσεις υπάρχει μεγάλη αλληλεπίδραση μεταξύ των εμπλεκόμενων μερών και έτσι η γνώση συνοδεύεται με παρακίνηση, ευαισθητοποίηση και αλλαγή συμπεριφοράς.

2.2.2 Οργανωσιακό μοντέλο

Οι σημαντικοί και σοβαροί κίνδυνοι ασφάλειας που ελλοχεύουν γενικότερα στο διαδίκτυο, κυμαίνονται όπως έχει προαναφερθεί, από την κλοπή των κωδικών πρόσβασης σε ανεπιθύμητα μηνύματα με κακόβουλο λογισμικό, σε εισβολή σε ιδιωτικό απόρρητο, σε παραβιάσεις πνευματικών δικαιωμάτων. Αυτοί οι κίνδυνοι εκτός από βλαβερές συνέπειες σε προσωπικό επίπεδο, μπορούν να προκαλέσουν και προβλήματα σε έναν οργανισμό όπως για παράδειγμα στη φήμη. Οι χρήστες με χαμηλή επίγνωση της ασφάλειας είναι συχνά απρόσεκτοι όταν χειρίζονται προσωπικές και εμπιστευτικές πληροφορίες, που περιλαμβάνουν την εμπιστευτικότητα, τη διαθεσιμότητα και την ακεραιότητα των προσωπικών πληροφοριών. Η πηγή των κινδύνων ασφαλείας μπορεί να προέλθει από το λογισμικό, το υλικό, το δίκτυο ή τις εν γένει τεχνικές δεξιότητες. Είναι επιτακτική ανάγκη μια οργάνωση ώστε να εκπαιδεύονται οι χρήστες συνειδητοποιώντας τις πηγές κινδύνου για την ασφάλεια και ταυτόχρονα να λαμβάνονται υπόψη τυχόν διορθωτικές ενέργειες εάν προκύψουν τρωτά σημεία (R.S. Shaw, Charlie C. Chen, Albert L. Harris, & Hui-Jou Huang, 2009).

Η κακή συμπεριφορά ασφαλείας πολλών χρηστών (π.χ. σφάλματα ασφαλείας χρηστών, απροσεξία και αμέλεια) έχει συμβάλλει κατά και καιρούς σε πολλές και καίριες παραβιάσεις της ασφάλειας των συστημάτων. Γι αυτό ένας αυξημένος αρκετά μεγάλος αριθμός οργανισμών αναγνωρίζει τη σημασία της ύπαρξης ενός προγράμματος εκπαίδευσης επάνω στα θέματα της ασφάλειας. Για να επιτευχθεί με επιτυχία ένα τέτοιο πρόγραμμα πρέπει να διασφαλιστεί ότι οι εργαζόμενοι επιτυγχάνουν τρία επίπεδα συνειδητοποίησης των κινδύνων : αντίληψη, κατανόηση και προβολή. Όσοι περισσότεροι εργαζόμενοι προχωρούν σε αυτά τα τρία επίπεδα τόσο η συμπεριφορά και η κουλτούρα των ανθρώπων αλλάζει με στόχο την ασφάλεια. Είναι απαραίτητο ωστόσο, να υπάρχει μια πιο συνεπής μεθοδολογία για την προσαρμογή ενός

προγράμματος εκπαίδευσης και εξοικείωσης με βάση τα επίπεδα συνειδητοποίησης της ασφάλειας (R.S. Shaw, Charlie C. Chen, Albert L. Harris, & Hui-Jou Huang, 2009):

1) Αντίληψη :

Το πρώτο βήμα για την εξασφάλιση ενός οργανισμού είναι να αντιληφθεί και να ανιχνεύσει πιθανούς κινδύνους ασφαλείας του επιχειρηματικού του περιβάλλοντος. Η αντίληψη θεωρείται η επίτευξη της κατανόησης για την παρουσία ή την επίγνωση μιας απειλής. Άρα οι πιθανότητες διαμόρφωσης μιας σωστή εικόνας και ορθής σκιαγράφησης των απειλών μπορεί να ενισχυθούν σε μεγάλο βαθμό με τη βελτίωση της αντίληψης αναφορικά με την ευαισθητοποίηση και επίγνωση της ασφάλειας. Για παράδειγμα, διεθνής εταιρεία υιοθέτησε την προσέγγιση αυτή και σταδιακά δρομολόγησε ένα online και offline πρόγραμμα εκπαίδευσης. Το αποτέλεσμα ήταν να ενισχύσουν με επιτυχία την αντίληψη σε περισσότερους από 100.000 υπαλλήλους σε 100 χώρες.

2) Κατανόηση

Η αντίληψη περί παρουσίας των κινδύνων είναι ανεπαρκής για την αντιμετώπιση τους εάν οι ίδιοι οι χρήστες δεν τους κατανοούν και δεν τους αξιολογούν. Η έμφαση στην κατάρτιση ενός προγράμματος εκπαίδευσης είναι να διασφαλιστεί ότι οι χρήστες γνωρίζουν πώς να ενσωματώσουν πληροφορίες από πολλές προερχόμενες πηγές και να τις ερμηνεύουν προς τη σωστή κατεύθυνση. Το πιο σημαντικό είναι ότι οι χρήστες πρέπει να έχουν τη δυνατότητα επικοινωνίας και διάδοσης της πληροφορίας διότι έτσι συμβάλλουν καθοριστικά στην καταπολέμηση περαιτέρω κινδύνων ασφαλείας στο εργασιακό περιβάλλον.

3) Προβολή

Για να αποφευχθεί η εμφάνιση δυνητικών κινδύνων, οι τελικοί χρήστες πρέπει να έχουν τη δυνατότητα να προβάλλουν ή να προβλέπουν το μελλοντικές επιθέσεις ασφαλείας. Η προβολή είναι το τρίτο επίπεδο της εκπαίδευσης αναφορικά με την βελτίωση και την ευαισθητοποίηση σχετικά με την ασφάλεια. Η ικανότητα πρόβλεψης μελλοντικών καταστάσεων, δεικνύει ότι οι χρήστες έχουν υψηλό επίπεδο κατανόησης του εργασιακού περιβάλλοντός τους και την ανάλογη ευθύνη . Ο απώτερος στόχος ενός αποτελεσματικού προγράμματος εκπαίδευσης είναι να προετοιμάσει τους χρήστες με την ικανότητα προβολής πιθανών κινδύνων ασφαλείας.

2.2.3 Θεωρητικό μοντέλο

Μια από τις απαιτήσεις των εκπαιδευτικών προγραμμάτων για την ασφάλεια, είναι ότι παρέχουν μια θεωρητική εξήγηση για το πώς και γιατί λειτουργεί το πρόγραμμα και ποιά είναι τα οφέλη που αποκομίζει ένας χρήστης. Αυτό σημαίνει ότι το πρόγραμμα κατάρτισης πρέπει να παρέχει

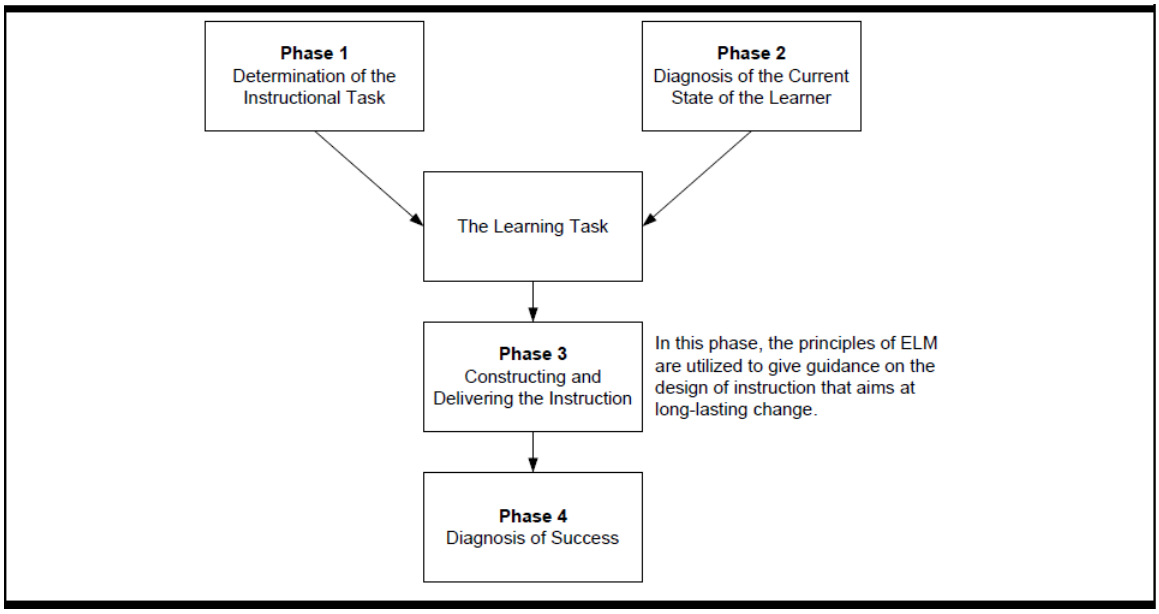
τις απαραίτητες πληροφορίες στους εισηγητές, ώστε να γνωρίζουν σε θεωρητικό επίπεδο το πώς το συγκεκριμένο πρόγραμμα βοηθά τους ανθρώπους να κατανοήσουν και να αφομοιώσουν τα νευραλγικά θέματα της ασφάλειας. Βέβαια, οι υποκείμενες θεωρίες πρέπει να μαθαίνουν και ποιες αρχές μάθησης αναμένεται να αλλάξουν τη συμμόρφωση των χρηστών. Ως δεύτερη προϋπόθεση, η βασική θεωρία θα πρέπει να παρέχει κατευθυντήριες γραμμές και για τις πρακτικές οδηγίες για την εφαρμογή αποτελεσματικής κατάρτισης. Από τις πιθανές θεωρίες, το μοντέλο πιθανότητας επεξεργασίας (Elaboration Likelihood Model / ELM) εξηγεί πόσο οι προβλέψιμες και μακροχρόνιες αλλαγές συμπεριφοράς μπορούν να επιτευχθούν μέσω της γνωστικής επεξεργασίας. Την ίδια στιγμή, επισημαίνει ότι οι αλλαγές μικρής διάρκειας μπορούν να αποφευχθούν από το γεγονός ότι δεν είναι βασιζόμενες σε συμβουλές. Κατά συνέπεια, το ELM βοηθά τους επαγγελματίες να κατανοήσουν πώς και γιατί η εκπαίδευση αναμένεται να λειτουργήσει. Η θεωρία του σχεδιασμού – η καθολική εποικοδομητική διδασκαλία Θεωρία (universal constructive instructional theory / UCIT) – δίδει το πλαίσιο για το σχεδιασμό διδασκαλίας που είναι προσαρμοσμένο για ένα ορισμένο μαθησιακό αντικείμενο (π.χ. συμμόρφωση με την πολιτική ηλεκτρονικού ταχυδρομείου). Οι δύο αυτές θεωρίες (UCIT και η ELM) αλληλοσυμπληρώνονται (Petri Puhakainen, Mikko Siponen, 2010)

1) Elaboration Likelihood Model (ELM)

Η συμμόρφωση και η εκπαίδευση του προσωπικού σε θέματα που αφορούν την ασφάλεια και την πολιτική αυτής, θα πρέπει να ακολουθούν τέτοιες εκπαιδευτικές μεθόδους και πρακτικές ώστε να επιτρέπει την επεξεργασία της πληροφορίας που λαμβάνεται σε γνωστικό επίπεδο και το είδος του κινήτρου αποτελεί απαραίτητη προϋπόθεση για τη γνωστική επεξεργασία. Με αυτόν τον τρόπο ο παραλήπτης είναι πιθανό να χρησιμοποιήσει τη γνωστική επεξεργασία, ενώ το χαμηλό κίνητρο θα επιφέρει αντίθετα αποτελέσματα. Κατά συνέπεια, όταν το στόχος της διδασκαλίας είναι να παρακινήσει την γνωστική και εμπειρική επεξεργασία της πληροφορίας, η συμμόρφωση με την πολιτική ασφαλείας η κατάρτιση θα πρέπει να στοχεύει σε μαθησιακά οφέλη που ένα είναι εξατομικευμένα.

2) Universal Constructive Instructional Theory (UCIT)

Το UCIT καθοδηγεί τη διαδικασία σχεδιασμού της εκπαίδευσης μέσω των παρακάτω τεσσάρων φάσεων: (α) προσδιορισμός του διδακτικού έργου, (β) διάγνωση της τρέχουσας κατάστασης του μαθητευόμενου, (γ) κατάρτιση και παροχή διδασκαλίας, και (δ) διάγνωση επιτυχίας (Σχήμα 1).



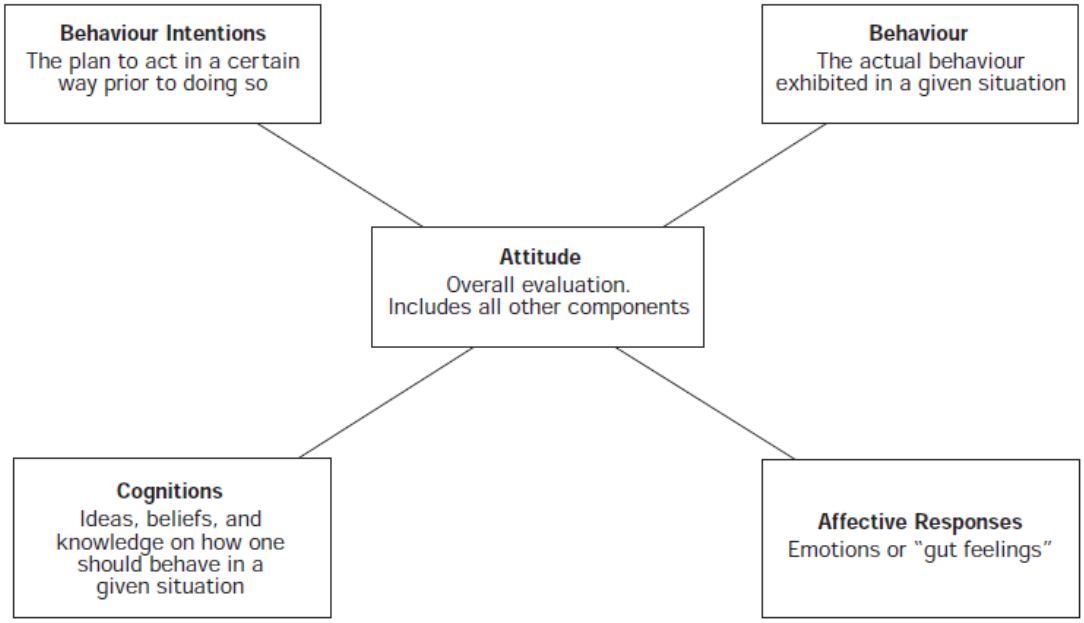
Σχήμα 1

Στη φάση (α) το εκπαιδευτικό καθήκον σχετίζεται με τη συμμόρφωση των χρηστών στις Πολιτικές ασφαλείας ενώ στη φάση (β), διερευνάται η τρέχουσα κατάσταση των εκπαιδευομένων σε σχέση με το εκπαιδευτικό πρόγραμμα. Δηλαδή ορισμένες από τις γνώσεις που απαιτούνται για τη συμμόρφωση με τις πολιτικές ασφάλειας ήδη γνωστές από τους χρήστες αλλά ορισμένες δεν έχουν ακόμη μαθευτεί και διδαχτεί. Η διαφορά μεταξύ των γνώσεων που απαιτούνται για τη συμμόρφωση και οι τρέχουσες γνώσεις των χρηστών ορίζουν τι πρέπει ακόμα οι χρήστες να διδαχτούν. Αυτή η διαδικασία ονομάζεται μαθησιακή εργασία. Στην τρίτη φάση ο στόχος είναι να βρεθούν βασικά ζητήματα για τον αποτελεσματικό σχεδιασμό της εκπαίδευσης (δηλαδή, προσαρμοσμένη ώστε να ταιριάζει με την οργάνωση και τις όποιες ειδικές ανάγκες). Ο εκπαιδευτής πρέπει να εξετάσει μόνο αυτές τις πτυχές στοχευμένα σύμφωνα με τις ανάγκες του target group. Το ELM χρησιμοποιείται στο τρίτο στάδιο του UCIT όπου οι αρχές της θεωρίας αυτής δίνουν την κατευθυντήρια γραμμή και τις οδηγίες για μια αλλαγή μεγάλης διάρκειας.. Στην τέταρτη φάση, η διάγνωση της επιτυχίας της διδασκαλίας επαληθεύεται από τον βαθμό συμμόρφωσης των χρηστών στην πολιτική ασφαλείας.

2.2.4 Ψυχολογικό μοντέλο – Κοινωνική ψυχολογία

Η κοινωνική ψυχολογία στην πραγματικότητα αφορά στην στάση που έχουν γενικά οι άνθρωποι απέναντι σε καταστάσεις της καθημερινότητας. Ο κλάδος της κοινωνικής ψυχολογίας έχει διεξάγει ανάλογες έρευνες σύμφωνα με την οποία εξετάζει την επιτυχή αλλαγή της στάσης των ανθρώπων και τα αποτελέσματα αυτής σε σχέση με την ευαισθητοποίησης και εκπαίδευση σε

θέματα ασφάλειας συστημάτων εντός ενός οργανισμού. Το παρακάτω σχήμα παρουσιάζει μια τυπική στάση των ανθρώπων και τον τρόπο συμπεριφοράς όπου όλες οι εκφάνσεις της είναι αλληλένδετες με τις πτυχές των ίδιων των συστατικών μερών της (M.E. Thomson, R. von Solms, 2009) όπως απεικονίζεται στο σχήμα 2 :



Σχήμα 2

Στο επίκεντρο όλων είναι η πραγματική στάση με όλα τα συστατικά της όπως για παράδειγμα οι προθέσεις, η γνώση, τα συναισθήματα. Σύμφωνα με τους M.E. Thomson, R. von Solms, έρευνες της κοινωνικής ψυχολογίας έχουν δείξει ότι υπάρχουν μέθοδοι που μπορούν να εφαρμοστούν και να αλλάξουν στην στάση του ατόμου και απατώνται στις επόμενες τρεις κατηγορίες :

- Άμεση αλλαγή συμπεριφοράς αγνοώντας στάσεις και γνώσεις
- Χρησιμοποίηση μια γενικότερης αλλαγής ώστε να επηρεάσει την στάση του ατόμου
- Αλλαγή στάσης ατόμου με την πειθώ.

1. Άμεση αλλαγή συμπεριφοράς αγνοώντας στάσεις και γνώσεις

Έχει αποδειχθεί ότι υπάρχουν τεχνικές που μπορούν να χρησιμοποιηθούν για να πείσουν ένα άτομο να συμπεριφέρονται με κάποιο τρόπο, ανεξάρτητα από το δική τους τη στάση απέναντι στο ίδιο θέμα. Αυτό μπορεί να συμβεί με τους εξής τρόπους :

- *Εκπαιδευτική οργάνωση* : Υπάρχουν δύο τεχνικές που εμπίπτουν σε αυτή την κατηγορία και είναι η μάθηση και η διαμόρφωση των χρηστών των συστημάτων και εργαζομένων.

Η μάθηση αναφέρεται σε μια κατάσταση όπου υπάρχει σχέση μεταξύ της ανταπόκρισης σε ένα ζήτημα και τις συνέπειές της. Αν η συμπεριφορά του ατόμου είναι η ενδεδειγμένη, τότε πρέπει να επαινείται ο εργαζόμενος διαφορετικά να επιπλήττεται. Η διαμόρφωση αναφέρεται σε μια κατάσταση όπου τα αρχικά πρότυπα είναι χαμηλά, και όσο το άτομο και οι ικανότητές του βελτιώνονται τότε επέρχεται και η σχετική ανταμοιβή.

