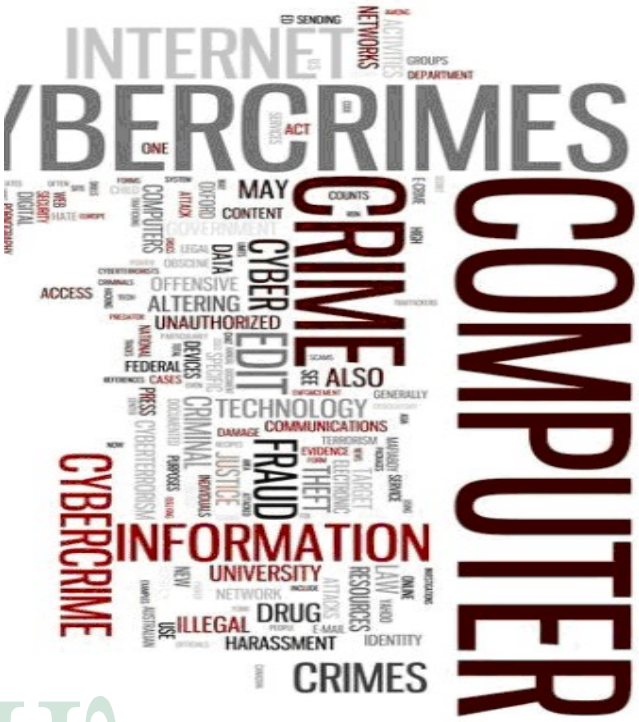
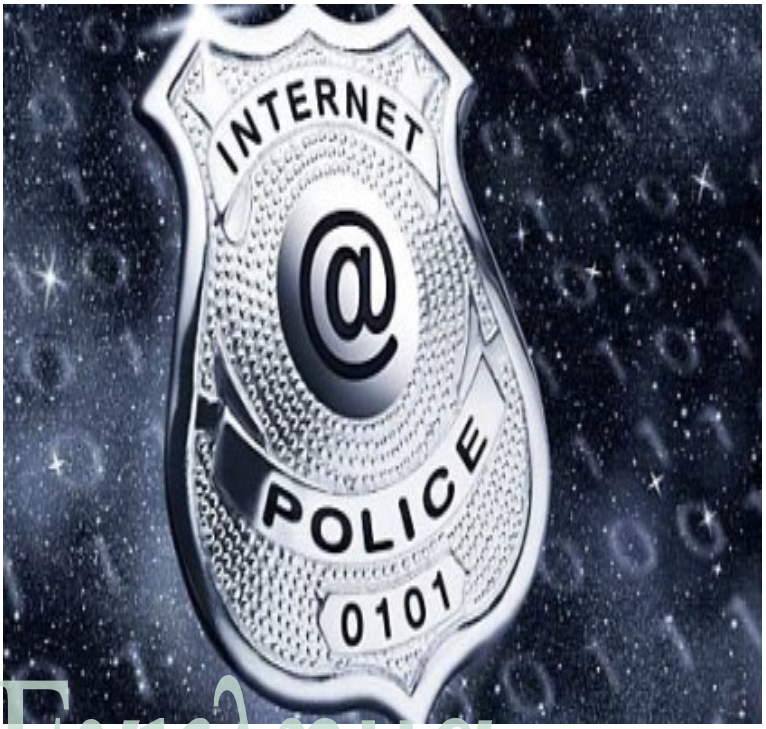
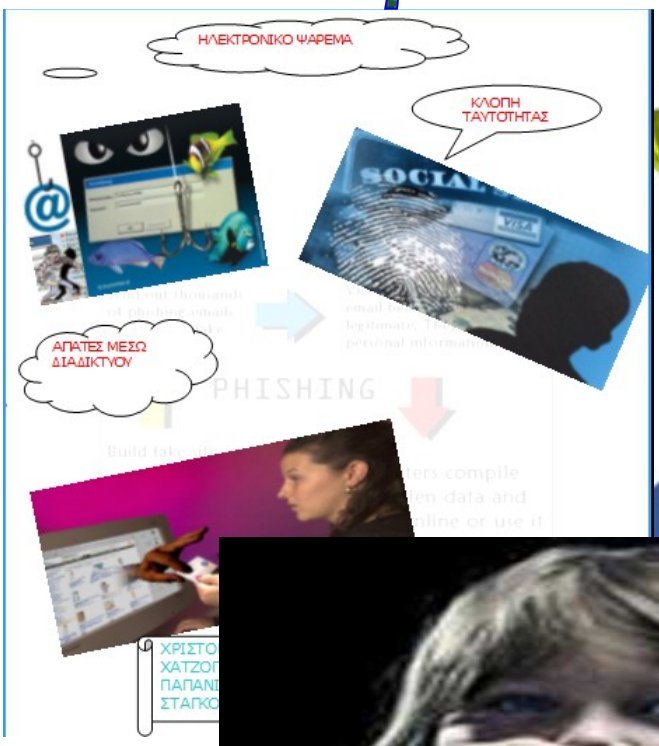




Ηλεκτρονικό Έγκλημα

Ηλεκτρονικό Έγκλημα



Περιεχόμενα

Περιεχόμενα....2
Η εργασία αυτή υλοποιήθηκε στα πλαίσια του μαθήματος «Ερευνητική εργασία»....5
Σχολικό έτος 2013-2014....5
Εργάστηκαν οι μαθητές του Β2 5
Η κάθε ομάδα ασχολήθηκε με τα παρακάτω διδακτικά αντικείμενα....5
Εισαγωγή....6
Ορισμός του ηλεκτρονικού εγκλήματος....6
Χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο....7
Αρχές που Εποπτεύουν την Προστασία του Διαδικτύου στην Ελλάδα 10
Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα....10
Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών....11
Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων....12
Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος....13
Μορφές Ηλεκτρονικού εγκλήματος 13
Κεφάλαιο1 14
Hacking & Cracking....14
Ορισμός του Hacker 14
Κατηγορίες των Hackers....14
Τρόπος Δράσης – Επιθέσεις των hacker....15
Επιπτώσεις Δράσης....16
Ελληνική νομοθεσία έναντι του Hacking/Cracking....17
Κεφάλαιο2....19
Πειρατεία Λογισμικού Η/Υ....19
Ορισμός....19
Πειρατεία στο Internet - το πρόβλημα και η αντιμετώπιση....19
Πιθανές συνέπειες από τη χρήση πειρατικού λογισμικού;....19
Ελληνική νομοθεσία έναντι της Πειρατεία Λογισμικού....19
Κεφάλαιο3....21
Τρομοκρατία και Διαδίκτυο.- Νέα τάξη Πραγμάτων....21
Καταπολέμηση της τρομοκρατίας στο διαδίκτυο: Ασφάλεια ή Απειλή;;; 22
Κεφάλαιο4....27
CYBER-BULLYING....27
Ορισμός....27
Αίτια....27
Μορφές Διαδικτυακού εκφοβισμού....27
Συνέπειες....28
Τρόποι αντιμετώπισης 28
Νομοθεσία....29
FACEBOOK....30
Κεφάλαιο 5....31
Ξέπλυμα μαύρου χρήματος 31
Ορισμός μαύρου χρήματος....31
Ψηφιακά νομίσματα....33

Περιεχόμενα

Επιπτώσεις του ξεπλύματος χρήματος....34
Οδηγίες εντοπισμού ύποπτων συναλλαγών για «ξέπλυμα μαύρου χρήματος»....35
Κεφάλαιο 6....38
Παιδική Πορνογραφία....38
Τι είναι παιδική πορνογραφία....38
Κίνδυνοι Κοινωνικών Δικτύων (Facebook)....39
Πραγματική περίσταση αληθούς γεγονότος....41
Πρόληψη γονέων για την παιδική πορνογραφία....42
Πού μπορεί να συμβεί:....43
Νομοθεσία παιδικής πορνογραφίας....44
Κεφάλαιο 7....46
Διακίνηση ναρκωτικών μέσω υπολογιστή....46
Στοιχεία της παραβατικότητας στην κοινωνία της....46
Αποτέλεσμα....47
Κεφάλαιο 8....48
Ηλεκτρονικό ψάρεμα (phishing)....48
Κεφάλαιο 9....51
Κλοπή ταυτότητας....51
Καταπολεμήστε την απάτη....53
Συμπέρασμα....53
Η πρώτη ελληνική δικαστική απόφαση για "κλοπή ταυτότητας"....54
Κεφάλαιο 10....55
Διαδικτυακές απάτες....55
Οι συνηθέστερες μορφές διαδικτυακής απάτης είναι οι ακόλουθες:....55
α) Χρεώσεις της πιστωτικής κάρτας πολιτών μέσω του διαδικτύου για αγορές, οι οποίες δεν πραγματοποιήθηκαν από τους ίδιους.....55
β) Διακίνηση μηνυμάτων με απατηλό περιεχόμενο, που επιδιώκουν την εξαπάτηση ανυποψίαστων πολιτών.....55
γ) «Απάτες 419» ή «Νιγηριανές Απάτες»....56
Κεφάλαιο 11....57
Κακόβουλο λογισμικό....57
Ορισμός....57
Είδη κακόβουλου λογισμικού....57
Ιοί....57
Δούρειοι ίπποι....59
Λογισμικά κατασκοπείας (Spyware)....60
Σκουλήκια (worm)....60
Λογισμικά εκφοβισμού (Scareware)....60
Προγράμματα καταγραφής πληκτρολογήσεων (Keylogger)....61
Rootkit....61
Exploit....61
Απάτες (Hoax) και ανεπιθύμητα μηνύματα (Spam)....61
Τρόποι αντιμετώπισης....61
Προστασία από τα κακόβουλα λογισμικά....61
Διατήρηση ασφαλούς λογαριασμού....63
Κεφάλαιο 12....64

Περιεχόμενα

Ανεπιθύμητη αλληλογραφία (SPAM).....64
Τι είναι το spam;.....64
Τα κυριότερα χαρακτηριστικά του Spam:.....64
Το spam είναι ένα φαινόμενο….....64
Τι μπορούμε να κάνουμε για να αποφύγουμε το Spam;.....65
Οι απλοί χρήστες:.....65
Οι επιλογές του απλού χρήστη για προστασία.....66
Προγράμματα αλληλογραφίας με δυνατότητα εντοπισμού της ενοχλητικής αλληλογραφίας (Spam - Junk Email).....66
Χρήση white lists.....66
Φιλτράρισμα με βάση τον αποστολέα και το περιεχόμενο.....66
Εξελιγμένα προγράμματα φιλτραρίσματος.....66
Επιλογές των διαχειριστών ηλεκτρονικού ταχυδρομείου.....66
Έλεγχος εγκυρότητας στο DNS και στους headers.....66
Χρήση SMTP Server που απορρίπτει γνωστούς spammers.....66
Χρήση προγραμμάτων προστασίας στον διακομιστή.....66
Φιλτράρισμα των SMTP συνδέσεων.....66
Παρακολούθηση.....66
Νομοθεσία για το spam 67
Βιβλιογραφία.....68

Η εργασία αυτή υλοποιήθηκε στα πλαίσια του μαθήματος «Ερευνητική εργασία»

Σχολικό έτος 2013-2014

Εργάστηκαν οι μαθητές του Β2

Ομάδα Α	Ομάδα Β	Ομάδα Γ	Ομάδα Δ	Ομάδα Ε
Νίκος Χαρτσιούδης	Τρακούδη Πετρούλα	Κωνσταντίνος Παπανικολόπουλος	Δήμητρα Μπουγαδούδη	Πελτέκης Γιώργος
Ταρλίνη Ραφαηλία	Στέλιος Μπουμπας	Χρυσάνθη Σταγκοπούλου	Μαρία Νικολούδη	Τατούδης Λεωνίδας
Στεφανία Χατζηκοτιανούδη	Χρύσα Τσιπλάκη	Νίκος Χριστόπουλος	Χριστίνα Μπορδούδη	Σμυρίδης Γιώργος
Χαβαρής Αντώνης	Τσακίρης Χρήστος	Αντιγόνη Χατζογλίδου	Παρασκευή Χατζηβασιλείου	

Η κάθε ομάδα ασχολήθηκε με τα παρακάτω διδακτικά αντικείμενα

Α′ ομάδα	Θα ασχοληθούν με το cyberbulling, διαδικτυακή τρομοκρατία, επιθέσεις σε δικτυακούς τόπους (facebook,chat rooms).
Β′ ομάδα	Θα ασχοληθούν με το κακόβουλο λογισμικό, επιθέσεις άρνησης εξυπηρέτησης, Ανεπιθύμητη αλληλογραφία.
Γ′ ομάδα	Θα ασχοληθούν με Ηλεκτρονικό ψάρεμα, απάτη στο διαδίκτυο και κλοπή ταυτότητας .
Δ′ ομάδα	Θα ασχοληθούν με παιδική πορνογραφία Διακίνηση ναρκωτικών και ξέπλυμα μαύρου χρήματος .
Ε′ ομάδα	Θα ασχοληθούν με κακόβουλες εισβολές σε δίκτυα (hacking, craking) και πειρατεία λογισμικού.

Υπεύθυνη καθηγήτρια : Καρακώστα Δήμητρα

Εισαγωγή

Ορισμός του ηλεκτρονικού εγκλήματος

Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Ως «Ηλεκτρονικό Έγκλημα», λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου.

Υιοθετώντας μια τριπλή προσέγγιση (Αγγέλης, 2000) που τείνει να επικρατήσει σήμερα, μπορούμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως:

- ·μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών
- ·μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές
- ·μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθ' οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής.

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλουν είναι: e-crime, cybercrime, computer-crime, internet related crime και hitech-crime .Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι ηλεκτρονικό έγκλημα, δικτυακό έγκλημα και έγκλημα του κυβερνοχώρου.

Βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής, κινητό τηλέφωνο, palmtop, notepad κλπ. Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ,ο οποίος μπορεί:

- Να αποτελεί τον στόχο κάποιας επίθεσης.
- Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης.
- Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος.

Αν θέλαμε να ορίσουμε το «Ηλεκτρονικό Έγκλημα» θα μπορούσαμε να πούμε ότι γενικότερα είναι κάθε παράνομη δραστηριότητα που για την διάπραξη αλλά και για την αντιμετώπισή της απαιτείται η τεχνολογική γνώση. Ο ορισμός του ηλεκτρονικού εγκλήματος έχει να κάνει με την οπτική γωνία από την οποία εξετάζεται. Αυτή η πολυμορφία του εγκλήματος είναι που δυσχεραίνει και τον νομοθέτη, ο όποιος αποφεύγει να του προσδώσει έναν ορισμό και είτε αφήνει αυτήν την αρμοδιότητα στα δικαστήρια και στην παραγόμενη νομολογία, είτε δανείζεται τους χρησιμοποιούμενους από την τεχνολογία όρους.

Χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο

Το έγκλημα στον κυβερνοχώρο είναι γρήγορο, διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.

Είναι εύκολο στη διάπραξή του, φυσικά για όσους το γνωρίζουν.

Για την τέλεσή του δεν απαιτούνται άριστες και εξειδικευμένες γνώσεις.

Μπορεί να διαπραχθεί χωρίς τη φυσική μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, πατώντας μόνο ορισμένα πλήκτρα του υπολογιστή του.

Δίνει τη δυνατότητα σε άτομα με ορισμένες ιδιαιτερότητες π.χ. σε όσους έχουν ροπή ή τάση στην παιδοφιλία ή τη χρήση υλικού παιδικής πορνογραφίας να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζήτησης ή μέσα από διαδικτυακά άμεσα ανά-μεταδιδόμενες συζητήσεις.

Είναι έγκλημα «χωρίς πατρίδα», παρότι τα αποτελέσματά του μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς στόχους.

Είναι κατά κανόνα, πολύ δύσκολο να προσδιοριστεί ο πραγματικός τόπος τέλεσής του.

Κατά τεκμήριο για τη διερεύνησή του απαιτείται συνεργασία δυο τουλάχιστον κρατών, δηλαδή του κράτους στο οποίο γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία. Περιπτώσεις που το έγκλημα στον κυβερνοχώρο περιορίζεται στα όρια ενός μόνο κράτους είναι ελάχιστες και σπάνιες.

Δεν υπάρχουν επαρκή στατιστικά στοιχεία ακόμη, όχι μόνο στον Ελληνικό, αλλά και στον διεθνή χώρο. Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου καταγγέλλονται. Και αυτό για να μην αμφισβητείται η αξιοπιστία των παθόντων, οι οποίοι κατά κανόνα είναι εταιρείες. Κατά συνέπεια ο «σκοτεινός αριθμός» της εγκληματικότητας στο χώρο του διαδικτύου είναι «ακόμα πιο σκοτεινός», από ότι στον «κοινό» εγκληματικό χώρο.

Η αστυνομική διερεύνησή του είναι πολύ δύσκολη, απαιτεί δε άριστη εκπαίδευση και εξειδικευμένες γνώσεις.

Εξειδικευμένες γνώσεις επίσης απαιτούνται και όσους άλλους ασχολούνται με την συγκεκριμένη μορφή εγκλήματος (εισαγγελείς, δικαστές, δικηγόρους).

Το Ηλεκτρονικό Έγκλημα, ανεξάρτητα από το εάν προσεγγιστεί από την στενή ή την ευρεία έννοια του, εμπεριέχει ορισμένα χαρακτηριστικά γνωρίσματα που το διαχωρίζουν από το παραδοσιακό έγκλημα. Τέτοια σημεία είναι τα εξής :

1. Το έγκλημα στον κυβερνοχώρο είναι γρήγορο, διαπράττεται σε πραγματικό χρόνο, ακόμα και σε δευτερόλεπτα, και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.

2. Είναι εύκολο στη διάπραξή του για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά.

3. Για την τέλεση του απαιτούνται άριστες και εξειδικευμένες γνώσεις

4. Οι κυβερνο-εγκληματίες πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα, αποστέλλοντας ηλεκτρονικά μηνύματα (e-mails) με ψευδή στοιχεία.

5. Μπορεί να διαπραχθεί από οποιοδήποτε μέρος, καθώς δεν απαιτείται η μετακίνηση του δράστη, και τα αποτελέσματά του να γίνονται ταυτόχρονα αισθητά σε πολλούς στόχους ανεξαρτήτου εδαφικού περιορισμού. Για αυτό, άλλωστε, και το αποκαλούν «έγκλημα χωρίς πατρίδα».

6. Ο εντοπισμός ενός ψηφιακού εγκληματία, κατά κανόνα, είναι πολύ δύσκολος (αλλά όχι ακατόρθωτος) να προσδιοριστεί καθώς επίσης και ο (πραγματικός) τόπος τέλεσής του και αυτό γιατί μπορεί ο δράστης να εντοπιστεί σε ένα συγκεκριμένο τόπο, τα αποδεικτικά στοιχεία, όμως, να βρίσκονται σε

διαφορετική και απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες.

7. Καθώς ο κίνδυνος ανακάλυψης του ηλεκτρονικού δράστη είναι μικρός, το ηλεκτρονικό έγκλημα αποδίδει μεγάλα κέρδη.

8. Ο αριθμός των θυμάτων τους συγκρινόμενος με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος.

9. Οι οικονομικές απώλειες που προξενούνται στα «ψηφιακά» εγκλήματα είναι πολύ μεγαλύτερες από εκείνες των θυμάτων των παραδοσιακών εγκλημάτων.

10.Καθώς για την διάπραξή του δεν απαιτείται φυσική μετακίνηση του δράστη, δίνει τη δυνατότητα σε άτομα με ορισμένες ιδιαιτερότητες, όπως για παράδειγμα παιδόφιλοι, να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται μαζί στις ίδιες ομάδες συζήτηση (π.χ. Newsgroups) ή μέσα από διαδικτυακά άμεσα αναμεταδιδόμενες συζητήσεις (π.χ. Internet Relay Chat).

11.Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα γιατί ελάχιστες περιπτώσεις κυβερνο-εγκλημάτων καταγγέλλονται διεθνώς με άμεση συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του διαδικτύου να χαρακτηρίζεται ακόμα πιο «σκοτεινό» από ότι το έγκλημα του πραγματικού κόσμου.

12.Η αστυνομική διερεύνηση του είναι πολύ δύσκολη και απαιτεί άριστη εκπαίδευση και εξειδικευμένες γνώσεις.

13.Οι οποίες εξειδικευμένες γνώσεις απαιτούνται και σε όσους, εκτός αστυνομίας, ασχολούνται με τη συγκεκριμένη μορφή εγκλήματος, όπως είναι οι εισαγγελείς, οι δικαστές, οι δικηγόροι.

14. Για την διερεύνησή του απαιτείται συνεργασία τουλάχιστον δύο κρατών : του κράτους που γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία.

Αρχές που Εποπτεύουν την Προστασία του Διαδικτύου στην Ελλάδα

Στην Ελλάδα, λειτουργούν τρείς ανεξάρτητες αρχές που εποπτεύουν σε ζητήματα ασφάλειας και προστασίας στο διαδίκτυο και στις επικοινωνίες γενικότερα και σε αυτές μπορούν να αναφερθούν σχετικά προβλήματα. Αυτές είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα , η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) και η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) . Και οι τρείς αυτοί φορείς έχουν το δικαίωμα να επιβάλλουν ιδιαίτερους όρους σχετικά με την τήρηση του απορρήτου των τηλεπικοινωνιών στις εταιρείες που διαθέτουν άδεια χρήσης τηλεπικοινωνιών δραστηριοτήτων και σε αυτές υπάγονται και οι Πάροχοι Υπηρεσιών Διαδικτύου (ISP's).

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η Αρχή Προστασίας Δεδομένων προσωπικού Χαρακτήρα, λειτουργεί από το 1977 σύμφωνα με τις διατάξεις του ν.2472/1997 και έχει ως αποστολή την εποπτεία της τήρησης του προσωπικού απορρήτου και στο Διαδικτύου. Σύμφωνα με το νόμο για την «Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα», ν.2774/1999, οι ιστοσελίδες που συγκεντρώνουν προσωπικά στοιχεία των επισκεπτών τους, όπως για παράδειγμα ονόματα, τηλέφωνα, διευθύνσεις e-mail, έχουν νομική υποχρέωση να τους ενημερώνουν για τον σκοπό που συλλέγονται αυτά τα στοιχεία καθώς και για το αν αυτά τα στοιχεία διατίθενται σε τρίτους.

Οι σημαντικότερες Οδηγίες της Α.Π.Δ.Π.Χ. είναι :

- Η Οδηγία 1122.2000 για τα κλειστά κυκλώματα τηλεόρασης και
- Η Οδηγία 115/2001 για την επεξεργασία δεδομένων των εργαζομένων
- Οι σπουδαιότερες αποφάσεις της Α.Π.Δ.Π.Χ. είναι :
- Η Απόφαση 50/2000 σχετικά με τους όρους για την νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης και της διαπίστωσης πιστοληπτικής ικανότητας.
- Η Απόφαση 120/2001 για την επεξεργασία Προσωπικών Δεδομένων σχετικά την παροχή υπηρεσιών καρτοκινητής τηλεφωνίας
- Η Απόφαση 1469.2000 για τη συλλογή προσωπικών δεδομένων από εταιρείες τηλεπικοινωνιακών δραστηριοτήτων.
- Η Απόφαση 147/2001 για την χρήση ευαίσθητων δεδομένων ενώπιον δικαστηρίου.

- Η Απόφαση 8/2003 σχετικά με την πρόσβαση τρίτου σε δεδομένα εταιρείας κινητής τηλεφωνίας για άσκηση δικαιώματος υπεράσπισης ενώπιον δικαστηρίου.

Τέλος, οι πιο άξιες προσοχής γνωμοδοτήσεις της Α.Π.Δ.Π.Χ. είναι :

- Η Γνωμοδότηση 71/2002 σχετικά με την επεξεργασία προσωπικών δεδομένων στην αυτόματη αναγνώριση της ταυτότητας του συνδρομητή καλούσας γραμμής σε ψηφιακά δίκτυα ενοποιημένων υπηρεσιών (ISDN),
- Η Γνωμοδότηση 78/2002 για τις προϋποθέσεις διασταύρωσης προσωπικών δεδομένων στο χώρο της σταθερής τηλεφωνίας,
- Η Γνωμοδότηση 86/2001 σχετικά με την είσοδο και παραμονή αλλοδαπών στην ελληνική επικράτεια,
- Η Γνωμοδότηση 15/2001 σχετικά με την ανάλυση γενετικού υλικού για σκοπούς εξιχνίασης εγκλημάτων και ποινικής δίωξης

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) λειτουργεί από το 2003 ως ανεξάρτητη αρχή σύμφωνα με τις διατάξεις του ν.3115/2003. Σκοπός της

Α.Δ.Α.Ε. είναι η προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιοδήποτε άλλο τρόπο. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου.