- *Κοινωνική μάθηση* : αναφέρεται στην συμπεριφορά των ανθρώπων που επηρεάζεται ανεξάρτητα από το αν έχουν συμμετοχή στην όλη εκπαιδευτική διαδικασία. Δηλαδή βλέπουν το πώς ανταμείβονται οι συνάδελφοί τους και τείνουν να συμπεριφέρονται με τον ίδιο τρόπο ώστε να απολαύσουν την ίδια αποδοχή.
- *Συμμόρφωση* : αναφέρεται στην συμμόρφωση ενός μεμονωμένου ατόμου στις νόρμες και τις λογικές μιας ομάδας. Άρα προσαρμόζουν τις ιδέες και τις πεποιθήσεις τους στη φόρμα της ομάδας.
- *Υπακοή* : είναι ένας ιδιαίτερος τρόπος για άμεση αλλαγή της συμπεριφοράς καθώς το άτομο ή ο εργαζόμενος καλείται να «υπακούσει» σε μιαν αρχή ή σε εντολές που κάλλιστα θα μπορούσαν να απορρίψουν λόγω θέσης ή εμπειρίας
- *Αμοιβαιότητα* : αναφέρεται στην κατάσταση όπου ένα άτομο επιστρέφει κατά κάποιο τρόπο μια χάρη σε έναν συνάδελφο ή ακόμα και όταν αυτή η χάρη έγινε προκειμένου να κερδίσει την αντίστοιχη εύνοια σε μεταγενέστερο χρόνο.
- *Δέσμευση* : αναφέρεται στην δέσμευση ότι ο εκπαιδευόμενος στο πρόγραμμα περί ασφάλειας, θα ακολουθήσει τα όσα διδάχθηκε.

2. Χρησιμοποίηση μια γενικότερης αλλαγής ώστε να επηρεάσει την στάση του ατόμου

Σε αυτό το κομμάτι συναντάμε τους τρόπους με τους οποίους μια αλλαγή στην συμπεριφορά οδηγεί σε αλλαγή της στάσης που είναι πιθανό να οδηγήσει με τη σειρά της σε μια πιο μακροπρόθεσμη αλλαγή και τροποποίηση της συμπεριφοράς :

- *Απόδοση* : αναφέρεται στην ανάγκη του ατόμου να αποδώσει με έναν συγκεκριμένο τρόπο συμπεριφοράς για κάποιον συγκεκριμένο λόγο και σκοπό. Αν δλδ πρόκειται να έχει κέρδος ή να προαχθεί τότε αποδίδει αναλόγως.
- *Αυτοπεποίθηση* : αναφέρεται κυρίως στα παιχνίδια ρόλων στα εκπαιδευτικά προγράμματα για ασφάλεια των πληροφοριακών συστημάτων όπου κάποιος συμμετέχοντας παίζει κάποιον ρόλο με διαφορετική οπτική γωνία στα θέματα της

ασφάλειας αλλά στην πραγματικότητα υποστηρίζει τον ρόλο αυτό που στο τέλος ωθούν τους υπόλοιπους να αλλάξουν την συμπεριφορά τους.

- *Διαφωνία* : αναφέρεται στην ασυνέπεια που δύναται να εμφανίσει ένας χρήστης ανάμεσα στις πεποιθήσεις ή τις στάσεις του σε σχέση με την πραγματική συμπεριφορά.

3. Αλλαγή στάσης ατόμου με την πειθώ.

Για την αλλαγή στάσης του ατόμου με πειθώ απαιτούνται τα κάτωθι σημεία :

- *Έκθεση* : αναφέρεται στην κατάσταση που κάποιος εκτίθεται σε μια πληροφορία χωρίς απαραίτητα να ακούσουν τον πραγματικό σκοπό της πληροφορίας. Πχ όταν ένας εργαζόμενος βρίσκεται σε ένα σεμινάριο περί ασφάλειας και παρόλο που δεν είναι συγκεντρωμένος σ' αυτό, βρίσκεται εκτεθειμένος στην πληροφορία.
- *Προσοχή* : αναφέρεται στην κατάσταση όπου ένας εργαζόμενος δίνει την απαραίτητη προσοχή στην πληροφορία που υποστηρίζει την συγκεκριμένη στάση και συμπεριφορά.
- *Κατανόηση* : αναφέρεται στην κατάσταση όπου η προσοχή και η έκθεση στην πληροφορία δεν έχουν αντίκτυπο εάν και εφόσον δεν κατανοούνται.
- *Αποδοχή* : αναφέρεται στην κατάσταση όπου μπορεί κάποιος να έχει κερδίσει την προσοχή ενός συμμετέχοντα στο σεμινάριο αλλά και να έχει κατανοήσει την πληροφορία αλλά πρέπει να την αποδεχτεί ώστε να έχει πραγματικό αντίκτυπο και να οδηγήσει σε αλλαγή στάσης και συμπεριφοράς.
- *Διατήρηση* : αναφέρεται στην κατάσταση όπου η αλλαγή στάσης και συμπεριφοράς δεν έχει προσωρινό χαρακτήρα αλλά διατηρείται και μακροπρόθεσμα.

Συμπερασματικά, τα εκπαιδευτικά προγράμματα για την ασφάλεια πρέπει να εφαρμόζονται σε όλους τους οργανισμούς είτε να επεκτείνονται ενώ οι αρχές της κοινωνικής ψυχολογίας όπως αναφέρθηκαν πρέπει να υπεισέλθουν για την βελτίωση των προγραμμάτων αυτών. Ωστόσο, πρέπει να τονίσουμε ότι η εκπαίδευση πρέπει να απευθύνεται από την ανώτατη διοίκηση, στο προσωπικό πληροφορικής έως τον τελικό χρήστη και να μην εστιάζει μόνο στον τελικό χρήστη.

2.3 Σύνοψη

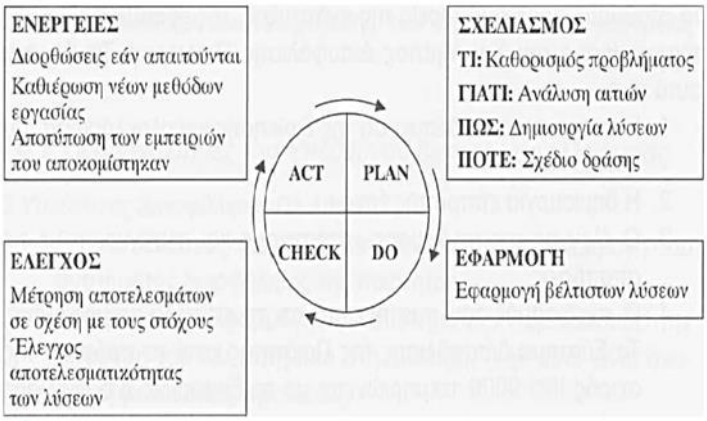
Όλα τα παραπάνω προγράμματα και οι τεχνικές εκπαίδευσης του προσωπικού, στοχεύουν σε πολύ συγκεκριμένες κατευθύνσεις. Συγκεκριμένα, το επιθυμητό αποτέλεσμα και η λογική μέσα από την διαδικασία αυτή είναι η προώθηση μιας κουλτούρας ασφάλειας μεταξύ όλων των

συμμετεχόντων ως μέσου προστασίας των συστημάτων πληροφορικής και των ηλεκτρονικών πλατφορμών όπως το e banking. Πέραν τούτου βασικοί άξονες είναι οι εξής (OECD, 2002) :

- Να αυξηθεί η ευαισθητοποίηση σχετικά με τους κινδύνους για τα συστήματα πληροφοριών και δικτύων · τις πολιτικές, τις πρακτικές, τα μέτρα και τις διαδικασίες.
- Την καλλιέργεια περισσότερης εμπιστοσύνης και άνεσης σε σχέση με την ασφαλή χρησιμοποίηση των συστημάτων και των δικτύων.
- Δημιουργία ενός γενικού πλαισίου αναφοράς που θα βοηθήσει τους εργαζόμενους να κατανοήσουν θέματα ασφάλειας και να σέβονται τις ηθικές αξίες στην ανάπτυξη και εφαρμογή πολιτικών, πρακτικών, μέτρων και διαδικασιών.
- Προώθηση της συνεργασίας και της ανταλλαγής πληροφοριών, ανάλογα με την περίπτωση, μεταξύ όλων των εργαζομένων αναφορικά με την ανάπτυξη και εφαρμογή των πολιτικών ασφαλείας, πρακτικών, μέτρων και διαδικασιών.
- Συνειδητοποίηση ότι η ασφάλεια αποτελεί σημαντικού στόχο και απώτερος σκοπός είναι δημιουργία και ανάπτυξη προτύπων.

Γίνεται λοιπόν αντιληπτό ότι ο λειτουργικός κίνδυνος που αντιμετωπίζουν οι Τράπεζες είναι αρκετά υψηλός καθώς εκτός από την ασφαλή λειτουργία του e banking και την αντιμετώπιση εξωτερικών απειλών, δεν θα πρέπει να παραβλεφθεί και ο κίνδυνος που προέρχεται εκ των έσω. Η πράξη έχει δείξει ότι τα προβλήματα που δημιουργούνται από αμελείς εργαζόμενους είναι πιο σημαντικά και πιθανόν και πιο συχνά σε εμφάνιση. Το σίγουρο είναι ότι προκύπτουν αρνητικά γεγονότα αναφορικά με την φήμη της Τράπεζας, νομικά θέματα σε ό,τι αφορά την προστασία των προσωπικών δεδομένων αλλά και την ίδια την περιουσία της Τράπεζας. Χαμένες εργατοώρες και αύξηση του κόστους χρημάτων που δαπανώνται προκειμένου να διορθωθούν τα προβλήματα που δημιουργούνται από τα λάθη των εργαζομένων, είναι γεγονότα που προκαλούν δυσάρεστες για τον οργανισμό καταστάσεις. Πρέπει να αναλογιστούμε ότι κάθε λάθος του εργαζομένου που οδηγεί στην πρόκληση κάποιου προβλήματος για να μπορέσει να διορθωθεί προϋποθέτει τις εξής ενέργειες :

- Στην περίπτωση που η εφαρμογή είναι in house τότε απαιτείται εντοπισμός του προβλήματος, ανάλυση, νέες προδιαγραφές, έλεγχος και δράσεις για διορθωτικές ενέργειες. Αυτό μπορεί να περιγραφεί και από τον κύκλο του Deming (Βασίλης Ν. Κέφης, 2014 ; J. Bank, 2000) όπου σχηματικά απεικονίζεται και κατωτέρω στο σχήμα 3 :



Σχήμα 3

Το πρώτο στάδιο του κύκλου αφορά τον Σχεδιασμό / Plan. Στην πραγματικότητα σε αυτό το σημείο πραγματοποιείται ο καθορισμός του προβλήματος, η ανάλυση των αιτιών, πώς μπορώ να λύσω το πρόβλημα και ποιο είναι το σχέδιο δράσης. Αφού έχουν συλλεχθεί τα απαραίτητα δεδομένα, ο κύκλος προχωρά στον επόμενο στάδιο που είναι η πράξη / εφαρμογή / Do του σχεδίου που ήδη έχει σχεδιαστεί. Ωστόσο, για να μπορέσω να προχωρήσω στο επόμενο βήμα, οφείλω να συγκρίνω τα δύο πρώτα στάδια ώστε να καταγράψω και να αποτυπώσω τι είναι αυτό που τελικά σχεδιάστηκε σαν απόδοση λύσης και τι πραγματικά εφαρμόστηκε στην πράξη. Αφού λοιπόν παρακολουθείται η απόδοση και βρίσκονται οι βέλτιστες λύσεις, το επόμενο στάδιο είναι αυτό του ελέγχου (Check) όπου στην πραγματικότητα καταγράφονται και μετριούνται τα αποτελέσματα σε συγκεκριμένη κλίμακα ώστε να προκύψει και η σχετική τους αποτελεσματικότητα. Τέλος, ακολουθούν οι διορθωτικές ενέργειες (Act) όπου με γνώμονα τα σχετικά ευρήματα της ροής, την γνώση που αποκομίστηκε σχεδιάζονται και προωθούνται οι διορθωτικές ενέργειες εφόσον τα αποτελέσματα δεν είναι ικανοποιητικά. Άρα στην ουσία καταρτίζεται νέο πλάνο έχοντας λάβει υπόψη όλα τα προηγούμενα αποτελέσματα, τις αιτίες κλπ. Αρά καταλαβαίνουμε πόσες εργατοώρες χάνονται απ' όλη αυτή την διαδικασία και τι λειτουργικό κόστος επιφέρει στην Τράπεζα.

- Στην περίπτωση που η εφαρμογή είναι από εξωτερικό προμηθευτή τότε απαιτείται να γνωστοποιηθεί το πρόβλημα στον προμηθευτή. Να ακολουθήσει το «νεκρό» χρονικό διάστημα όπου ο προμηθευτής θα προβεί στην ανάλυση του προβλήματος και σε ποιες διορθωτικές ενέργειες (πιθανόν όπως και στην ανωτέρω περιγραφόμενη διαδικασία). Εννοείται ότι δίνεται και ο χρονικός ορίζοντας υλοποίησης της διόρθωσης. Άρα εδώ θα πρέπει να συνεκτιμήσουμε τους διαθέσιμους χρηματικούς πόρους που θα πρέπει να σπαταληθούν προς τον προμηθευτή αλλά και το «νεκρό» χρονικό διάστημα που το πρόβλημα παραμένει και τους κινδύνους που δύναται να ακολουθήσουν σε ένα τρωτό περιβάλλον.

Επομένως, η επιμόρφωση, η ευαισθητοποίηση και η εκπαίδευση του προσωπικού γίνεται πιο επιτακτική από ποτέ.

Κεφάλαιο 3

Εμπειρική Έρευνα

Στο παρόν κεφάλαιο θα αναπτυχθεί η εμπειρική έρευνα που διεξήχθη, προκειμένου να αναδειχτεί η ανάγκη εκπαίδευσης του προσωπικού των Τραπεζών σε θέματα ασφάλειας.

3.1 Στόχοι Έρευνας

Η εμπειρική έρευνα της συγκεκριμένης διατριβής βασίστηκε κυρίως στο γεγονός ότι η ασφάλεια και η εκπαίδευση που πρέπει να λαμβάνει το προσωπικό δεν πρέπει να αντιμετωπίζεται ως κάτι απτό, συγκεκριμένο και δεδομένο. Αλλά θα πρέπει να αντιμετωπίζεται ως θέμα στρατηγικής σημασίας καθώς διακυβεύονται συμφέροντα της Τράπεζας τα οποία σε καμία περίπτωση δεν πρέπει να απεμπολούνται. Στόχοι λοιπόν είναι να αναδειχθεί το επίπεδο εκπαίδευσης των εργαζομένων σε ό,τι αφορά θέματα ασφάλειας και μέσω αυτού να αποδειχτεί ότι είναι καίριας σημασίας η συνεχής ενημέρωση των εργαζομένων. Οι κίνδυνοι δεν είναι στατικοί αλλά δυναμικοί και αυξάνονται ολοένα. Επιπροσθέτως, εκτός από τους κινδύνους των κακόβουλων λογισμικών, η ημιμάθεια των ίδιων των εργαζομένων αποτελεί σοβαρό κίνδυνο για την ίδια την Τράπεζα

3.2 Μεθοδολογία

Η ποιοτική προσέγγιση που επιλέχθηκε για την διεξαγωγή της έρευνας είναι η συνέντευξη εργαζομένων καθώς ένα απλό κλειστό ερωτηματολόγιο πιθανόν να οδηγήσει την κρίση του ερωτώμενου σε μια συγκεκριμένη απάντηση. Αντίθετα η συνέντευξη έχει την λογική της διαλεκτικής μεθόδου όπως ακριβώς την ανέπτυξε ο αρχαίος Έλληνας φιλόσοφος Πλάτων. Το νόημα της διαλεκτικής αναφέρεται ειδικότερα στη λογική αμφισβήτηση δηλαδή στην αρχική τέχνη του «διαλέγεσθαι» με ερωτήσεις και στη συνέχεια αποκρίσεις. Κατά αυτόν τον τρόπο καταφέρνουμε να συλλέγουμε όσο τον δυνατόν περισσότερο στοιχεία τα οποία κατά την διαδικασία υποβολής των ερωτήσεων με λογική αλληλουχία, ο ερωτώμενος να δίδει μια σειρά από αυθόρμητες απαντήσεις. Με τον όρο συνέντευξη εννοούμε την διαδικασία κατά την οποία

ένας άνθρωπος με συγκεκριμένη ιδιότητα θέτει ερωτήσεις προφορικά σε κάποιον για να μάθει την άποψή του για διάφορα θέματα, να μάθει προσωπικές πληροφορίες, κλπ., και οι απαντήσεις γνωστοποιούνται σε ευρύτερο κοινό.

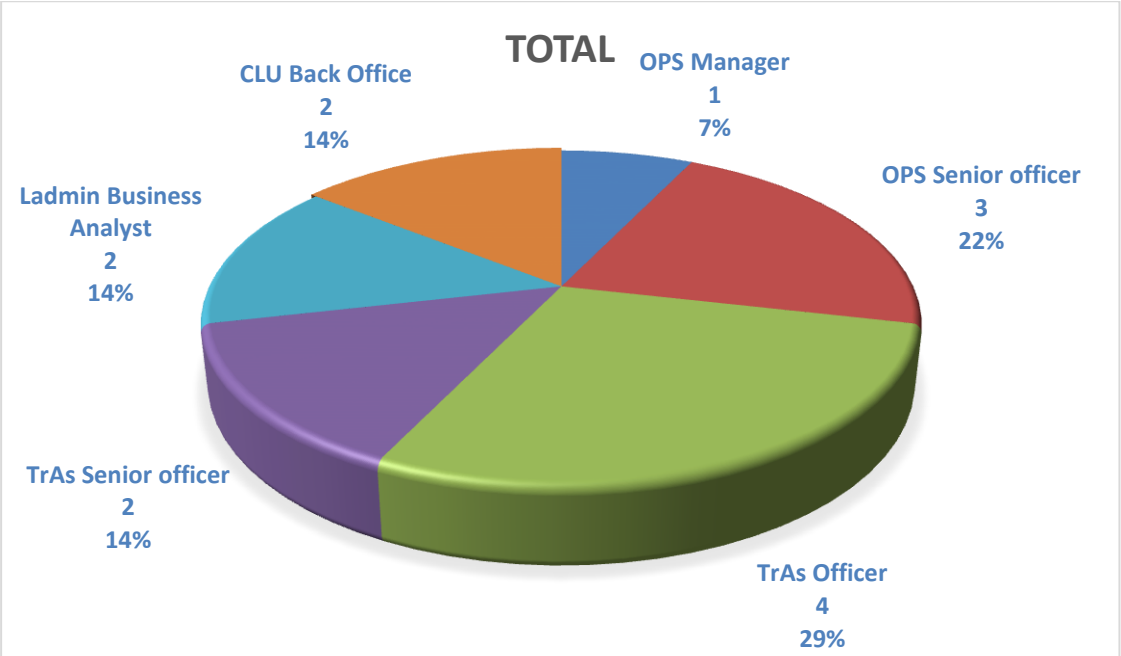
Σύμφωνα με τους HJ Rubin, IS Rubin, 2011, όρισαν τις συνεντεύξεις ως, κάθε λεκτική επιβεβαίωση ή την αποφυγή της παρατήρησης ή τυχόν επίσημων, ανεπίσημων ή ανεπιθύμητων απαντήσεων σε σχετικές ερωτήσεις. Οι συνεντεύξεις έλαβαν χώρα ως κύριο εργαλείο για τη συλλογή δεδομένων, όπως αυτές να παρέχουν σε βάθος πληροφορίες σχετικά με ένα συγκεκριμένο ερευνητικό ζήτημα ή ερώτηση. Ο αριθμός των ερωτηθέντων ήταν 14 για την συγκεκριμένη έρευνα και έγινε σε διάστημα ενός μηνός ενώ οι ερωτήσεις ήταν 10 (όπου μαζί με τα υποερωτήματα ανάλογα με την απάντηση έφταναν στις 12, παρατίθενται αναλυτικά στο σχετικό παράρτημα Α). Οι συνεντεύξεις έλαβαν χώρα περίπου στα μέσα Νοεμβρίου 2017. Με δύο από τους ερωτώμενους η συνέντευξη έγινε τηλεφωνικά καθώς η πρόσβαση δεν ήταν εύκολη, τηρώντας όμως κάθε προβλεπόμενη διαδικασία. Άλλωστε σύμφωνα με σχετική έρευνα των Nicol Korner-Bitenski, Sharon Wood-Dauphinee, Stanley Shapiro, Rubin Becker, 1994, η δυναμική της τηλεφωνικής συνέντευξης είναι η ίδια όπως και της προφορικής. Οι υπόλοιπες έγιναν face to face σύμφωνα με τις απαραίτητες συμφωνίες και επίσημες διαδικασίες.