Στις αρμοδιότητες της Α.Δ.Α.Ε. περιλαμβάνεται το δικαίωμα διενέργειας ελέγχων, αποδοχής και εξέτασης καταγγελιών αλλά και έκδοσης κανονιστικών κειμένων. Οι σημαντικότερες από αυτές είναι :

Να διενεργεί αυτεπαγγέλτως ή έπειτα από καταγγελία τακτικούς ή έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών, άλλων δημόσιων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημόσιου τομέα και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία. 􀀩 Να καλεί σε ακρόαση τις διοικήσεις, τους νόμιμους εκπροσώπους και τους υπαλλήλους των ως άνω δημοσίων υπηρεσιών ή ιδιωτικών εταιριών.

Να συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών και με ευρωπαϊκούς ή διεθνείς οργανισμούς.

Να γνωμοδοτεί και να απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και για τη διαδικασία άρσης αυτού.

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Ε.Τ.) αποτελεί σημαντική αρχή στο χώρο του διαδικτύου καθώς αποτελεί την εθνική ρυθμιστική αρχή σε θέματα τηλεπικοινωνιών. Είναι ανεξάρτητη διοικητική αρχή με έδρα την Αθήνα και απολαμβάνει διοικητικής και οικονομικής αυτοτέλειας. Τα μέλη της Ε.Ε.Ε.Τ. διορίζονται με απόφαση του Υπουργού Μεταφορών και Επικοινωνιών μετά από προηγούμενη επιλογή τους από την Διάσκεψη των Προέδρων της Βουλής με την αυξημένη πλειοψηφία των τεσσάρων πέμπτων των μελών της. Ως μέλη της Ε.Ε.Ε.Τ. επιλέγονται πρόσωπα εγνωσμένου κύρους, που απολαμβάνουν ευρείας κοινωνικής αποδοχής και διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους ικανότητα στον τεχνικό, οικονομικό ή νομικό τομέα. Κατά την εκτέλεση των καθηκόντων τους, τα μέλη της Ε.Ε.Ε.Τ. δεσμεύονται από το νόμο, έχουν δε υποχρέωση τήρησης των αρχείων αντικειμενικότητας και αμεροληψίας. Επίσης, υποχρεούνται στην τήρηση εμπιστευτικότητας, εμπορικών πληροφοριών για τέσσερα χρόνια μετά την εκούσια ή ακούσια αποχώρηση τους από την Ε.Ε.Ε.Τ. .

Η Ε.Ε.Ε.Τ. χορηγεί άδειες σε Πάροχους Τηλεπικοινωνιακών Υπηρεσιών, στους οποίους ανήκουν και οι Πάροχοι Υπηρεσιών Διαδικτύου (ISP's), ενώ ρυθμίζει τον τομέα των τηλεπικοινωνιών, ασκώντας παράλληλα και έλεγχο σε αυτό, και εποπτεύεται την τηλεπικοινωνιακή αγορά.

Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος

Η Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος είναι ειδική αυτοτελής Κεντρική Υπηρεσία της Ελληνικής Αστυνομίας με αποστολή τη διερεύνηση, εξιχνίαση και δίωξη εγκλημάτων που τελέστηκαν σε βάρος των συμφερόντων του δημοσίου και της Εθνικής Οικονομίας ή έχουν τα χαρακτηριστικά του οργανωμένου οικονομικού εγκλήματος, καθώς και οποιαδήποτε εγκλήματα διαπράττονται με τη χρήση του διαδικτύου. Υπάγεται απευθείας στον Αρχηγό της Ελληνικής Αστυνομίας και εποπτεύεται στην προανακριτική της δράση από τον Εισαγγελέα του Οργανωμένου Εγκλήματος. Άρχισε τη λειτουργία της τον Ιούλιο του 2011 και διέπεται από ειδικό θεσμικό πλαίσιο.

Μορφές Ηλεκτρονικού εγκλήματος

Κύριες μορφές Κυβερνοεγκλημάτων που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος/ΔΑΑ

1. Cracking και hacking
2. Διακίνηση-πειρατεία λογισμικού
3. Διαδικτυακή Τρομοκρατία
4. Cyber bulling
5. Ξέπλυμα Μαύρου χρήματος
6. Παιδική πορνογραφία
7. Διακίνηση ναρκωτικών
8. Πιστωτικές κάρτες-Phishing
9. Κλοπή ταυτότητας
10. Απάτες μέσω Διαδικτύου
11. Κακόβουλο Λογισμικό
12. Spam

Κεφάλαιο1

Hacking & Cracking

Ορισμός του Hacker

Χάκερ (Hacker) ονομάζεται το άτομο το οποίο εισβάλει σε υπολογιστικά συστήματα και πειραματίζεται με κάθε πτυχή τους. Ένας χάκερ έχει τις κατάλληλες γνώσεις και ικανότητες να διαχειρίζεται σε μεγάλο βαθμό υπολογιστικά συστήματα. Συνήθως οι χάκερς είναι προγραμματιστές, σχεδιαστές συστημάτων αλλά και άτομα τα οποία ενώ δεν ασχολούνται επαγγελματικά με τομείς της πληροφορικής έχουν αναπτύξει τέτοιες δεξιότητες και δουλεύουν είτε σε ομάδες (hacking-groups) είτε μόνοι τους. Αν οι πράξεις τους αυτές είναι κακόβουλες αποκαλούνται κράκερ.

Κατηγορίες των Hackers

Τα τελευταία χρόνια, οι χάκερς είναι ευρέως γνωστοί ως οι κακοί του κυβερνοχώρου και έχουν χαρακτηριστεί από την κοινωνία μας, ως εγκληματίες.

Είναι γνωστοί επίσης ως *crackers* ή *black hats*. Ο όρος κράκερ χρησιμοποιήθηκε για να διακρίνει όσους αποκτούν πρόσβαση σε υπολογιστικά συστήματα, προκαλώντας όμως σ' αυτά και σοβαρές ζημιές.

Οι όροι black / white / gray hats αφορούν ομάδες των hacker ανάλογα με τις ηθικές τους αρχές. Ο όρος black hats χαρακτηρίζει τα άτομα εκείνα που έχουν υψηλή ειδίκευση στους υπολογιστές, τα οποία όμως, χρησιμοποιούν τις δεξιότητές τους με μη ηθικούς τρόπους.

Είναι σημαντικό να κατανοήσουμε ότι οι χάκερς δεν είναι όλοι τους κακόβουλοι αλλά υπάρχουν και άνθρωποι της hacking κοινότητας που εισβάλλουν σε κάποιο σύστημα στα πλαίσια των ηθικών αρχών για να αναγνωρίσουν ποια είναι τα τρωτά σημεία, οι οποίοι είναι γνωστοί και ως **white hat hackers**. Οι white hats είναι οι hacker που χρησιμοποιούν την ικανότητά τους σαφώς κατά ηθικό τρόπο. Είναι παραδείγματος χάρη, οι υπάλληλοι εταιρειών, οι οποίοι έχουν άδεια να επιτίθενται στα δίκτυο και τα συστήματα της εταιρείας τους για τον καθορισμό των αδυναμιών. Επίσης white hats, είναι και οι πράκτορες της μυστικής υπηρεσίας που χρησιμοποιούν τις ικανότητές τους στο όνομα της εθνικής ασφάλειας ή για τη διερεύνηση και την επίλυση διάφορων εγκλημάτων. Έχουν, δηλαδή,

καθήκον να χρησιμοποιούν τις γνώσεις τους με τέτοιο τρόπο, ώστε να επωφεληθούν άλλοι άνθρωποι ή υπηρεσίες.

Στο μέσο των white hats και black hats βρίσκονται οι gray hats. Οι **Gray hat hackers**, περιλαμβάνουν τους εθελοντές hacker, δηλαδή, τα άτομα αυτά που χρησιμοποιούν τους υπολογιστές για τη διερεύνηση και την προσπάθεια να τιμωρήσουν τους υποτιθέμενους εγκληματίες του κυβερνοχώρου. Επίσης, χαρακτηρίστηκαν και ως «hacktιβιστές (hacktivists)», δηλαδή τα άτομα που χρησιμοποιούν τους υπολογιστές και το διαδίκτυο για να μεταφέρουν πολιτικά μηνύματα, μεταξύ άλλων οι Harley(2006) και Falk(2005) οι οποίοι ξεχωρίζουν για αυτή την δράση τους στο άρθρο του Brian A. Pashel με τίτλο «Teaching Students to Hack».

Τρόπος Δράσης – Επιθέσεις των hacker.

Η πρόσβαση ενός hacker στο σύστημα του υποψήφιου θύματός του προϋποθέτει δύο στάδια: ένα προπαρασκευαστικό και ένα κύριο.

Αρχικά στο προπαρασκευαστικό στάδιο ο hacker, συγκεντρώνει πληροφορίες (information gathering) για το σύστημα που επιθυμεί να προσβάλλει και προσπαθεί να αποκτήσει πρόσβαση σ' αυτό αποκτώντας τους κωδικούς εισόδου (password cracking), αποκτώντας έτσι τα δικαιώματα (privileges) ενός νόμιμου χρήστη του συστήματος.

Στο **κύριο στάδιο** ο hacker, επιδιώκει την εκπλήρωση των σκοπών για τους οποίους μπήκε παράνομα στο συγκεκριμένο σύστημα και αποχωρεί από αυτό προσπαθώντας να μην αφήσει ίχνη που θα μπορούν να οδηγήσουν στην ανακάλυψη της ταυτότητάς του, ενώ παράλληλα φροντίζει να διατηρήσει την επανεισόδο του στο σύστημα, όποτε πάλι ο ίδιος το επιθυμήσει.

Για καθένα από τα βήματα αυτά του hacker μπορούμε να πούμε τα ακόλουθα.

→Η συλλογή πληροφοριών

Το βήμα αυτό αποτελεί ίσως το βασικότερο σκαλοπάτι στην κλίμακα ενός επιτυχημένου hacking. Όσα περισσότερα γνωρίζει ένας hacker για ένα σύστημα τόσο περισσότερο αυξάνονται οι πιθανότητες που έχει για να εισβάλλει σ' αυτό χωρίς μάλιστα να γίνει αντιληπτός. Οι πιθανές ερωτήσεις για τις οποίες οι απαντήσεις που θα πάρει θα αποδειχθούν σημαντικές, έχουν να κάνουν συνήθως τόσο με το ανθρώπινο δυναμικό (διαχειριστές, μηχανικούς, χειριστές, χρήστες) του συστήματος όσο και με το ίδιο το

σύστημα (hardware, λειτουργικό που χρησιμοποιεί, ενδεχόμενες ιδιομορφίες του κλπ.). Τις πληροφορίες αυτές ο hacker μπορεί να τις πάρει από το ίδιο το σύστημα, την επιχείρηση στην οποία αυτό ανήκει, τους ειδικούς (τεχνικούς, επιστήμονες) των Η/Υ και άλλους συναδέλφους του.

→**Εισβολή στο σύστημα** : Απόκτηση των κωδικών εισόδου και απόκτηση των δικαιωμάτων ενός νόμιμου χρήστη.

Ένα σύστημα λειτουργεί σωστά από τη στιγμή που ο μηχανισμός αναγνώρισης της ταυτότητας (πιστοποίηση) των νόμιμων χρηστών του είναι αξιόπιστος. Για το λόγο αυτό η εξουδετέρωση του μηχανισμού αυτού αποτελεί το κύριο μέλημα κάθε hacker.

→**Ο hacker μέσα στο σύστημα:**

Από τη στιγμή που ο hacker θα αποκτήσει πρόσβαση στο σύστημα του στόχου του το τι θα κάνει στη συνέχεια εξαρτάται από το σκοπό για τον οποίο έκανε το hacking. Ανεξάρτητα από το ποιο είναι πάντως το βασικό του κίνητρο είναι βέβαιο πως μεταξύ άλλων θα συγκεντρώσει πληροφορίες και για τη λειτουργία του συστήματος αυτού καθώς και ότι θα προσπαθήσει να εκμεταλλευτεί τις δυνατότητές του και γενικότερα τα δικαιώματα που παρέχονται στους νόμιμους χρήστες του. Κάποιες από τις δυνατότητες που έχει ο hacker είναι να καταστρέψει/διαγράψει στοιχεία και να κλέψει εμπιστευτικά αρχεία και πληροφορίες, να αποκτήσει έλεγχο στο σύστημα και να μεταβάλλει δεδομένα πρόσβασης με σκοπό τον αποκλεισμό χρηστών καθώς και να χρησιμοποιήσει ένα σύστημα για την αποστολή δεδομένων σε τρίτο σύστημα. Ολοκληρώνοντας δε την «επίσκεψή» του θα προσπαθήσει να εξαφανίσει τα ίχνη της και παράλληλα να αφήσει «ανοικτή την πόρτα» και για μελλοντικές ανάλογες δραστηριότητες στο ίδιο σύστημα.

Επιπτώσεις Δράσης

Οι ενέργειες των χάκερς επιφέρουν κοινωνικές, οικονομικές, πολιτικές, καθώς και επιχειρησιακές συνέπειες. Οι χρήστες μπορούν να πέσουν θύματα κλοπής των χρημάτων τους από τραπεζικούς λογαριασμούς ή πιστωτικές κάρτες.

Τα ανυποψίαστα θύματα μπορούν να γίνουν δέκτες εκβιασμών, εν αγνοία τους να γίνουν κόμβος ενός botnet, να γίνουν ενδιάμεσοι κόμβοι παροχής κακόβουλου λογισμικού, αποστολείς μηνυμάτων spam, να φιλοξενούν παράνομους servers κ.α.

Σε οργανισμούς και ιδιώτες δημιουργείται οικονομικό αντίκτυπο καθώς μπορεί να σπιλωθεί η φήμη μιας επιχείρησης με αποτέλεσμα η επιχείρηση να χάσει τους πελάτες της, ειδικότερα όταν πρόκειται για την προστασία των προσωπικών δεδομένων των πελατών.

Με τις ιδιωτικές προσωπικές πληροφορίες προσβάσιμες σε όλους υπάρχει κίνδυνος της υποκλοπής της ταυτότητάς τους και άλλων εμπιστευτικών τους πληροφοριών από άτομα με κακή πρόθεση.

Ελληνική νομοθεσία έναντι του Hacking/Cracking

Ο Ν. 1805/88, αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes) και στο βαθμό που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον Διαδικτύου (Internet), τότε τα άρθρα αυτά εφαρμόζονται και στις συγκεκριμένες περιπτώσεις.

Στην ελληνική νομοθεσία όμως, δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Διαδικτύου και να ρυθμίζει τη συμπεριφορά των χρηστών του Διαδικτύου από άποψη Ποινικού Δικαίου. Ως εκ τούτου, η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων διεθνών οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων.

Ανεξάρτητα όμως από το εάν ο ανωτέρω νόμος και οι διεθνείς συνεργασίες επαρκούν ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της Πληροφορικής, το βέβαιον είναι ότι, δεν επαρκούν για την τελεία αντιμετώπιση των εγκλημάτων που έχουν τελεστεί με τη χρήση του Διαδικτύου.

Πρόσφατα τέθηκε σε ισχύ το Π.Δ. 47/2005, από την Α.Δ.Α.Ε. (Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών), το οποίο αφορά τις διαδικασίες, τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του. Ενώ, σύντομα αναμένεται να τεθεί σε ισχύ η Συνθήκη της Βουδαπέστης.

Αρθρο 370Β

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών. Ως απόρρητα θεωρούνται κι εκείνα που ο

νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.

3. Αν πρόκειται για στρατιωτικό ή διαπλαστικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παρ. 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.

4. Οι πράξεις που προβλέπονται στις παρ.1 και 2 διώκονται ύστερα από έγκληση.

Κεφάλαιο2

Πειρατεία Λογισμικού Η/Υ

Ορισμός

Πειρατεία Λογισμικού θεωρείται η χωρίς άδεια χρήση ενός προγράμματος Η/Υ, στην οποία περιλαμβάνεται η εγκατάσταση, αναπαραγωγή, αντιγραφή και διανομή του. Σύμφωνα με την παγκόσμια μελέτη της διεθνούς εταιρείας ερευνών IDC που πραγματοποιήθηκε για λογαριασμό της Business Software Alliance (BSA, Μάιος 2006), η πειρατεία λογισμικού στην Ελλάδα για το 2006 μειώθηκε κατά 3 ποσοστιαίες μονάδες φθάνοντας το 61%, ενώ η αξία του παράνομα εγκατεστημένου λογισμικού στη χώρα μας εκτιμάται στα €128 εκατομμύρια.

Πειρατεία στο Internet - το πρόβλημα και η αντιμετώπιση

Μέχρι πριν λίγα χρόνια, η πειρατεία στο Internet αποτελούσε ελάχιστη εμπορική απειλή για τη μουσική βιομηχανία. Αυτό άλλαξε λόγω των νέων τρόπων συμπίεσης δεδομένων που ανακαλύφθηκαν και λόγω της αύξησης της διαθέσιμης ταχύτητας μεταφοράς δεδομένων στο Δίκτυο. Η ηλεκτρονική πειρατεία πλέον απειλεί τη βιωσιμότητα του ηλεκτρονικού εμπορίου μουσικής. Το IFPI συντονίζει τις ενέργειες της διεθνούς δισκογραφίας για προστασία των δικαιωμάτων της με τεχνολογικά μέσα και νομικές ενέργειες.

Πιθανές συνέπειες από τη χρήση πειρατικού λογισμικού;

- Προσβολή της φήμης και του ονόματος της επιχείρησής σας
- Ποινικές, αστικές και διοικητικές κυρώσεις
- Έλλειψη τεχνικής υποστήριξης και δωρεάν αναβαθμίσεων από τους προμηθευτές λογισμικού
- Προσβολή του πληροφοριακού συστήματος από Ιούς, κακόβουλο λογισμικό κ.α.

Ελληνική νομοθεσία έναντι της Πειρατεία Λογισμικού

Άρθρο 370Γ
1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική

ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.
2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.
3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.
4. Οι πράξεις των παρ. 1 έως 3 διώκονται ύστερα από έγκληση.

Αρθρο 386Α - Απάτη με υπολογιστή -

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα.

Νομοθεσία διαδικτυακών εγκλημάτων στην αλλοδαπή
Στην Αγγλία από τον Φεβρουάριο του 2001, οι hacker, αναλόγως με τη σημασία του χτυπήματος θεωρούνται και τρομοκράτες.
Στην Αμερική θεωρείται τρομοκρατική οποιαδήποτε πράξη μη εξουσιοδοτημένης πρόσβασης σε Η/Υ, και τιμωρείται με φυλάκιση ως και ισόβια (ανάλογα με τη σημασία της εισβολής), χωρίς δυνατότητα μείωσης τις ποινής.

Κεφάλαιο3

Τρομοκρατία και Διαδίκτυο.- Νέα τάξη Πραγμάτων.

Η παρουσία τρομοκρατικών ομάδων στο διαδίκτυο είναι ένα σχετικά νέο φαινόμενο το οποίο βρίσκεται σε έξαρση την τελευταία δεκαπενταετία κυρίως. Ακριβείς εκτιμήσεις για τον αριθμό των δικτυακών τόπων ενεργού τρομοκρατικής ομάδας ποικίλλουν λόγω των δυσκολιών μέτρησης. Εκτιμάται ωστόσο ότι από το 1996 που δεν έφταναν τις 100 ιστοσελίδες έχουμε σήμερα ξεπεράσει τις 8000.

Η ανάπτυξη της χρήσης του διαδικτύου από τρομοκρατικές ομάδες οφείλεται στα βασικά χαρακτηριστικά του διαδικτύου:

- Ευκολία πρόσβασης που διευκολύνει την μαζικοποίηση των ακροατηρίων σε παγκόσμιο επίπεδο
- Ελάχιστοι νόμοι συγκριτικά με τον φυσικό κόσμο
- Λιγότερη λογοκρισία και έλεγχος
- Ταχύτητα μετάδοσης και συνεχής ροή πληροφοριών
- Μηδαμινό κόστος
- Ανωνυμία της επικοινωνίας
- Περιβάλλον πολυμέσων

Έτσι κάνοντας χρήση του Διαδικτύου οι τρομοκρατικές ομάδες στοχεύουνε σε:

- Συλλογή πληροφοριών για εν δυνάμει στόχους
- Συγκέντρωση οικονομικών πόρων και ανθρώπινου δυναμικού
- Δημοσιότητα και Φήμη
- Παραπλάνηση των διωκτικών αρχών
- Παραπληροφόρηση και Προπαγάνδα

Ο Abu Musab al-Zarqawi ένας εκ των θεωρητικών της AL QAEDA είχε επισημάνει το 2005 ότι «η επανάσταση στις επικοινωνίες και τα παγκόσμια δορυφορικά κανάλια από κοινού με το ΔΙΑΔΙΚΤΥΟ, έχουν διευρύνει τους ορίζοντες της σκέψης των ανθρώπων». Θεωρείται ο κατ' εξοχήν αρχιτέκτονας της ένταξης της AL QAEDA στο σύγχρονο διαδικτυακό χώρο, ενώ είχε αφιερώσει το μεγαλύτερο μέρος της ζωής τους στην προώθηση των προπαγανδιστικών τάσεων του JIHAD. Κάνοντας πράξη αυτό που ο ίδιος κήρυττε, εντός ενός μικρού διαστήματος τεσσάρων μηνών τον Απρίλιο και τον Μάιο του 2004 απέκτησε μεγάλη φήμη συνδυάζοντας ακραίες μορφές βίας και την προώθησή τους με

βίντεο μέσω Διαδικτύου. Τον Απρίλιο του 2004 ο al-Zarqawi δημοσίευσε ένα ηχητικό ντοκουμέντο 30 λεπτών στο οποίο εξηγούσε το ποιος ήταν, γιατί πάλευε και λεπτομέρειες των επιθέσεων στις οποίες αυτός και η ομάδα του ήταν υπεύθυνοι. Ένα μήνα αργότερα προχώρησε σε μία ακόμη πιο ανατριχιαστική δημοσιοποίηση στο διαδίκτυο, ενός βίντεο με τον αποκεφαλισμό ενός Αμερικανού ομήρου προκειμένου να δημιουργήσει εντυπώσεις τόσο στους συμμάχους του όσο και στους εχθρούς. Η πράξη αυτή αύξησε τη δημοτικότητά του και τον έκανε ήρωα στα μάτια χιλιάδων jihadis.

Έτσι η AL QAEDA άρχισε να χρησιμοποιεί το Διαδίκτυο τόσο για να προσελκύσει νέα μέλη ή να προετοιμάσει μελλοντικές επιθέσεις, όσο και για να ριζοσπαστικοποιήσει σε παγκόσμιο επίπεδο μέλη ή πιθανούς υποψήφιους, οι οποίοι συμφωνούν με την ατζέντα της.

Στα τελευταία τρία χρόνια έχουν αυξηθεί κατά γεωμετρική πρόοδο οι «ιστοσελίδες αντίστασης» στο Διαδίκτυο με πληροφορίες για τους Ισλαμιστές τρομοκράτες στη Σαουδική Αραβία, στο Ιράκ κ.α., ενώ οι «Τζιχαντιστικές Ταξιαρχίες των ΜΜΕ», προωθούν προπαγανδιστικά VIDEOS, μηνύματα μέσω ηλεκτρονικού ταχυδρομείου και εικόνες-χάρτες, που αφορούν πολλά θέματα. Ακόμη οργανώσεις, όπως η Χαμάς και η Χεζμπολάχ, διατηρούν ιδιαίτερα εξελιγμένες ιστοσελίδες στο Διαδίκτυο, ενώ το ONLINE περιοδικό AL-BATTAR, σε μηνιαία βάση, πληροφορεί τους JIHADISTS για πολλά επιμέρους ζητήματα.

Καταπολέμηση της τρομοκρατίας στο διαδίκτυο: Ασφάλεια ή Απειλή;;;

Τα τελευταία χρόνια, η τρομοκρατία αποτελεί κυρίαρχο θέμα συζήτησης ανάμεσα στις ηγεσίες της Ε.Ε. Η ελευθερία που παρέχει το Διαδίκτυο και η επιρροή που ασκεί στους χρήστες του καθιστά το Διαδίκτυο ως το πιο ανεξέλεγκτο και ισχυρό όπλων των τρομοκρατικών οργανώσεων. Στην προσπάθεια, όμως, να δαμαστεί αυτή η δύναμη, οι ηγεσίες εισχωρούν σε επικίνδυνα πεδία και θέτουν σε κίνδυνο τα θεμελιώδη ανθρώπινα δικαιώματα.

Τυπικό παράδειγμα είναι η πρόταση που εξέτασε στις 23/09/2008 η Ολομέλεια του Ευρωπαϊκού Κοινοβουλίου σχετικά με την καταπολέμηση της τρομοκρατίας στο Διαδίκτυο. Σύμφωνα με το άρθρο «Διαδίκτυο και Τρομοκρατία» , η πρόταση, όπως εκπονήθηκε από την Ευρωπαϊκή Επιτροπή και συζητείται στο Συμβούλιο των Υπουργών, βασίζεται στην αυτονόητη παραδοχή πως κάποιοι τρομοκράτες μπορεί να χρησιμοποιούν και το Διαδίκτυο για να υποκινήσουν τρομοκρατικές πράξεις. Δυστυχώς, προκειμένου να αποτρέψουν οποιαδήποτε μηνύματα, προσκλήσεις και συζητήσεις τρομοκρατικού περιεχομένου και να διασφαλίσουν τη σύλληψη των μελών τρομοκρατικών ομάδων, προσέφυγαν στη ψήφιση μέτρων τα οποία καταπατούν βασικά ανθρώπινα δικαιώματα. Παρακάτω παρατίθενται ορισμένα από τα μέτρα:

1. Να οδηγείται στη φυλακή κάθε πολίτης που γράφει στο Διαδίκτυο οτιδήποτε μπορεί να θεωρηθεί από μια διωκτική αρχή ότι συνιστά πρόθεση προτροπής τρομοκρατικής πράξης.
2. Εισηγείται την ενοχή όποιου «είτε υποστηρίζει άμεσα είτε έμμεσα τα τρομοκρατικά εγκλήματα».

3. Μπορεί να διωχθεί κάποιος αν τα γραφόμενά του επέφεραν, σύμφωνα πάντα με την εκτίμηση των διωκτικών αρχών, την υποκίνηση τρομοκρατικής πράξης.

Ευτυχώς, η Ευρωπαϊκή Επιτροπή αναίρεσε το ψήφισμα της τις επόμενες ημέρες.

Παρόλα αυτά έχουν ληφθεί μέτρα σχετικά με την καταπολέμηση της τρομοκρατίας, καθώς όλοι οι μεγάλοι ιστότοποι λειτουργούν στο πλαίσιο κάποιων όρων λειτουργίας, οι οποίοι θέτουν ορισμένους περιορισμούς ως προς το περιεχόμενο των όσων αναρτούν οι χρήστες, ενώ στο Facebook και στο YouTube, κατά κανόνα αφαιρείται υλικό που προάγει ή παρουσιάζει τρομοκρατική βία.

Επισημαίνεται, ότι η αμερικανική νομοθεσία απαγορεύει την παροχή υπηρεσιών όπως ηλεκτρονικά μηνύματα κτλ. σε ομάδες που έχουν «χαρακτηρισθεί» τρομοκρατικές, όπως η Al Qaeda και οι Taliban, αλλά πέραν της συνταγματικής κατοχύρωσης της ελευθερίας του λόγου, ταυτόχρονα, τις περισσότερες φορές είναι αδύνατος ο εντοπισμός της διασύνδεσης του ηλεκτρονικού λογαριασμού ενός προσώπου με μια τρομοκρατική ομάδα.

Γενικά, η ηθική ανωτερότητα της δημοκρατίας είναι ότι, στα μέτρα περιφρούρησης και προστασίας της, δεν περιλαμβάνονται η παρακολούθηση των σκέψεων και των λεγόμενων των πολιτών της. Σκοπός της είναι να προστατεύει πάντα τα ανθρώπινα δικαιώματα καθώς είναι αυτά που την ορίζουν.

Δύσκολο να πιστέψει κανείς ότι ο εγκέφαλος μίας τρομοκρατικής οργάνωσης όπως η **Al-Qaida** διέθετε υπολογιστή, όχι όμως και πρόσβαση στο διαδίκτυο. Ο λόγος γίνεται φυσικά για τον **Osama bin Laden** ο οποίος είχε αναπτύξει ένα σύστημα επικοινωνίας με τα υπόλοιπα μέλη της τρομοκρατικής οργάνωσης χωρίς ο ίδιος να έχει πρόσβαση στο διαδίκτυο και χωρίς να αφήνει πουθενά "ψηφιακά αποτυπώματα".

Σύμφωνα με **αναφορά** του Associated Press, ο Osama bin Laden έγραφε τα μηνύματα που ήθελε να μεταφέρει στα μέλη σε έναν υπολογιστή ο οποίος δεν είχε πρόσβαση στο διαδίκτυο. Στη συνέχεια αποθήκευε τα μηνύματα σε μία μικρή flash memory την οποία παρέδιδε σε έναν έμπιστο άνθρωπο. Ο τελευταίος

πήγαινε σε κάποιο net cafe, έστελνε τα μηνύματα, λάμβανε τις απαντήσεις και τις αποθήκευε πάλι στη flash memory. Στη συνέχεια τις μετέφερε πίσω στο κρησφύγετο όπου ο Osama bin Laden τις διάβαζε στο δικό του υπολογιστή. Με τη χρονοβόρα και κουραστική αυτή διαδικασία ο Osama bin Laden είχε καταφέρει να επικοινωνεί με τα μέλη της οργάνωσης με έναν τρόπο που του εξασφάλιζε ανωνυμία και κάποια ασφάλεια.

Το παραπάνω περιστατικό δείχνει μία πτυχή ενός μεγαλύτερου φαινομένου που αφορά την τρομοκρατία στο διαδίκτυο.

Τι είναι όμως το διαδίκτυο για τους τρομοκράτες; Ένα μέσο για εξάπλωση προπαγάνδας, μία παγκόσμια απειλή, ένας εύκολος τρόπος επικοινωνίας ή μήπως όλα τα παραπάνω;

Ο αριθμός των ιστοσελίδων με τρομοκρατικό περιεχόμενο σήμερα έχει εκτιναχθεί σε περισσότερες από 5000. Μέσα από τις σελίδες αυτές οι τρομοκρατικές οργανώσεις επιδιώκουν τη στρατολόγηση νέων μελών και την εξάπλωση της οργάνωσης μέσα από κείμενα προπαγάνδας.

Μία έρευνα από την Διεθνή Επιτροπή για τον Πυρηνικό Αφοπλισμό (**International Commission on Nuclear Non-proliferation and Disarmament -ICNND**) καταδεικνύει την πιθανότητα να εισβάλλουν τρομοκράτες σε κάποιο σύστημα και να προκαλέσουν μία πυρηνική καταστροφή. Σύμφωνα πάντα με την ίδια έρευνα κάτι τέτοιο ίσως να ήταν και πιο εύκολο από το να πάρουν στα χέρια τους οι τρομοκράτες μία πυρηνική βόμβα.

Τι είναι όμως αυτό που κάνει τόσο ελκυστικό το διαδίκτυο σε ομάδες και οργανώσεις με τέτοιους σκοπούς;

• Ευκολία πρόσβασης, γεγονός που διευκολύνει την δημιουργία μαζικών ακροατηρίων σε παγκόσμιο επίπεδο

• Ελάχιστοι νόμοι στον ‘διαδικτυακό κόσμο’ σε σύγκριση με τον πραγματικό
• Ελάχιστη λογοκρισία

• Ταχύτατη και συνεχή ροή πληροφοριών

• Χαμηλό κόστος

• Ανωνυμία στην επικοινωνία και ένα πλούσιο περιβάλλον εφαρμογών. Με τους τρομοκράτες να αλλάζουν IP και servers καθημερινά η καταπολέμηση της τρομοκρατίας μοιάζει πολύ δύσκολο εγχείρημα. Το άμεσο κλείσιμο κάθε δικτυακού τόπου με τρομοκρατικό περιεχόμενο δεν φαίνεται να είναι η καλύτερη λύση στο πρόβλημα καθώς ένας τέτοιος δικτυακός τόπος μπορεί να

οδηγήσει στην ανακάλυψη των ατόμων που κρύβονται από πίσω και στηρίζουν οικονομικά αυτές τις οργανώσει.

Πως μπορεί λοιπόν να δοθεί λύση στο πρόβλημα της χρήσης του διαδικτύου από τους τρομοκράτες; Μήπως θα πρέπει να υπάρξει νομοθεσία που να καθορίζει τη χρήση του; Ή κάτι τέτοιο θα ήταν αντίθετο στην ελευθερία του ατόμου να χρησιμοποιεί το διαδίκτυο όπως το ίδιο επιλέγει; Αλήθεια που αρχίζει και που τελειώνει η ελευθερία του ατόμου;

Πριν από μερικά χρόνια ο μόνος τρόπος επιρροής της κοινής γνώμης από τους τρομοκράτες ήταν τα παραδοσιακά μέσα μαζικής ενημέρωσης: το ραδιόφωνο, η τηλεόραση και οι εφημερίδες. Φυσικά, επειδή αυτοί οι ατραποί πληροφόρησης είναι πολιτικά ελεγχόμενοι και διαθέτουν συστήματα επιλεκτικής διάχυσης της είδησης, οι οργανώσεις της διεθνούς και εγχώριας τρομοκρατίας ανακάλυψαν στο διαδίκτυο μία ατόφια και ανεξέλεγκτη μέθοδο εξάπλωσης της ιδεολογίας τους. Η κατασκευή μίας ιστοσελίδας –υπό το ένδυμα μιας καθ'όλα θεμιτής πολιτικής παρέμβασης –είναι ανέξοδη, διαθέτει επίφαση νομιμότητας και μπορεί παράλληλα η δημοσιοποίηση βίντεο εκτελέσεων προσελκύει τα σκανδαλοθηρικά "sites", αλλά και την "blogοσφαιρα", προκαλώντας το δημόσιο αίσθημα, αλλά και όλους τους "μη φυσιολογικούς" επισκέπτες, που αρέσκονται στη θέα τέτοιων αποτρόπαιων θεαμάτων.

Μία συνηθισμένη μέθοδος των τρομοκρατών είναι η χρήση ιών, κακόβουλου λογισμικού, spy ware κλπ, μικρά προγράμματα, με τα οποία καταλαμβάνουν υπολογιστές, για να τους χρησιμοποιήσουν, όταν χρειαστεί, για τη μαζική επίθεση εναντίον κυβερνητικών ή στρατιωτικών ιστοσελίδων, αλλού και εναντίον του hardware ή για την καταστροφή ολόκληρων δομών.

Μετά την 11η Σεπτεμβρίου, οι αρχές όλου του κόσμου έχουν στρέψει την προσοχή τους στο Ίντερνετ, γιατί θεωρείται το νούμερο ένα μέσο προώθησης της τρομοκρατίας. Πριν από λίγες ημέρες, μάλιστα, κέντρο παρακολούθησης του Διαδικτύου στον Καναδά ανέφερε στην ετήσια έκθεσή του πως η τρομοκρατία αποτελεί πλέον τον υπ' αριθμόν ένα κίνδυνο του Ίντερνετ. Ο ρόλος του Δικτύου στη στρατολόγηση, εκπαίδευση και χρηματοδότηση τρομοκρατών είναι πλέον πολύ σημαντικός.

Στην έκθεση αναφέρονται 7.000 ιστοσελίδες, blogs, ομάδες συζήτησης και sites με βίντεο που περιέχουν τρομοκρατικό υλικό. Από αυτά, 600 βρίσκονται στην πρώτη γραμμή επικινδυνότητας.

Ο διευθυντής της Europol, Rob Wainwright, καταθέτοντας στο ΕΚ στις 19 Απριλίου, επεσήμανε δε τη στενή σχέση τρομοκρατίας, οργανωμένου εγκλήματος, εμπορίου ναρκωτικών και την αυξανόμενη χρήση του ίντερνετ για

τη στρατολόγηση τρομοκρατών. Προσέθεσε πάντως ότι το 2010 σημαδεύθηκε από αισθητή μείωση των επιθέσεων και περισσότερες συλλήψεις υπόπτων. Ο Wainwright δήλωσε επίσης ότι οι τρομοκρατικές οργανώσεις αποδεικνύονται ολοένα και πιο ευέλικτες στον τρόπο λειτουργίας και χρηματοδότησής τους, με αυξανόμενες ενδείξεις διεθνούς συνεργασίας μεταξύ τους, με χρήση του ίντερνετ, αλλά και αυξανόμενων δεσμών μεταξύ τρομοκρατίας και οργανωμένου εγκλήματος.

Με την επίκληση του "αντιτρομοκρατικού πολέμου" και της "εθνικής ασφάλειας", πολλές χώρες έχουν προχωρήσει σε ένα ιδιότυπο καθεστώς ελέγχου και επόπτευσης του διαδικτύου. Στην Τουρκία ένας νέος νόμος που ρυθμίζει ζητήματα σχετικά με την ελεύθερη πλοήγηση στο διαδίκτυο έχει προκαλέσει τεράστιες αντιδράσεις. Το φιλτράρισμα των ιστοσελίδων με βάση τις κατηγορίες «οικογενειακό», «παιδικό», «εσωτερικό» και «κανονικό» θεωρείται ως μια προσπάθεια ελέγχου σε μια χώρα που προσπαθεί να εξελιχθεί σε μια δυτικού τύπου δημοκρατία. Στο γειτονικό Ιράν επιχειρείται μια ακόμα μεγαλύτερη επόπτευση του διαδικτύου, μέσα από την δημιουργία ενός νέου, εθνικού και πλήρως ελεγχόμενου Ίντερνετ. Αν και προβάλλεται ως φθηνότερο και αποτελεσματικότερο από το υπάρχον, σκοπός του δεν είναι άλλος από τον έλεγχο των πληροφοριών που θα εισέρχονται στην χώρα. Στην Κίνα, χαρακτηριστικό παράδειγμα χώρας με έντονη λογοκρισία, έχουν μπλοκαριστεί πάνω από 18.000 ιστοσελίδες. Με κάθε διαφωνούντα να χαρακτηρίζεται (ως συνήθως) τρομοκράτης, το κινεζικό καθεστώς σε κάθε εργατική, εθνική ή αντικαθεστωτική δράση, χρησιμοποιεί την διαδικτυακή δύναμη του, απομονώνοντας τις δράσεις αυτές από τον έξω κόσμο.

Κεφάλαιο4

CYBER-BULLYING

Ορισμός

Ο όρος **Διαδικτυακός εκφοβισμός** (Cyber-bullying) αφορά τον εκφοβισμό, την απειλή, την ταπείνωση ή την παρενόχληση παιδιών, προεφήβων και εφήβων που δέχονται μέσω της χρήσης του Διαδικτύου είτε άλλων ψηφιακών τεχνολογιών από ομηλίκους τους. Ακόμη ,παρατηρείται η συμμετοχή συνομήλικων και από τις δυο πλευρές, ή τουλάχιστον η συμμετοχή ενός ενήλικα υποκινούμενη από κάποιον ανήλικο εναντίων άλλων ανηλίκων.

Ένα φαινόμενο των τελευταίων ετών το Cyber-bullying, έχει αρχίσει και παίρνει ανησυχητικές διαστάσεις και στη χώρα μας αφού τα περισσότερα πλέον παιδιά στην εφηβεία έχουν πρόσβαση στο διαδίκτυο και διατηρούν προφίλ σε ιστοσελίδες κοινωνικής δικτύωσης

Αίτια

Συχνά οι νέοι οδηγούνται στον Διαδικτυακό εκφοβισμό εξαιτίας της βίωσης έντονων συναισθημάτων που μπορεί να προέρχεται τόσο από τις προβληματικές σχέσεις που υπάρχουν στο οικογενειακό περιβάλλον όσο και εξαιτίας μιας ευρύτερης κοινωνικής δυσλειτουργικότητας που παρουσιάζει το άτομο. Δεν είναι λίγες και οι περιπτώσεις όπου ο διαδικτυακός εκφοβισμός λειτουργεί και ως μέσον ψυχαγωγίας για τους δράστες, τα αισθήματα των οποίων ικανοποιούνται με τις αντιδράσεις των θυμάτων.

Μορφές Διαδικτυακού εκφοβισμού

- Επαναλαμβανόμενη αποστολή ηλεκτρονικών ή τηλεφωνικών μηνυμάτων
- Δημιουργία ψεύτικων διαδικτυακών προφίλ
- Είσοδος σε προσωπικούς διαδικτυακούς λογαριασμούς του ατόμου
- Αποστολή φωτογραφιών του ατόμου ή αλλού είδους μαγνητοσκοπημένου υλικού
- Αποστολή προσωπικών πληροφοριών του ατόμου σε πολλαπλούς παραλήπτες
- Αποστολή απειλητικών μηνυμάτων σε αλλά άτομα υποκρινόμενοι το άτομο που εκφοβίζεται
- Πειράγματα με στόχο τη διασκέδαση

Συνέπειες

Το φαινόμενο του Διαδικτυακού εκφοβισμού εγκυμονεί σοβαρές επιπτώσεις για την ψυχική υγεία του θύματος, αλλά και του θύτη. Η αυτοεκτίμηση του ατόμου που υφίσταται Διαδικτυακό εκφοβισμό πλήττεται έντονα τόσο ώστε σε μερικές περιπτώσεις συνδέεται με το αίσθημα της ενοχής. Το άτομο αρχίζει να αναπαράγει αρνητικές σκέψεις και η επίδοση των κοινωνικών του ικανοτήτων μειώνεται σημαντικά. Κάποιες φορές η αυτοκτονία θεωρείται ως η μοναδική λύση στο πρόβλημα. Άτομα που δέχτηκαν έντονα Διαδικτυακό εκφοβισμό ενδέχεται στο μέλλον να παρουσιάσουν μεγαλύτερη αστάθεια στις διαπροσωπικές τους σχέσεις συνοδευμένη από την κοινωνική απομόνωση.

Από την άλλη, οι εκφοβιστές τείνουν να είναι άτομα με έντονη αντικοινωνική συμπεριφορά, επιρρεπή στο αλκοόλ και απομονωμένα από τους συνομηλίκους. Μακροπρόθεσμα αντιλαμβάνονται ότι ο εκφοβισμός δεν αποτελεί μορφή ικανοποίησης και αναγνώρισης, βιώνοντας έτσι έντονη προσωπική απογοήτευση.

Τρόποι αντιμετώπισης

Οι γονείς καλούνται να ακούσουν το παιδί με προσοχή και να το προτρέψουν να αναφέρει όσο πιο αναλυτικά γίνεται τα γεγονότα και τα πρόσωπα που το έχουν φέρει σε δύσκολη θέση. "Έχουμε τη δυνατότητα να αποκλείσουμε τον αποστολέα των ενοχλητικών μηνυμάτων και να αγνοήσουμε αυτά. Όταν πρόκειται για απειλητικά μηνύματα, μπορούμε να αναφέρουμε το περιστατικό στις Αρχές (Αστυνομία).

Γενικά, μπορούμε σε κάθε περίπτωση να έρθουμε σε επικοινωνία με τις Αρχές και να προσπαθήσουμε, σε συνεννόηση με τη Διοίκηση του σχολείου, να εντοπίσουμε τη λύση στους κόλπους του σχολείου και εξωδικαστικά χωρίς να δημιουργήσουμε επιπλέον προβλήματα στα εμπλεκόμενα μέρη. Ακόμη, μέλημα του Διευθυντή της Δίωξης Ηλεκτρονικού εγκλήματος είναι στα περιστατικά cyber bullying που έρχονται στην υπηρεσία του να προσπαθεί μέσα από τον διάλογο μεταξύ των εμπλεκομένων ανήλικων μαθητών αλλά και των διευθυντών των σχολείων να βρούνε λύση χωρίς την εμπλοκή των Ανηλίκων με δικαστήρια. Επιπρόσθετα, οι άμεσα ενδιαφερόμενοι θα μπορούσαν να απευθυνθούν στη γραμμή υποστήριξης και καταγγελιών Safeline.gr.

Νομοθεσία

Σύμφωνα με όσα ορίζει η διάταξη στην παράγραφο 3 που προστέθηκε με το Ν. 3727/2008:
«**Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, αποκτά επαφή με πρόσωπο που δεν συμπλήρωσε τα 15 έτη και, με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπεια του ανηλίκου στο πεδίο της γενετήσιας ζωής του, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση, ο ενήλικος τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.» Ο νομοθέτης εδώ, με τον όρο «ή άλλου επικοινωνιακού μέσου**».

FACEBOOK

Το Facebook έχει καταστεί σημαντικό εργαλείο στα χέρια τρομοκρατών ,όλο και περισσότεροι τρομοκράτες χρησιμοποιούν το Facebook, με σκοπό να προσεγγίσουν πιθανούς υποστηρικτές, να σχεδιάσουν τρομοκρατικές επιθέσεις καθώς τους επιτρέπεται να συγκεντρώσουν παντός τύπου πληροφορίες, οι οποίες συχνά αφορούν προσωπικά δεδομένα χρηστών που χρησιμοποιούν για παράνομους σκοπούς. Επιπλέον, δύνανται να έρθουν σε επαφή μέσω του διαδικτύου εύκολα και ανώνυμα, επιτυγχάνοντας έτσι καλύτερη οργάνωση των τρομοκρατικών τους σχεδίων. Πρόσφατη, μάλιστα έρευνα του **Ελληνικού Κέντρου Ασφαλούς Διαδικτύου** έδειξε ότι τρεις στους δέκα εκπαιδευτικούς (ποσοστό 32%) στην Ελλάδα έχουν έρθει αντιμέτωποι στο σχολείο, με κάποιο ζήτημα ψηφιακής παρενόχλησης, ψηφιακού εκφοβισμού ή συκοφαντικής δυσφήμισης μαθητών από άλλους μαθητές μέσω κινητού τηλεφώνου, Facebook ή άλλης διαδραστικής πλατφόρμας.

'Ένας έφηβος που θα δεχθεί τέτοιο εκφοβισμό είναι σημαντικό να θέσει τα όρια του και να μην απαντήσει με τον ίδιο τρόπο, εξαπολύοντας απειλές ή βρίζοντας. Πρέπει οπωσδήποτε να αναφέρει το περιστατικό σε ένα ενήλικα, είτε πρόκειται για γονείς είτε κάποιο εκπαιδευτικό ή άλλο κοντινό και έμπιστο άτομο και φυσικά να το καταγγείλει, ακόμα και μόνος του. Μπορεί να απευθυνθεί στη γραμμή **Safeline 2811 391615** ή απευθείας στη Δίωξη ηλεκτρονικού εγκλήματος, όταν δέχεται σοβαρές απειλές.

Κεφάλαιο 5

Ξέπλυμα μαύρου χρήματος

Ορισμός μαύρου χρήματος

Με τον όρο βρώμικο χρήμα, ή μαύρο χρήμα και ευρύτερα μαύρα, καθιερώθηκε να χαρακτηρίζεται, περισσότερο δημοσιογραφικά, οποιοδήποτε είδος εσόδου από παράνομη πράξη, ή ακόμη και έσοδο από νόμιμη πράξη το οποίο στη συνέχεια δεν δηλώνεται, κατά παράβαση της υφιστάμενης φορολογικής νομοθεσίας. Και στις δύο περιπτώσεις ανάγεται σε οικονομικό έγκλημα.

Στην μεν πρώτη περίπτωση το προϊόν της παράνομης πράξης δεν δηλώνεται προκειμένου να μην αποκαλυφθεί αυτή και οι δράστες της, στη δε δεύτερη περίπτωση για να μην υποστεί φορολογική επιβάρυνση, που επίσημα χαρακτηρίζεται αδήλωτο έσοδο.

Συνέπεια αυτού του χαρακτηρισμού είναι κατ᾽ αντίθεση η διάκριση του χρήματος σε «καθαρό χρήμα» που προέρχεται από νόμιμες δραστηριότητες και το οποίο στη συνέχεια δεν υποκρύπτεται και το «βρώμικο χρήμα», ή «μαύρο χρήμα» που υποκρύπτεται.

Συνέχεια των παραπάνω «ξέπλυμα χρήματος», ή «ξέπλυμα μαύρου χρήματος», (που λέγεται κατ᾽ έμφαση, ή πλεονασμό), καθιερώθηκε ομοίως να χαρακτηρίζεται οποιαδήποτε οικονομική συναλλαγή που γίνεται με διάθεση

μαύρου χρήματος, επί νόμιμης πράξης που επιφέρει οικονομικό αγαθό το οποίο στη συνέχεια δεν υποκρύπτεται, μεταβαλλόμενο έτσι σε καθαρό χρήμα. Απλούστερα παραδείγματα είναι η κατάθεση μαύρου χρήματος σε τράπεζα και στην συνέχεια η ανάληψη για κάλυψη οικονομικών αναγκών, ή η απ' ευθείας αγορά μετοχών από χρηματιστήριο, κ.ά.