Οι ερωτηθέντες κυμαίνονταν από Managers, Senior officers, Officers, Business Analysts και Back Office από τέσσερις διαφορετικούς τομείς ήτοι Consumer Lending Unit (εφεξής CLU), Loan Administration (εφεξής LAdmin), Operations (εφεξής OPS), Trouble Assets (εφεξής TrAs), . Ο πίνακας 1 παρουσιάζει μια συνοπτική κατανομή των συνεντευξιαζόμενων ανά Τομέα εργασίας και θέση στον Οργανισμό :

Sector	Respondent position in the Bank	# interviewees
OPS	Manager	1
	Senior officer	3
TrAs	Officer	4
	Senior officer	2
Ladmin	Business Analyst	2
CLU	Back Office	2
Grand Total		**14**

Πίνακας 1.

Ενώ σε επίπεδο ποσοστού μπορεί να αναλυθεί ως κάτωθι διάγραμμα 1 :



Διάγραμμα 1

3.3 Αποτελέσματα έρευνας και ανάλυση

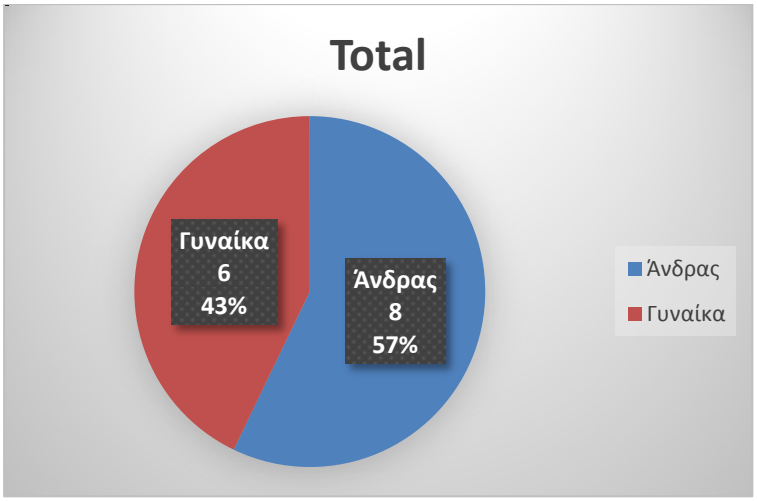
Η παρούσα ενότητα παρουσιάζει αναλυτικά την σχετική ανάλυση των στοιχείων που λήφθηκαν κατά την διάρκεια της συνέντευξης.

3.3.1 Δημογραφικά στοιχεία

Όλοι οι συμμετέχοντες έχουν διατηρήσει την ανωνυμία τους καθόλη την διάρκεια των συνεντεύξεων καθώς στα ερωτηματολόγια δεν είναι απαιτούμενο να συμπληρωθεί το ονοματεπώνυμο. Από τον τομέα CLU επιλέχθηκαν τυχαία δύο εργαζόμενοι έχοντας την ίδια θέση στο οργανόγραμμα ήτοι Back office. Από τον τομέα του OPS επιλέχθηκαν τυχαία 4 εργαζόμενοι εκ των οποίων ένας Manager και τρεις Senior Officer. Από τον τομέα TrAs επιλέχθηκαν 6 άτομα εκ των οποίων οι τέσσερις είναι officers ενώ οι δύο είναι Senior officers. Τέλος, από τον τομέα LAdmin επιλέχτηκαν 2 άτομα τα οποία κατέχουν τη θέση του Business Analyst.

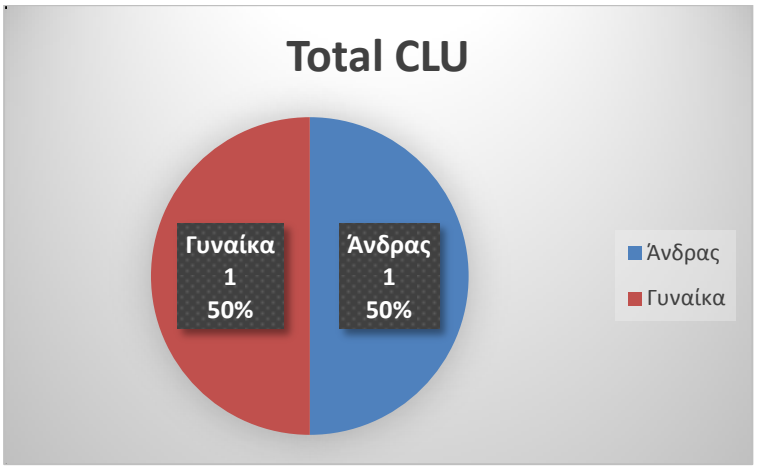
Ακολουθούν σχετικά γραφήματα ανάλογα με το φύλο, την ηλικία και τις σπουδές :

Διάγραμμα 2 : Σύνολο ερωτηθέντων σύμφωνα με το φύλο τους

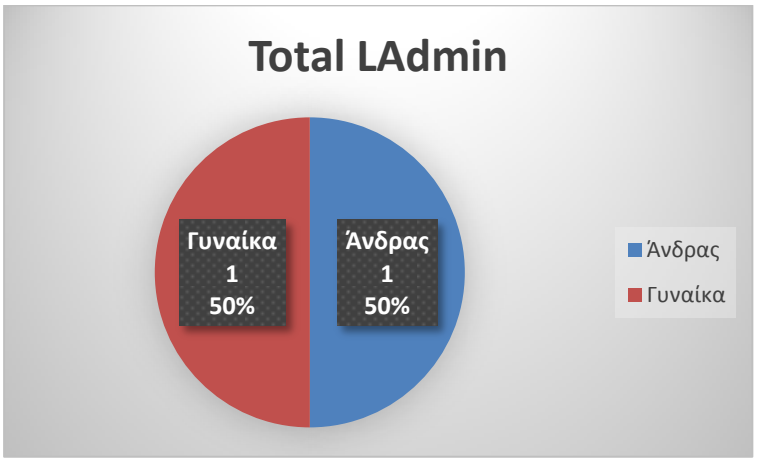


Διάγραμμα 2

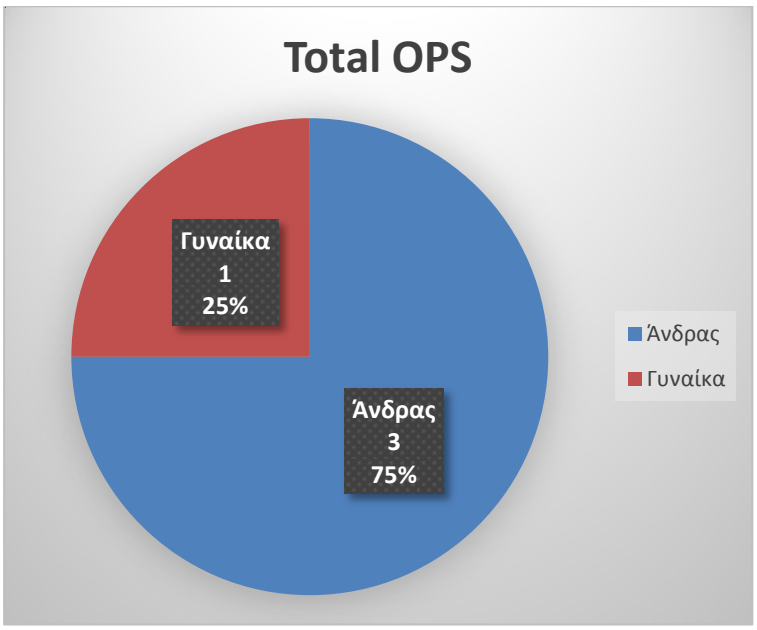
Διαγράμματα 3, 4, 5, 6 : Φύλο ανά τομέα εργασίας



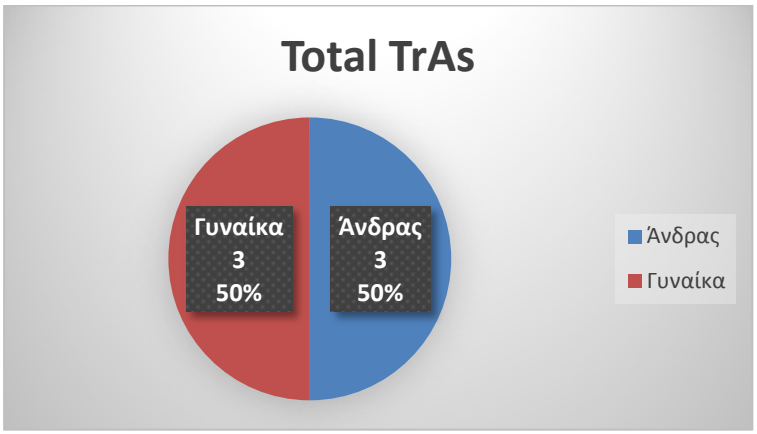
Διάγραμμα 3



Διάγραμμα 4



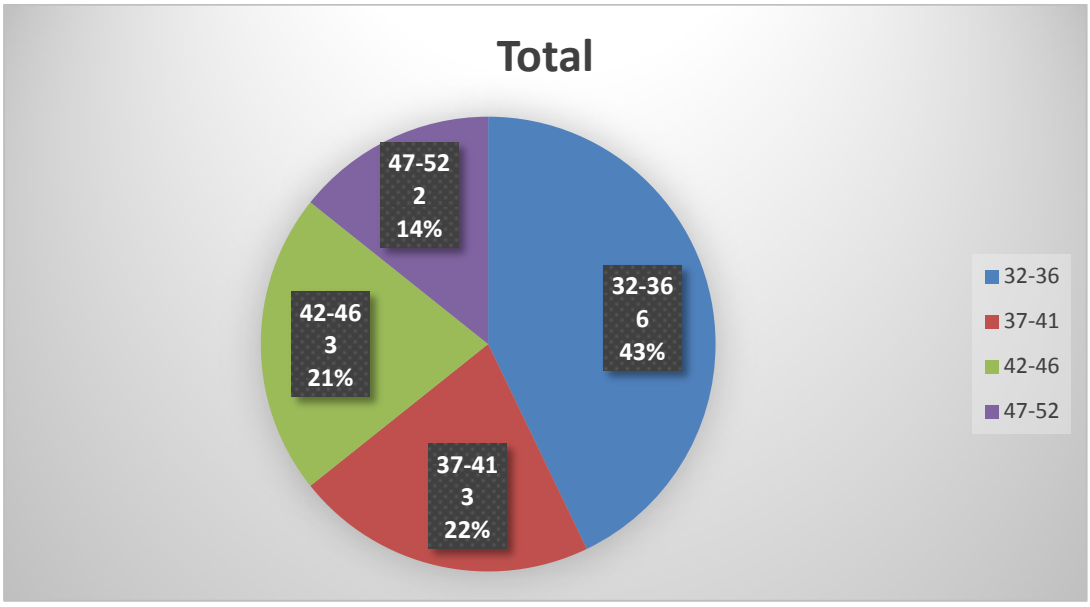
Διάγραμμα 5



Διάγραμμα 6

Σχετικά με τις ηλικίες και το επίπεδο των σπουδών των ερωτηθέντων παραθέτουμε επί συνόλου τα στατιστικά στοιχεία. Σημειώνεται ότι όπου σπουδές ΑΕΙ νοούνται οι ανώτατες σπουδές στην τριτοβάθμια εκπαίδευση, όπου ΤΕΙ νοούνται οι σπουδές σε τεχνολογικά ιδρύματα και ΙΕΚ νοούνται τα ινστιτούτα επαγγελματικής κατάρτισης.

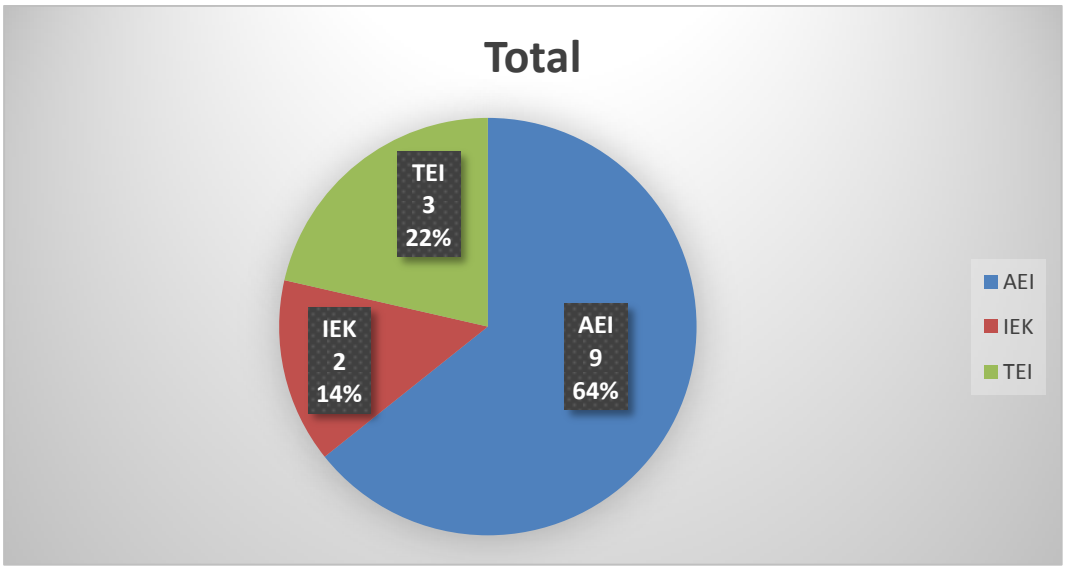
Εύρος ηλικίας επί συνόλου ερωτώμενων στο Διάγραμμα 7



Διάγραμμα 7

Παρατηρούμε ότι η πλειοψηφία αποτελείται από εργαζόμενους νεαρής ηλικίας.

Στο επόμενο διάγραμμα 8 αποτυπώνεται το μορφωτικό επίπεδο των εργαζομένων που συμμετείχαν στην έρευνα



Διάγραμμα 8

Ομοίως παρατηρούμε ότι οι 9 από τους 14 ερωτώμενους είναι πτυχιούχοι πανεπιστημίων.

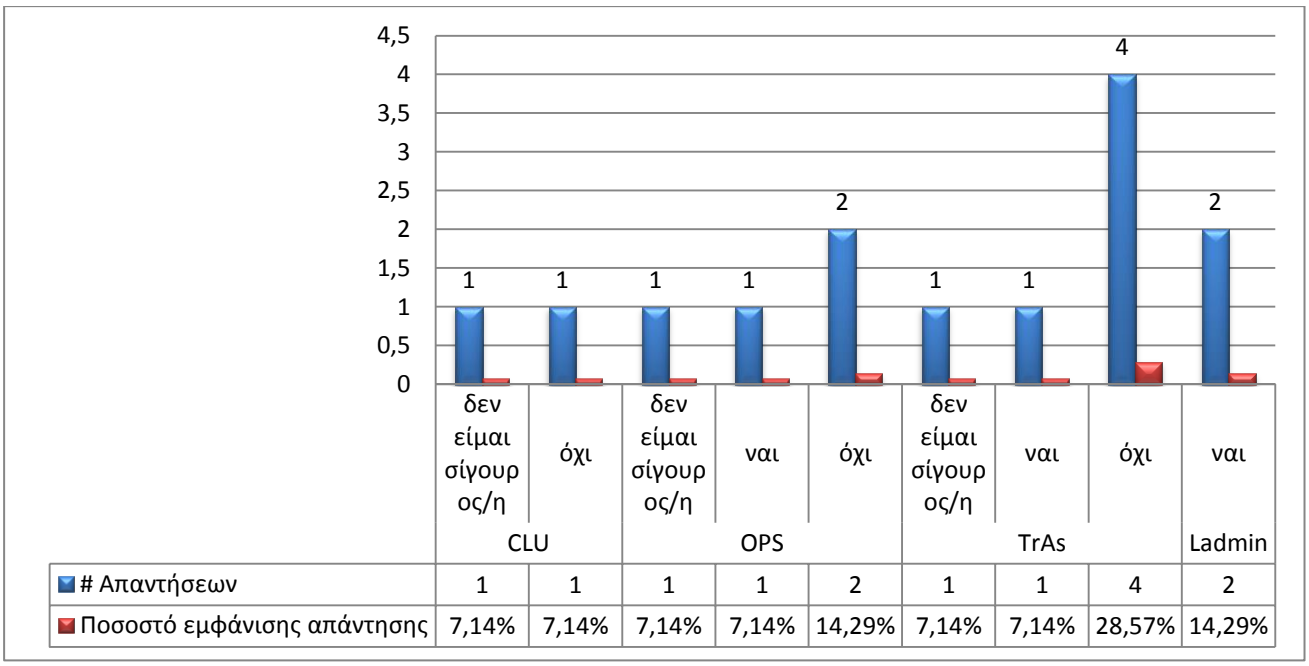
3.3.2 Ανάλυση ερωτήσεων και απαντήσεων

Για την σχετική ανάλυση των απαντήσεων επί των ερωτήσεων θα ακολουθήσει αρχικά η αποτύπωση της ερώτησης και στη συνέχεια ανά τμήμα, θα εστιάσουμε σε εκείνες τις απαντήσεις που κρίνονται κομβικές για την διεξαγωγή ασφαλών συμπερασμάτων. Για την πιο βατή μελέτη της συγκεκριμένης παραγράφου, επιλέχθηκε να γίνει αναφορά στις απαντήσεις σε ποσοτικό επίπεδο. Η πλήρης αποτύπωση των απαντήσεων, παρατίθεται στο παράρτημα Β.