Φορείς μαύρου χρήματος ή ξεπλύματος χρήματος μπορεί να είναι τόσο φυσικά πρόσωπα όσο και νομικά πρόσωπα (ιδιωτικού ή δημοσίου δικαίου), ή ακόμα και κυβερνήσεις χωρών. Γενικά το μαύρο χρήμα και οι όποιες δραστηριότητες επ' αυτού συνιστούν ευρύτερα την έννοια της παραοικονομίας. Αναφορά σε πολύ μεγάλα ποσά μαύρου χρήματος τότε αυτή ανάγεται σε εκδήλωση οργανωμένου εγκλήματος.

Τα διάφορα κράτη προκειμένου να αντιμετωπίσουν φαινόμενα παραγωγής μαύρου χρήματος θεσπίζουν κατάλληλες νομοθεσίες για την πάταξή τους, μεταξύ των οποίων μπορεί να είναι ειδικές ελεγκτικές υπηρεσίες, περιορισμοί ελεύθερης διακίνησης χρήματος, κ.λπ.

Το Ξέπλυμα Μαύρου Χρήματος αφορά την διαδικασία με την οποία τα παράνομα έσοδα μετατρέπονται σε νόμιμα. Σχεδόν σε όλες τις χώρες έχουν παρατηρηθεί φαινόμενα ξεπλύματος μαύρου χρήματος και συνήθως αφορούν την μεταφορά των χρημάτων σε διάφορες χώρες με στόχο την απόκρυψη της προέλευσης τους. Τα άτομα που προσπαθούν να ξεπλύνουν τα χρήματα τους το κάνουν με στόχο να μπορέσουν να τα χρησιμοποιήσουν , διότι σε άλλη περίπτωση οι συναλλαγές που θα πραγματοποιήσουν θα τους συνδέσουν με τις παράνομες δραστηριότητες από όπου προήλθαν και τα χρήματα. Τα παράνομα έσοδα μπορούν να προέρχονται από διάφορες συναλλαγές ,Ωστόσο οι συνηθέστερες περιπτώσεις είναι οι εξής: εμπόριο, ναρκωτικών ,Υπεξαίρεση ,Διεφθαρμένοι πολιτικοί ,Δημόσιοι λειτουργοί ,Μαφιόζοι ,Απατεώνες.

Η Βασική διαδικασία ξεπλύματος χρημάτων γίνεται σε τρία στάδια :

1.Placement –Σε Αυτό το στάδιο Τα λεφτά τοποθετούνται σε ένα νόμιμο οικονομικό ίδρυμα .Τις Περισσότερες φορές είναι τράπεζα ,Οπότε τα χρήματα έχουν την μορφή τραπεζικών καταθέσεων .Σε Αυτό το στάδιο υπάρχει και το μεγαλύτερο ρίσκο της όλης διαδικασίας καθώς μεγάλα ποσά καταθέσεων κινούν υποψίες και οι τράπεζες είναι υποχρεωμένες να αναφέρουν υψηλής αξίας συναλλαγές.

2Layering Το Στάδιο του layering αφορά την μεταφορά των χρημάτων σε μία αλυσίδα οικονομικών συναλλαγών με στόχο να καταστήσουν δύσκολη την παρακολούθηση της πορείας τους .Τα layering μπορεί να αποτελείται από διάφορες τραπεζικές συναλλαγές και εμβάσματα μεταξύ διαφορετικών

τραπεζικών λογαριασμών σε διαφορετικά ονόματα και σε διαφορετικές χώρες , Γίνονται καταθέσεις και αναλήψεις έτσι ώστε να αλλάζει συνεχώς το ποσό των χρημάτων στους λογαριασμούς και το νόμισμα Επίσης Αγοράζονται αγαθά υψηλής αξίας (αυτοκίνητα ,σκάφη ,σπίτια κ.τ.λ.) Έτσι ώστε να αλλάζει μορφή των χρημάτων. Αυτό Το στάδιο είναι και το πιο πολύπλοκο της όλης διαδικασίας και ως στόχο έχει να κάνει τα «μαύρα» Χρήματα όσο το δυνατόν πιο δύσκολο να εντοπιστούν .

3Integration Στο Στάδιο του integrate, τα χρήματα επανατοποθετούνται στο κυρίως οικονομικό σύστημα σε νόμιμη μορφή καθώς πλέον φαίνεται

ότι προέρχονται από νόμιμες συναλλαγές .Όταν αναφερόμαστε στο κυρίως οικονομικό σύστημα εννοούμε την τελική μεταφορά των χρημάτων σε λογαριασμό κάποιας τοπικής επιχείρησης στην οποία τα πλέον νόμιμα χρήματα επενδύονται και φαίνεται ότι έχουν προέλθει από την πώληση κάποιου σκάφους στο στάδιο του layering ή κάποιας άλλης αγοράς.

Οι εποχές που το ξέπλυμα βρώμικου χρήματος γινόταν σε καζίνο, μέσω ασφαλιστήριων συμβολαίων ή με δελτία Προ-Πο ανήκουν πια στο παρελθόν. Πλέον, οι κακοποιεί έχουν πολύ περισσότερες δυνατότητες χάρη στο Internet. Πως όμως πραγματοποιείται το ξέπλυμα; Ποια είναι τα εργαλεία που υπάρχουν για τη μετατροπή "μαύρου" χρήματος σε νόμιμο εισόδημα;

Ψηφιακά νομίσματα

Μια πολύ διαδεδομένη πρακτική είναι μέσω ψηφιακών νομισμάτων τύπου Bitcoin, WebMoney κλπ. Η διαδικασία είναι απλή: αγοράζει κανείς ψηφιακά νομίσματα χρησιμοποιώντας "μαύρο" χρήμα και στη συνέχεια κάνει πληρωμές σε τρίτο ο οποίος μετατρέπει το ψηφιακό νόμισμα σε φυσικό. Με δεδομένο ότι στην περίπτωση των υπηρεσιών αυτών δεν έχουν πιστοποίηση ταυτότητας, όπως λ.χ. στο Paypal, όλα γίνονται πολύ πιο εύκολα.

Online Gaming

Όσο και αν ακούγεται περίεργο, ανάμεσα στους φανατικούς των online παιχνιδιών, υπάρχουν και οι "επαγγελματίες". Σε παιχνίδια ή ψηφιακούς κόσμους (όπως λ.χ. στο Second Life ή στο World of Warcraft) μπορεί κανείς να αγοράσει με πραγματικό χρήμα ψηφιακά αγαθά και υπηρεσίες και όσα δε χρησιμοποιήσει, στη συνέχεια να τα ξαναμετατρέψει σε ρευστό, αυτή τη φορά νόμιμο.

Παραπλανητικά e-mail

Λογικά όλοι κάποια στιγμή έχουμε λάβει spam mails όπου μας προτείνουν τη συμμετοχή σε κάποια έξυπνη επιχειρηματική κίνηση, από την οποία μπορούμε να βγάλουμε εύκολα εκατομμύρια, απλά μεταφέροντας ποσά μέσω του λογαριασμού μας. Παρότι πολλές φορές στόχος των e-mail αυτών είναι το άδειασμα των λογαριασμών, υπάρχουν πολλές περιπτώσεις όπου πραγματικά γίνονται μεταφορές χρημάτων και πραγματικά ο "συνεργάτης" προσφέρει και αμοιβή, πολύ απλά γιατί έχουμε μετατραπεί σε συνεργό του.

Προσφορά εργασίας από το σπίτι

Με παρόμοιο τρόπο μπορεί να λειτουργούν και αγγελίες για εργασία από το σπίτι που προσφέρουν εύκολα λεφτά σε σύντομο χρονικό διάστημα. Αντικείμενο της εργασίας μπορεί απλά να είναι ...η μεταφορά χρημάτων μέσω του λογαριασμού του εργαζομένου, με άλλα λόγια το ξέπλυμα χρήματος.

Online στοιχιματικές υπηρεσίες

Αποτελεί μάλλον και τον πιο γνωστό τρόπο ξεπλύματος χρήματος στη χώρα μας, καθώς πολλά έχουν ακουστεί σχετικά με το στοίχημα και τους αγώνες ποδοσφαίρου στην Ελλάδα. Η διαδικασία είναι απλή, αρκεί να έχεις τους κατάλληλους συνεργάτες, προέδρους ομάδων, ποδοσφαιριστές ή διαιτητές. Τοποθετείς τα χρήματα που θέλεις να ξεπλύνεις σε συγκεκριμένους αγώνες και στη συνέχεια εισπράττεις το κέρδος ως νόμιμο χρήμα. Προφανώς, συνεννοημένη πρέπει να είναι και η online στοιχιματική εταιρεία, η οποία θα "ζητήσει" το ισοζύγιο κερδών και "χασούρας" να είναι αντίστοιχο με τη γκανιότα της.

Επιπτώσεις του ξεπλύματος χρήματος

Η οικονομική βιβλιογραφία υποδεικνύει ότι το ξέπλυμα χρήματος μπορεί να διαστρεβλώσει τα οικονομικά δεδομένα και κατά συνεπεία τη μακροοικονομική ανάλυση και πολιτική. Επίσης, υπάρχουν άμεσες επιπτώσεις στην αποταμίευση ως αποτέλεσμα αλλαγών στην διανομή εισοδήματος και στη διάβρωση της εμπιστοσύνης των χρηματοοικονομικών αγορών. Οι επιπτώσεις επηρεάζουν το θύμα ,το δράστη ,το δημόσιο τομεα , την οικονομία και την κοινωνία και άλλοτε εμφανίζονται άμεσα και μακροπρόθεσμα.

Επιπτώσεις στο θύμα και στο δράστη :

Το ξέπλυμα χρήματος συνδέεσαι πάντα με ένα διαπραχθέν αδίκημα και αυτό έχει σαν αποτέλεσμα τα κεφαλαία που παράγονται να περνάνε από την κατοχή του θύματος στον δράστη. Έτσι λοιπόν γίνεται ανακατανομή πλούτου από το θύμα στο θύτη κάνοντας την ανίχνευση του πιο δύσκολη, ώστε οι δράστες να μπορούν να απολαύσουν τους καρπούς των κοπών τους. Όπως αναφέρει ο Mackrell (1997) , το ξέπλυμα χρήματος κάνει κάποια αδικήματα να αξίζουν, χαρίζει νομιμότητα και σεβασμό στους πιο αναξίους ανθρώπους στην κοινωνία, δίνει οικονομική δύναμη σε εγκληματίες στερώντας την από τον νομό. Έτσι λοιπόν .Σαν αποτέλεσμα του ξεπλύματος χρήματος τα εγκλήματα αποδίδουν . Αυτό το άμεσο αποτέλεσμα του ξεπλύματος χρήματος δηλαδή απώλειες των θυμάτων και τα κέρδη των δραστών του εγκλήματος επισημαίνονται και από το διεθνές νομισματικό ταμείο (1998).

Επιπτώσεις στην παραγωγή ,το εισόδημα και την εργασία:

Το ξέπλυμα χρήματος μειώνει την παραγωγή και την εργασία αφού μεταφέρει τα κεφαλαία από τομείς με μεγάλη παραγωγικότητα π.χ. ρούχα, παπούτσια , σε πιο στείρους τομείς π.χ. έργα τέχνης , κοσμήματα. Αυτό οδηγεί σε καθαρή ζημία στην οικονομία ασχέτως με το που θα ξοδεύονταν τα κεφαλαία διαφορετικά.

Οδηγίες εντοπισμού ύποπτων συναλλαγών για «ξέπλυμα μαύρου χρήματος»

Οδηγίες προς συγκεκριμένες κατηγορίες επιχειρήσεων και επαγγελματιών (φοροτεχνικούς, λογιστές, κτηματομεσίτες, εταιρείες κεφαλαίου επιχειρηματικών συμμετοχών) για τους τρόπους με τους οποίους θα εντοπίζουν ύποπτες

περιπτώσεις για «ξέπλυμα μαύρου χρήματος» περιλαμβάνονται σε εγκύκλιο της Γενικής Γραμματείας Δημοσίων Εσόδων του υπουργείου Οικονομικών. Μεταξύ άλλων καλούνται τα αρμόδια στελέχη και υπεύθυνοι των επιχειρήσεων αυτών να είναι ιδιαίτερα προσεκτικοί όταν εντοπίζουν τα ακόλουθα:

1. Απροθυμία πελάτη να προσκομίσει κατά τη σύναψη της συναλλαγής τα προβλεπόμενα έγγραφα επαλήθευσης της ταυτότητάς του ή προσκόμιση εγγράφων αμφιβόλου γνησιότητας ή παροχή ανεπαρκών ή ανακριβών πληροφοριών.
2. Εκπρόσωπος νομικού προσώπου, αρνείται να δώσει τα προβλεπόμενα έγγραφα πιστοποίησης της ταυτότητας του νομικού προσώπου.
3. Επιμονή του πελάτη για πληρωμή σε μετρητά συναλλαγών άνω των 15.000 ευρώ.
4. Υπάρχουν πληροφορίες από εξωτερική πηγή ότι πελάτης εμπλέκεται σε δραστηριότητες που πιθανώς συνδέονται με φοροδιαφυγή ή ότι διάγει πολυτελή βίο.
5. Διενεργούνται συχνές ή σημαντικού ύψους συναλλαγές.
6. Χρησιμοποιείται προσωπικός λογαριασμός του ιδιοκτήτη ή του υπαλλήλου εταιρείας, αντί του εταιρικού λογαριασμού, για τη διενέργεια συναλλαγών.
7. Πραγματοποιούνται αγορές αγαθών μεγάλης αξίας, όπως σκαφών αναψυχής, πολυτελών αυτοκινήτων ή έργων τέχνης, από πρόσωπα εγκατεστημένα σε περιοχή εξωχώριων δραστηριοτήτων ή χώρα χαμηλής φορολογίας.
8. Δικηγόρος χρησιμοποιεί προσωπικούς του λογαριασμούς για συναλλαγές προσώπων που εκπροσωπεί.
9. Ασυνήθης νευρικότητα κατά τη διεξαγωγή συναλλαγής.
10. Μη επίδειξη εύλογου ενδιαφέροντος από τον πελάτη για τους όρους της συναλλαγής.
11. Άρνηση του πελάτη να έχει προσωπικές επαφές με την επιχείρηση.
12. Επαναλαμβανόμενες όμοιες συναλλαγές για ποσά λίγο κάτω από το ελάχιστο όριο των 15.000 ευρώ
13. Συχνή αλλαγή διεύθυνσης που δεν δικαιολογείται από την επαγγελματική δραστηριότητα.
14. Περιπτώσεις πελατών με αλλαγή του βιοτικού τους επιπέδου.
15. Το τηλέφωνο του σπιτιού ή της επιχείρησης του πελάτη είναι απενεργοποιημένο.
16. Η ύπαρξη υπόνοιας ίδρυσης εικονικών επιχειρήσεων.
17. Αγοραπωλησία ακινήτου χωρίς να έχει τηρηθεί ο απαιτούμενος από τον νόμο τύπος, π.χ. με ιδιωτικό συμφωνητικό.
18. Το ακίνητο έχει περιέλθει στην κυριότητα του πωλητή πολύ πρόσφατα (διαδοχικές αγοραπωλησίες).

17. Οι ενδεικτικές περιπτώσεις συμπεριφοράς υπαλλήλων υπόχρεων προσώπων που μπορεί να θεωρηθούν ως ύποπτες για πρόθεση νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες είναι οι ακόλουθες:
18. Ο υπάλληλος κάνει σπάταλο τρόπο ζωής που δεν μπορεί να δικαιολογηθεί από τον μισθό του.
19. Ο υπάλληλος παραλείπει να συμμορφωθεί με αναγνωρισμένες πολιτικές διαδικασίες και μεθόδους.
20. Ο υπάλληλος είναι απρόθυμος να πάρει άδεια.
21. Αλλαγές στην απόδοση ή στον τρόπο συμπεριφοράς του υπαλλήλου.
22. Υπάλληλος διατηρεί κοινωνικές σχέσεις πέραν του συνήθους με πελάτες της εταιρείας.

Κεφάλαιο 6

Παιδική Πορνογραφία

Τι είναι παιδική πορνογραφία

Οι αναζητήσεις που αφορούν την παιδική πορνογραφία ανέρχονται στις 116.000. Η παιδική πορνογραφία αποτελεί μια ιδιαίτερη μορφή παιδικής σεξουαλικής κακοποίησης, μαζί με την παιδική πορνεία, την παιδεραστία, την ασέλγεια, τις θωπείες και την επίδειξη. Η έξαρση της παιδικής πορνογραφίας είναι που προκαλεί ιδιαίτερα μεγάλη αίσθηση, καθώς συγκεκριμένα στη Δυτική Ευρώπη έχουν αποκαλυφθεί πολλά τέτοια κυκλώματα. Στην Ελλάδα άλλαξε ο ποινικός κώδικας όσον αφορά την τιμωρία τέτοιων αδικημάτων, συγκεκριμένα ,η παιδική πορνογραφία τιμωρείται και όταν σκοπός του δράστη δεν είναι η αποκόμιση κέρδους, ο οποίος σκοπός βέβαια, θεωρείται επιβαρυντική περίπτωση, όταν υφίσταται. Προσδιορίζεται ως τιμωρητέο υλικό παιδικής πορνογραφίας η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο φορέα του σώματος ή μέρους του σώματος ανηλίκου, με τρόπο που καταφανώς προκαλεί γενετήσια διέγερση.

Είναι γεγονός πως η παιδική πορνογραφία στιγματίζει ανεπανόρθωτα ένα παιδί γι’αυτό και οι γονείς είναι ιδιαιτέρως επιφυλακτικοί και προσπαθούν να προστατεύσουν τα παιδιά τους από τους κινδύνους του διαδικτύου ,οι οποίοι ελλοχεύουν και μέσω της παρακολούθησης τέτοιον υλικών

Σεξουαλική κακοποίηση είναι οποιουδήποτε τύ.που επαφή ενός ενήλικου (παιδόφιλος) με ένα παιδί με στόχο τη σεξουαλική ικανοποίηση του ενηλίκου, ο οποίος έχει πάντα την αποκλειστική ευθύνη μιας τέτοιας πράξης.

Ο παιδόφιλος, στα γενικά του χαρακτηριστικά, είναι συνήθως άντρας, άνω των 30 ετών, με λίγους φίλους της ηλικίας του και συχνάζει σε χώρους με παιδιά όπως παιδικές χαρές, Ίντερνετ καφέ, αθλητικά κέντρα κ.α. Συχνά μάλιστα εργάζεται με παιδιά, ενώ δεν αποκλείεται να είναι άτομο «υπεράνω πάσης υποψίας». Σε

πολλές περιπτώσεις είναι γνωστό μέλος της εκάστοτε τοπικής κοινωνίας και συνήθως ανήκει στο περιβάλλον του παιδιού ή και της οικογένειας.

Όπως έχει αποδειχθεί σε αρκετές περιπτώσεις στην πράξη, χρησιμοποιεί τα ηλεκτρονικά μέσα κοινωνικής δικτύωσης, προκειμένου να αποκτήσει πρόσβαση σε παιδιά, ενώ ενδέχεται να προσποιείται τον έφηβο για να συζητά και να παίζει παιχνίδια μαζί τους στο Διαδίκτυο. Στοχεύει σε συγκεκριμένες ηλικίες και φύλο, συνήθως παιδιά προεφηβικής ηλικίας, και δρα μεθοδικά και με υπομονή για να κερδίσει την εμπιστοσύνη τους. Μπορεί επίσης να προβεί σε πράξεις συναισθηματικού εκβιασμού ή να απειλήσει το παιδί, προκειμένου να μην αποκαλύψει τις δραστηριότητές του στους γονείς του.

Μιλήστε στα παιδιά σας, κερδίστε την εμπιστοσύνη τους. Πρέπει να πιστεύουν ότι μπορούν να σας πουν οτιδήποτε χωρίς να φοβούνται ή να ντρέπονται. Μιλήστε τους για το σώμα τους. Πείτε τους τι να προσέχουν. Διδάξτε τους τις συμπεριφορές που είναι αποδεκτές απέναντι στους άλλους ενήλικες, αλλά και απέναντι στα παιδιά της ηλικίας τους.

Κίνδυνοι Κοινωνικών Δικτύων (Facebook)

Οι κίνδυνοι στο facebook και η χρήση των social networks είναι από τα μεγαλύτερα θέματα συζήτησης των ημερών. Τα δίκτυα κοινωνικής δικτύωσης (social network) γοητεύουν τους μαθητές, που βρίσκουν ότι η ηλεκτρονική κοινωνική δικτύωση είναι ο βολικότερος τρόπος επικοινωνίας.

Σε έρευνα που πραγματοποιήθηκε για τη χρήση του facebook από μαθητές διαπιστώθηκαν τα εξής:

• Τα κορίτσια καταλαμβάνουν ακραίες θέσεις, δηλαδή είτε χρησιμοποιούν το Facebook πολλές ώρες ή είναι περιστασιακοί χρήστες, Τα αγόρια εμφανίζονται

πιο ευνοϊκά διακείμενα απέναντι στην κοινωνική δικτύωση από ότι τα κορίτσια. και είναι περισσότερο εξαρτημένα από τη χρήση του Facebook.

• Οι περιστασιακοί χρήστες του Facebook στην πλειοψηφία τους ασχολούνται με τους φίλους τους, ενώ όσοι επενδύουν πολύ χρόνο είναι κατά κύριο λόγο μοναχικοί χρήστες.

• Πολλοί θεώρησαν ότι η ηλεκτρονική κοινωνική δικτύωση είναι ο βολικότερος τρόπος επικοινωνίας, που θα αντικαταστήσει το email και τις πιο συμβατικές μορφές διάδρασης. Κανόνιζαν τα ραντεβού τους μέσω του Facebook αντί να τηλεφωνήσουν, συζητούσαν γι' αυτό με τους φίλους τους και χρησιμοποιούσαν την ηλεκτρονική ιδιόλεκτο (αργκό).

• Πολλοί χρήστες δήλωσαν ότι αυτό που τους συναρπάζει στο Facebook είναι ότι γνωρίζουν άτομα που μοιράζονται τα ίδια ενδιαφέροντα, ότι έχουν πρόσβαση σε πληροφορίες που τους ενδιαφέρουν, ακόμη και ότι συγκροτούν ομάδες μελέτης για τις εξετάσεις.

• Οι περισσότεροι δήλωσαν ότι μέσω της εφαρμογής αυτής κατάφεραν να επανασυνδεθούν με άτομα ή φίλους που είχαν χάσει εδώ και καιρό.

• Αρκετοί χρήστες είχαν κουραστεί από το 'φακέλωμα' μέσω Facebook, μέσω του οποίου ο καθένας γνώριζε και μετέδιδε ποια η ψυχική διάθεση του χρήστη, τι έκανε όλες τις χρονικές στιγμές κλπ. Οι περισσότεροι από αυτούς πιστεύουν ότι η μόδα του Facebook θα περάσει και θα αντικατασταθεί με κάτι πολύ πιο ενδιαφέρον, επειδή ξεπέρασε το μέτρο. Το διαδίκτυο έχει κανόνες αυτορρύθμισης

Το Facebook παρέχει το προσωπείο της αυτοεκτίμησης. Πολλοί αρθρώνουν συναισθήματα μέσα από αυτό, που δεν θα τολμούσαν να τα πουν στην πραγματική ζωή. Το ένστικτο και το συναίσθημα απελευθερώνεται. Αρκετοί χρήστες διατηρούσαν παραπάνω από δύο λογαριασμούς στο Facebook με διαφορετικά χαρακτηριστικά κάθε φορά. Πολλαπλές και σχιζοειδείς προσωπικότητες.