Ερώτηση 1 : Μπορείτε σας παρακαλώ να αναφέρετε αν γνωρίζετε τις πολιτικές ασφαλείας που σχετίζονται με τα Πληροφοριακά Συστήματα της Τράπεζας ; Ειδικότερα για το e banking γνωρίζετε τις αντίστοιχες πολιτικές ;

Στην ερώτηση αυτή τα αποτελέσματα που λάβαμε δεν ήταν ενθαρρυντικά. Πιο συγκεκριμένα, από τους τους OPS οι δύο δεν γνώριζαν καθόλου τις πολιτικές ασφαλείας ενώ εντύπωση προκαλούν οι απαντήσεις από το τμήμα του TrAs όπου από τους 6 ερωτώμενους οι 4 δεν γνώριζαν τις σχετικές πολιτικές. Μόνο το τμήμα του LAdmin γνώριζε τις πολιτικές και απάντησαν σωστά. Από το τμήμα του CLU οι απαντήσεις που δόθηκαν ήταν μοιρασμένες ως προς την γνώση των πολιτικών ασφαλείας. Στο παρακάτω διάγραμμα απεικονίζεται η σχετική κατανομή :

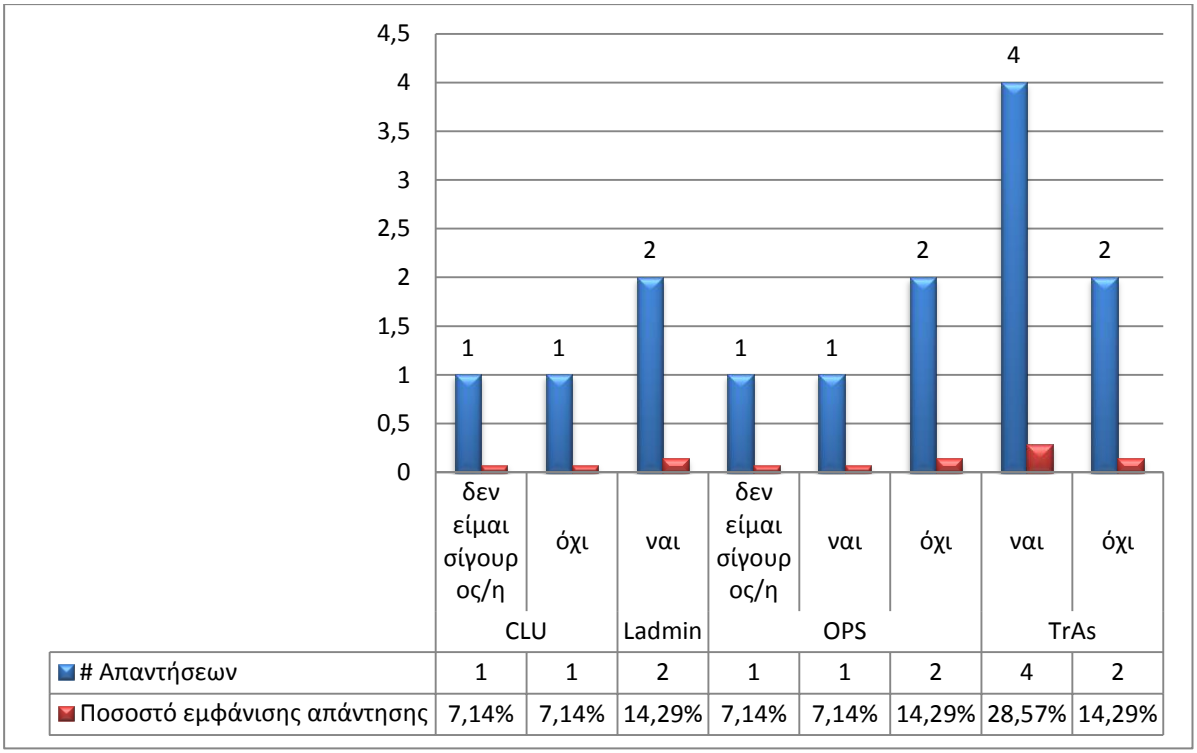
Διάγραμμα 9 : Γνώση πολιτικών Ασφαλείας ανά τμήμα



Ερώτηση 2 : Μπορείτε σας παρακαλώ να περιγράψετε με λίγα λόγια τι ακριβώς είναι το Malware ή αλλιώς κακόβουλο λογισμικό ;

Σε αυτήν την ερώτηση αναμέναμε να λάβουμε απαντήσεις οι οποίες δεν θα ήταν καθόλου ενθαρρυντικές. Ωστόσο, οι απαντήσεις ήταν τέτοιες που οδηγηθήκαμε στο συμπέρασμα ότι η γενικότερη έκρηξη της τεχνολογίας και η χρήση όλων των φορητών συσκευών σε συνδυασμό με τα σχετικά περιστατικά που αναρτώνται στο διαδίκτυο, δείχνει ότι υπάρχει μια γενικότερη αίσθηση. Απόλυτα σωστές απαντήσεις όπως αναμενόταν δόθηκε από το τμήμα του LAdmin λόγω της φύσης εργασίας τους. Εντύπωση προκαλεί το τμήμα του TrAs όπου ενώ στην προηγούμενη ερώτηση οι 4 από τους 6 δεν γνώριζαν τις πολιτικές ασφαλείας, στην ερώτηση αυτή αντιστράφηκαν οι όροι και οι 4 από τους 6 έδωσαν σωστό ορισμό. Υπήρξαν και περιπτώσεις που δήλωσαν αβέβαιοι ως προς την απάντηση όπως το ίδιο συνέβη και στο τμήμα των OPS και CLU. Στο παρακάτω διάγραμμα αποτυπώνονται αναλυτικά οι απαντήσεις.

Διάγραμμα 10 : Σωστός ορισμού για κακόβουλο λογισμικό

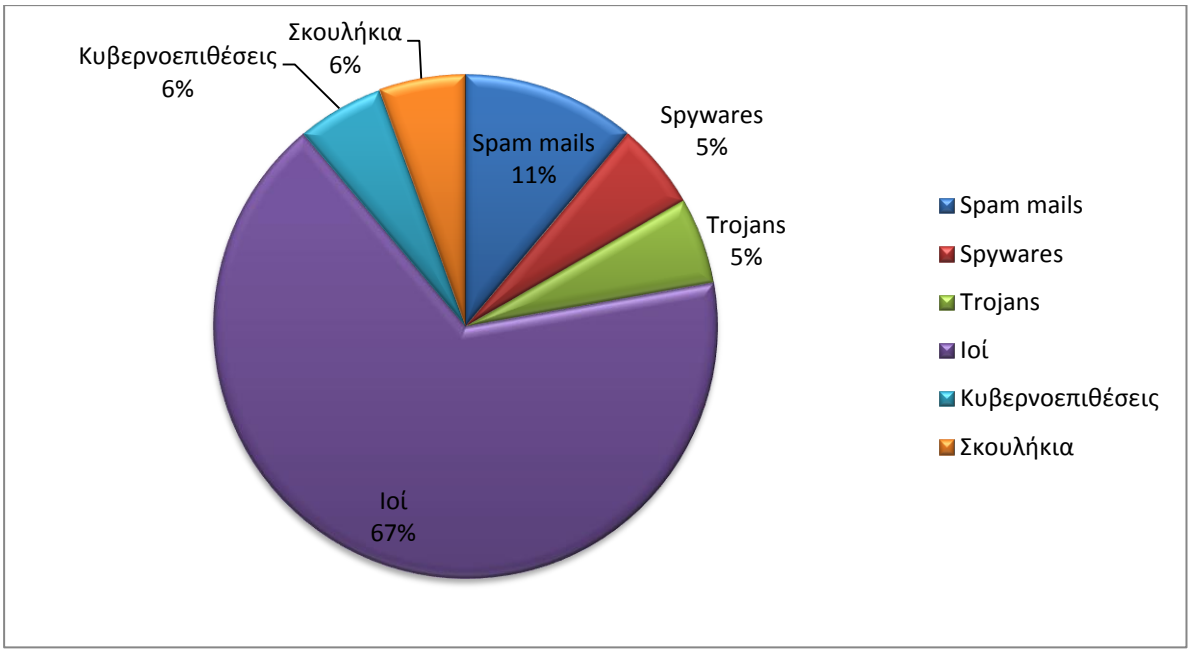


Ερώτηση 3 : Μπορείτε να μας πείτε δύο κατηγορίες από κακόβουλο λογισμικό ; αν δεν γνωρίζετε μπορείτε να σκεφτείτε ;

Σ' αυτήν την ερώτηση την πρωτοκαθεδρία την έλαβαν οι ιοί. Πολύ λίγες απαντήσεις λάβαμε σχετικά με άλλες κατηγορίες κακόβουλων λογισμικών όπως για παράδειγμα σκουλήκια,

Trojans, Spywares κλπ. Αυτό πρακτικά σημαίνει ότι δεν υπάρχει η σωστή γνώση περί κακόβουλων λογισμικών, δεν γίνεται διαχωρισμός των απειλών και όλα θεωρούνται ως ιοί. Διαφορετικές κατηγορίες πέραν από τους ιούς, λάβαμε από το τμήμα του LAdmin και από τους δύο ερωτώμενους ενώ από τα λοιπά τμήματα λάβαμε κάποιες κατηγορίες αποσπασματικά. Παρατίθεται το σχετικό διάγραμμα με τις κατηγορίες των κακόβουλων λογισμικών όπως δόθηκαν στις απαντήσεις.

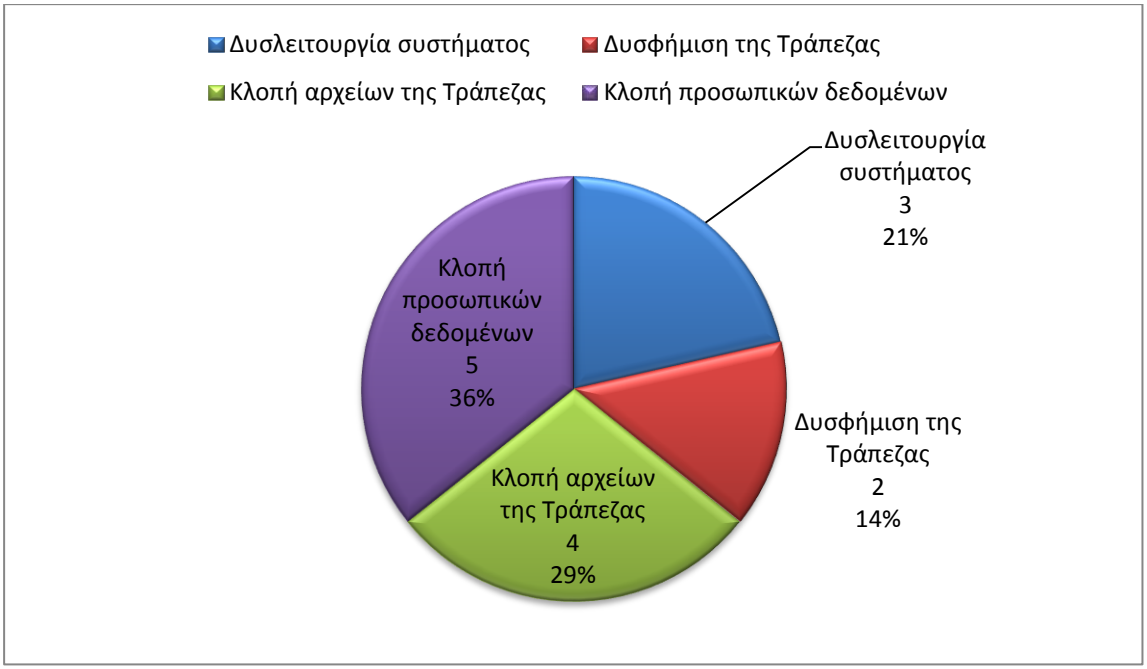
Διάγραμμα 11 : Κατηγορίες κακόβουλων λογισμικών



<u>Ερώτηση 4</u> : Γνωρίζετε τις συνέπειες που μπορεί να προκαλέσει ένα κακόβουλο λογισμικό στην Τράπεζα ;

Στην ερώτηση αυτή, οι απαντήσεις που λάβαμε ήταν μοιρασμένες ανάμεσα σε κλοπή προσωπικών δεδομένων και σε κλοπή αρχείων της Τράπεζας, καθώς απαντήθηκαν από τους 9 συμμετέχοντες. Οι υπόλοιποι 5 διαφοροποιήθηκαν δηλώνοντας ως συνέπειες την γενικότερη δυσλειτουργία των συστημάτων και την δυσφήμηση της Τράπεζας στην αγορά. Οι διαφοροποίηση προήλθε από τα τμήματα των OPS (μία απάντηση), από το τμήμα του TrAs διαφοροποιήθηκαν οι 2 ερωτώμενοι, ενώ από το τμήμα του CLU διαφοροποιήθηκαν και οι δύο ερωτώμενοι. Παρατίθεται το σχετικό διάγραμμα.

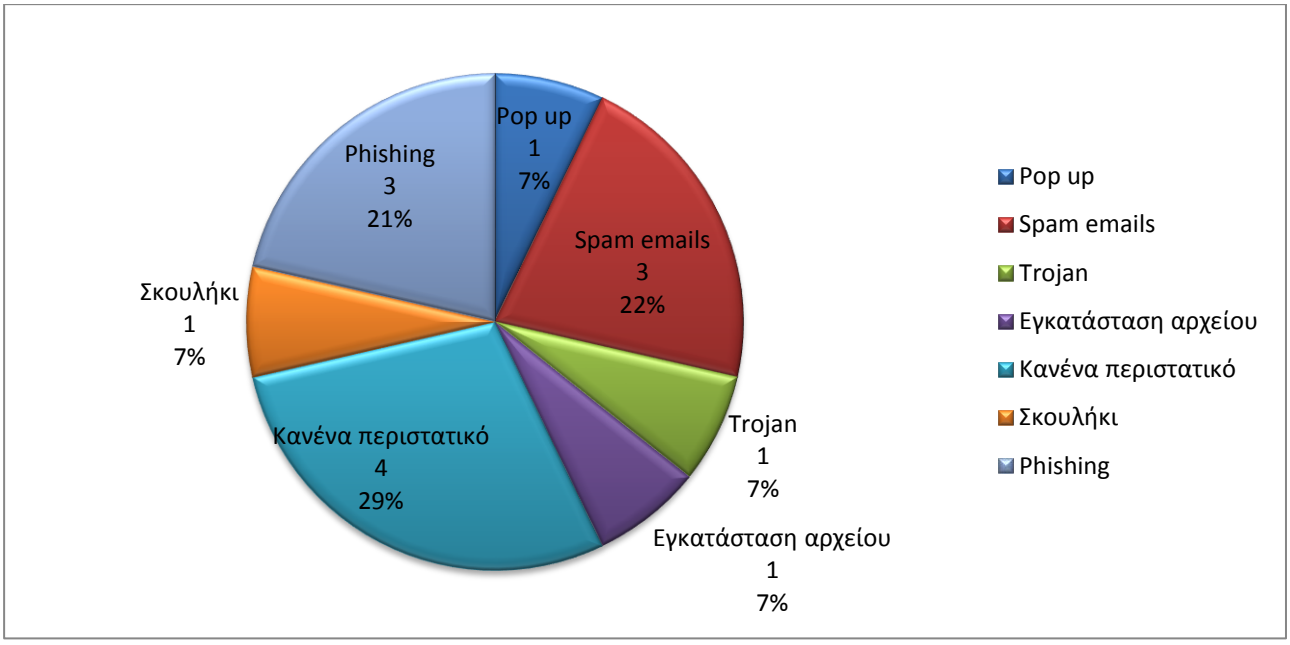
Διάγραμμα 12, κατηγορίες συνεπειών βάση απαντήσεων



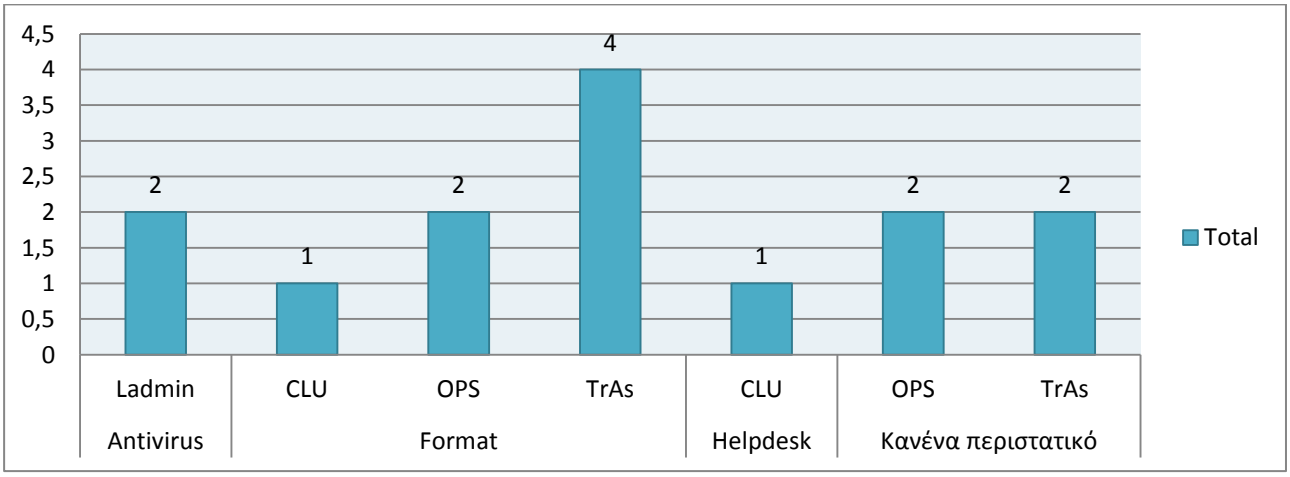
Ερώτηση 5 : Έχετε πέσει θύμα ποτέ από ένα τέτοιου είδους κακόβουλο λογισμικό ; εάν ναι πως αντιδράσατε ;

Στην συγκεκριμένη ερώτηση οι απαντήσεις που λάβαμε παρουσίασαν μεγάλη ποικιλία από τα είδη του κακόβουλου λογισμικού που αντιμετώπισαν οι ερωτώμενοι. Έτσι διαπιστώσαμε περιπτώσεις όπως για παράδειγμα pop ups, Trojans, αρχεία, spam mails, phishing, σκουλήκια. Αίσθηση προκάλεσαν 4 ερωτώμενοι από τα τμήματα του TrAs και OPS οι οποίοι δήλωσαν ότι ουδέποτε αντιμετώπισαν κάποιο περιστατικό. Πιθανόν να πρόκειται για προσεκτικούς χρήστες ωστόσο συνδυάζοντας τις απαντήσεις που δόθηκαν από τις προηγούμενες ερωτήσεις καταλήγουμε ότι ίσως και να έχουν πέσει θύματα και να μην το γνωρίζουν. Σχετικά με το κομμάτι της αντίδρασης, οι ερωτώμενοι που δήλωσαν ότι είχαν δεχθεί επιθέσεις, μόνο το τμήμα του LAdmin αντέδρασε ψύχραιμα τρέχοντας κάποιο antivirus πρόγραμμα ενώ από τα υπόλοιπα τμήματα διαπιστώσαμε πανικό, φόβο και έλλειψη σχετικής γνώσης αντιμετώπισης αφού απευθύνθηκαν σε τεχνικούς και ειδικούς για format ή οδηγίες. Παρακάτω παρατίθενται δύο διαγράμματα για την ερώτηση 5.

Διάγραμμα 13 : Κατανομή κακόβουλων περιστατικών



Διάγραμμα 14 : Τρόπος αντιμετώπισης ανά τμήμα

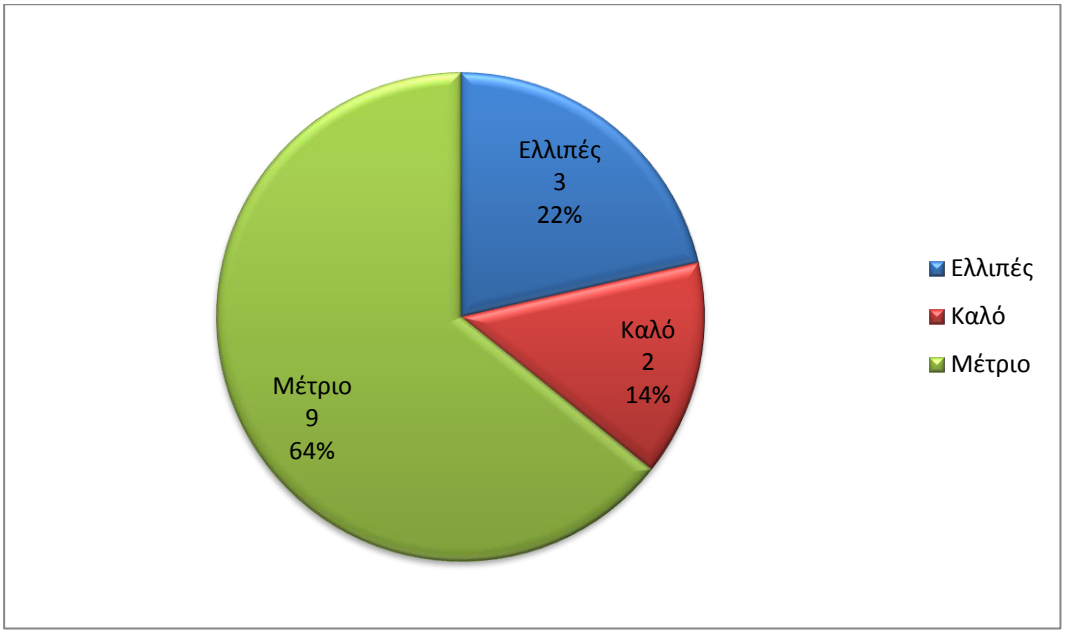


Ερώτηση 6 : Πως θα χαρακτηρίζατε το επίπεδο ενημέρωσης του προσωπικού της Τράπεζας σχετικά με θέματα ασφάλειας ;

Από τις απαντήσεις που λάβαμε από όλους τους ερωτώμενους βλέπουμε ότι όλοι σχεδόν συμφωνούν ότι το επίπεδο ενημέρωσης δεν επαρκεί αφού οι 9 δήλωσαν ότι είναι μέτριο ενώ εντύπωση προκαλούν 3 απαντήσεις που δήλωσαν ότι το επίπεδο ενημέρωσης είναι ελλιπές. Αυτές οι απαντήσεις προήλθαν από τα τμήματα των OPS, CLU, TrAs, ενώ συνδυάζοντας τα αποτελέσματα από προηγούμενες απαντήσεις καταλαβαίνουμε ότι υπάρχει γενικότερη έλλειψη

γνώσης και εκπαίδευσης. Μόνο δύο ερωτώμενοι δήλωσαν ικανοποιημένοι από την ενημέρωση που λαμβάνουν. Παρατίθεται το σχετικό διάγραμμα με τις απαντήσεις.