• Σε χρήστες μικρότερης ηλικίας αναπτύσσεται ανταγωνισμός για το ποιος θα προσελκύσει περισσότερους φίλους, κυρίως του αντιθέτου φύλου

• Οι γυναίκες χρήστες προβάλλουν τις περισσότερες φορές ένα μυστηριώδη εαυτό, που περιμένει να ανακαλυφθεί από κάποιο χρήστη με έξοχα προσόντα, γρήγορο στη γραφή και με καλές ατάκες. Οι φωτογραφίες που τοποθετούν στο προφίλ τους είναι προκλητικές μερικές φορές ή παρμένες από τον κόσμο των κινουμένων σχεδίων. Οι άντρες χρήστες συνήθως επαίρονται για τα σωματικά τους προσόντα και για τον 'τσαμπουκά' που μπορούν να επιδείξουν

Επιπλέον πολύς κόσμος κρύβει την πραγματική του ηλικία, αλλά οι ερευνητές διατείνονται ότι όταν επιτρέπεις στα παιδιά να παραβαίνουν τους κανόνες στέλνεις λάθος μήνυμα. Και, όπως υποστηρίζουν, αφήνεις τα παιδιά χαλαρά σε έναν ψηφιακό κόσμο για τον οποίο μπορεί να μην είναι προετοιμασμένα, εκθέτοντάς τα στις απειλές της πραγματικής ζωής.

Πραγματική περίσταση αληθούς γεγονότος

Οι κίνδυνοι για τα μικρής ηλικίας μέλη των κοινωνικών δικτύων δεν είναι υποθετικοί. Ο Χεμανσού Νίγκαμ, ο πρώην αξιωματούχος ασφαλείας του MySpace, που σήμερα διευθύνει μια εταιρεία συμβούλων για την ασφάλεια στο Ιντερνετ, θυμάται ένα πρόσφατο συμβάν. Στην πολιτεία της Νέας Υόρκης, είπε, ένα 11χρονο αγόρι έκανε φίλη στο Facebook ένα κορίτσι από την τάξη του. Αλλά ο λογαριασμός του κοριτσιού ήταν ψεύτικος και το πρόσωπο που βρισκόταν πίσω από αυτόν άρχισε να ανεβάζει φωτογραφίες του αγοριού σε ιστοσελίδες σεξουαλικού περιεχομένου, συνοδεύοντάς θες με πρόστυχα σχόλια.

Όταν οι φωτογραφίες του αγοριού άρχισαν να εμφανίζονται σε αναζητήσεις του Google, το σχολείο υποψιάστηκε ότι τις είχε ανεβάσει ο ίδιος και κάλεσε τους γονείς του. Τα άλλα παιδιά άρχισαν να τον πειράζουν. «Μπορεί να εξελιχθεί σε εφιάλτη για έναν 11χρονο, που ήθελε απλώς να συνομιλεί με φίλους του», είπε ο κ. Νίγκαμ. Το 2006, 31% των 12χρονων στις Ηνωμένες Πολιτείες χρησιμοποιούσαν σελίδες κοινωνικής δικτύωσης, σύμφωνα με έρευνα του Κέντρου Pew, και το ποσοστό αυτό αυξήθηκε στο 38% στα μέσα του 2009, οπότε πραγματοποιήθηκε η τελευταία σχετική έρευνα

Το ComScore, μια εταιρεία που μετράει την κίνηση στο Διαδίκτυο, υπολογίζει ότι 3,6 εκατ. από τους 153 εκατ. επισκέπτες μηνιαίως του Facebook στη χώρα είναι κάτω των 12 ετών. Κάποιοι από αυτούς τους επισκέπτες μπορεί να μην έχουν λογαριασμό και απλώς επισκέπτονται τις κοινές σελίδες, ανέφερε το ComScore.

Οι εταιρείες Ιντερνέτ έχουν συστήσει κανόνες για τους χρήστες μικρής ηλικίας, επειδή πρέπει να συμμορφωθούν με τον Νόμο για την Ηλεκτρονική Προστασία των Παιδιών του 1998, σύμφωνα με τον οποίο οι ιστοσελίδες που συλλέγουν πληροφορίες από παιδιά κάτω των 13 ετών πρέπει να έχουν τη γονική συναίνεση. Η απόκτηση όμως αυτής της συναίνεσης είναι περίπλοκη και ακριβή υπόθεση, οπότε εταιρείες όπως η Facebook και η Google, στην οποία ανήκει το YouTube, απορρίπτουν όποιον προσπαθεί να εγγραφεί σε ηλικία κάτω των 13 ετών. Facebook, Google και Yahoo αρνήθηκαν να αποκαλύψουν πόσα παιδιά περνούν τα εμπόδια, αλλά διατείνονται ότι προσπαθούν να εφαρμόσουν τους κανόνες.

Οι σελίδες κοινωνικής δικτύωσης δεν διαθέτουν δικλίδες ασφαλείας για τα μικρά παιδιά και παρότι το Facebook διαθέτει τέτοιες, εντούτοις τα παιδιά που υποκρίνονται ότι είναι πάνω από 18 τις παρακάμπτουν, με αποτέλεσμα να μένουν εκτεθειμένα.

Πρόληψη γονέων για την παιδική πορνογραφία

Συζητείστε με το παιδί σας για τους κινδύνους του Διαδικτύου, χωρίς βέβαια να απαγορεύσετε τη χρήση του. Εξηγείστε του ότι δεν πρέπει να δίνει προσωπικές πληροφορίες (ονοματεπώνυμο, διεύθυνση κ.λπ.) ή να στέλνει φωτογραφίες σε αγνώστους μέσω Διαδικτύου.

Σκόπιμο είναι να φροντίσετε ώστε να έχετε πρόσβαση στο Διαδίκτυο από το σπίτι, ώστε να μπορείτε να ελέγχετε τις ηλεκτρονικές δραστηριότητες του παιδιού σας και να μη χρειάζεται να πηγαίνει σε Ίντερνετ καφέ.

Ρωτήστε το παιδί σας ποιες ιστοσελίδες επισκέπτεται ή/και ελέγξτε το μόνοι σας μέσω των «αγαπημένων» και του «ιστορικού περιήγησης» του προγράμματος φυλλομετρητή (browser) και κάντε του προτάσεις για ηλεκτρονικές διευθύνσεις κατάλληλες για την ηλικία του.

Λάβετε επίσης υπόψη ότι τα παιδιά στην εφηβεία μπορεί να είναι αντιδραστικά και να αναζητούν την ιδιωτικότητα, ενώ πολλές αλλαγές στη συμπεριφορά τους μπορεί να οφείλονται στο σεξουαλικό ξύπνημα της εφηβικής ηλικίας. Σταθείτε δίπλα τους με τρόπο διακριτικό και όχι παρεμβατικό.

Παιδική πορνογραφία ορίζεται ως οι αναπαραστάσεις ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες. Μερικές φορές ο ορισμός περιλαμβάνει εικόνες που

έχουν υποστεί επεξεργασία από ηλεκτρονικό υπολογιστή. Η παιδική πορνογραφία θεωρείται έγκλημα και υπόκειται σε ποινικές κυρώσεις.

Η παιδική πορνογραφία ορίζεται διαφορετικά από τη νομοθεσία της κάθε χώρας. Σύμφωνα με τη Σύμβαση για τα Διαδικτυακά Εγκλήματα του Συμβουλίου της Ευρώπης, η παιδική πορνογραφία έχει τις εξής μορφές:

Ένας ανήλικος που συμμετέχει σε σεξουαλική δραστηριότητα.

Ένα άτομο που συμμετέχει σε σεξουαλική δραστηριότητα προσποιούμενο ότι είναι ανήλικο.

Ρεαλιστικές εικόνες που αναπαριστούν ένα ανήλικο να συμμετέχει σε σεξουαλικές δραστηριότητες.

Η εξάπλωση των κυκλωμάτων παιδοφιλίας είναι ανησυχητική. Τα κυκλώματα αυτά είναι ομάδες ατόμων, τα οποία εργάζονται μαζί μέσω του Διαδικτύου με στόχο τη συλλογή και διανομή πορνογραφικού υλικού για τη δική τους ικανοποίηση. Τέτοιες ενέργειες αποτελούν έγκλημα και υπόκεινται στο νόμο.

Πού μπορεί να συμβεί:

- Σε ιστοσελίδες τις οποίες χειρίζονται κυκλώματα παιδοφιλίας
- Σε ηλεκτρονικά μηνύματα με φωτογραφίες παιδικής πορνογραφίας
- Αντιμετώπιση:
- Αν γνωρίζουμε κάποιον που ασχολείται με την παιδική πορνογραφία, τον καταγγέλλουμε στην ιστοσελίδα www.cyberethics.info, στο τηλέφωνο 22674747 (Γραμμή Καταγγελιών HotLine) ή/και στην αστυνομία.
- ✓ Αποφεύγουμε διαδικτυακές συζητήσεις με αγνώστους και κυρίως δεν συμφωνούμε ποτέ να συναντήσουμε κάποιο «φίλο» που, μόλις γνωρίσαμε διαδικτυακά.
- ✓ Αν κάποια διαδικτυακή συζήτηση μάς κάνει να νιώσουμε άβολα την σταματάμε αμέσως και αναφέρουμε το γεγονός σε κάποιο ενήλικα
- ✓ Δεν στέλνουμε φωτογραφίες που είναι δυνατό να μας εκθέσουν μέσω του ηλεκτρονικού ταχυδρομείου.
- ✓ Δεν ανεβάζουμε σε ιστοσελίδες κοινωνικού δικτύου π.χ. στο Facebook ή Hi5 φωτογραφίες μας, οι οποίες είναι προκλητικές.

Νομοθεσία παιδικής πορνογραφίας

Στελέχη της Δίωξης Ηλεκτρονικού Εγκλήματος, μετά από αστυνομική διαδικτυακή έρευνα, πραγματοποίησαν τον τελευταίο μήνα παράλληλες επιχειρήσεις σε Αττική, Θεσσαλονίκη, Ροδόπη, Ηράκλειο και Χανιά, όπου διαπιστώθηκε ότι 15 κατηγορούμενοι κατείχαν σε ψηφιακή μορφή «σκληρό» υλικό παιδικής πορνογραφίας.

Από την περαιτέρω ψηφιακή ανάλυση των ηλεκτρονικών ιχνών, προέκυψε ότι δύο από τους κατηγορούμενους προσέλκυαν ανήλικους, μέσω forums, chat-rooms και των social media καθώς προφασιζόμενοι ότι είναι συνομήλικοι τους, αποσπούσαν ερωτικές τους φωτογραφίες και βίντεο και στη συνέχεια τους εκβίαζαν για να συνευρεθούν ερωτικά μαζί τους. Επιπλέον διαπιστώθηκε ότι διαμοίραζαν υλικό παιδικής πορνογραφίας σε άλλους χρήστες του διαδικτύου, ενώ ακόμα επιδίωκαν την ανταλλαγή και την πώληση του υλικού αυτού.

Στο πλαίσιο της συνεργασίας με τις αντίστοιχες Υπηρεσίες της Interpol και της Europol, διαπιστώθηκε ότι πέντε (5) από τους συλληφθέντες είχαν καταβάλλει μεγάλα χρηματικά ποσά, είτε για την αγορά ψηφιακού υλικού παιδικής πορνογραφίας, είτε για την απευθείας παρακολούθηση υλικού κακοποίησης ανηλίκων, από «κρυφή» ιστοσελίδα του εξωτερικού. Παράλληλα διαμοίραζαν αυτό το υλικό σε άλλους χρήστες του διαδικτύου, μέσω ιστοσελίδων και προγραμμάτων ανταλλαγής αρχείων (Peer to Peer).

Σχετική νομοθεσία: Ν. 3064/2002 (για πρώτη φορά εισήχθη στον Ελληνικό Ποινικό Κώδικα το άρθρο 348Α, το οποίο μεταξύ άλλων αφορούσε στη «διακίνηση παιδικής πορνογραφίας μέσω Διαδικτύου»), Ν. 3625/2007 και Ν. 3666/2008 ο οποίος και συμπεριέλαβε το έγκλημα του 348Α στις περιπτώσεις άρσης του απορρήτου των επικοινωνιών.

Πέρα όμως από τη διακίνηση παιδικής πορνογραφίας, οι ανήλικοι χρήστες έρχονται να αντιμετωπίσουν και άλλων παράνομες πράξεις όπως είναι η προσβολή της γενετήσιας αξιοπρέπειας. Αυτού του είδους η πράξη ποινικοποιείται βάσει του 337 άρθρο του Ποινικού Κώδικα και δυστυχώς λαμβάνει χώρα καθημερινά. Σύμφωνα με όσα ορίζει η διάταξη στην παράγραφο 3 που προστέθηκε με το Ν. 3727/2008:

«Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, αποκτά επαφή με πρόσωπο που δεν συμπλήρωσε τα 15 έτη και, με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπεια του ανηλίκου στο πεδίο της γενετήσιας ζωής του,

τιμωρείται με φυλάκιση τουλάχιστον δύο ετών. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση, ο ενήλικος τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.» Ο νομοθέτης εδώ, με τον όρο «ή άλλου επικοινωνιακού μέσου».

Αντιθέτως, όταν ο ενήλικος πέραν της επικοινωνίας με την/ον ανήλικο, προσποιείται επιπλέον τον ανήλικο με σκοπό να τον προσεγγίσει ευκολότερα και εν τέλει να έρθει σε σεξουαλική επαφή μαζί του στον πραγματικό κόσμο, τότε γίνεται λόγος για το φαινόμενο "Grooming". Παρά το γεγονός ότι δεν υπάρχει ο όρος "grooming" στον ελληνικό ποινικό κώδικα, εν τούτοις αυτή η πράξη τιμωρείται βάσει του άρθρου 348Β Π.Κ., όπως αυτό προστέθηκε με το Ν. 3727/2008. Κύριο στοιχείο της αντικειμενικής υπόστασης του 348 Π.Κ. είναι ο ενήλικας μέσω της τεχνολογίας πληροφόρησης και επικοινωνίας να αποσκοπεί στην αποπλάνηση του παιδιού (339 Π.Κ.) και στο φυσικό κόσμο.

Κεφάλαιο 7

Διακίνηση ναρκωτικών μέσω υπολογιστή

Μέσω κλειστού group στο FACEBOOK γίνονταν οι«παραγγελίες» ναρκωτικών ουσιών, κινητών τηλεφώνων νέας γενιάς, φορτιστών,φορητών υπολογιστών ακόμη και όπλων, σε ενδιαφερόμενους έγκλειστους διαφόρων φυλακών της χώρας.

Στοιχεία της παραβατικότητας στην κοινωνία της

Η Κοινωνία της πληροφορίας δεν είναι μόνο μία κοινωνία γνώσης και ανάπτυξης . Τα δίκτυα ως ρεπλίκα της κοινωνίας χαρακτηρίζονται και περιέχουν όλες τις πλευρές της. Οι εγκληματίες έχουν επίσης ανακαλύψει τον κυβερνοχώρο. Η εγκληματικότητα αυτή έχει διάφορες μορφές: επίθεση κατά πληροφορικών συστημάτων, διάδοση παιδικής πορνογραφίας, απάτη, παραβιάσεις πνευματικής ιδιοκτησίας, προσβολές της ιδιωτικότητας, υποστήριξη της διάπραξης παραδοσιακών εγκλημάτων όπως η διακίνηση ναρκωτικών ή το δουλεμπόριο. Πρέπει να σημειωθεί ο ιδιαίτερα ευάλωτος χαρακτήρας της σημερινής κοινωνίας της πληροφορίας: η οικονομία, η διοίκηση και η κοινωνία είναι σε πολύ υψηλό βαθμό εξαρτημένες από την αποτελεσματικότητα και την ασφάλεια των πληροφορικών συστημάτων. Είναι μία κοινωνία υψηλών ευκαιριών και ευχερειών αλλά ταυτόχρονα μία κοινωνία κινδύνων.

Η ανωνυμία ως βασικό χαρακτηριστικό του δικτύου έχει σοβαρές συνέπειες για το ποινικό δίκαιο. Δεν δυσχεραίνει απλώς τη διαλεύκανση των εγκλημάτων αλλά δημιουργεί σοβαρό πρόβλημα και ως προς τις αποδείξεις. Ένα άλλο σοβαρό κοινωνιολογικό-εγκληματολογικό στοιχείο είναι ότι η ανωνυμία ενθαρρύνει τους χρήστες του Διαδικτύου να επιχειρήσουν εγκληματικές πράξεις τις οποίες δεν θα επιχειρούσαν παρά μόνο στον κυβερνοχώρο καθώς στον χώρο αυτό δεν φαίνεται να έχει διαμορφωθεί μία ηθική τάξη και δομή με σαφείς κανόνες δεοντολογίας, επιταγές και απαγορεύσεις.

Η διάδοση της τεχνολογίας των υπολογιστών σε όλες τις πλευρές της ζωής, η διασύνδεση των υπολογιστών σε διεθνή δίκτυα έχουν καταστήσει το έγκλημα πιο διαφοροποιημένο, πιο επικίνδυνο και διεθνοποιημένο. Τα νέα συστήματα έχουν ειδικά χαρακτηριστικά που διευκολύνουν τους δράστες αλλά δυσχεραίνουν το έργο των διωκτικών αρχών (πολλαπλά συστήματα λογισμικού και hardware, έλλειψη εμπειρίας πολλών χρηστών, ανωνυμία, κρυπτογράφηση, διεθνής κινητικότητα)

Αποτέλεσμα

Η παραβατικότητα καθίσταται όλο και συχνότερο, πολυπλοκότερο και επικινδυνότερο φαινόμενο.

Τα εγκλήματα αυτά μπορούν να πραγματοποιηθούν από τον καθένα και να πλήξουν τον καθένα. Δεν χρειάζεται καν να εγκαταλείψει κανείς τον χώρο του σπιτιού του.

Το computer crime έχει αποκτήσει κινητικότητα και διεθνή χαρακτήρα

Το computer crime και το Διαδίκτυο έχουν αποκτήσει μεγάλη ελκυστικότητα για το οργανωμένο έγκλημα

Η «δόση» είναι βασισμένη σε ηχητικά κύματα, τα οποία έχουν ενσωματωθεί με ειδική επεξεργασία σε κοινά μουσικά αρχεία .mp3 και πωλούνται ως αρχεία .drg. Όπως εξηγούν οι ειδικοί, πρόκειται για συγκεκριμένα κύματα συχνότητας 3 έως 30 Hertz (τα λεγόμενα υποηχητικά κύματα) που επηρεάζουν τη λειτουργία του εγκεφάλου προκαλώντας διάφορες αντιδράσεις. Για παράδειγμα, τα κύματα άλφα (τα οποία κυμαίνονται από 7 έως 13 Hertz) έχουν χαλαρωτική δράση, όμως υπάρχουν και άλλα που προκαλούν αντιθέτως υπερδιέγερση και ευφορία. Ήδη οι αρχές έχουν εντοπίσει αμέτρητες ιστοσελίδες όπου μπορούν οι ενδιαφερόμενοι να βρουν τη δόση τους. Μάλιστα, υπάρχει και ιστοσελίδα όπου παρέχονται οδηγίες χρήσης του νέου ναρκωτικού για τους αρχάριους και πωλούνται CDs με τραγούδια-«δόσεις». Επίσης, στέλνονται e-mail σε ανήλικους με τραγούδια δόσεις που αν τα ακούσουν θα φτιάξουν... κεφάλι στην κυριολεξία, αφού τα ηχητικά αυτά ναρκωτικά δρουν κατευθείαν στον εγκέφαλο.

Κεφάλαιο 8

Ηλεκτρονικό ψάρεμα (phishing)

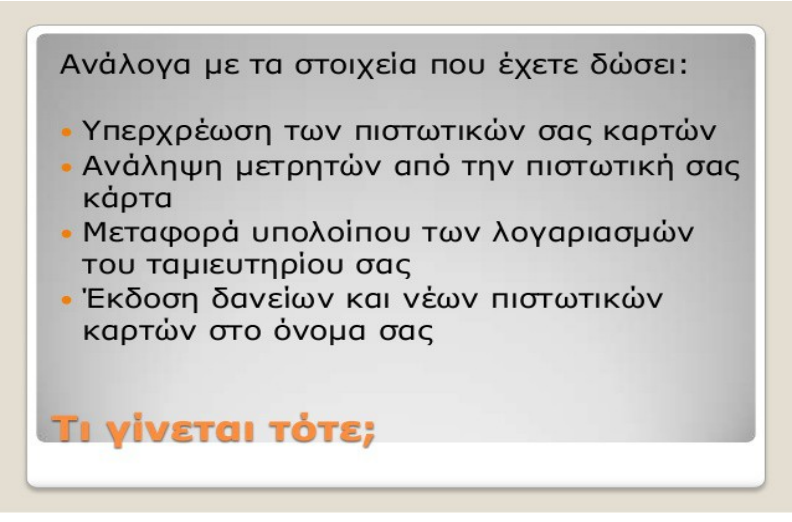
Ορισμός:

Το ηλεκτρονικό "ψάρεμα" είναι ένας τρόπος εξαπάτησης των χρηστών υπολογιστών με στόχο να τους κάνει να αποκαλύψουν προσωπικές πληροφορίες ή οικονομικά στοιχεία, μέσω ενός παραπλανητικού μηνύματος ηλεκτρονικού ταχυδρομείου ή μιας παραπλανητικής τοποθεσίας Web. Μια συνηθισμένη απάτη ηλεκτρονικού "ψαρέματος" ξεκινά με ένα μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο μοιάζει με μια επίσημη ειδοποίηση από αξιόπιστη πηγή, όπως τράπεζα, εταιρεία πιστωτικής κάρτας ή ευυπόληπτη εταιρεία ηλεκτρονικού εμπορίου. Οι παραλήπτες του μηνύματος ηλεκτρονικού ταχυδρομείου κατευθύνονται στο να επισκεφθούν μια τοποθεσία Web, η οποία έχει δημιουργηθεί με στόχο την εξαπάτησή τους, όπου τους ζητείται να παράσχουν προσωπικές πληροφορίες, όπως ο αριθμός ή ο κωδικός πρόσβασης κάποιου λογαριασμού τους. Στη συνέχεια, οι πληροφορίες αυτές χρησιμοποιούνται συνήθως για την υποκλοπή ταυτότητας.

Πώς γίνεται:

Μια συνηθισμένη απάτη ηλεκτρονικού ‘’ψαρέματος’’ ξεκινά με ένα μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο μοιάζει με μια επίσημη ειδοποίηση από μια αξιόπιστη πηγή όπως μια τράπεζα εταιρία πιστωτικής κάρτας ή ευυπόληπτη εταιρεία ηλεκτρονικού εμπορίου. Οι παραλήπτες του μηνύματος ηλεκτρονικού ταχυδρομείου κατευθύνονται στο να επισκεφθούν μια τοποθεσία Web η οποία έχει δημιουργηθεί με στόχο την εξαπάτησή τους, όπου τους ζητείται να παράσχουν προσωπικές πληροφορίες, όπως ο αριθμός ή ο κωδικός πρόσβασης κάποιου λογαριασμού τους. Στη συνέχεια, οι πληροφορίες αυτές χρησιμοποιούνται συνήθως για την υποκλοπή ταυτότητας.