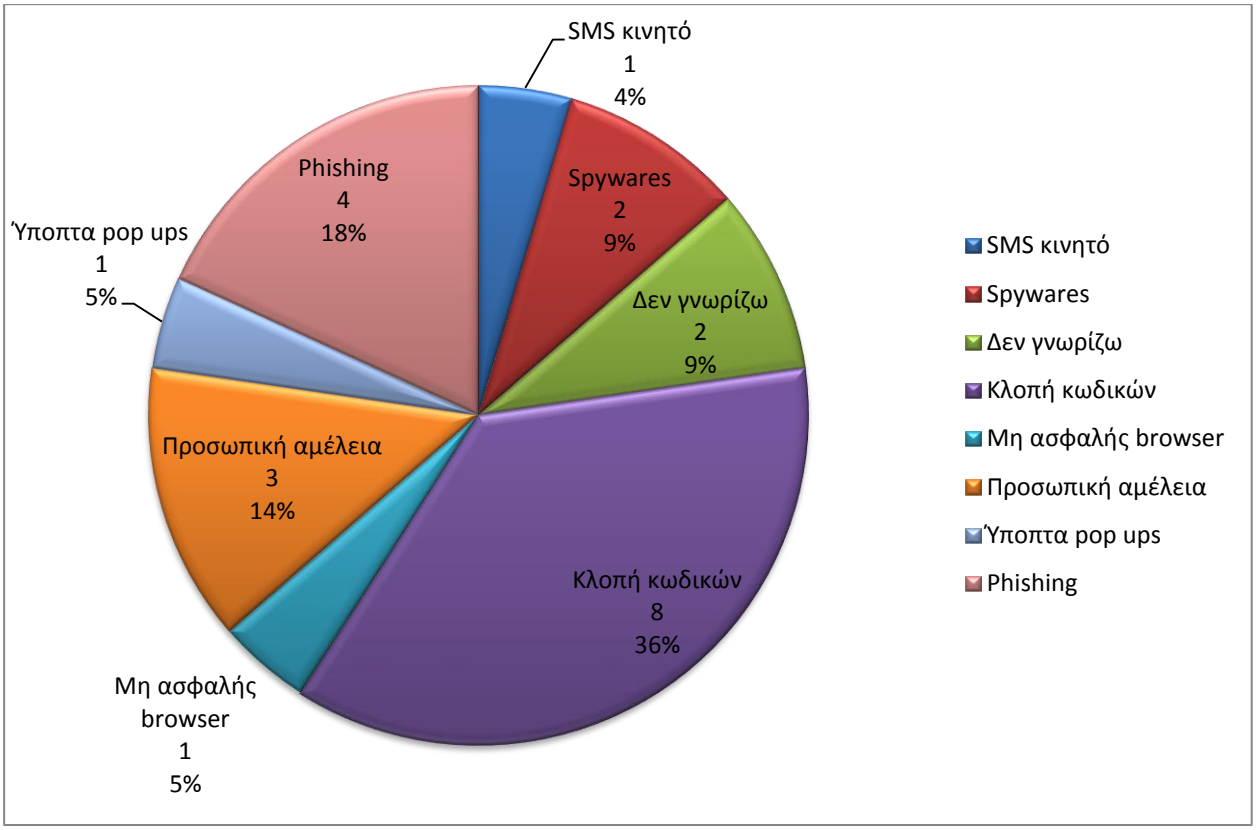
Διάγραμμα 15 : Επίπεδο ενημέρωσης προσωπικού



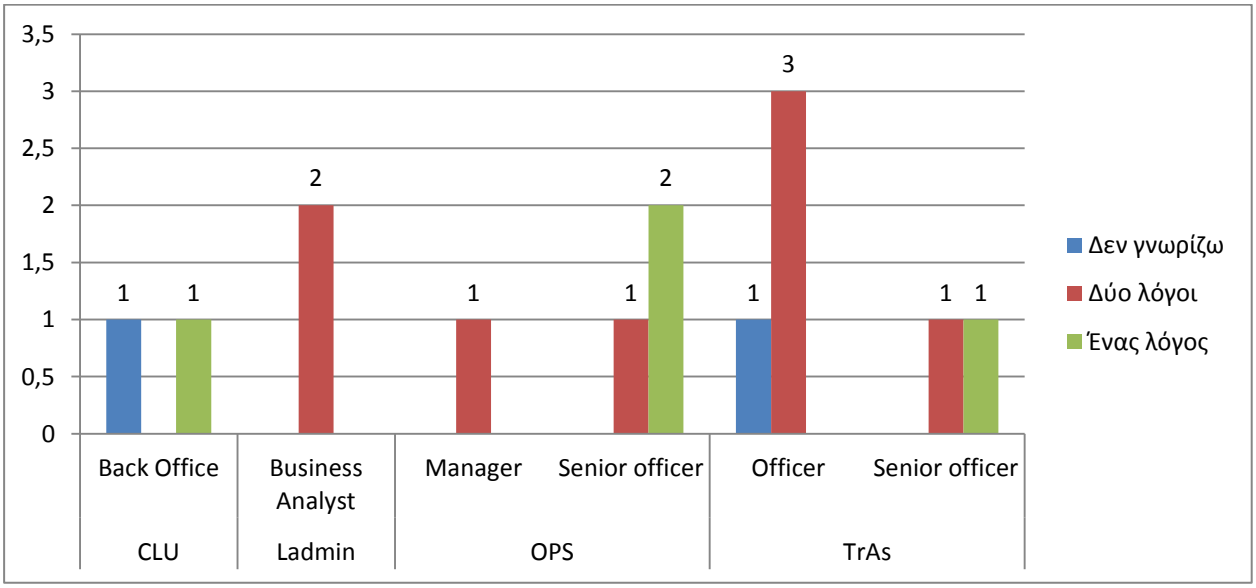
Ερώτηση 7 : Ποιοι πιστεύετε ότι είναι οι κυριότεροι λόγοι που συντελούν στην παραβίαση του e banking ; αν γνωρίζετε παρακαλώ παραθέστε μας δύο παραδείγματα. Αν όχι παρακαλώ μπορείτε να σκεφτείτε δύο περιπτώσεις ;

Σε αυτήν την ερώτηση μόνο το τμήμα του LAdmin έδωσε σαν απάντηση δύο διαφορετικούς λόγους παραβίασης. Γενικότερα δόθηκαν 8 απαντήσεις που δήλωσαν δύο λόγους ενώ 4 δήλωσαν μόνο έναν. Ωστόσο, υπήρξαν και δύο ερωτώμενοι από το τμήμα του CLU και TrAs έκαστος που δεν γνώριζαν κανέναν λόγο. Από τους υπόλοιπους που μας έδωσαν έστω έναν λόγο καταγράψαμε πολλούς και διαφορετικούς τύπους λόγους παραβίασης του ebanking. Παρατίθενται τα σχετικά διαγράμματα ανά τμήμα και λόγο.

Διάγραμμα 16 : Κατανομή λόγων για παραβίαση e banking



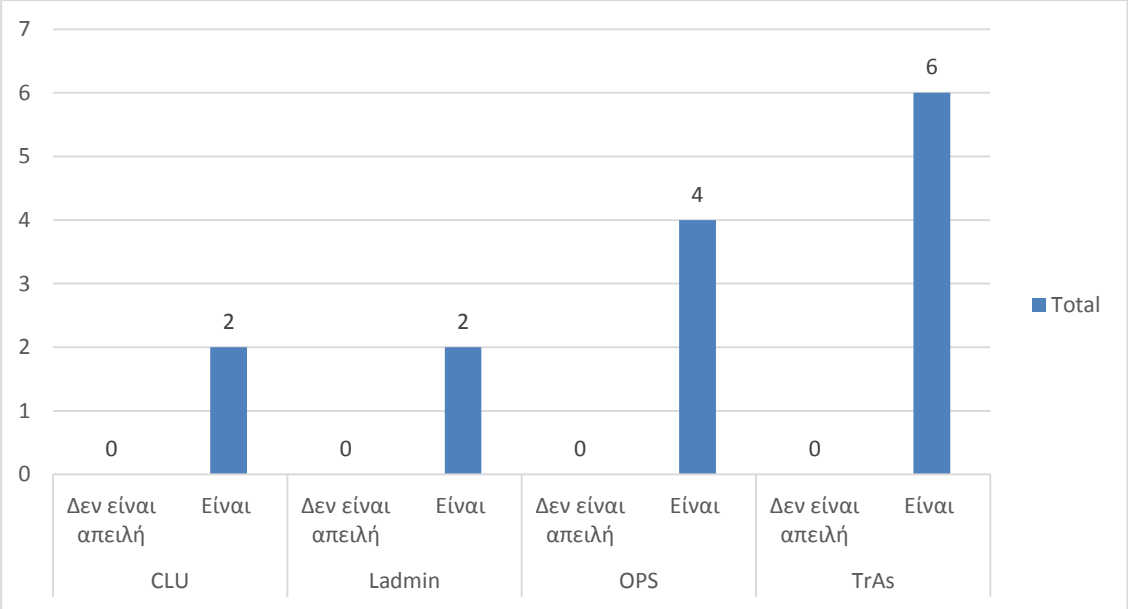
Διάγραμμα 17 : Κατανομή γνώσης περισσότερου του ενός λόγου για παραβίαση e banking ανά τμήμα και θέση



Ερώτηση 8 : Μελέτες στο εξωτερικό έχουν δείξει ότι ο μεγάλος κίνδυνος για την επίθεση από κακόβουλο λογισμικό προέρχεται από τον ίδιο τον ανθρώπινο παράγοντα και λάθη στα οποία υποπίπτει. Συμφωνείτε ως προς αυτό ;

Τα αποτελέσματα σε αυτή την ερώτηση ήταν συντριπτικά καθώς και οι 14 ερωτώμενοι συμφώνησαν ότι ανθρώπινος παράγοντας και η αμέλεια που επιδεικνύει αποτελεί τον μεγαλύτερο κίνδυνο για την Τράπεζα.

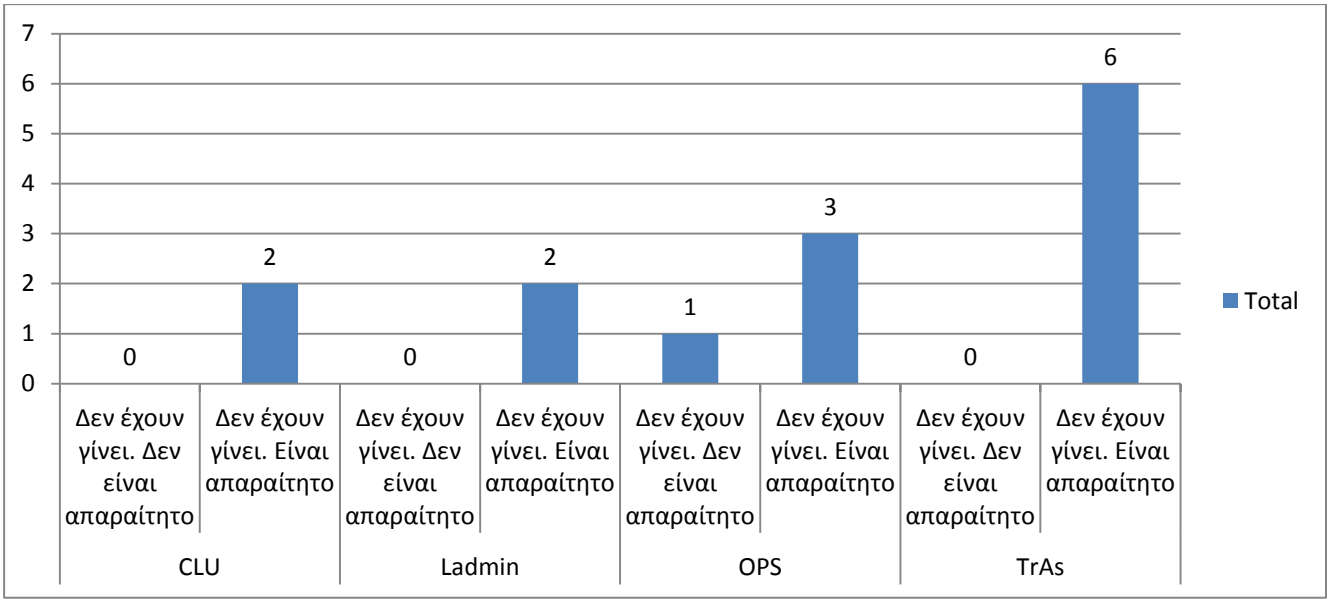
Διάγραμμα 18 : κατανομής απειλής του ανθρώπινου παράγοντα (καθολική συμφωνία και των 14 ερωτώμενων)



Ερώτηση 9 : Α) Έχουν γίνει ειδικά σεμινάρια για ενημέρωση, πρόληψη και προστασία από κακόβουλο λογισμικό ; Β) Αν όχι, πιστεύετε ότι είναι απαραίτητο να γίνουν αυτά τα σεμινάρια ; Γ) Αν ναι, θεωρείτε ότι απαιτείται ενημέρωση για νέα ήδη κακόβουλων λογισμικών και συνεχής επιμόρφωση ;

Και σε αυτήν την ερώτηση, όπως και στην προηγούμενη, υπάρχει σχεδόν πλήρης συμφωνία αναφορικά με την ανάγκη διεξαγωγής σχετικών σεμιναρίων. Μόνο ένας ερωτώμενος από το τμήμα των OPS δήλωσε ότι δεν είναι απαραίτητο να διεξαχθούν επιμορφωτικά σεμινάρια παρά το γεγονός ότι δεν έχουν γίνει, θεωρώντας ότι ήδη υπάρχουσες ενημερώσεις είναι αρκετές. Ωστόσο, τα μέχρι τώρα αποτελέσματα της έρευνας δεν δικαιώνουν την απάντηση αυτή.

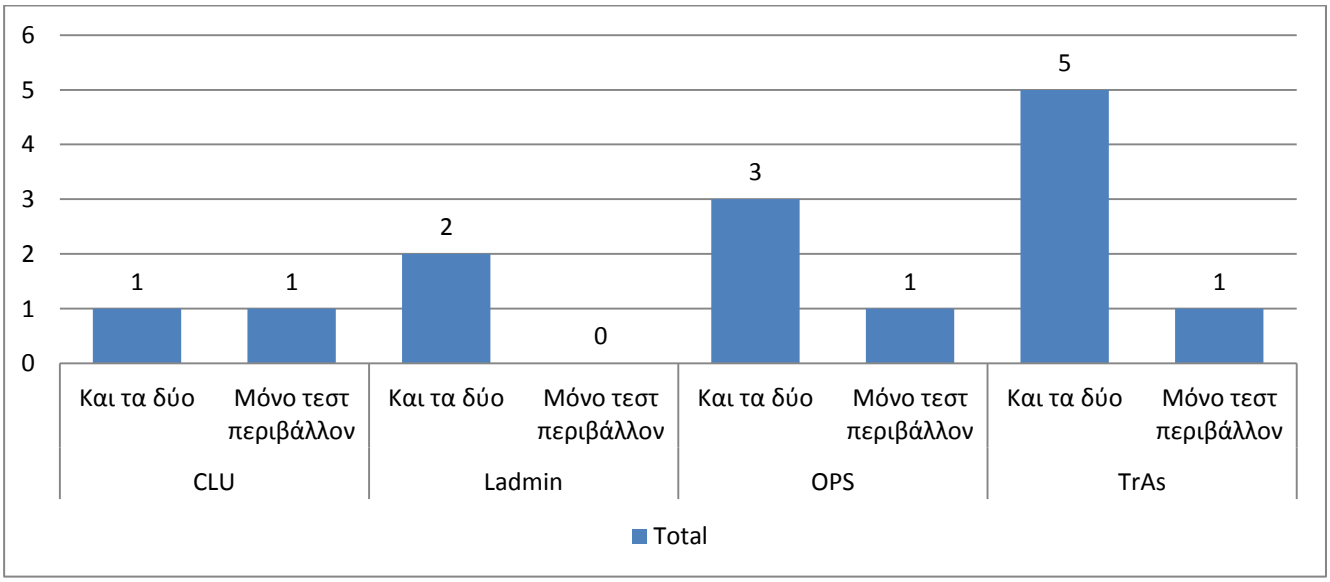
Διάγραμμα 19 : Σεμινάρια και ανάγκη διεξαγωγής τους ανά τμήμα.



<u>Ερώτηση 10</u> : Τι θεωρείτε πιο σημαντικό ; την έκδοση οδηγιών προς όλο το προσωπικό ή εκπαίδευση σε τεστ περιβάλλον με αναπαραγωγή επιθέσεων από κακόβουλο λογισμικό ; γιατί ;

Σε συνέχεια της ομοφωνίας των προηγούμενων ερωτήσεων, έτσι και στην τελευταία ερώτηση, οι 11 από τους 14 ερωτώμενους πιστεύουν ότι για την καλύτερη εκπαίδευση και επιμόρφωση είναι απαραίτητος ο συνδυασμός των σχετικών ενημερώσεων μέσω οδηγιών και της χρήσης ειδικού τεστ περιβάλλοντος σε υπολογιστή. Μικρή διαφοροποίηση παρουσίασαν 3 ερωτώμενοι από τα τμήματα CLU, OPS, TrAs έκαστος, όπου πιστεύουν ότι χρειάζεται μόνο η διεξαγωγή εκπαίδευσης και αναπαραγωγή επιθέσεων σε τεστ περιβάλλον μέσω υπολογιστή.

Διάγραμμα 20 : Ανάγκη εκπαίδευσης εκτός από τις οδηγίες



3.4 Συμπεράσματα και σχολιασμός

Από την μέχρι τώρα ανάλυση και έρευνα διαπιστώνουμε ότι η ασφάλεια που πρέπει να διέπει την περιήγηση στις πλατφόρμες e banking και γενικότερα στα συστήματα ενός οργανισμού, είναι ζωτικής και ύψιστης σημασίας για τον ίδιο τον οργανισμό. Και αυτό προκύπτει από το γεγονός ότι οι Τράπεζες για παράδειγμα όπως είδαμε διαθέτουν ιδιαίτερους τρόπους και μηχανισμούς για την προστασία και την ασφάλεια των συναλλαγών μέσω e banking αλλά και για την ασφάλεια από επιθέσεις κακόβουλων λογισμικών, ωστόσο πάντα στην εξίσωση της ασφάλειας θα υπεισέρχεται ο ανθρώπινος παράγοντας. Από τις συνεντεύξεις που διεξήχθησαν διαπιστώσαμε ότι οι εργαζόμενοι, δεν έχουν πλήρη γνώση και σαφή εικόνα για το τι εστί ασφάλεια, πολιτική ασφάλειας, κακόβουλο λογισμικό. Από την άλλη όμως υπάρχει καθολική συμφωνία στο γεγονός ότι ο άνθρωπος είναι ο νούμερο ένα κίνδυνος για την ασφάλεια ενός συστήματος, μιας πλατφόρμας ή οτιδήποτε σχετίζεται με σύστημα και διαδίκτυο.

Από το δείγμα των 14 ερωτώμενων οι 6 ήταν γυναίκες και 8 ήταν άνδρες ενώ το μεγαλύτερο ποσοστό εξ αυτών ήταν σε ηλικιακό φάσμα μεταξύ 32 -36 ετών (43%). Η πλειοψηφία αυτών είναι απόφοιτοι κάποιου πανεπιστημίου (AEI) σε ποσοστό 64% και οι υπόλοιποι είναι απόφοιτοι τεχνολογικού ιδρύματος (TEI) σε ποσοστό 22% και ινστιτούτου επαγγελματικής κατάρτισης (ΙΕΚ) σε ένα μικρό ποσοστό της τάξεως 14%. Επιπλέον, επιλέχτηκε δείγμα με διαφορετικές θέσεις εντός οργανισμού και από διαφορετικά κομμάτια ώστε να υπάρχουν όσο το δυνατόν περισσότερες και ποικίλες απόψεις κι έτσι να καταστεί εφικτή η εξαγωγή ασφαλέστερων συμπερασμάτων σχετικά με την διεξαχθείσα έρευνα.

Γενικότερα, το προσωπικό κάθε εταιρίας οφείλει να ενημερώνεται αλλά και να συμμορφώνεται στις εκάστοτε πολιτικές ασφαλείας. Στην $1^{η}$ ερώτηση αναφορικά με το αν γνωρίζουν τις πολιτικές ασφαλείας που διέπουν την Τράπεζα και κατ' επέκταση το e banking βλέπουμε ότι μόλις το 28,57% των ερωτώμενων γνώριζαν την απάντηση (ένας από τα OPS, ένας από TrAs και δύο από LAdmin) ενώ η πλειοψηφία σε ποσοστό 50% δήλωσε ότι δεν γνώριζε καθόλου τις πολιτικές ασφαλείας. Το υπόλοιπο 21,43% δήλωσε πως δεν είναι σίγουρο για το αν γνωρίζει τις πολικές. Αυτό πρακτικά σημαίνει ότι ένα τόσο σημαντικό ζήτημα για την Τράπεζα δεν έχει επιδεχθεί της δέουσας προσοχής. Στην $2^{η}$ ερώτηση για τον ορισμό ενός κακόβουλου λογισμικού το 50% έδωσε σωστό ορισμό με το απόλυτο να το έχει το τμήμα του LAdmin όπου και οι δύο εργαζόμενοι έδωσαν σωστό ορισμό. Αντίθετα το υπόλοιπο 50% χωρίζεται σε κατηγορίες εργαζομένων που δεν έδωσαν σωστό ορισμό διότι δεν τον γνώριζαν (35,71%) και ένα μικρό κομμάτι δήλωσε ότι δεν είναι σίγουρο (14,29%). Άρα μπορούμε να σκεφτούμε ότι ένα πολύ μεγάλο μέρος του προσωπικού ίσως να μην γνωρίζει τι σημαίνει κακόβουλο λογισμικό και κατ'

επέκταση υπάρχει και άγνοια στον τρόπο αντιμετώπισης. Αυτό μπορούμε να το διαπιστώσουμε και από την ερώτησή μας αν γνωρίζουν δύο κατηγορίες κακόβουλων λογισμικών. Η πλειοψηφία της τάξεως ~ 67% (12 απαντήσεις) δήλωσε σαν κύρια κατηγορία τους ιούς ενώ το υπόλοιπο ποσοστό των απαντήσεων μοιράστηκε ανάμεσα σε spam mails (2 απαντήσεις), spywares (1 απάντηση), Trojans (1 απάντηση), σκουλήκια (1 απάντηση) αλλά και κυβερνοεπιθέσεις (1 απάντηση).

Αναφορικά με το ερώτημα σχετικά με τις συνέπειες οι απαντήσεις έδειξαν περιορισμό σε 4 μεγάλες κατηγορίες και αυτές ήταν η κλοπή των προσωπικών δεδομένων (5 απαντήσεις ήτοι 36%), κλοπή αρχείων της Τράπεζας (4 απαντήσεις ήτοι 29%), δυσλειτουργία συστήματος (3 απαντήσεις ήτοι 21%), δυσφήμιση της Τράπεζας (2 απαντήσεις ήτοι 14%). Στην ερώτησή μας για το αν έχουν πέσει θύμα κάποιου κακόβουλου λογισμικού μόλις οι 4 δεν είχαν αντιμετωπίσει κάποιο περιστατικό (29%) ενώ οι υπόλοιπο έχουν βρεθεί αντιμέτωποι με κάποιο περιστατικό με κύριες κατηγορίες τα spam emails (3 περιπτώσεις, 21%) και το phishing (3 περιπτώσεις, 21%). Οι υπόλοιπες κατηγορίες κακόβουλων λογισμικών δηλώθηκαν από μία φορά (ποσοστό 7%) και αφορούν σε σκουλήκι, Trojan, εγκατάσταση κάποιου αρχείου και pop up windows. Από τους εργαζόμενους που έπεσαν θύμα κάποιου κακόβουλου λογισμικού δλδ 10 εργαζόμενοι που αντιστοιχεί σε ποσοστό 71% από το σύνολο των ερωτώμενων, παρατηρούμε ότι οι 7 από αυτούς ενήργησαν με άγχος και πανικό και γι αυτό ζήτησαν βοήθεια από τεχνικό ώστε να προβεί σε format του υπολογιστή τους (ποσοστό 70% στους 10 εργαζόμενους), ένας ζήτησε βοήθεια από το helpdesk και μόλις 2 ενήργησαν σχετικά ψύχραιμα χρησιμοποιώντας κάποιο πρόγραμμα antivirus. Γίνεται άμεσα αντιληπτό ότι η έλλειψη ενημέρωσης και εκπαίδευσης του προσωπικού είναι έκδηλη. Αν για παράδειγμα υπήρχε πιο συστηματική εκπαίδευση σχετικά με θέματα ευαισθητοποίησης για την ασφάλεια από κακόβουλα λογισμικά αλλά και το πώς αντιμετωπίζονται, σίγουρα θα μπορούσαμε να πούμε ότι θα είχαμε περιορισμένα κρούσματα αλλά και καλύτερο τρόπο αντιμετώπισης. Το συμπέρασμα αυτό ενισχύεται σε μεγάλο βαθμό με την αμέσως επόμενη ερώτηση για το επίπεδο ενημέρωσης του προσωπικού σε θέματα ασφάλειας. Μόνο το 14% απάντησε ότι είναι καλό ενώ το 64% θεωρεί ότι είναι μέτριο και το υπόλοιπο 22% είναι ελλιπές.

Στην ερώτησή μας αναφορικά με τους λόγους που συντελείται η παραβίαση του e banking (ζητήσαμε να μας αναφέρουν δύο), οι απαντήσεις που δόθηκαν κατανέμονται σε διαφορετικές κατηγορίες. Την πρωτιά την κατέχει η κλοπή των κωδικών με 8 απαντήσεις και 36% σε ποσοστό και ακολουθούν : phishing με 4 απαντήσεις (18%), προσωπική αμέλεια 3 απαντήσεις (14%), spywares 2 απαντήσεις (9%) και από μία απάντηση ύποπτα pop ups, μη ασφαλής browser, sms σε κινητό (5%). Ωστόσο υπήρξαν και δύο εργαζόμενοι οι οποίοι δεν γνώριζαν καθόλου κάποιον

λόγο (9%) ποσοστό το οποίο είναι αρκετά ανησυχητικό. Από αυτή την ερώτηση όπου στην πραγματικότητα ζητήσαμε δύο λόγους παραβίασης μόνο οι μισοί (7 εργαζόμενοι, 50%) κατάφεραν να δώσουν δύο κατηγορίες και 5 εργαζόμενοι (~35,7%) έδωσαν έστω έναν.

Η ανθρώπινη αμέλεια ωστόσο και το γεγονός ότι ο ανθρώπινος παράγοντας τείνει να είναι ο πιο επικίνδυνος από όλους τους υπόλοιπους που έχουν αναφερθεί, δείχνει ομοφωνία και συμφωνία καθολοκληρία. Ήταν πολύ ξεκάθαρο στις απαντήσεις που λάβαμε γεγονός που καταδεικνύει ο άνθρωπος έχει και το μεγαλύτερο μέρος της ευθύνης σε κάθε πιθανό πρόβλημα που προκύπτει από επιθέσεις κακόβουλων λογισμικών. Γι αυτό τον λόγο, αμέσως μετά ρωτήσαμε κατά πόσο έχουν γίνει επιμορφωτικά σεμινάρια για θέματα ασφάλειας και αν γενικότερα θεωρούν ότι είναι απαραίτητο να γίνουν. Τα αποτελέσματα επιβεβαίωσαν με εμφατικό τρόπο την ανάγκη εκπαίδευσης του προσωπικού για το τί νοείται ασφάλεια, τους τρόπους πρόληψης και αντιμετώπισης κακόβουλων ενεργειών αλλά και το τί νοείται κακόβουλη ενέργεια (είτε αφορά κάποιο λογισμικό είτε είναι ενέργεια εκ των έσω). Από τους 14 ερωτώμενους, οι 13 δήλωσαν ότι δεν έχουν τέτοιου είδους σεμινάρια και ότι κρίνεται απαραίτητο και επιβεβλημένο να λαμβάνουν χώρα σε τακτά χρονικά διαστήματα. Το ποσοστό του ~92,8% δεν αφήνει περιθώρια για αμφιβολίες για την κρισιμότητα και την σημασία που πρέπει να έχει στον κάθε οργανισμό, και εν προκειμένω στην Τράπεζα, η εκπαίδευση σε θέματα ασφάλειας.

Στο τελευταίο σκέλος της συνέντευξης, απευθύναμε το ερώτημα για το τι πιστεύει ο καθένας ότι είναι καλύτερο και πιο σημαντικό για την επιμόρφωση του προσωπικού : έκδοση οδηγιών ή εκπαίδευση σε τεστ περιβάλλον ενός υπολογιστή. Η συντριπτική πλειοψηφία της τάξεως του ~78,5% (11 απαντήσεις) πιστεύει ότι απαιτείται και η θεωρητική προσέγγιση όπως για παράδειγμα έκδοση οδηγιών, υπηρεσιακά σημειώματα κλπ αλλά και η πρακτική προσέγγιση με σεμινάρια με αναπαραγωγή επιθέσεων, βίντεο, ομιλίες κλπ. Το υπόλοιπο 21,5% (3 απαντήσεις) πιστεύουν ότι αυτό που λείπει και χρειάζεται είναι η πρακτική προσέγγιση υπό την έννοια ότι πιθανόν τις γραπτές οδηγίες να μην τις διαβάσει το προσωπικό με προσοχή (ίσως να μην τις μελετήσει και καθόλου).

Μέσα από τα παραπάνω αποτελέσματα της διεξαχθείσας έρευνας, εύκολα μπορεί να διαπιστώσει κανείς ότι οι εργαζόμενοι πρέπει να ευαισθητοποιηθούν περισσότερο, να κατανοήσουν και να αφομοιώσουν τις απειλές και τις συνέπειες αυτών, να μάθουν τους τρόπους πρόληψης προκειμένου να διαφυλάσσεται τόσο η δικιά τους ασφάλεια όσο και της Τράπεζας. Στα πλαίσια λοιπόν, της στρατηγικής που ακολουθεί η Τράπεζα θα πρέπει να δοθεί έμφαση και στην βελτίωση των ποιοτικών χαρακτηριστικών των εργαζομένων σε θέματα ασφάλειας. Η τεχνολογία αλλάζει, εξελίσσεται και δεν είναι ποτέ στατική. Επομένως ο ανθρώπινος

παράγοντας οφείλει να ακολουθεί τις αλλαγές, να ενημερώνεται, να εκπαιδεύεται εφόσον πάντα αποτελεί τον ακρογωνιαίο λίθο της επιτυχίας και ταυτόχρονα το πλέον επικίνδυνο παράγοντα για την πρόκληση σοβαρών βλαβών σε έναν οργανισμό.

3.5 Επίλογος και προτάσεις

Η εξέλιξη της τεχνολογίας έφερε τεράστια ανάπτυξη στις σύγχρονες συναλλαγές. Ο τραπεζικός κλάδος προκειμένου να παραμείνει ανταγωνιστικός, εισήλθε δυναμικά στον χώρο του ηλεκτρονικού επιχειρήν και δημιούργησε πλατφόρμες ηλεκτρονικής τραπεζικής ώστε ο κάθε χρήστης να μπορεί να συναλλάσσεται σε καθημερινή βάση μέσα από αυτές. Η πρόσβαση είναι γρήγορη, βολική και διαθέσιμη όλο το εικοσιτετράωρο, ανεξάρτητα από την τοποθεσία του πελάτη. Επιπλέον, οι τράπεζες μπορούν να παρέχουν περισσότερες υπηρεσίες αποτελεσματικά και με σημαντικά χαμηλότερο κόστος. Παρόλα αυτά, η αλματώδης άνθηση και ανάπτυξη της τεχνολογίας πέραν των θετικών που προσφέρει, συμπαρασύρει μαζί τους και πολλούς κινδύνους που ακούνε στο όνομα κακόβουλα λογισμικά. Γι αυτό τον λόγο οι Τράπεζες, έχουν αναπτύξει μηχανισμούς ασφαλείας και τρόπους άμυνας προκειμένου να αποκρούσουν παράνομες εισβολές στα συστήματά της που θα προκαλέσουν ανεπανόρθωτες ζημιές. Βέβαια, δεν θα πρέπει να παραβλέπουμε το γεγονός ότι η ασφάλεια των συστημάτων μια Τράπεζας μπορεί να προσπεραστεί και να διασπαστεί μέσα από λάθη και αδυναμίες των ανθρώπων που τα διαχειρίζονται ή από αμέλεια μη εξουσιοδοτημένων χρηστών. Η πολιτική ασφαλείας που εφαρμόζει η Τράπεζα σκοπό έχει σαν βασικά και αναντικατάστατο συστατικό την περιγραφή των κανόνων και των διαδικασιών που πρέπει να ακολουθούνται για την προστασία των πληροφοριακών συστημάτων.

Η αποτελεσματική εφαρμογή μιας πολιτικής προϋποθέτει ότι είναι κατανοητή και αποδεκτή από όλους. Επομένως, η εκπαίδευση του προσωπικού σε θέματα ασφάλειας βελτιώνει την ικανότητα του τελικού χρήστη να κατανοήσει την πολιτική, την πρόληψη, την αντιμετώπιση των κινδύνων, γεγονός που καθιστά την εκπαίδευση πρωταρχικής σημασίας για την εξασφάλιση της τήρησης των πολιτικών και της επιτυχίας του οργανισμού. Οι εργαζόμενοι οποιοδήποτε level πρέπει να είναι κατάλληλα εκπαιδευμένοι όχι μόνο σχετικά με τις ευθύνες τους και τα καθήκοντά τους αλλά και την τήρηση της ασφάλειας. Η ενημέρωση και η επιμόρφωση πρέπει να είναι συνεχής και οι πολιτικές ασφάλειας να επικαιροποιούνται όντας διαθέσιμες σε όλους. Γι αυτό τον σκοπό, τα επιμορφωτικά σεμινάρια θα πρέπει να διοργανώνονται με γνώμονα την προνόηση, την έγκαιρη και έγκυρη επικαιροποιημένη γνώση σε θέματα ασφάλειας και κακόβουλων λογισμικών. Πριν από αυτό όμως, οι Τράπεζες πρέπει να εντοπίσουν τα τρωτά τους σημεία, με

ποιον τρόπο οι εργαζόμενοι λειτουργούν, πώς αντιδρούν σε ενδεχόμενες απειλές ή λάθη εξ αμελείας των ίδιων. Για να το πετύχουν αυτό προτείνονται τα εξής :

- Σταθερή και τακτική παρακολούθηση του εργασιακού περιβάλλοντος στο να διασφαλιστεί ότι η ομαλή και ασφαλής λειτουργία δεν παρεκκλίνει από λάθη και παραβιάσεις. Έτσι, ο τακτικός αυτός έλεγχος επιτρέπει στην διοίκηση να μπορεί να εντοπίσει οι παραβιάσεις μέσα από ανεπαίσθητες αλλαγές που έχουν συμβεί ενώ μέσα από τις συγκεντρωτικές αναφορές διαγράφονται οι πιθανές τάσεις παραβιάσεων. Αυτή η πτυχή της παρακολούθησης μπορεί να αποδειχθεί πολύ χρήσιμη, ειδικά σε ένα μεγάλο ίδρυμα.
- Η ανάλυση, η δημιουργία αναφορών και οι μελλοντικές τάσεις μπορούν με την σειρά τους να προσφέρουν την απαραίτητη γνώση στην Τράπεζα ώστε να ανακαλύψει την αιτία, τον δράστη και, ενδεχομένως, τον λόγο για την οποιαδήποτε παράβαση (κίνητρα).

Τα παραπάνω λοιπόν, θα αποτελέσουν την απαρχή για την δομή μιας αποτελεσματικότερης και πιο διαδραστικής εκπαίδευσης των εργαζόμενων.

Κλείνοντας, επισημαίνουμε την ανάγκη ότι για να είναι αποτελεσματικά τα προγράμματα πρέπει να είναι προσαρμοσμένα με τέτοιο τρόπο ώστε να απευθύνονται σε όλο το προσωπικό αλλά με στοχευμένο τρόπο ήτοι ανώτατη διοίκηση, εργαζομένους πληροφορικής και τελικούς χρήστες. Ο λόγος είναι ξεκάθαρος, εφόσον οι ανάγκες κάθε διακριτού τμήματος είναι διαφορετικές. Οφείλουν οι Τράπεζες να συνειδητοποιήσουν ότι δεν αρκεί μόνο η επένδυση στην ανάπτυξη γραμμών άμυνας και δικλείδων ασφαλείας στα συστήματα τους. Διότι για την άρτια απόδοση των μέτρων και πολιτικών ασφαλείας απαιτείται η συμμετοχή του εργαζόμενου/χρήστη και η συνεχής του επιμόρφωση. Άρα, θα πρέπει ο τραπεζικός κλάδος να προχωρήσει και επενδύσει μεγαλύτερα ποσά στην εκπαίδευση και υποστήριξη των εργαζομένων ελαχιστοποιώντας τους κινδύνους και τις απώλειες που μπορεί να υποστεί.

Παράρτημα Α : Ερωτηματολόγιο

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Το παρόν ερωτηματολόγιο δημιουργήθηκε προκειμένου να διερευνήσουμε και να αναδείξουμε την σημαντικότητα της εκπαίδευσης το προσωπικού του Ομίλου σε θέματα ασφάλειας για την χρήση του e banking. Η συνέντευξη θα είναι ανώνυμη και δεν απαιτείται να συμπληρωθούν στοιχεία που να αποκαλύπτουν την ταυτότητά σας.