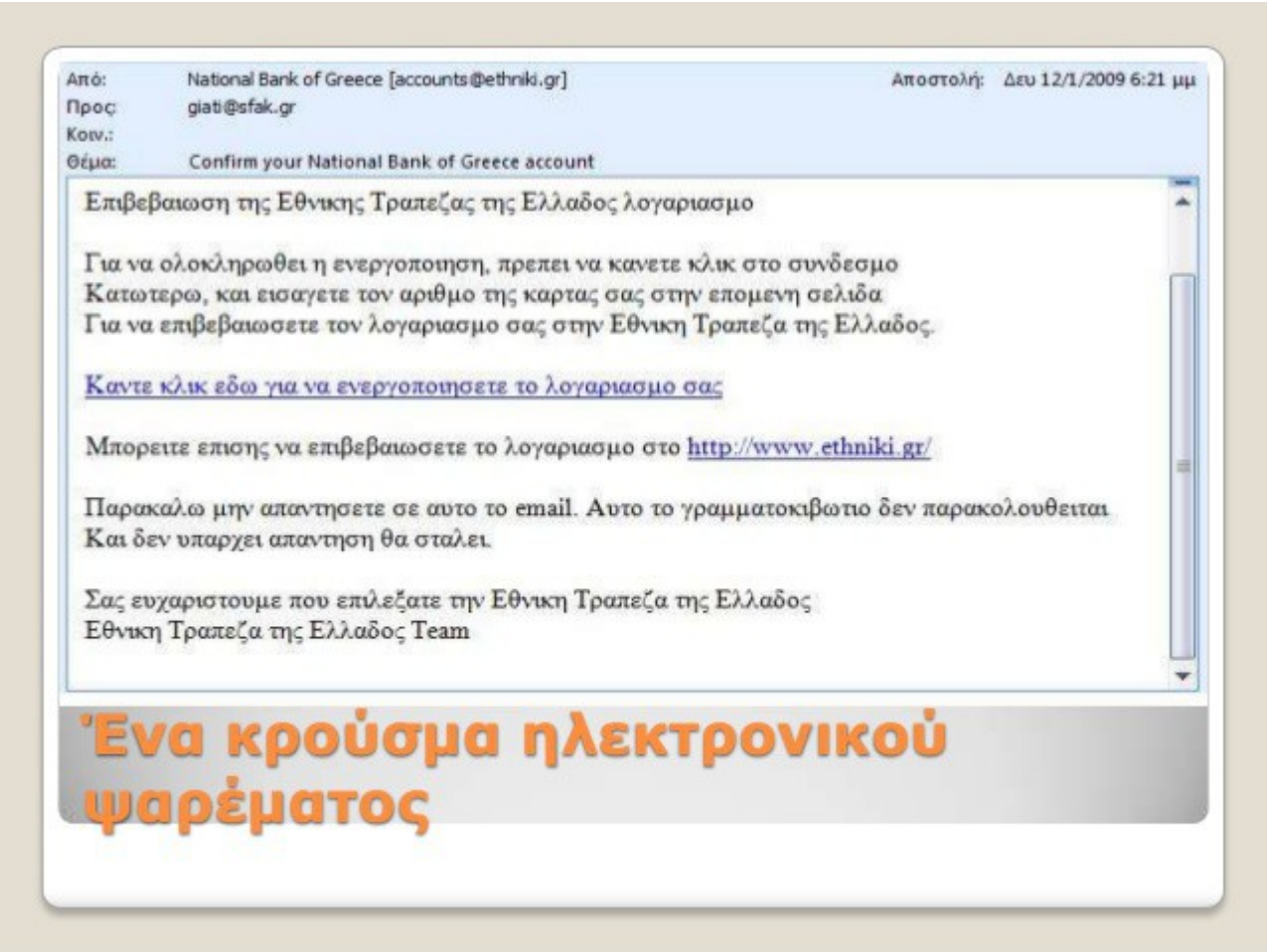
Οι συνέπειες:



Τι πρέπει να προσέχουμε:

- Τον αποστολέα μπορεί να δείχνει αληθοφανής
- Την γλώσσα του θέματος και του μηνύματος (συνήθως στα αγγλικά)
- Ορθογραφικά και συντακτικά λάθη στο κείμενο
- Που οδηγούν οι σύνδεσμοι που πατάμε

Παράδειγμα μηνύματος ηλεκτρονικού ψαρέματος



6 σημαντικά μέτρα προστασίας:

- Αγνοείστε <<ύποπτα>> e-mail με τα οποία ζητούνται προσωπικά στοιχεία (αριθμός λογαριασμού, μυστικοί προσωπικοί κωδικοί ,ονοματεπώνυμα κ.α.) ή περιέχουν συνδέσμους (links) σε <<άγνωστες>> ιστοσελίδες.
- Οι τράπεζες δεν πρόκειται για κανέναν λόγο να ζητήσουν προσωπικά στοιχεία μέσω e-mail ή τηλεφώνου. Για το λόγο αυτό διαγράφουν τα e-mail αυτά ως πλαστά και να αγνοείται αντίστοιχες πιθανές τηλεφωνικές κλήσεις.
- Να βεβαιώνεστε ότι βρίσκεστε στη σωστή διεύθυνση της τράπεζας σας.
- Να μην συνδέεστε ποτέ με την ιστοσελίδα της τράπεζάς σας μέσω εξωτερικού συνδέσμου (link) που παρέχει κάποιος τρίτος και ιδιαίτερα μέσω e-mail.
- Να βεβαιώνεστε ότι στην ιστοσελίδα της Ηλεκτρονικής Τραπεζικής της τράπεζάς σας εμφανίζεται το εικονίδιο με το ‘’λουκέτο’’ μέσω του οποίου μπορείτε ανοίγοντας το με διπλό κλικ, να επιβεβαιώσετε ότι βρίσκεστε στο ασφαλές περιβάλλον της Τράπεζάς σας.
- Ρυθμίστε το λειτουργικό σύστημα του υπολογιστή σας και το πρόγραμμα antivirus που χρησιμοποιείτε, ώστε να ενημερώνονται αυτόματα . Αν δεν γνωρίζετε πώς να το κάνετε συμβουλευτείτε τον προμηθευτή του υπολογιστή σας .

Τι προβλέπει η ελληνική νομοθεσία σχετικά με το ηλεκτρονικό ψάρεμα

:Επειδή η μέθοδος “phishing” βασίζεται στην πλάνη του θύματος με σκοπό την περιουσιακή του ζημία, είναι προφανές ότι οι Phishers μέσω αυτής προσπορίζουν στον εαυτό τους ή/και σε τρίτους παράνομο περιουσιακό όφελος. Επειδή δε οι δράστες έχουν γνώση και θέληση σχετικά με την παράνομη δραστηριότητά τους, συμπεραίνεται ότι το “phishing” συνιστά απάτη, κατά το άρθρο 386 του Ποινικού Κώδικα, σύμφωνα με το οποίο «όποιος με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών»

.

Κεφάλαιο 9

Κλοπή ταυτότητας

Εισαγωγή

Πέρσι η Ομοσπονδιακή Επιτροπή Εμπορίου των Η.Π.Α. έλαβε περισσότερες από διακόσιες πενήντα χιλιάδες καταγγελίες για κλοπή ταυτότητας, ενώ υπάρχουν κι άλλες περιπτώσεις που δεν έχουν καταγγελθεί. Η κλοπή ταυτότητας είναι η συνηθέστερη καταγγελία από καταναλωτές προς την Ομοσπονδιακή Επιτροπή Εμπορίου. Ασφαλώς, η κλοπή των στοιχείων ταυτότητας δεν είναι το χειρότερο μέρος του εγκλήματος, το καταστροφικό μέρος είναι το τι κάνουν με τα στοιχεία οι εγκληματίες. Απάτη πιστωτικών καρτών. Απάτες με υποθήκες και εταιρείες κοινής ωφελείας. Άδειασμα τραπεζικών λογαριασμών.

Ένα έγκλημα δύο φάσεων

Η κλοπή ταυτότητας είναι μια διαδικασία δύο φάσεων. Καταρχάς, κάποιος κλέβει τα προσωπικά σας δεδομένα. Στη συνέχεια, ο κλέφτης χρησιμοποιεί αυτές τις πληροφορίες για να προσποιηθεί ότι είναι εσείς και να διαπράξει απάτη. Είναι σημαντικό να καταλάβετε αυτή την προσέγγιση δύο βημάτων, γιατί πρέπει να αναπτύξετε τις άμυνές σας και στα δύο επίπεδα.

Προστασία των στοιχείων σας

Για να αποφύγετε να γίνετε θύμα, προστατέψτε τα προσωπικά σας δεδομένα επιμελώς. Αν οι κλέφτες ταυτότητας δεν μπορούν να έχουν πρόσβαση σε ζωτικά δεδομένα όπως ο αριθμός ταυτότητας ή οι αριθμοί τραπεζικών λογαριασμών σας, δεν μπορούν να σας εξαπατήσουν.

Κάποιες κλοπές ταυτότητας γίνονται με τον παραδοσιακό τρόπο. Οι κλέφτες ψάχνουν τα σκουπίδια, κλέβουν την αλληλογραφία και χρησιμοποιούν τεχνικές

εξαπάτησης για να σας ξεγελάσουν να τους αποκαλύψετε ευαίσθητες λεπτομέρειες. Από εσάς εξαρτάται να προστατέψετε τα προσωπικά σας δεδομένα. Ακολουθούν μερικές πρώτες, βασικές συμβουλές:

1. Μην δίνετε τον αριθμό ταυτότητάς σας, λογαριασμών ή προσωπικά σας στοιχεία, από το τηλέφωνο.
2. Διατηρείτε τα σημαντικά έγγραφα σε ένα κλειδωμένο χρηματοκιβώτιο.
3. Παραλαμβάνετε και στέλνετε αλληλογραφία με ευαίσθητα προσωπικά δεδομένα από το ταχυδρομείο.
4. Χρησιμοποιείτε τη δυνατότητα αυτόματης κατάθεσης της μισθοδοσίας σας.

Η online κλοπή ταυτότητας είναι ένα μεγάλο και συνεχώς αυξανόμενο πρόβλημα. Στις απάτες phishing και pharming, οι κλέφτες χρησιμοποιούν πλαστά μηνύματα email και πλαστές ιστοσελίδες για να μιμηθούν νομότυπους οργανισμούς. Εκμεταλλεύονται την εμπιστοσύνη σας, προσπαθώντας να σας κάνουν να αποκαλύψετε τα προσωπικά σας δεδομένα, όπως κωδικούς πρόσβασης ή αριθμούς λογαριασμού. Παρομοίως, οι χάκερ και οι ιοί μπορούν να διεισδύσουν στον υπολογιστή σας και να εγκαταστήσουν προγράμματα keystroke logger για να κλέψουν δεδομένα ή να καταγράψουν ονόματα λογαριασμών και κωδικούς πρόσβασης καθώς τα πληκτρολογείτε.

Μπορείτε να σταματήσετε τους επίδοξους κλέφτες ταυτότητας, εφαρμόζοντας την κατάλληλη πρόληψη.

- Αποθηκεύετε τις ευαίσθητες πληροφορίες σε προστατευμένα με κωδικό πρόσβασης αρχεία και καταλόγους.
- Χρησιμοποιείτε προγράμματα διαχείρισης κωδικών πρόσβασης, όπως τα Norton Internet Security και Norton 360, για την αυτόματη συμπλήρωση πληροφοριών εισόδου, παρακάμπτοντας το πληκτρολόγιο.
- Μάθετε να ξεχωρίζετε τα παραπλανητικά email, ιστοσελίδες και άλλες ενδείξεις ότι πρόκειται για phishing και pharming.
- Κάνετε οικονομικές συναλλαγές online μόνο με ασφαλείς ιστοσελίδες με διευθύνσεις URL που ξεκινούν με "https:" ή που η ταυτότητά τους είναι εξακριβωμένη από εταιρείες όπως η VeriSign.
- Εγκαταστήστε προσωπικό τείχος προστασίας, προστασία antivirus, antispyware και antispam, τα οποία είναι όλα διαθέσιμα στην ίδια οικογένεια προγραμμάτων ασφαλείας με το Norton Internet Security ή το Norton 360 της Symantec.

Καταπολεμήστε την απάτη

Αν και μπορείτε να κάνετε πολλά για να προστατέψετε την ταυτότητά σας, κάποια πράγματα δεν είναι στο χέρι σας. Ακόμα κι αν προσέχετε τα δεδομένα σας, αυτό δεν σημαίνει ότι κανείς δεν πρόκειται να κάνει hacking στους υπολογιστές του εργοδότη σας ή της τράπεζάς σας. Για αυτό και είναι σημαντικό να έχετε συνεχώς το νου σας στους λογαριασμούς σας και στην κίνηση της πιστωτικής σας κάρτας.

Μπορεί να περάσουν αρκετοί μήνες μέχρι να ανακαλύψετε ότι έχετε πέσει θύμα κλοπής ταυτότητας. Σε αυτό το διάστημα, οι κλέφτες μπορούν να αδειάσουν τους λογαριασμούς σας ή να χρεωθούν σημαντικά ποσά στο όνομά σας.

Ελέγχετε τακτικά την κίνηση των πιστώσεών σας για ασυνήθιστες δραστηριότητες. Αν δείτε οτιδήποτε ασυνήθιστο ή απροσδόκητο, όπως μια νέα γραμμή πίστωσης που δεν έχετε ανοίξει εσείς, αντιμετωπίστε το αμέσως. Εν τω μεταξύ, παρακολουθείτε τη δραστηριότητα σε όλους σας τους οικονομικούς λογαριασμούς, από τις τραπεζικές επενδύσεις ως τις πιστωτικές κάρτες. Αν οι τράπεζες με τις οποίες συνεργάζεστε προσφέρουν ενημερώσεις δραστηριότητας, εγγραφείτε για να τις λαμβάνετε. Και αν λάβετε μια ενημέρωση ή η τράπεζά σας αναφέρει ασυνήθιστη δραστηριότητα λογαριασμού, ελέγξτε τι συμβαίνει το συντομότερο δυνατό.

Αν κάποιος έχει κλέψει την ταυτότητά σας, κάντε γρήγορα βήματα για να ελαχιστοποιήσετε τη ζημιά. Κλείστε τους οικονομικούς λογαριασμούς που μπορεί να έχουν διαρρεύσει. Ακυρώστε την ταυτότητά σας ή άλλα έγγραφα που ίσως να χάσατε. Ελέγχετε και παρακολουθείτε προσεκτικά και τακτικά τις κινήσεις των πιστώσεών σας για τα επόμενα χρόνια.

Στη συνέχεια, αναφέρετε το έγκλημα στις αρμόδιες αρχές. Ενημερώστε το τοπικό σας αστυνομικό τμήμα και κάντε καταγγελία στην Ομοσπονδιακή Επιτροπή Εμπορίου. Στη συνέχεια, χρησιμοποιήστε δημόσια διαθέσιμους πόρους για να βρείτε βοήθεια για να επανακτήσετε τις απώλειές σας και να αποτρέψετε την περαιτέρω ζημιά. Μπορούν να σας βοηθήσουν ο γενικός εισαγγελέας της περιοχής σας, η Ομοσπονδιακή Επιτροπή Εμπορίου και μη κερδοσκοπικές οργανώσεις προστασίας από κλοπή ταυτότητας.

Συμπέρασμα

Η κλοπή ταυτότητας έχει γίνει πλέον καθημερινότητα. Για να αποφύγετε να πέσετε θύμα, προστατέψτε επιμελώς τα προσωπικά σας δεδομένα, παρακολουθείτε τους λογαριασμούς και τις πιστωτικές σας κινήσεις και

ανταποκριθείτε γρήγορα σε τυχόν ενδείξεις ότι γίνεται από άλλους χρήση της ταυτότητάς σας.

Η πρώτη ελληνική δικαστική απόφαση για "κλοπή ταυτότητας"

Όταν κάποιος άγνωστος έχει χρησιμοποιήσει παρανόμως τα στοιχεία ταυτότητας ενός ατόμου και έχει προκαλέσει κάποιου είδους απάτη σε βάρος του, οι αρχές είναι σχεδόν απίθανο να εντοπίσουν τον δράστη. Το φαινόμενο της "κλοπής ταυτότητας" ξεπερνά κατά πολύ τις κλασικές περιπτώσεις πλαστογραφίας και συνδέεται με την παράνομη χρήση προσωπικών δεδομένων. Καθώς εισερχόμαστε όμως στην περιοχή της προστασίας προσωπικών δεδομένων, η ευθύνη δεν αφορά μόνο τον δράστη, αλλά και την εταιρία που δέχθηκε τα στοιχεία ταυτότητας, εφόσον αποδειχθεί ότι υπήρχε πλημμελής έλεγχος της ακρίβειας των πιστοποιητικών που προσκομίζει ο δράστης. Στην απόφαση που ακολουθεί, υποστηρίχθηκε ότι η σύναψη σύμβασης υπηρεσιών κινητής τηλεφωνίας από άτομο που δεν ήταν ο κάτοχος των στοιχείων ταυτότητας που προσκόμισε, εγείρει ζητήματα ευθύνης της ίδιας της εταιρίας που δέχθηκε τα στοιχεία, ως προς τον έλεγχο ομοιότητας ανάμεσα στην υπογραφή στο δελτίο ταυτότητας και την υπογραφή που έθεσε ο άγνωστος στο σώμα της σύμβασης. Πρόκειται για προδικαστική απόφαση, αφού ως προς την ουσία το δικαστήριο διέταξε επανάληψη της διαδικασίας, αλλά ως προς το νομικό μέρος είναι η πρώτη φορά που γίνεται δεκτή η εν λόγω νομική βάση, δηλαδή το θεσμικό πλαίσιο για την προστασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, για να διερευνηθεί η ευθύνη της εταιρίας και να εξεταστεί η αποζημίωση του θύματος.

Κεφάλαιο 10

Διαδικτυακές απάτες

Οι συνηθέστερες μορφές διαδικτυακής απάτης είναι οι ακόλουθες:

α) Χρεώσεις της πιστωτικής κάρτας πολιτών μέσω του διαδικτύου για αγορές, οι οποίες δεν πραγματοποιήθηκαν από τους ίδιους.

Στις περιπτώσεις αυτές, κάποιος κακόβουλος χρήστης του διαδικτύου δημιουργεί μια πλασματική ιστοσελίδα και με αυτόν τον τρόπο καταφέρνει να συγκεντρώνει στοιχεία κι αριθμούς πιστωτικών καρτών χρηστών του διαδικτύου, οι οποίοι έχοντας εξαπατηθεί, νομίζουν ότι πρόκειται για κάποιο διαδικτυακό κατάστημα και κάνουν τις αγορές τους.

Επιπλέον, αρκετές είναι οι περιπτώσεις όπου επιτήδειοι καταφέρνουν να αποκτούν φυσική πρόσβαση στα στοιχεία πιστωτικών καρτών πολιτών τα οποία εν συνεχεία χρησιμοποιούν σε διαδικτυακές αγορές, καθώς για τις αγορές αυτές δεν είναι απαραίτητη η φυσική κατοχή της πιστωτικής κάρτας, παρά μόνο τα στοιχεία αυτής.

Επιπροσθέτως, σε αρκετές περιπτώσεις οι χρήστες του διαδικτύου δίνουν οι ίδιοι άθελά τους τα στοιχεία σε κακόβουλους χρήστες του διαδικτύου (phishing). Ειδικότερα, ο ανυποψίαστος πολίτης λαμβάνει μήνυμα ηλεκτρονικού ταχυδρομείου από Πιστωτικό Ίδρυμα, στο οποίο τηρεί λογαριασμό, με το οποίο του ζητείται να συμπληρώσει τα στοιχεία του (ονοματεπώνυμο, αριθμό λογαριασμού και πιστωτικής κάρτας κλπ.), για λόγους πχ. ενημέρωσης των αρχείων της τράπεζας. Το μήνυμα, μέσω υπερσυνδέσμου, τους οδηγεί σε μια πλασματική ιστοσελίδα της τράπεζας, με αποτέλεσμα ο πολίτης να πείθεται και να χορηγεί τα επίμαχα στοιχεία.

β) Διακίνηση μηνυμάτων με απατηλό περιεχόμενο, που επιδιώκουν την εξαπάτηση ανυποψίαστων πολιτών.

Ειδικότερα, ο τρόπος δράσης των κακόβουλων δραστών στην εν λόγω μορφή απάτης, που περιγράφεται υπό τον όρο «Ισπανικό Λόττο», είναι η μαζική αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας σε τυχαίους χρήστες του διαδικτύου, με τα οποία τους ενημερώνουν ότι έχουν κερδίσει ένα μεγάλο

χρηματικό ποσό της τάξεως των εκατομμυρίων δολαρίων σε ηλεκτρονική κλήρωση του διαδικτύου.

Οι δημιουργοί των μηνυμάτων αυτών, για να γίνουν πιστευτοί, χρησιμοποιούν παραπλήσια ονόματα μεγάλων εταιρειών (πχ. Microsoft , Yahoo κλπ) και συνοδεύουν τα μηνύματα που αποστέλλουν με πλαστά πιστοποιητικά όσον αφορά στην υποτιθέμενη ηλεκτρονική κλήρωση.

Η απάτη έγκειται στο γεγονός ότι ζητούν από τους υποτιθέμενους νικητές την προπληρωμή κάποιων φόρων ή/και εξόδων εκταμίευσης των χρημάτων, ποσό που συνήθως είναι της τάξης των μερικών χιλιάδων δολαρίων.

γ) «Απάτες 419» ή «Νιγηριανές Απάτες»

διαδικτύου, με τα οποία τους πληροφορούν ότι κάποιος κάτοχος ιδιαίτερα μεγάλης περιουσίας έχει αποβιώσει και είτε δεν υφίσταται κανείς κληρονόμος και ο παραλήπτης του μηνύματος έχει επιλεγεί ούτως ώστε να κληρονομήσει αυτός την περιουσία. Στις περιπτώσεις αυτές αποστέλλονται, μηνύματα σε τυχαίους χρήστες του ία, είτε για να καταστεί δυνατό να αποδεσμευτεί η περιουσία, χρειάζεται αυτή να μεταφερθεί σε τραπεζικό λογαριασμό του εξωτερικού και ο παραλήπτης του μηνύματος ενημερώνεται ότι εάν διαθέσει το λογαριασμό του, θα αποκτήσει κάποιο ποσοστό επί της περιουσίας αυτής.

Σε άλλες περιπτώσεις, άτομα από τη Νιγηρία αναζητούν τη βοήθεια επιχειρηματιών ή ελεύθερων επαγγελματιών με σκοπό να μεταφέρουν τα κεφάλαιά τους, τα οποία προέρχονται από εγκληματικές πράξεις (λαθρεμπόριο, απάτες, δωροδοκία κλπ.), υποσχόμενοι για τη συνεργασία αυτή υψηλό ποσοστό αμοιβής. Για το σκοπό αυτό, κάνουν χρήση τίτλων επίσημων φορέων της χώρας τους (Υπουργεία, Κεντρική Τράπεζα, Εθνική Εταιρεία Πετρελαίων Νιγηρίας κλπ.), χρησιμοποιούν τίτλους κυβερνητικών ή στρατιωτικών παραγόντων με υπαρκτά και ψεύτικα ονόματα ή προφασίζονται σχέση τους με «διάσημα» ή «σημαντικά» πρόσωπα.

Η απάτη έγκειται στο γεγονός ότι οι αποστολείς των μηνυμάτων ζητούν από τους παραλήπτες να τους αποστείλουν τα προσωπικά τους στοιχεία, τα στοιχεία των τραπεζικού λογαριασμού και πιστωτικής κάρτας κλπ. προκειμένου επιτευχθεί η συνεργασία τους και η αποκόμιση των χρηματικών ποσών.

Κεφάλαιο 11

Κακόβουλο λογισμικό

Ορισμός

Το κακόβουλο λογισμικό (ή «Malware») είναι ένας περιεκτικός όρος που περιγράφει όλα τα είδη προγραμμάτων υπολογιστή, τα οποία εκτελούν ενέργειες χωρίς τη συγκατάθεση του χρήστη και προκαλούν βλάβες. Μεταξύ αυτών περιλαμβάνονται οι ιοί, οι δούρειοι ίπποι, τα λογισμικά κατασκοπείας (Spyware), τα σκουλήκια (worm), τα λογισμικά εκφοβισμού (Scareware), τα προγράμματα καταγραφής πληκτρολογήσεων (Keylogger), τα Rootkit και τα Exploit. Οι επιπτώσεις διαφέρουν ανάλογα με το είδος του κακόβουλου λογισμικού. Εκτείνονται από περιορισμό της ταχύτητας εργασίας και υποκλοπή σημαντικών δεδομένων, μέχρι πλήρη έλεγχο του συστήματος

Εχει σκοπό να καταστρέψει υπολογιστές και δίκτυα. Αν υπάρχει κακόβουλο λογισμικό στον υπολογιστή σας, μπορεί να παραβιάσει τους ελέγχους ασφαλείας του Facebook και να αποκτήσει πρόσβαση στο λογαριασμό σας. Το λογισμικό αυτό συλλέγει πληροφορίες από το λογαριασμό σας, στέλνει ενημερώσεις κατάστασης ή μηνύματα που φαίνεται να προέρχονται από εσάς, ή γεμίζει το λογαριασμό σας με διαφημίσεις που κρασάρουν τον υπολογιστή.

Το κακόβουλο λογισμικό μεταδίδεται ως εξής:

- Αν προσπαθήσετε να παρακολουθήσετε ένα "βίντεο σοκ" που δημοσίευσε ένας φίλος σας σε μια ενημέρωση κατάστασης.
- Αν επισκεφτείτε έναν ιστότοπο που ισχυρίζεται ότι προσφέρει ειδικές λειτουργίες του Facebook.
- Αν κατεβάσετε για το πρόγραμμα περιήγησης ένα πρόσθετο (add-on) που ισχυρίζεται ότι κάνει κάτι σχεδόν εξωπραγματικό

Είδη κακόβουλου λογισμικού

Ιοί

Ο ιός είναι ένα πρόγραμμα που προκαλεί βλάβη σε κάποιο σύστημα. Το λογισμικό είναι συνήθως κρυμμένο σε κάποιο άλλο αρχείο ή πρόγραμμα. Κάθε φορά που γίνεται εκκίνηση του αντίστοιχου προγράμματος ή αρχείου, εκτελείται ο ιός. Ο ιός μπορεί π.χ. να διαγράψει δεδομένα ή να οδηγήσει στην κατάρρευση του λειτουργικού συστήματος. Ωστόσο, οι τυπικοί ιοί έχουν σχεδόν εξαλειφθεί. Οι

χάκερ χρησιμοποιούν άλλα κακόβουλα λογισμικά, τα οποία είναι πιο προσοδοφόρα.