Δημογραφικά Στοιχεία :

Φύλο	
Ηλικία	
Τμήμα εργασίας	
Σπουδές	
Θέση	
Χρήστης e banking (ναι / όχι)	

1. Μπορείτε σας παρακαλώ να αναφέρετε αν γνωρίζετε τις πολιτικές ασφαλείας που σχετίζονται με τα Πληροφοριακά Συστήματα της Τράπεζας ; Ειδικότερα για το e banking γνωρίζετε τις αντίστοιχες πολιτικές ;
2. Μπορείτε σας παρακαλώ να περιγράψετε με λίγα λόγια τι ακριβώς είναι το Malware ή αλλιώς κακόβουλο λογισμικό ;
3. Μπορείτε να μας πείτε δύο κατηγορίες από κακόβουλο λογισμικό ; αν δεν γνωρίζετε μπορείτε να σκεφτείτε ;
4. Γνωρίζετε τις συνέπειες που μπορεί να προκαλέσει ένα κακόβουλο λογισμικό στην Τράπεζα ;
5. Έχετε πέσει θύμα ποτέ από ένα τέτοιου είδους κακόβουλο λογισμικό ; εάν ναι πως αντιδράσατε ;
6. Πως θα χαρακτηρίζατε το επίπεδο ενημέρωσης του προσωπικού της Τράπεζας σχετικά με θέματα ασφάλειας ;

7. Ποιοι πιστεύετε ότι είναι οι κυριότεροι λόγοι που συντελούν στην παραβίαση του e banking ; αν γνωρίζετε παρακαλώ παραθέστε μας δύο παραδείγματα. Αν όχι παρακαλώ μπορείτε να σκεφτείτε δύο περιπτώσεις ;
8. Μελέτες στο εξωτερικό έχουν δείξει ότι ο μεγάλος κίνδυνος για την επίθεση από κακόβουλο λογισμικό προέρχεται από τον ίδιο τον ανθρώπινο παράγοντα και λάθη στα οποία υποπίπτει. Συμφωνείτε ως προς αυτό ;
9. Α) Έχουν γίνει ειδικά σεμινάρια για ενημέρωση, πρόληψη και προστασία από κακόβουλο λογισμικό ;

   Β) Αν όχι, πιστεύετε ότι είναι απαραίτητο να γίνουν αυτά τα σεμινάρια ;

   Γ) Αν ναι, θεωρείτε ότι απαιτείται ενημέρωση για νέα ήδη κακόβουλων λογισμικών και συνεχής επιμόρφωση ;
10. Τι θεωρείτε πιο σημαντικό ; την έκδοση οδηγιών προς όλο το προσωπικό ή εκπαίδευση σε τεστ περιβάλλον με αναπαραγωγή επιθέσεων από κακόβουλο λογισμικό ; γιατί ;

Παράρτημα Β : Απαντήσεις συνεντεύξεων

Ερώτηση 1 : Μπορείτε σας παρακαλώ να αναφέρετε αν γνωρίζετε τις πολιτικές ασφαλείας που σχετίζονται με τα Πληροφοριακά Συστήματα της Τράπεζας ; Ειδικότερα για το e banking γνωρίζετε τις αντίστοιχες πολιτικές ;

- Απαντήσεις από OPS :
  - Όχι δεν τις γνωρίζω επακριβώς. Από μία γρήγορη σκέψη πιστεύω ότι οι πολιτικές ασφαλείας αναφέρονται στην σωστή χρήση των κωδικών και όσο πιο σύνθετοι είναι τόσο το καλύτερο.
  - Νομίζω ότι οι πολιτικές ασφαλείας αναφέρουν ότι δεν πρέπει να αποθηκεύω τους κωδικούς μου και να τους γνωστοποιώ σε τρίτους.
  - Όχι δεν τις γνωρίζω καθόλου. Δεν θυμάμαι αν μας τις έχουν στείλει αλλά και αν ακόμα τις έχουν στείλει πιθανόν να μην έχω δώσει την δέουσα προσοχή.
  - Ναι τις γνωρίζω. Αφορούν την σωστή χρήση των emails που παραλαμβάνουμε, την σωστή χρήση διαδικτύου, τους κωδικούς πρόσβασης. Δηλαδή θα πρέπει να προσέχουμε το περιεχόμενο των emails και τον αποστολέα, οι κωδικοί θα πρέπει να είναι προσωπικοί και να τηρούνται όλες οι οδηγίες που δίδονται κλπ.
- Απαντήσεις από LAdmin :
  - Ναι τις γνωρίζω επακριβώς. Οι πολιτικές ασφαλείας θεσπίζονται προκειμένου να διαφυλάξουμε τα συμφέροντα της Τράπεζας αλλά και τα δικά μας. Πρέπει συγκεκριμένοι άνθρωποι να κάνουν συγκεκριμένες εργασίες (οι κοινώς λεγόμενοι εξουσιοδοτημένοι χρήστες), τα συστήματα και οι πλατφόρμες πρέπει να είναι ακέραιες και διαθέσιμες. Συμπεριλαμβάνουν την χρήση emails, λογισμικών κλπ. Είναι η φύση της εργασίας μου τέτοια που οφείλω να γνωρίζω τις πολιτικές.
  - Ασφαλώς και τις γνωρίζω. Οι πολιτικές ασφαλείας αφορούν όλους τους εργαζόμενους και θεσπίζονται από το IT και τον Τομέα Οργάνωσης και Σχεδιασμού. Συνοπτικά να σας αναφέρω ότι πρόκειται για ασφαλή χρήση των συσκευών που παρέχει η Τράπεζα, ασφαλή χρήση του εταιρικού email με προσοχή στα περιεχόμενα και τους αποστολείς κλπ.
- Απαντήσεις από CLU :
  - Γνωρίζω κάποιες από αυτές αλλά όχι όλες και δεν είμαι απόλυτα σίγουρος/η γι αυτό που θα πω. Ξέρω σίγουρα ότι οι κωδικοί ασφαλείας πρέπει να είναι προσωπικοί και σύνθετοι. Επίσης πρέπει να είμαστε προσεκτικοί στο διαδίκτυο.

- Όχι δεν τις θυμάμαι. Τις έχω διαβάσει πριν αρκετό καιρό αλλά θεώρησα ότι δεν είναι τόσο σημαντικό αφού εμπιστεύομαι όλα όσα λαμβάνω σε email και ο κωδικός πρόσβασης είναι κάτι εύκολο που χρησιμοποιώ παντού.

➢ Απαντήσεις από TrAs :

- Όχι δεν τις γνωρίζω καθόλου, φαντάζομαι μιλούν για θέματα φυσικής ασφάλειας στο κτίριο
- Δεν είμαι απόλυτα σίγουρος/η αλλά πρέπει να μιλάνε για το πώς πρέπει να δημιουργούμε σύνθετους κωδικούς ασφαλείας.
- Όχι δεν τις ξέρω, ο φόρτος εργασίας είναι τέτοιος που δεν έχω ασχοληθεί όσο θα έπρεπε με το θέμα αυτό
- Δεν τις ξέρω καθώς δεν έχω πολύ καιρό που βρίσκομαι σ' αυτό το τμήμα. Φαντάζομαι κάθε τμήμα έχει και διαφορετικές όπως ακριβώς οι διαδικασίες.
- Βεβαίως και τις γνωρίζω. Οι πολιτικές ασφαλείας έχουν σκοπό την προστασία της Τράπεζας από εμάς τους ίδιους προσέχοντας σε ποιες ιστοσελίδες εισερχόμαστε, τι κατεβάζουμε από το ίντερνετ γενικά. Οφείλουμε να προσέχουμε τους κωδικούς πρόσβασης να είναι προσωπικοί, σύνθετοι και να μην έχουν ημερομηνίες γέννησης.
- Όχι δεν τις ξέρω. Δεν τις έχω διαβάσει αν και ξέρω ότι μπορώ να τις βρω μέσα από τους επικεφαλής των αντίστοιχων τμημάτων.

<u>Ερώτηση 2</u> : Μπορείτε σας παρακαλώ να περιγράψετε με λίγα λόγια τι ακριβώς είναι το Malware ή αλλιώς κακόβουλο λογισμικό ;

➢ Απαντήσεις από OPS :

- Κακόβουλο λογισμικό είναι όταν κάποιος προσπαθεί να σε μπερδέψει και να σου κλέψει τους κωδικούς και ύστερα να προκαλέσει πρόβλημα στον υπολογιστή σου.
- Είναι κάθε προσπάθεια από έναν εξωτερικό χρήστη να υποκλέψει προσωπικές πληροφορίες.
- Κακόβουλο λογισμικό είναι επί της ουσίας εγκατάσταση λογισμικού άγνωστου προς εμάς με σκοπό να συλλέξει προσωπικές πληροφορίες, κωδικούς ή να αντιγράφει την διεύθυνση ip μας και να την οικειοποιείται αυτός με ότι αυτό συνεπάγεται. Σκοπός επίσης είναι το να αποσπάσει χρήματα από εμάς ή ακόμα και να δημιουργήσει πρόβλημα στην λειτουργία του υπολογιστή μέσω εγκατάστασης ιών.

- Δεν ξέρω ακριβώς αλλά πιστεύω ότι είναι οτιδήποτε έχει να κάνει με ιούς που εγκαθίστανται στον υπολογιστή.

- Απαντήσεις από LAdmin :
  - Κακόβουλο λογισμικό είναι εγκατάσταση άγνωστου λογισμικού με σκοπό την υποκλοπή ευαίσθητων πληροφοριών, προσωπικών δεδομένων (πχ. κωδικών) προκειμένου να προκληθεί πρόβλημα στη λειτουργία του υπολογιστή ή ανάληψη/μεταφορά χρηματικών ποσών.
  - Είναι προγράμματα τα οποία προκαλούν προβλήματα στην λειτουργία του υπολογιστή. Πολλές φορές ο εισβολέας αποκτάει τον έλεγχο του υπολογιστή μας ζητώντας την καταβολή ποσού για να αποδεσμεύσει τυχόν αρχεία. Τύπου τέτοιου λογισμικού είναι οι ιοί, τα Trojans.
- Απαντήσεις από CLU :
  - Δεν είμαι σίγουρος/η αλλά νομίζω ότι είναι κάθε πρόγραμμα που δεν τηρεί τις προδιαγραφές και δημιουργεί πρόβλημα στην λειτουργία του συστήματος.
  - Κακόβουλο λογισμικό θεωρείται όταν κάποιος προσπαθεί να σου υποκλέψει τις προσωπικές σου πληροφορίες.
- Απαντήσεις από TrAs :
  - Είναι λογισμικό που στρέφεται κατά της Τράπεζας και του πελάτη δημιουργώντας πιθανόν πρόβλημα στο σύστημα και στις συναλλαγές.
  - Είναι προγράμματα που κατεβαίνουν στα χρησιμοποιούμενα devices, μέσω των οποίων μπορούν να ληφθούν προσωπικές πληροφορίες και όχι μονό που χρησιμοποιούνται από τρίτους. Αυτά τα προγράμματα περιλαμβάνουν ιούς που καταστρέφουν αρχεία ή προκαλούν γενικότερη δυσλειτουργία.
  - Κακόβουλο λογισμικό είναι το πρόγραμμα εκείνο που έχει ρυθμιστεί από τον προγραμματιστή του έτσι ώστε να προκαλέσει βλάβες σε ένα υπολογιστικό σύστημα.
  - Η εγκατάσταση άγνωστου λογισμικού με σκοπό την υποκλοπή ευαίσθητων πληροφοριών, προσωπικών δεδομένων (πχ. κωδικών) προκειμένου να προκληθεί πρόβλημα στη λειτουργία του υπολογιστή ή ανάληψη/μεταφορά χρηματικών ποσών.
  - Λογισμικό το οποίο μπορεί να οδηγήσει σε διαγραφή ή απόκτηση δεδομένων από τρίτο χρήστη και το οποίο αποστέλλεται είτε μέσω ηλεκτρονικού μηνύματος είτε μέσω download από σελίδες στο internet.

- Δεν γνωρίζω ακριβώς αλλά πιστεύω ότι πρόκειται για ενέργειες υπαλλήλων οι οποίοι για προσωπικούς λόγους προσπαθούν να δημιουργήσουν πρόβλημα στην Τράπεζα σβήνοντας αρχεία και εγκαθιστώντας άλλα.

Ερώτηση 3 : Μπορείτε να μας πείτε δύο κατηγορίες από κακόβουλο λογισμικό ; αν δεν γνωρίζετε μπορείτε να σκεφτείτε ;

- Απαντήσεις από OPS :
  - Όχι δεν γνωρίζω κάποια κατηγορία. Πιθανολογώ ότι σ' αυτά εντάσσονται οι ιοί.
  - Γνωρίζω σίγουρα τους ιούς. Αλλά δεν ξέρω κάποια άλλη κατηγορία από αυτούς.
  - Πιστεύω πως θα μπορούσε να είναι οι ιοί και τα spam mails.
  - Δεν ξέρω κάποια κατηγορία ή υποκατηγορία παρά μόνο τους εντάσσω σε ένα γενικό σύνολο που ονομάζονται ιοί.
- Απαντήσεις από LAdmin :
  - Δύο μεγάλες κατηγορίες είναι οι ιοί και τα σκουλήκια.
  - Σίγουρα είναι οι ιοί. Ωστόσο από πρόσφατη έρευνα που διάβασα στο ίντερνετ και σε συνδυασμό με τις μεγάλες κυβερνοεπιθέσεις που έγιναν πριν λίγους μήνες (περίπου τέλη Μαΐου) θεωρούνται και τα Trojans.
- Απαντήσεις CLU :
  - Δεν ξέρω να σας πω δύο αλλά σίγουρα είναι οι ιοί.
  - Μπορούμε να πούμε τους ιούς και τα spywares που τα θυμάμαι από κάποιο μάθημα του Πανεπιστημίου
- Απαντήσεις TrAs :
  - Δύο κατηγορίες είναι οι ιοί και οι κυβερνοεπιθέσεις όπως έγινε και πρόσφατα.
  - Είναι οι ιοί. Δεν ξέρω κάποια άλλη αυτή την στιγμή. Ιούς εννοώ τα πάντα που μπορούν να βλάψουν ένα σύστημα.
  - Δεν ξέρω κάτι άλλο πέρα από τους ιούς.
  - Οι ιοί είναι σίγουρα μια κατηγορία. Δυστυχώς δεν έχω κάτι άλλο που μπορώ να σκεφτώ αφού με ο όρος ιός είναι πολύ διαδεδομένος και χρησιμοποιείται ευρέως.
  - Θεωρώ σίγουρα ότι είναι οι ιοί και από εκεί και πέρα τα ύποπτα emails που περιέχουν κακόβουλα προγράμματα.
  - Γνωρίζω μόνο τους ιούς σαν γενική κατηγορία που συμπεριλαμβάνει τα πάντα.

<u>Ερώτηση 4</u> : Γνωρίζετε τις συνέπειες που μπορεί να προκαλέσει ένα κακόβουλο λογισμικό στην Τράπεζα ;

- Απαντήσεις από OPS :
  - Ναι τις γνωρίζω : κλοπή δεδομένων, κλοπή ή διαγραφή αρχείων, μπλοκάρισμα τερματικού
  - Ναι τις γνωρίζω. Κλοπή προσωπικών δεδομένων είναι ένα παράδειγμα.
  - Ναι, μία από τις συνέπειες είναι η προσπάθεια του εισβολέα να παρακολουθήσει τα ίχνη μας και εν συνεχεία να τις εκμεταλλευτεί εναντίον μας
  - Ένα κακόβουλο λογισμικό μπορεί να «ρίξει» ένα υπολογιστικό σύστημα ή να τοποθετήσει ιό ο οποίος θα αντλεί πληροφορίες μέσω των κινήσεων του χρήστη και να προκαλέσει βλάβες, ειδικότερα εάν έχει την δυνατότητα εκείνη να προσαρμόζεται στις τυχόν αλλαγές που γίνονται για την αντιμετώπισή του.
- Απαντήσεις από LAdmin :
  - Προσπάθεια κλοπής προσωπικών δεδομένων και κλοπής αρχείων που σκοπό έχουν να βλάψουν τόσο προσωπικά τον εργαζόμενο αλλά και την ίδια την Τράπεζα.
  - Κλοπή αρχείων και πελατολογίων της Τράπεζας με σκοπό την χρήση τους από τον εισβολέα ή την απαίτηση για καταβολή χρημάτων.
- Απαντήσεις από CLU :
  - Σκοπός σε μια τέτοια περίπτωση είναι η καταστροφή αρχείων της Τράπεζας και δυσφήμισή της καθώς οι επιθέσεις που γίνονται τον τελευταίο καιρό έχουν στο στόχαστρο τους τις Τράπεζες γενικότερα.
  - Δημιουργία σύγχυσης στους χρήστες καθώς σε μια τέτοια περίπτωση τα συστήματα δεν ανταποκρίνονται με σκοπό να μην εκτελούνται καθημερινές εργασίες.
- Απαντήσεις από TrAs :
  - Το πιθανότερο είναι ότι αυτοί που επιδιώκουν τέτοιους είδους ενέργειες είναι το να υποκλέψουν σημαντικά στοιχεία της Τράπεζας για δικό τους όφελος.
  - Πρόσφατα διάβασα στο ίντερνετ ότι τέτοιου είδους ενέργειες γίνονται ολοένα και πιο συχνά στις Τράπεζες (Anonymous) και σκοπός είναι να βλάψουν τα συστήματα που διαθέτουμε δημιουργώντας πρόβλημα στην γενικότερη λειτουργία

- Προφανώς τα κίνητρα μιας τέτοιας ενέργειας με κακόβουλα λογισμικά είναι η δυσφήμιση της Τράπεζας.
- Τις πιο πολλές φορές συμβαίνει για κλοπή δεδομένων όπως τα χαρτοφυλάκια της Τράπεζας, λογαριασμούς κλπ
- Συνήθως αυτός που προσπαθεί να αποκτήσει πρόσβαση στα συστήματα της Τράπεζας το κάνει για να έχει στοιχεία από την βάση δεδομένων και να τα εκμεταλλευτεί για δικό του όφελος.
- Αν και δεν ξέρω αν έχει συμβεί κάτι τέτοιο στο παρελθόν θεωρώ πως γίνεται για κλοπή προσωπικών δεδομένων, κωδικών και λογαριασμών για απόσπαση χρημάτων.

Ερώτηση 5 : Έχετε πέσει θύμα ποτέ από ένα τέτοιου είδους κακόβουλο λογισμικό ; εάν ναι πως αντιδράσατε ;

- Απαντήσεις από OPS :
  - Όχι δεν έχει τύχει μέχρι στιγμής να εντοπίσω κάτι σχετικό. Τουλάχιστον κάτι που να ξέρω.
  - Ναι έχει τύχει μία φορά όχι βέβαια σε εργασιακό χώρο αλλά στον προσωπικό μου υπολογιστή. Ενώ βρισκόμουν σε μια σελίδα πάτησα μια pop up φόρμα που έλεγε ότι έχω 11 ιούς εγκατεστημένους και έπρεπε να τρέξω κάποιο πρόγραμμα να τους «καθαρίσει». Δεν κατάλαβα ότι αυτό το πρόγραμμα ήταν το ίδιο κακόβουλο λογισμικό. Ζήτησα άμεσα την βοήθεια τεχνικού.
  - Όχι δεν θυμάμαι να έχω αντιμετωπίσει κάποιο πρόβλημα. Στο σπίτι δεν χρησιμοποιώ πολύ τον υπολογιστή.
  - Ναι μου έχει συμβεί πριν αρκετό καιρό. Τοποθέτησα ένα στικάκι και έτρεξα ένα αρχείο exe. Από εκείνη την στιγμή και έπειτα έβγαλε μια μπλε οθόνη στην οποία δεν θυμάμαι το μήνυμα. Για την επιδιόρθωση απευθύνθηκα αμέσως σε τεχνικό ο οποίος με ενημέρωσε ότι έκανε format.
- Απαντήσεις από LAdmin :
  - Ναι μου έχει τύχει να βρω στην εισερχόμενη αλληλογραφία κάποιο mail το οποίο προέρχεται από Τράπεζα και με ενημέρωνε ότι έχω πέσει θύμα κλοπής και πρέπει να δώσω τα στοιχεία μου για να μου αντιλογίσουν το ποσό. Δεν ανησύχησα, απλά έτρεξα το antivirus.

- Έχει τύχει στο παρελθόν να εργάζομαι στο laptop και να ανοίγουν ξαφνικά παράθυρα. Έτρεξα antivirus.

- Απαντήσεις από CLU :
  - Μου έχει τύχει στην εργασία μου όπου έλαβα ένα spam email. Επικοινώνησα αμέσως με το helpdesk της Τράπεζας.
  - Πριν λίγο καιρό και ενώ βρισκόμουν στο internet πάτησα κάποιο link για να με οδηγήσει σε κάποια άλλη σελίδα αλλά αυτό γέμισε διαφημίσεις και κόλλησε ο explorer. Έκλεισα τον υπολογιστή και έκανα restart. Το πρόβλημα παρέμεινε και μίλησα με τεχνικό ο οποίος έκανε format.
- Απαντήσεις από TrAs :
  - Μου έχει τύχει και το διαπίστωσα όταν άλλαξε για κάποιο λόγο το search engine και από google με πήγαινε σε κάποιο άλλο. Ανησύχησα και το πήγα σε τεχνικό.
  - Δεν θυμάμαι να μου έχει συμβεί κάποιο περιστατικό ούτε στην δουλειά αλλά ούτε και στο σπίτι.
  - Νομίζω ότι μου έχει τύχει καθώς πριν ένα μήνα και εντελώς ξαφνικά, κόλλαγαν όλες μου οι σελίδες περιήγησης. Το πήγα σε τεχνικό και απ' ότι μου είπε ήταν ένα είδος ιού που λέγεται σκουλήκι. Έκανε format και αποκαταστάθηκε το πρόβλημα.
  - Πρόσφατα είδα μια διαφήμιση που έλεγε ότι έχω κερδίσει ένα κινητό τηλέφωνο γνωστής εταιρίας. Πάτησα στην διαφήμιση και με οδήγησε σε κάποιο Link όπου ζητούσε προσωπικά στοιχεία. Έκλεισα τον υπολογιστή και μίλησα με τεχνικό ο οποίος έκανε format.
  - Όχι δεν έχει τύχει ποτέ να πέσω θύμα κάποιου κακόβολου λογισμικού.
  - Δεν έχω αντιμετωπίσει κάτι ιδιαίτερο εκτός από ύποπτα emails τα οποία δεν ανοίγω και τρέχω πάντα antivirus.

Ερώτηση 6 : Πως θα χαρακτηρίζατε το επίπεδο ενημέρωσης του προσωπικού της Τράπεζας σχετικά με θέματα ασφάλειας ;

- Απαντήσεις από OPS :
  - Το επίπεδο θα το χαρακτήριζα μέτριο.
  - Θεωρώ πως είναι ελλιπές. Οι εξελίξεις συνεχώς αλλάζουν και απαιτείται πιο λεπτομερής καταγραφή και ενημέρωση.