Υπάρχουν πολλοί τύποι υπολογιστικών ιών, όπως ιοί αρχείων, ιοί της περιοχής εκκίνησης (boot sector), ιοί σκουλήκια και προγράμματα δούρειοι ίπποι (Trojan Horse). Υπάρχουν πολλοί τύποι υπολογιστικών ιών, όπως ιοί αρχείων, ιοί της περιοχής εκκίνησης (boot sector), ιοί σκουλήκια και προγράμματα δούρειοι ίπποι (Trojan Horse).

•Ιοί περιοχής εκκίνησης - Αυτοί οι ιοί μολύνουν δισκέτες και σκληρούς δίσκους. Ο ιός φορτώνεται πριν από το λειτουργικό σύστημα. Ήταν οι πρώτοι ιοί που εμφανίστηκαν.

•Ιοί αρχείων – σ' αυτή τη κατηγορία ανήκει η πλειοψηφία των ιών και η πιο εύκολα αντιμετωπίσιμη κατηγορία. Είναι μικρά εκτελέσιμα αρχεία. Προσκολλούνται σε ένα αρχείο, συνήθως αρχείο εφαρμογής. Το βασικό γνώρισμα των ιών είναι ότι δημιουργούν αντίγραφα του εαυτού τους μέσα σε άλλα αρχεία. Τα αρχεία αυτά είναι εκτελέσιμα ή αρχεία βιβλιοθηκών. Οι ιοί είτε αντικαθιστούν κάποιο τμήμα του κώδικα του αρχείου (χωρίς να μεταβάλλουν το μέγεθός του) είτε προσκολλώνται σε αυτό.

•Ιοί σκουλήκια (Worms): Έχουν την ικανότητα αναπαραγωγής χωρίς να χρησιμοποιούν άλλα αρχεία. Ο τρόπος διάδοσης τους είναι το διαδίκτυο με τη βοήθεια των δικτυακών πρωτοκόλλων, εκμεταλλευόμενοι τα προβλήματα ασφαλείας των λειτουργικών συστημάτων ή με τη βοήθεια των μηνυμάτων του ηλεκτρονικού ταχυδρομείου. Οι ιοί σκουλήκια αποκτούν προσπέλαση στο βιβλίο διευθύνσεων του υπολογιστή (όπου κρατούνται οι διευθύνσεις ηλεκτρονικού ταχυδρομείου με τις οποίες επικοινωνεί ο χρήστης του υπολογιστή) και αποστέλλει μολυσμένα μηνύματα. Αρκετές φορές χρησιμοποιούν σαν αποστολέα ένα όνομα από το βιβλίο διευθύνσεων. Όσοι παραλήπτες ανοίξουν το ηλεκτρονικό μήνυμα μολύνονται. Η διάδοση των ιών worm με αυτή τη μέθοδο είναι αστραπιαία. Στη συνέχεια γίνεται αναφορά σε δύο ιούς σκουλήκια τον Blaster και τον Sobig.

Η έκρηξη του Blaster έγινε την 11η Αυγούστου 2003. Το μεσημέρι της ίδιας μέρας είχαν μολυνθεί 7.000 υπολογιστές και το βράδυ 330.000. Ο ιός ήταν προγραμματισμένος να επιτεθεί στο δικτυακό τόπο της Microsoft στις 16 Αυγούστου. Οι τεχνικοί της Microsoft πρόλαβαν και άλλαξαν τις διευθύνσεις των διακομιστών της εταιρίας και η επίθεση απέτυχε.
Μια εβδομάδα αργότερα έκανε την εμφάνισή του η έκτη έκδοση ενός ακόμα ιού του Sobig. Ο ιός αυτός μεταδιδόταν μέσω ηλεκτρονικού ταχυδρομείου και επιβάρυνε τα συστήματα ηλεκτρονικής αλληλογραφίας. Ο Sobig ήταν πολυμορφικός ιός. Όταν οι χρήστες άνοιγαν το μολυσμένο μήνυμα ο κώδικας του ιού ξεκινούσε την αναπαραγωγή του. Έβρισκε τις διευθύνσεις

αλληλογραφίας του χρήστη και έστελνε μολυσμένα μηνύματα. Οι μολυσμένοι υπολογιστές θα επιχειρούσαν να συνδεθούν στο διαδίκτυο και Παρασκευή και Κυριακή από τις 0:00 έως τις 3:00. Τότε επικοινωνούσαν με 20 διακομιστές και θα κατέβαζαν επιπλέον λογισμικό.
Η εξάπλωση του ιού ήταν τεράστια. Οι διακομιστές αλληλογραφίας κατακλύστηκαν από μηνύματα που μετέφεραν τον ιό. Η America On Line (παροχέας διαδικτύου στις ΗΠΑ) έλαβε σε μία μέρα 31 εκατομμύρια μηνύματα (τρεις φορές περισσότερα από το κανονικό). Τα 11,5 εκατομμύρια ήταν μολυσμένα μηνύματα με τον Sobig. Μέσα σε μία εβδομάδα στάλθηκαν 200 εκατομμύρια μολυσμένα μηνύματα. Η όλη δραστηριότητα του ιού σταμάτησε στις 10 Σεπτεμβρίου καθώς έτσι είχε προγραμματιστεί ο ιός.

<u>Δούρειοι ίπποι</u>

•Δούρειος ίππος - Αυτοί οι ιοί δρουν αθόρυβα. Μολύνουν τον υπολογιστή και αναμένουν κάποιο γεγονός ανάλογα με το προγραμματισμό τους. Συνήθως δεν πολλαπλασιάζοντας και δεν εξαπλώνονται σε άλλους υπολογιστές. Για να μολυνθεί ένας υπολογιστής ο χρήστης του πρέπει να κατεβάσει και να εκτελέσει τον ιό. Αυτό γίνεται συνήθως με ένα ηλεκτρονικό μήνυμα όπου ο ιός είναι συνημμένος και ο χρήστης πείθεται να τον εκτελέσει. Όταν ο ιός δούρειος ίππος εγκατασταθεί στέλνει μέσω διαδικτύου τις κατάλληλες πληροφορίες στο δημιουργό του ώστε αυτός να πάρει τον έλεγχο του υπολογιστή και να χρησιμοποιηθεί σε διάφορες παράνομες και επιβλαβείς ενέργειες.

Ο όρος «δούρειος ίππος» είναι δανεισμένος από το γνωστό δούρειο ίππο του τρωικού πολέμου. Στην «Ιλιάδα» του Ομήρου ο Οδυσσέας κρύβει τους στρατιώτες του στο εσωτερικό ενός ξύλινου αλόγου, το οποίο προσφέρει ως δώρο στους αντιπάλους του, στην Τροία, ώστε να κατορθώσουν να περάσουν μέσα από τα τείχη της πόλης. Όσον αφορά τον τομέα των υπολογιστών, οι δούρειοι ίπποι είναι καμουφλαρισμένοι σαν κανονικά προγράμματα, αλλά περιέχουν ένα βλαβερό κώδικα που επιτρέπει την υποκλοπή αρχείων και το ν έλεγχο του συστήματος. Οι δούρειοι ίπποι διαδίδονται αυτόματα. Ο χρήστης εγκαθιστά το πρόγραμμα στον υπολογιστή, χωρίς να γνωρίζει ότι πρόκειται για βλαβερό λογισμικό.

Οι δούρειοι ίπποι βοηθούν τους χάκερ να δημιουργούν μικρά δίκτυα μεμονωμένων υπολογιστών. Σήμερα οι χάκερ επενδύουν όλο και περισσότερο σε δίκτυα τύπου Bot, τα οποία αποτελούνται από εκατομμύρια μολυσμένους υπολογιστές, μέσω των οποίων εκτελούν παράνομες ενέργειες. Το «Bot» είναι ένα πρόγραμμα υπολογιστή, το οποίο είναι σε θέση να εκτελεί σε μεγάλο βαθμό εργασίες αυτόματα, χωρίς να χρειάζεται ανθρώπινη παρέμβαση. Τα δίκτυα Bot αποτελούνται από περισσότερα Bot, συνδεδεμένα μεταξύ τους.

Λογισμικά κατασκοπείας (Spyware)

Όπως δηλώνει και η ονομασία τους, τα λογισμικά κατασκοπείας κατασκοπεύουν το μολυσμένο υπολογιστή. Το πρόγραμμα καταγράφει τη συμπεριφορά πλοήγησης του χρήστη του υπολογιστή στο διαδίκτυο και στέλνει τις πληροφορίες που συγκεντρώνει στον κατασκευαστή του λογισμικού κατασκοπείας ή σε τρίτα πρόσωπα εν αγνοία του χρήστη. Τα λογισμικά κατασκοπείας απαιτούν μεγάλη υπολογιστική ισχύ. Οι χρήστες μπορούν να υποψιαστούν την παρουσία τους λόγω της μείωσης στην ταχύτητα του υπολογιστή. Εκτός αυτού, τα λογισμικά κατασκοπείας μπορούν να προκαλέσουν πρόσθετα κενά ασφαλείας, εμποδίζοντας τις ενημερώσεις λογισμικού. Τα λογισμικά κατασκοπείας χρησιμοποιούνται μερικές φορές σε συνδυασμό με κακόβουλα λογισμικά τύπου Browser Hijacker. Εν προκειμένω, αντί για τις προεπιλεγμένες αρχικές σελίδες του προγράμματος περιήγησης, εμφανίζονται κάποιες ελεγχόμενες σελίδες, οι οποίες οδηγούν σε άλλες διαφημιστικές σελίδες.

Σκουλήκια (worm)

Το σκουλήκι, ή «worm», είναι ένα πρόγραμμα υπολογιστή ή μια δέσμη ενεργειών, που πολλαπλασιάζεται αυτόνομα στον προσβεβλημένο υπολογιστή. Ενώ οι ιοί διαδίδονται στον τομέα εκκίνησης του υπολογιστή, τα σκουλήκια δεν μολύνουν άλλα αρχεία ή τον τομέα εκκίνησης. Το κακόβουλο λογισμικό αποστέλλει μεταξύ άλλων προσωπικά δεδομένα και κωδικούς πρόσβασης, προσφέροντας στον εισβολέα πρόσβαση στη σύνδεση στο διαδίκτυο. Έτσι, ο υπολογιστής μπορεί π.χ. να χρησιμοποιηθεί για την αποστολή ανεπιθύμητων μηνυμάτων (spam) ή την επίθεση στο διαδικτυακό διακομιστή. Τα σκουλήκια προκαλούν μεγαλύτερη οικονομική ζημία σε σύγκριση με τους ιούς. Προσπαθούν ενεργά να προσβάλλουν περισσότερους υπολογιστές και εγκαθίστανται συνήθως στον υπολογιστή μέσω επισυνάψεων E-Mail ή κενών ασφαλείας στα προγράμματα ηλεκτρονικής αλληλογραφίας. Επίσης, διαδίδονται μέσω φορητών συσκευών αποθήκευσης δεδομένων, όπως τα USB Stick και τα CD-Rom.

Λογισμικά εκφοβισμού (Scareware)

Τα λογισμικά εκφοβισμού (Scareware) προκαλούν ανασφάλεια και ανησυχία στο χρήστη του υπολογιστή. Ενημερώνουν το χρήστη μέσω αναδυόμενων παραθύρων ή ελεγχόμενων ιστοσελίδων ότι ο υπολογιστής του έχει προσβληθεί από ιούς και προσφέρουν ένα υποτιθέμενο δωρεάν πρόγραμμα προστασίας από ιούς για λήψη από το διαδίκτυο. Για τη διαγραφή των δήθεν ιών απαιτείται, φυσικά, η καταβολή κάποιου χρηματικού ποσού. Εάν ο πελάτης αρνηθεί να εισαγάγει τον αριθμό της πιστωτικής του κάρτας, αρχίζει να βομβαρδίζεται με διάφορα προειδοποιητικά μηνύματα.

Προγράμματα καταγραφής πληκτρολογήσεων (Keylogger)

Τα προγράμματα καταγραφής πληκτρολογήσεων (Keylogger) είναι προγράμματα, τα οποία καταγράφουν κρυφά κάθε πληκτρολόγηση και μερικές φορές αποθηκεύουν στιγμιότυπα της οθόνης. Στη συνέχεια, τα προγράμματα καταγραφής πληκτρολογήσεων στέλνουν τις κλεμμένες πληροφορίες στον εισβολέα μέσω E-Mail ή μέσω άμεσης μεταφοράς δεδομένων.

Rootkit

Τα Rootkit βοηθούν στο καμουφλάρισμα άλλων κακόβουλων λογισμικών, αποκρύπτοντας τα κακόβουλα προγράμματα από τα λογισμικά ασφαλείας. Ελέγχουν, δηλαδή, το λειτουργικό σύστημα, δυσκολεύοντας την αναζήτηση του κακόβουλου λογισμικού. Τα λογισμικά αυτού του είδους προστατεύουν και τους χάκερ, καθώς οι πληροφορίες του εισβολέα διαγράφονται ή κωδικοποιούνται.

Exploit

Το «Exploit» είναι ένα μικρό κακόβουλο πρόγραμμα, το οποίο χρησιμοποιεί τα κενά ασφαλείας του συστήματος και τις δυσλειτουργίες των προγραμμάτων για την εγκατάσταση λογισμικού στον υπολογιστή. Γι’ αυτό, οι χρήστες θα πρέπει να χρησιμοποιούν διαρκώς μικροκώδικες και ενημερώσεις, ώστε να μην προσβάλλονται από Exploit.

Απάτες (Hoax) και ανεπιθύμητα μηνύματα (Spam)

Οι απάτες (Hoax) και τα ανεπιθύμητα μηνύματα (Spam) δεν είναι κακόβουλα λογισμικά με τη στενή έννοια του όρου. Θα τα αναλύσουμε παρακάτω.

Τα Hoax είναι αλυσίδες E-Mail που, εκτός από τις διάφορες ψευδείς πληροφορίες παντός είδους, περιλαμβάνουν την προτροπή προώθησης του μηνύματος σε όλους τους φίλους και γνωστούς. Τα Hoax συνήθως δεν προκαλούν άμεσες βλάβες. Απλώς επιβαρύνουν χωρίς λόγο το δίκτυο.

Τρόποι αντιμετώπισης

Προστασία από τα κακόβουλα λογισμικά

Προστασία από τα κακόβουλα λογισμικά προσφέρουν τα λογισμικά ασφαλείας, τα οποία προσφέρονται από τους διάφορους κατασκευαστές. Λόγω της μεγάλης αύξησης των κακόβουλων λογισμικών, προσφέρονται περιεκτικά πακέτα προστασίας με τη μορφή σουίτας, τα οποία, εκτός από προγράμματα

ανίχνευσης ιών και φίλτρο ανεπιθύμητων μηνυμάτων, περιλαμβάνουν λογισμικό αποκλεισμού διαφημίσεων, έλεγχο ιστοτόπου κ.α.

Ωστόσο, αποτελεί προσωπική ευθύνη του χρήστη το να χειριστεί με σύνεση τα διάφορα E-Mail, τις επισυνάψεις, τις λήψεις από το διαδίκτυο και τα διαφημιστικά παράθυρα. Δεν συνιστάται το άνοιγμα των επισυνάψεων ή των συνδέσμων των ανεπιθύμητων μηνυμάτων. Το καλύτερο είναι να διαγράφει κανείς τα ανεπιθύμητα μηνύματα χωρίς να τα ανοίγει. Επίσης, θα πρέπει να αποφεύγεται η λήψη περιεχομένων από άγνωστες ιστοσελίδες. Εάν επιθυμείτε παρόλα αυτά να λάβετε το περιεχόμενο, θα πρέπει να ελέγχεται αρχικά το αρχείο μέσω του προγράμματος ανίχνευσης ιών. Επίσης, θα πρέπει να γίνεται οπωσδήποτε τακτική ενημέρωση του προγράμματος περιήγησης διαδικτύου, του προγράμματος ηλεκτρονικής αλληλογραφίας, του λειτουργικού συστήματος και του λογισμικού ασφαλείας. Εκτός αυτού, οι χρήστες θα πρέπει να δημιουργούν έναν λογαριασμό χρήστη με περιορισμένα δικαιώματα και να εργάζονται μόνο μέσω αυτού. Το κακόβουλο λογισμικό έχει τόσα δικαιώματα, όσα ο χρήστης που το ενεργοποιεί. Τα δικαιώματα διαχειριστή χρειάζονται μόνο για την εγκατάσταση προγραμμάτων ή τη ρύθμιση των παραμέτρων. Όταν αντιληφθείτε ότι ο υπολογιστής σας έχει μολυνθεί με κακόβουλο λογισμικό:

1. Αλλάξτε τον κωδικό πρόσβασης στο Facebook
2. •Σαρώστε τον υπολογιστή σας.
3. •Ξεκινήστε τη σάρωση για ιούς (μία μόνο φορά).
4. •Κατεβάστε το Microsoft Security Essentials.
5. Αναβαθμίστε το πρόγραμμα περιήγησης που χρησιμοποιείτε. Οι τρέχουσες εκδόσεις των προγραμμάτων περιήγησης διαθέτουν ενσωματωμένη προστασία. Το Facebook υποστηρίζει τα εξής προγράμματα περιήγησης:

   •Mozilla Firefox.

   •Safari.

   •Google Chrome.

   •Internet Explorer.
6. Αφαιρέστε τυχόν ύποπτα πρόσθετα του προγράμματος περιήγησης

Αν εγκαταστήσατε κάποιο πρόσθετο και τώρα ο λογαριασμός σας στέλνει σπαμ, ίσως ο υπολογιστής σας να έχει μολυνθεί με κακόβουλο λογισμικό.

Διατήρηση ασφαλούς λογαριασμού

Τρόποι διατήρησης:

Μην πατάτε ποτέ ύποπτους συνδέσμους, ακόμη και αν προέρχονται από κάποιο φίλο σας ή κάποια εταιρεία που γνωρίζετε. Αυτό ισχύει τόσο για τους συνδέσμους που σας στέλνουν στο Facebook (π.χ. σε μια συνομιλία ή δημοσίευση) όσο και για τους συνδέσμους που λαμβάνετε μέσω email. Αν κάποιος από τους φίλους σας πατήσει ένα σύνδεσμο σπαμ, μπορεί να σας στείλει κατά λάθος σπαμ ή να σας προσθέσει με ετικέτα σε μια δημοσίευση σπαμ. Επίσης δεν πρέπει να κατεβάζετε περιεχόμενο (π.χ. αρχεία.exe) για το οποίο δεν είστε απόλυτα σίγουροι. Μάθετε πώς να αναγνωρίζετε τα ύποπτα email.

Επιλέξτε έναν μοναδικό, ισχυρό κωδικό πρόσβασης. Δημιουργήστε έναν κωδικό με τουλάχιστον έξι χαρακτήρες, συνδυάζοντας γράμματα, ψηφία και σημεία στίξης. Μην χρησιμοποιήσετε τον ίδιο κωδικό με άλλους λογαριασμούς σας. Μάθετε πώς μπορείτε να αλλάξετε τον κωδικό σας.

Για κανένα λόγο δεν πρέπει να αποκαλύπτετε τα στοιχεία με τα οποία συνδέεστε (π.χ. τη διεύθυνση email και τον κωδικό πρόσβασης). Κάποια άτομα ή κάποιες σελίδες μπορεί να σας υποσχεθούν κάτι (π.χ. δωρεάν μονάδες πόκερ) αν τους δώσετε τα στοιχεία με τα οποία συνδέεστε. Αυτές οι προσφορές προέρχονται από εγκληματίες του Διαδικτύου και παραβιάζουν τους Όρους χρήσης του Facebook. Αν σας ζητηθεί ποτέ να πληκτρολογήσετε ξανά τον κωδικό πρόσβασης στο Facebook (π.χ. όταν κάνετε αλλαγές στις ρυθμίσεις του λογαριασμού σας), βεβαιωθείτε ότι στη διεύθυνση URL της σελίδας εξακολουθεί να υπάρχει το τμήμα facebook.com/.

Συνδεθείτε από τη διεύθυνση www.facebook.com. Ορισμένες φορές, οι κακόβουλοι χρήστες δημιουργούν εικονικές σελίδες που μοιάζουν με τη σελίδα σύνδεσης του Facebook, ελπίζοντας ότι θα συμπληρώσετε τη διεύθυνση email σας και τον κωδικό πρόσβασης. Πριν συμπληρώσετε τα στοιχεία σύνδεσης, ελέγξτε προσεκτικά τη διεύθυνση URL (διαδικτυακή διεύθυνση) της σελίδας. Αν έχετε αμφιβολία, πληκτρολογήστε τη διεύθυνση facebook.comστο πρόγραμμα περιήγησης. Έτσι θα μεταβείτε στον πραγματικό ιστότοπο του Facebook.

Κεφάλαιο 12

Ανεπιθύμητη αλληλογραφία (SPAM)

Τι είναι το spam;

Spam είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων που απευθύνονται σε ένα σύνολο παραληπτών του Διαδικτύου χωρίς αυτοί να το επιθυμούν και χωρίς να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον εν λόγω αποστολέα. Το Spam συχνά έχει την μορφή ενημερωτικών ή διαφημιστικών μηνυμάτων για προϊόντα ή υπηρεσίες τα οποία φθάνουν στο γραμματοκιβώτιο μας χωρίς να έχουμε ζητήσει την εν λόγω πληροφόρηση. Η αλληλογραφία αυτή λοιπόν μπορεί να χαρακτηριστεί ως απρόκλητη ή ανεπιθύμητη αλληλογραφία.

Τα κυριότερα χαρακτηριστικά του Spam:

- **Απρόκλητο:** δηλαδή δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα.
- **Εμπορικό:** Πολλές φορές το spam αφορά την αποστολή μηνυμάτων εμπορικού σκοπού με σκοπό την προβολή και την διαφήμιση προϊόντων και υπηρεσιών με σκοπό την προσέλκυση πελατών και την πραγματοποίηση πωλήσεων.
- **Μαζικό:** Το spam συνίσταται στην μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών. Συνήθως το ίδιο μήνυμα ή ελαφρά διαφοροποιημένο στέλνεται σε ένα μεγάλο πλήθος παραληπτών.

Το spam είναι ένα φαινόμενο….

- **δυσάρεστο, ενοχλητικό και απαράδεκτο** από τους παραλήπτες. Πολλές φορές προβάλει αμφίβολης ποιότητας προϊόντα και υπηρεσίες, ενώ συνηθισμένη είναι η προβολή ύποπτων οικονομικών δραστηριοτήτων τύπου πυραμίδων κλπ. Αλλα μηνύματα περιέχουν ή διαφημίζουν σεξουαλικό περιεχόμενο.

- **Οδηγεί σε κατάχρηση πόρων του Διαδικτύου.** Η κατάχρηση αυτή επιβαρύνει τα δίκτυα με κατανάλωση εύρους ζώνης, αποθηκευτικών και υπολογιστικών πόρων στα κεντρικά συστήματα διανομής αλληλογραφίας (e-mail servers). Αντίστοιχα προβλήματα προκαλεί στην πρόσβαση και στα συστήματα των χρηστών.

- **Θέτει σε κίνδυνο την ασφάλεια και την αξιοπιστία του διαδικτύου:** Οι spammers βρίσκονται σε συνεχή αναζήτηση συστημάτων τα οποία θα μπορούσαν να χρησιμοποιήσουν για την αποστολή των μηνυμάτων τους.

- Πολλά μηνύματα αυτής της κατηγορίας μεταφέρουν επισυναπτόμενα τα οποία μπορεί να είναι **ιοί ή δούρειοι ίπποι**, οι οποίοι θέτουν σε κίνδυνο την ασφάλεια των συστημάτων. Το τελευταίο διάστημα μεγάλο ποσοστό ανεπιθύμητης και επικίνδυνης αλληλογραφίας είναι αποτέλεσμα της δράσης ιών που έχουν προσβάλει διάφορα συστήματα διασυνδεμένα στο Διαδίκτυο.

Τι μπορούμε να κάνουμε για να αποφύγουμε το Spam;

Οι απλοί χρήστες:

- **Μη δημοσιεύετε την διεύθυνση ηλεκτρονικού ταχυδρομείου σας.**

Βάζοντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου σε μια ιστοσελίδα είναι σχεδόν σίγουρο ότι σύντομα θα δείτε μηνύματα Spam στο γραμματοκιβώτιο σας.

- **Μη δίνετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας, σε οργανισμούς που δεν εμπιστεύεστε.**

Να είστε προσεκτικοί όταν επισκέπτεστε διάφορους δικτυακούς τόπους και σας ζητείτε η συμπλήρωση προσωπικών και στοιχείων επικοινωνίας, όπως το e-mail. Αν είστε αναγκασμένοι να δώσετε τη διεύθυνση ηλ. ταχυδρομείου, διαβάστε προσεκτικά τους όρους χρήσης και την πολιτική εχεμύθειας για την οποία δεσμεύεται ο συγκεκριμένος οργανισμός.

- **Μην απαντάτε στο spam**.

Μην απαντάτε στους spammers ακόμα και στην ένδειξη για διαγραφή από τις mail λίστες τους. Είναι μια παγίδα με τελικό αποτέλεσμα

Να διαπιστωθεί η εγκυρότητα της mail διεύθυνσης σας και επομένως να γίνει στόχος αποστολής επιπλέον μηνυμάτων.

Να χάνετε το χρόνο σας και να σπαταλάτε πόρους χωρίς λόγο, ενώ δεν υπάρχει αποτέλεσμα.

- **Αναφέρετε κάθε μήνυμα Spam που λαμβάνετε.**

Υπάρχουν σχετικές υπηρεσίες του Διαδικτύου οι οποίες διατηρούν λίστες spammers. Τις λίστες αυτές αξιοποιούν πολλοί εξυπηρετητές ηλεκτρονικού ταχυδρομείου για τον περιορισμό του Spam που φθάνει στους χρήστες. Στις υπηρεσίες αυτές μπορείτε να αναφέρετε τα μηνύματα τύπου Spam που φθάνουν σε σας.

- **Διαδώστε την γνώση σας και την εμπειρία σας σε σχέση με το Spam.**

Μιλήστε στους χρήστες του δικτύου σας, μαθητές, εκπαιδευτικούς, διοικητικό προσωπικό, στην οικογένεια σας και τους φίλους σας για το θέμα του Spam και την αντιμετώπιση του. Είναι αρκετά συνηθισμένο οι spammers συγκεντρώνουν e-mail διευθύνσεις από τις απαντήσεις χρηστών του Διαδικτύου.

- **Ελέγξτε τα συστήματα σας ώστε να είναι σωστά διαμορφωμένα και ασφαλή.**

Ένα μεγάλο ποσοστό του Spam διαδίδεται από mail servers που δεν είναι σωστά διαμορφωμένοι, αλλά ακόμα και από συστήματα χρηστών.

Οι επιλογές του απλού χρήστη για προστασία.

- ✓ Προγράμματα αλληλογραφίας με δυνατότητα εντοπισμού της ενοχλητικής αλληλογραφίας (Spam - Junk Email).
- ✓ *Χρήση white lists.*
- ✓ *Φιλτράρισμα με βάση τον αποστολέα και το περιεχόμενο.*
- ✓ *Εξελιγμένα προγράμματα φιλτραρίσματος.*

Επιλογές των διαχειριστών ηλεκτρονικού ταχυδρομείου

- 💻 *Έλεγχος εγκυρότητας στο DNS και στους headers.*
- 💻 *Χρήση SMTP Server που απορρίπτει γνωστούς spammers.*
- 💻 *Χρήση προγραμμάτων προστασίας στον διακομιστή.*
- 💻 *Φιλτράρισμα των SMTP συνδέσεων.*
- 💻 *Παρακολούθηση.*

Νομοθεσία για το spam

Ο Νόμος 2251 του 1994 αποτελεί τον πιο σημαντικό νόμο που ρυθμίζει ζητήματα προστασίας του καταναλωτή. Περιέχει ορισμούς των εννοιών του καταναλωτή, του προμηθευτή, της σύμβασης από απόσταση και άλλων.

Η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή μέσω τηλεφώνου, τηλεομοιοτυπίας(φαξ),ηλεκτρονικού ταχυδρομείου, αυτόματης κλήσης ή άλλου ηλεκτρονικού μέσου επικοινωνίας επιτρέπεται μόνο αν συναινεί ρητά ο καταναλωτής.Ανεξάρτητα από τον περιορισμό της προηγούμενης παραγράφου, η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή με οποιονδήποτε τρόπο άμεσης επικοινωνίας (άμεση διαφήμιση) επιτρέπεται μόνο αν ο προμηθευτής ή άλλος για λογαριασμό του προμηθευτή κάνει χρήση στοιχείων ή πληροφοριών προσωπικού χαρακτήρα του καταναλωτή που περιήλθαν σε γνώση του από τις προηγούμενες συναλλακτικές σχέσεις του με τον καταναλωτή, από γενικά προσιτές πηγές, όπως κατάλογο ή άλλα δημοσιευμένα στοιχεία, ή από άλλο φυσικό ή νομικό πρόσωπο, εφόσον ο καταναλωτής εγκρίνει ρητά τη μεταβίβαση των προσωπικών του στοιχείων για το σκοπό της άμεσης διαφήμισης. Ο διαφημιστής είναι υποχρεωμένος να αναφέρει στον καταναλωτή τον τρόπο με τον οποίο περιήλθαν σε γνώση του τα προσωπικά στοιχεία του καταναλωτή. Στις περιπτώσεις αυτές, ο προμηθευτής οφείλει να διακόψει κάθε μορφή άμεσης διαφήμισης και να διαγράψει τα προσωπικά στοιχεία του καταναλωτή, εφόσον το ζητήσει ο καταναλωτής. Η άμεση διαφήμιση θα πρέπει να γίνεται με τρόπο που να μην προσβάλλει την ιδιωτική ζωή του καταναλωτή.

Βιβλιογραφία

Ορισμοί Ηλεκτρονικού Εγκλήματος Μορφών και Ποινικών Κυρώσεων :

http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=0&langENENENEN

Hacking & Cracking:

http://el.wikipedia.org/wiki/%CE%A7%CE%AC%CE%BA%CE%B5%CF%81

Πειρατεία Λογισμικού

http://el.wikipedia.org/wiki/%CE%A0%CE%B5%CE%B9%CF%81%CE%B1%CF%84%CE%B5%CE%AF%CE%B1

cyber Bulling – Ηλεκτρονική τρομοκρατία

http://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%85%CE%B1%CE%BA%CF%8C%CF%82_%CE%B5%CE%BA%CF%86%CE%BF%CE%B2%CE%B9%CF%83%CE%BC%CF%8C%CF%82

http://www.infokids.gr/2011/11/cyber-bullying-%CF%84%CE%AF-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CE%BA%CE%B1%CE%B9-%CF%80%CF%8E%CF%82-%CF%84%CE%BF-%CE%B1%CE%BD%CF%84%CE%B9%CE%BC%CE%B5%CF%84%CF%89%CF%80%CE%AF%CE%B6%CE%BF%CF%85%CE%BC/

http://www.lawnet.gr/news/oi-tromokrates-drastiriopoiountai-meso-facebook-sumfona-me-ereuna-27713.html

http://el.wikipedia.org/wiki/%CE%A4%CF%81%CE%BF%CE%BC%CE%BF%CE%BA%CF%81%CE%B1%CF%84%CE%AF%CE%B1

http://news.kathimerini.gr/4dcgi/_w_articles_ell_1_20/03/2009_308302

Παιδική πορνογραφία

http://www.pi.ac.cy/InternetSafety/sec_kindinoi_pornografia.html

http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=0&langENENENEN

Βιβλιογραφία

Ξέπλυμα μαύρου χρήματος

http://www.hellenicparliament.gr/UserFiles/c8827c35-4399-4fbb-8ea6-aebdc768f4f7/%CE%A3%CE%A7%CE%95%CE%94%CE%99%CE%9F%20%CE%9D%CE%9F%CE%9C%CE%9F%CE%A5%20%28%CE%9D%CE%91%CE%A1%CE%9A%CE%A9%CE%A4%CE%99%CE%9A%CE%91%29.pdf

http://www.moneyguru.gr/search-results/ArtMID/527/ArticleID/124/xeplima-vromikou-xrimatos

Ηλεκτρονικό ψάρεμα:

https://support.google.com/chrome/answer/99020?hl=el

http://www.slideshare.net/ChristosSotiropoulos/phishing-16709528

http://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF

http://oneiros.gr/blog/2005/10/26/amateurphishers/

http://windows.microsoft.com/el-gr/windows-vista/what-is-phishing

Κλοπή ταυτότητας:

http://www.saferinternet.gr/index.php?childobjId=Category143&objId=Category43&parentobjId=Page3

http://gr.norton.com/identity-theft-primer/article

http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/YOUTH/YOUTH_INTRO/YOUTH_BOOKLET.PDF

http://www.google.com/intl/el_gr/goodtoknow/online-safety/identity-theft/

Διαδικτυακές απάτες:

http://www.astynomia.gr/index.php?Itemid=128&id=3686&option=ozo_conent&perform=view

http://www.protothema.gr/greece/article/310674/sustaseis-apo-tin-elas-gia-diadiktuakes-apates/

Βιβλιογραφία

http://magazine.apopsi.com.cy/2009/10/2150

http://www.inewsgr.com/96/nigirianes-apates.htm

Κακόβουλο λογισμικο Spam

http://www.sch.gr/2010-04-07-09-22-34/-spam?lang=en

http://www.sch.gr/2010-04-07-09-22-34/-spam/%CE%A3%CE%B5%CE%BB%CE%AF%CE%B4%CE%B1-2?lang=en&limit=1&limitstart=1#content

http://www.sch.gr/2010-04-07-09-22-34/-spam/%CE%A3%CE%B5%CE%BB%CE%AF%CE%B4%CE%B1-3?lang=en&limitstart=2#content

https://el-gr.facebook.com/help/320234818071511

https://support.google.com/adwords/answer/2375413?hl=el

http://el.wikipedia.org/wiki/%CE%9A%CE%B1%CE%BA%CF%8C%CE%B2%CE%BF%CF%85%CE%BB%CE%BF_%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CF%8C

https://el-gr.facebook.com/help/320234818071511

https://support.google.com/adwords/answer/2375413?hl=el

http://el.wikipedia.org/wiki/%CE%9A%CE%B1%CE%BA%CF%8C%CE%B2%CE%BF%CF%85%CE%BB%CE%BF_%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CF%8C

Παράρτημα 1: Αφίσα cyber Bulling

Παράρτημα

Παράρτημα 2:φυλλάδιο σχετικό με το Hacking –cracking- Πειρατεία Λογισμικού

HACKING-CRACKING-PIRACY

Hacking και Cracking

- Hacking είναι η διαδικασία εξουδιοδωτημένων ή μη, προσπαθειών παράκαμψης μηχανισμώς προστασίας συστημάτων πληροφορίας ή δικτύων.
- Με απλά λόγια Hacking σημαίνει το να βρήσκεις αδυναμίες σε έναν υπολογιστή ή σε δίκτυα υπολογιστών.

- Εγκαταστήστε ένα ισχυρό Anti-Virus.
- Εκτελείτε πάντα έναν έλεγχο με το Anti-Virus πριν κατεβάσετε κάποιο αρχείο ή πρόγραμμα απο το διαδίκτυο.
- Αποφείγετε την παράθεση προσωπικών λεπρομερειών όπως: αριθμό τηλεφώνου, αριθμό πιστοτικής κλπ. σε αγνώστους.
- Εγκαταστείστε ένα καλό Firewall.
- Εγκαταστείστε ένα καλό Spyware
- Αποφύγετε την χρήση πλαστού λογισμικού.

✓ Η συλλογή πληροφοριών
✓ Εισβολή στο σύστημα
✓ Η πρόσβαση του hacker μέσα στο σύστημα

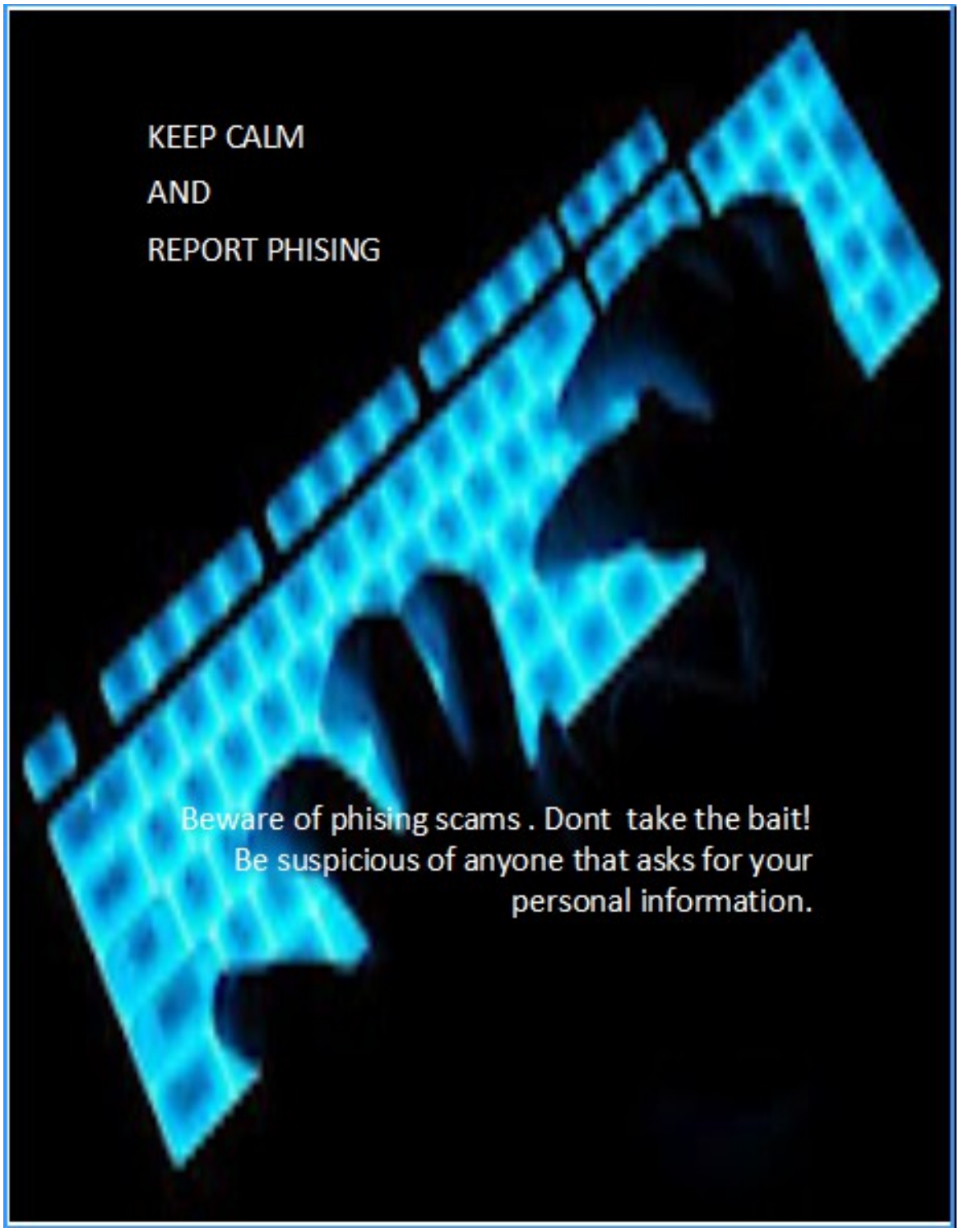
ΠΕΙΡΑΤΕΙΑ ΛΟΓΙΣΜΙΚΟΥ Η/Υ

Πιθανές συνέπειες από τη χρήση πειρατικού λογισμικού:

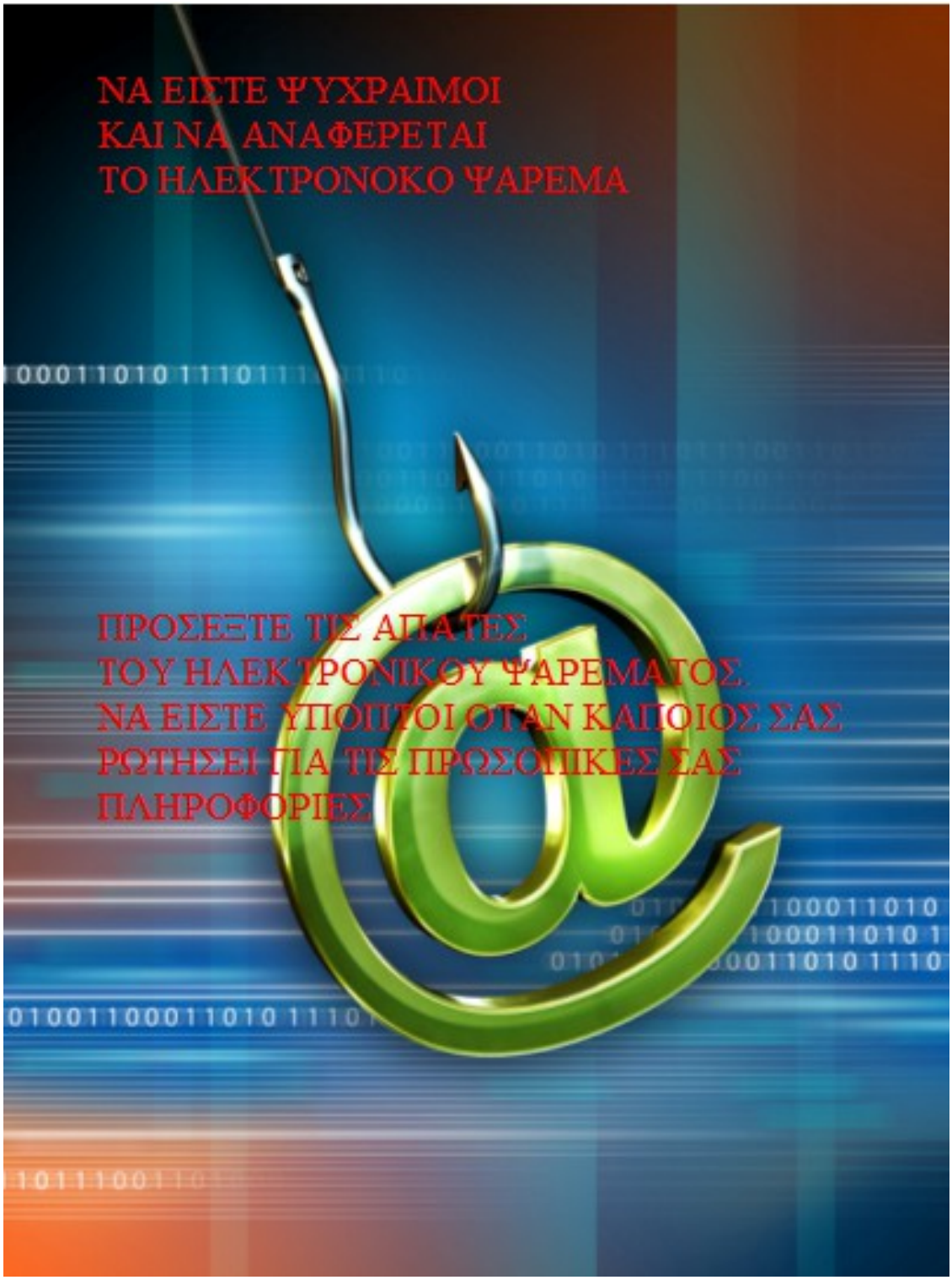
- Προσβολή της φήμης και του ονόματος της επιχείρησής σας
- Ποινικές, αστικές και διοικητικές κυρώσεις
- Έλλειψη τεχνικής υποστήριξης και δωρεάν αναβαθμίσεων

Παράρτημα

Παράρτημα 3: Αφίσα Σχετική με το Phising στα Αγγλικά



Παράρτημα 4: Αφίσα Σχετική με το Phising στα Ελληνικά



Παράρτημα 5: Φυλλάδιο ενημερωτικό Σχετική με το Phising

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

1.Από ηλεκτρονική απάτη:

- *Να είστε ιδιαίτερα προσεκτικοί και να μην ανοίγετε συνημμένα, όταν προέρχονται από άγνωστους αποστολείς.*
- *Εγκαταστήστε και μην παραλείπετε να ενημερώνετε τακτικά το λογισμικό τείχους προστασίας, καταπολέμησης ιών και spyware.*
- *Μην δίνετε ποτέ τα προσωπικά σας στοιχεία σε απάντηση σε email, σε τοποθεσία web στην οποία οδηγηθήκατε μέσω ενός εξωτερικού συνδέσμου ή σε ένα αναδυόμενο παράθυρο που εμφανίζεται σε μια πραγματική τοποθεσία web. Αντίθετα, ανοίξτε ένα νέο παράθυρο στο πρόγραμμα περιήγησης και πληκτρολογήστε απευθείας στη γραμμή διεύθυνσης το URL της τοποθεσίας ώστε να είστε σίγουροι για τη γνησιότητά της.*
- *Ελέγχετε τακτικά τα αντίγραφα κινήσεων τραπεζικών λογαριασμών και πιστωτικών καρτών.*
- *Οι ισχυροί κωδικοί πρόσβασης διαθέτουν τουλάχιστον οκτώ χαρακτήρες και χρησιμοποιούν συνδυασμό γραμμάτων, αριθμών και συμβόλων.*

2.Από ηλεκτρονικό ψάρεμα:

- Να είστε ιδιαίτερα προσεκτικοί με τα email που ζητούν προσωπικές, εμπιστευτικές πληροφορίες—*ιδιαίτερα οικονομικής φύσης. Οι νόμιμες, αξιόπιστες εταιρείες δεν θα ζητήσουν ποτέ ευαίσθητες προσωπικές πληροφορίες μέσω email.*
- Μην υποκύψετε στις πιέσεις *να δώσετε άμεσα τις προσωπικές πληροφορίες που σας ζητούνται. Οι απατεώνες χρησιμοποιούν συνήθως εκφοβιστικές τακτικές απειλώντας ότι εάν ο χρήστης δεν προβεί άμεσα στην ενημέρωση συγκεκριμένων πληροφοριών θα απενεργοποιηθεί ο λογαριασμός του ή θα καθυστερήσει η παροχή ορισμένων υπηρεσιών. Αυτό που πρέπει να κάνετε είναι να απευθυνθείτε απευθείας στον αποστολέα και να επιβεβαιώσετε τη γνησιότητα του μηνύματος.*
- Μην συμπληρώνετε ποτέ τα προσωπικά στοιχεία σας *σε φόρμες ενσωματωμένες σε μηνύματα email.*
- Μάθετε να ξεχωρίζετε τα γενικού χαρακτήρα μηνύματα που ζητούν *πληροφορίες. Τα παραπλανητικά μηνύματα συνήθως δεν είναι προσωποποιημένα, σε αντίθεση με τα γνήσια στα οποία συνήθως η τράπεζά σας αναφέρεται στον αριθμό λογαριασμού που διατηρείτε σε αυτήν.*

ΕΝΝΟΙΕΣ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΓΝΩΡΙΖΟΥΜΕ

➢ *Ηλεκτρονική απάτη*

Αναφέρεται σε κάθε μορφής απάτη με χρήση email, τοποθεσιών web, chat room ή message board. Τα παραπάνω μέσα χρησιμοποιούνται για την παραπλάνηση πιθανών θυμάτων, για τη διενέργεια πλαστών συναλλαγών ή για τη μεταφορά κλεμμένων χρημάτων σε χρηματοπιστωτικά ιδρύματα ή σε άλλους παραλήπτες που εμπλέκονται στο έγκλημα.

➢ *Κλοπή ταυτότητας*

Η πράξη της κλοπής και της χρήσης της ταυτότητας ενός άλλου προσώπου για τη διάπραξη δόλιας ενέργειας ή άλλων εγκλημάτων.

➢ *Phishing*

Phishing είναι η προσπάθεια παραπλάνησης ανθρώπων για την υποκλοπή εμπιστευτικών πληροφοριών, όπως αριθμών κοινωνικής ασφάλισης και κωδικών πρόσβασης. Συνήθως γίνεται με την αποστολή παραπλανητικών email ή άμεσων μηνυμάτων που μοιάζουν με αληθινά σε συνδυασμό με πλαστές τοποθεσίες web που ζητούν τα προσωπικά στοιχεία των χρηστών.

Παράρτημα