- Θεωρώ πως είναι καλό. Συνεχώς έρχονται emails που μας ενημερώνουν για ό,τι πιθανόν συμβαίνει.
- Κατά την άποψη μου το προσωπικό χρίζει περισσότερης ενημέρωσης για θέματα ασφάλειας τόσο για το καλό του οργανισμού όσο και σε προσωπικό επίπεδο.

➢ Απαντήσεις από LAdmin :

- Αν και η φύση της δουλειάς είναι τέτοια που σημαίνει ότι θα πρέπει να είμαστε ενήμεροι για τις εξελίξεις σε θέματα ασφάλειας και παρόλο που η Τράπεζα συνεχώς ενημερώνει όλες τις διαδικασίες, θα χαρακτήριζα την ενημέρωση μέτρια διότι χρειάζονται άλλοι τρόποι και μέθοδοι προκειμένου να γίνουν τα μέτρα πιο κατανοητά και εφαρμόσιμα απ' όλους.
- Θα απαντήσω σε επίπεδο συνόλου και όχι σε προσωπικό επίπεδο. Διότι αλλιώς τα αντιλαμβάνεται ο κάθε ένας και ανάλογα με την θέση εργασίας του. Νομίζω πως είναι μέτρια και θα πρέπει να βρεθούν δραστικότερα μέτρα για την ενημέρωση του προσωπικού.

➢ Απαντήσεις από CLU :

- Πιστεύω πως είναι ελλιπής η ενημέρωση. Στην πράξη ενημερωνόμαστε από παλαιούς συναδέλφους ή από το internet μέσα από διάφορα πραγματικά γεγονότα.
- Η ενημέρωση του προσωπικού για τέτοια θέματα κρίνεται από μέρους μου μέτρια καθώς έρχονται συνεχώς ενημερώσεις αλλά δεν ξέρω κατά πόσο ο κόσμος τις μελετάει. Άρα χρειάζεται κάτι άλλο προκειμένου να κεντρίσει το ενδιαφέρον.

➢ Απαντήσεις από TrAs :

- Η ενημέρωση γενικότερα είναι μέτρια. Θα έπρεπε να είναι συχνότερη.
- Μέτρια διότι δίνεται προτεραιότητα στις καθημερινές εργασίες αλλά όχι τόσο στην εκτέλεση αυτών με ασφάλεια.
- Πιστεύω πως είναι καλή αν αναλογιστεί κανείς ότι σε κάθε περίπτωση μας στέλνουν ενημέρωση από το IT για αυτά τα περιστατικά.
- Περίμενα κάτι περισσότερο γιατί οι εξελίξεις τρέχουν και οι απατεώνες βρίσκουν τρόπους να ξεπερνάνε κάθε εμπόδιο σε επίπεδο ασφάλειας. Άρα καλό είναι να ενημερωνόμαστε πιο συχνά.
- Δεν έχω ενημερωθεί όσο καιρό είμαι στο κομμάτι αυτό. Άρα δεν μπορώ να πω κάτι άλλο παρά ελλιπές παρά το γεγονός ότι σίγουρα η Τράπεζα ενημερώνει. Ό,τι έχω μάθει είναι από τους συνεργάτες μου.
- Είναι μέτρια η ενημέρωση καθώς όταν και όποτε γίνει, είναι μέσα από κάποιο email που λίγοι δίνουν σημασία.

Ερώτηση 7 : Ποιοι πιστεύετε ότι είναι οι κυριότεροι λόγοι που συντελούν στην παραβίαση του e banking ; αν γνωρίζετε παρακαλώ παραθέστε μας δύο παραδείγματα. Αν όχι παρακαλώ μπορείτε να σκεφτείτε δύο περιπτώσεις ;

- Απαντήσεις από OPS :
  - Δύο λόγοι είναι η προσωπική αμέλεια και η χρήση μη ασφαλών passwords
  - Μόνο η κλοπή passwords. Δεν μπορώ να σκεφτώ κάτι άλλο
  - Είναι η κλοπή των passwords αλλά και επίσης είναι ιοί που εγκαθίστανται στον υπολογιστή και καταγράφουν όσα πληκτρολογείς.
  - Νομίζω ότι είναι μόνο το σπάσιμο του password. Αν είναι σύνθετο τότε δεν πιστεύω ότι υπάρχει σοβαρός κίνδυνος.
- Απαντήσεις από LAdmin :
  - Σίγουρα είναι τα προγράμματα που είναι ικανά να σπάσουν τους κωδικούς αλλά και τα spywares.
  - Ο ανθρώπινος παράγοντας είναι κρίσιμος καθώς από δικά του λάθη και αστοχίες εκθέτει τον εαυτό του σε κίνδυνο όπως με ένα εύκολο password ή με το να πατήσει σε Link που δεν είναι της Τράπεζας αλλά απατεώνων.
- Απαντήσεις από CLU :
  - Μόνο εάν το site δεν είναι ασφαλές και είναι σε κάποιο κλώνο του αυθεντικού.
  - Δεν γνωρίζω κάποιους λόγους για το πώς μπορεί να παραβιαστεί το e banking.
- Απαντήσεις από TrAs :
  - Νομίζω ότι είναι η κλοπή του Password. Δεν ξέρω κάτι άλλο που να συντελεί κίνδυνο.
  - Πιστεύω ότι τα προγράμματα που τυχόν κάποιος κατεβάσει εμπεριέχουν ιούς που υποκλέπτουν τους κωδικούς αλλά και ιστοσελίδες του e banking οι οποίες είναι ψεύτικες.
  - Προσωπική αμέλεια μπορεί να δώσει την ευκαιρία σε κάποιον να κλέψει τους κωδικούς μου. επίσης θα μπορούσα να πω ότι υπάρχουν περιπτώσεις από διάφορα mails που σε παραπέμπουν σε κάποιες πλατφόρμες που μοιάζουν με την επίσημη ιστοσελίδα της Τράπεζας.
  - Δυστυχώς δεν γνωρίζω.
  - Είναι η κλοπή των κωδικών για υπεξαίρεση χρημάτων και η χρησιμοποίηση μη ασφαλούς browser.

- Τα ύποπτα pop ups που μπορεί να φαίνονται από Τράπεζα ακόμα και ψεύτικα μηνύματα στο κινητό προκειμένου να πατήσεις στο Link που αναφέρουν και να οδηγηθείς μέσω κινητού σε ψεύτικη σελίδα.

Ερώτηση 8 : Μελέτες στο εξωτερικό έχουν δείξει ότι ο μεγάλος κίνδυνος για την επίθεση από κακόβουλο λογισμικό προέρχεται από τον ίδιο τον ανθρώπινο παράγοντα και λάθη στα οποία υποπίπτει. Συμφωνείτε ως προς αυτό ;

- Απαντήσεις από OPS :
  - Συμφωνώ, μιας και η κακή και μη συμμορφούμενη στους κανόνες χρήση αποτελεί τις περισσότερες φορές τον κύριο παράγοντα για να αποτελέσει κάποιος στόχο από κακόβουλο λογισμικό.
  - Ναι εφόσον δεν λαμβάνονται σοβαρά τα θέματα ασφαλείας ή δεν μελετώνται σωστά οι ενημερώσεις από την Τράπεζα.
  - Σίγουρα ο ανθρώπινος παράγοντας έχει κρίσιμη σημασία στην ασφάλεια από κακόβουλο λογισμικό.
  - Από τη στιγμή που σε ένα σύστημα υπεισέρχεται ο άνθρωπος τότε σίγουρα αποτελεί κίνδυνο.
- Απαντήσεις από LAdmin :
  - Εννοείται ότι αποτελεί απειλή καθώς η αμέλεια που μπορεί να επιδείξει μπορεί να αποβεί καταστροφική.
  - Φυσικά και αποτελεί την νούμερο 1 απειλή καθώς από τον άνθρωπο κατασκευάζονται αυτά τα λογισμικά.

- Απαντήσεις από CLU :
  - Εξυπακούεται πως αποτελεί απειλή και μάλιστα μεγάλη αν αναλογιστεί κανείς και την σύγχρονη ιστορία.
  - Σαφώς είναι απειλή αφού ακατάλληλα άτομα μπορούν να αποκτήσουν προσβάσεις σε σημαντικές πληροφορίες.
- Απαντήσεις από TrAs :
  - Συμφωνώ ότι ο άνθρωπος αποτελεί απειλή καθώς άθελά του μπορεί να διαγράψει αρχεία, να εγκαταστήσει λογισμικά, να τροποποιήσει βάσεις δεδομένων.

- Ο άνθρωπος ίσως αποτελεί την μεγαλύτερη απειλή όλων καθώς η απληστία και η δόξα τον καθιστούν αδίστακτο.
- Βεβαίως και είναι απειλή αφού από αυτόν ξεκινάνε οι επιθέσεις αυτές
- Ναι είναι απειλή και μάλιστα ο ιθύνων νους στις περισσότερες των περιπτώσεων.

Ερώτηση 9 : Α) Έχουν γίνει ειδικά σεμινάρια για ενημέρωση, πρόληψη και προστασία από κακόβουλο λογισμικό ; Β) Αν όχι, πιστεύετε ότι είναι απαραίτητο να γίνουν αυτά τα σεμινάρια ; Γ) Αν ναι, θεωρείτε ότι απαιτείται ενημέρωση για νέα ήδη κακόβουλων λογισμικών και συνεχής επιμόρφωση ;

- Απαντήσεις από OPS :
  - Όχι δεν έχουν γίνει κάποια ειδικά σεμινάρια και κρίνεται επιβεβλημένο πλέον να γίνονται.
  - Όχι δεν θυμάμαι να έχω παρευρεθεί σε κάτι τέτοιο. Νομίζω πως είναι απαραίτητο.
  - Όχι δεν έχει γίνει κάτι σχετικό και κρίνεται απαραίτητο να γίνει.
  - Όχι δεν έχει λάβει χώρα τέτοιο σεμινάριο και θεωρώ ότι δεν είναι απαραίτητο.
- Απαντήσεις από LAdmin :
  - Όχι δεν έχει διοργανωθεί τέτοιο σεμινάριο και καλό είναι να γίνεται και μάλιστα σε συχνή βάση.
  - Όχι και πρέπει να γίνονται σε ετήσια βάση τουλάχιστον 2 διότι οι απατεώνες εφευρίσκουν καινούρια κακόβουλα λογισμικά.
- Απαντήσεις από CLU :
  - Απ' όσο θυμάμαι ουδέποτε έχουν γίνει. Μετά από αυτή την συνέντευξη διαπιστώνω ότι είναι απαραίτητο.
  - Σίγουρα δεν έχουν γίνει και θεωρώ ότι τελικά πρέπει να γίνονται για να ενημερωνόμαστε για όλες τις απειλές.
- Απαντήσεις από TrAs :
  - Πέρα από τις ενημερώσεις που μας έρχονται, δεν έχει γίνει κάτι σχετικό σε επίπεδο σεμιναρίου ενώ βλέπουμε ότι πρέπει να γίνονται.
  - Όχι και κρίνεται σκόπιμο να ενημερωθούμε πιο αναλυτικά από τους αρμόδιους.
  - Όχι και καλό θα είναι να μεριμνήσει η Τράπεζα και να εντάξει τέτοιους είδους εκπαιδεύσεις.

- Δεν έχει γίνει και θεωρώ απαραίτητο να γίνεται διότι αποκομίζουμε και προσωπικό όφελος καθώς διαχειριζόμαστε ηλεκτρονικούς υπολογιστές, τάμπλετς, κινητά σε καθημερινή βάση.
- Όχι και θα ήθελα να γίνεται κάτι τέτοιο ακόμα και σε μορφή e learning.
- Δεν έχουμε κάνει κάποιο τέτοιο σεμινάριο. Νομίζω ότι απαιτείται διότι είναι στα πλαίσια των Τραπεζικών μας καθηκόντων να τηρούμε τις διαδικασίες και τους κανόνες ασφαλείας.

Ερώτηση 10 : Τι θεωρείτε πιο σημαντικό ; την έκδοση οδηγιών προς όλο το προσωπικό ή εκπαίδευση σε τεστ περιβάλλον με αναπαραγωγή επιθέσεων από κακόβουλο λογισμικό ; γιατί ;

- Απαντήσεις από OPS :
  - Θεωρώ ότι πρέπει να γίνονται και τα δύο καθώς η θεωρία εξομοιώνεται αποτελεσματικά και σε τεστ περιβάλλον.
  - Οπωσδήποτε πρέπει να γίνονται και τα δύο καθώς το ένα συμπληρώνει το άλλο.
  - Χρειάζονται και τα δύο. Και η γραπτή ενημέρωση βοηθάει αλλά η αναπαραγωγή τέτοιων περιπτώσεων συμβάλλει στην πλήρη κατανόηση.
  - Πιστεύω ότι χρειάζεται να γίνεται μόνο σε τεστ περιβάλλον γιατί στην πράξη τις οδηγίες δεν τις διαβάζει κανείς.
- Απαντήσεις από LAdmin :
  - Σίγουρα και τα δύο. Είναι προτιμότερο να δεις στην πράξη – εκτός από την θεωρία – πως ακριβώς δρα ένα τέτοιο λογισμικό.
  - Και οι τρόποι είναι σημαντικοί γιατί έτσι όλοι οι εργαζόμενοι θα έχουν «βιώσει» μια δυσάρεστη κατάσταση και θα δουν τί επιπτώσεις επέρχονται σε επίπεδο Τράπεζας και αξιοπιστίας
- Απαντήσεις από CLU :
  - Νομίζω ότι επειδή οι οδηγίες είναι αρκετά περίπλοκες έχω την άποψη ότι πρέπει να τα βλέπουμε σε τεστ περιβάλλον για να κατανοούμε πλήρως την επικινδυνότητα
  - Χρειάζονται και τα δύο καθώς το κάθε ένα έχει την δικιά του σκοπιμότητα και χρησιμότητα.
- Απαντήσεις από TrAs :
  - Και τα δύο. Στην μεν πρώτη περίπτωση διότι η έκδοση οδηγιών είναι κάτι πιο άμεσο και εύχρηστο προς το προσωπικό και στη δε δεύτερη περίπτωση ένα εξειδικευμένο σεμινάριο 1 με 2 φορές τον χρόνο θα φέρει πιο κοντά τον υπάλληλο με μια πραγματικότητα της οποίας κοινωνός γίνεται άμεσα κάθε μέρα.

- Κατά την γνώμη μου η εκπαίδευση του προσωπικού με σεμινάρια σε τεστ περιβάλλοντος βοηθάει καλύτερα στην ορθότερη γνώση και αντίληψη των πραγμάτων.
- Απαιτούνται και τα δύο. Οι οδηγίες να δίνονται όσο πιο συχνά γίνονται και να είναι επικαιροποιημένες σύμφωνα με τις εξελίξεις ενώ μια φορά τον χρόνο πρέπει να γίνεται και η ανάλογη εκπαίδευση σε τεστ περιβάλλον.
- Επειδή και τα δύο είναι αλληλένδετα, πιστεύω ότι πρέπει να γίνονται και τα δύο.
- Ξεκάθαρα η Τράπεζα πρέπει να επενδύσει και στην εκπαίδευση εκτός από την θεωρία.
- Θα είναι πρωτοποριακό να γίνει μια αναπαραγωγή τέτοιων περιστατικών σε τεστ περιβάλλον με θύματα εμάς του ίδιους. Θεωρία και πράξη σε πλήρη εξέλιξη.

Βιβλιογραφία και Αναφορές

1. Milosevic Nikola, History of Malware, 2013

2. Ενωση Ελληνικών Τραπεζών, Internet Banking : Νομικά Ζητήματα από την Διεξαγωγή Τραπεζικών συναλλαγών στο διαδίκτυο 2003

3. Aggelopoulos, Michiotis, E-banking: challenges and opportunities in the Greek banking sector, 2011

4. Kruegel, Fighting Malicious Software, 2012

5. Steven Furnell, Jeremy Ward, Malware comes of age: The arrival of the true computer parasite, 2004

6. Aburrous, Maher, Hossain, Alamgir, Dahal, Keshav and Thabtah, Fadi, Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies. Journal of Cognitive Computation, 2010 3

7. Antonio San Martino and Xavier Perramon, Phishing Secrets: History, Effects, and Countermeasures, 2009

8. K. C. Laudon, J. P. Laudon, Πληροφοριακά Συστήματα Διοίκησης - Διοίκηση της ψηφιακής επιχείρησης, 2006

9. K. C. Laudon, C. G. Traver, Επιμέλεια Γ. Γκαντζιάς, Ηλεκτρονικό εμπόριο - Επιχειρήσεις, Τεχνολογία, Κοινωνία, 2014

10. Παπασωτηρίου, Ασφάλεια Δικτύων Υπολογιστών, 2003

11. Σ. Κ. Κάτσικας, Δ. Γκρίτζαλης, Ασφάλεια Πληροφοριακών Συστημάτων, 2004

12. Sam Johnson, Nick Twilley, Tianyi Zhang, Zhanni Zhou, & Suijun Wu, Mobile Computing, 2014

13. Morten Hertzum, Niels Jørgensen, Mie Nørgaard, usable security and e-banking: ease of use vis-à-vis security, 2004

14. Koskosas Ioannis, E-banking security: A communication perspective, 2011

15. Microsoft, Defining Malware: FAQ, 2003.

16. Kaspersky Lab, Report On DDoS Attacks In Q1 2017: The Lull Before The Storm, 2017

17. Albrechtsen and Hovden, Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study, 2010

18. Kirsty Vaughan and Anna MacVicar, Employees, pre-implementation attitudes and perceptions to e-learning A banking case study analysis, 2004

19. Laerte Peotta, Marcelo D. Holtz, Bernardo M. David, Flavio G. Deus, Rafael Timóteo de Sousa Jr, A formal classification of internet banking attacks and vulnerabilities, 2011

20. Francois Mouton, Louise Leenen a, H.S. Venter, Computers and Security, 2016

21. Seppo Pahnila, Mikko Siponen and Adam Mahmoodb, Employees' Behavior towards IS Security Policy Compliance, 2007

22. Petri Puhakainen, Mikko Siponen, improving employees' compliance through Information systems security training, 2010

23. R.S. Shaw, Charlie C. Chen, Albert L. Harris, & Hui-Jou Huang, The Impact Of Information Richness On Information Security Awareness Training Effectiveness, 2009

24. M.E. Thomson, R. von Solms, Information security awareness: educating your users effectively, 2009

25. Bilal Khan, Khaled S. Alghathbar, Syed Irfan Nabi1, and Muhammad Khurram Khan, Effectiveness of information security awareness methods based on psychological theories, 2011

26. Thomas Thostheim, Security Analysis of electronic voting and online banking systems, 2007

27. OECD, Guidelines for the Security of Information Systems and Networks, 2002

28. Benjamin D. Cone, Cynthia E. Irvine, Michael F. Thompson, Thuy D. Nguyen, A video game for cyber security training and awareness, 2007.

29. HJ Rubin, IS Rubin, Qualitative interviewing : the art of hearing data, 2011

30. Nicol Korner-Bitenski, Sharon Wood-Dauphinee, Stanley Shapiro, Rubin Becker, Health-Related Information Postdischarge: Telephone Versus Face-to-Face Interviewing, 1994

31. Βασίλης Ν. Κέφης, Διοίκηση Ολικής Ποιότητας, 2014

32. J. Bank, Μάνατζμεντ Ολικής Ποιότητας, 2000

33. https://haystax.com/

34. https://www.nuix.com/

35. http://kasperskycontenthub.com/presscenter/files/2014/06/Kaspersky_Report_Mobile_Malware_Evolution_2013.pdf

36. https://www.pcsteps.gr/category/software/hlektroniki-asfaleia/

37. http://www.cnn.gr/tech/story/55871/prosoxi-ayta-einai-ta-25-xeirotera-passwords-toy-kosmoy

38. https://en.wikipedia.org/wiki/Malware

39. https://en.wikipedia.org/wiki/Principle_of_least_privilege

40. https://en.wikipedia.org/wiki/Defense_in_depth_(computing)

41. http://www.piraeusbank.gr/el/idiwtes/trapezikes-ypiresies/e-banking/asfaleia-synallagon

42. https://www.alpha.gr/e-banking/gr/upostirixi-asfaleia/hrisima-eggrafa-ergaleia/

43. https://el.wikipedia.org/wiki/dialektiki