Ηλεκτρονικό Έγκλημα
Electronic crime

ΓΕΝΙΚΟ ΛΥΚΕΙΟ ΑΛΙΑΡΤΟΥ

ΕΡΕΥΝΗΤΙΚΗ ΕΡΓΑΣΙΑ

Β΄ ΤΕΤΡΑΜΗΝΟ

ΣΧΟΛΙΚΟ ΕΤΟΣ 2014-15

ΑΛΙΑΡΤΟΣ, ΜΑΪΟΣ 2015

Εργάστηκαν οι μαθητές του Β1 τμήματος του Γενικού Λυκείου Αλιάρτου

Σύνθεση ομάδων και εργασίες που έχουν αναλάβει:

<table>
<tr><th colspan="2">Ομάδες - θέματα</th><th>Ερωτήματα που θα διερευνήσει κάθε ομάδα</th></tr>
<tr><td colspan="3">Ομάδα 1η : Ηλεκτρονικό έγκλημα</td></tr>
<tr><td>1</td><td>Αντωνίου Σέρι</td><td rowspan="3">Ορισμός (τι είναι)
Χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο
Διαδικασία έρευνας
Νομοθεσία</td></tr>
<tr><td>2</td><td>Γιαννουκάκη Ελένη</td></tr>
<tr><td>3</td><td>Κατσιφή Αναστασία</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3">Ομάδα 2η : Μορφές εγκλήματος στον Κυβερνοχώρο</td></tr>
<tr><td>1</td><td>Αντωνίου Ευαγγελία</td><td rowspan="5">Μορφές Κυβερνοεγκλήματος
Περιγραφή των παρακάτω μορφών:
1. Κακόβουλες εισβολές σε δίκτυα (Hacking και cracking)
2. Κακόβουλο λογισμικό
3. Επιθέσεις Άρνησης Εξυπηρέτησης
4. Ανεπιθύμητη Αλληλογραφία (Spamming)
5. Επιθέσεις σε δικτυακούς τόπους (sites)
6. Κλοπή ταυτότητας</td></tr>
<tr><td>2</td><td>Δαραμάρα Αγγελική</td></tr>
<tr><td>3</td><td>Ζαρκαδούλα Δέσποινα</td></tr>
<tr><td>4</td><td>Καπούλας Απόστολος</td></tr>
<tr><td>5</td><td>Κολοβός Παναγιώτης</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3">Ομάδα 3η : Μορφές εγκλήματος στον Κυβερνοχώρο ….συνέχεια…..</td></tr>
<tr><td>1</td><td>Αδάμου Εβίτα</td><td rowspan="5">7. Ηλεκτρονικό ψάρεμα (Phising)
8. Πειρατεία λογισμικού
9. Απάτη στο Διαδίκτυο
10. Διακίνηση παιδικού πορνογραφικού υλικού
11. Ξέπλυμα χρήματος
12. Διαδικτυακή τρομοκρατία
13. Επιθέσεις παρενόχλησης (cyberbulling)</td></tr>
<tr><td>2</td><td>Βίτση Γωγώ</td></tr>
<tr><td>3</td><td>Καρανάσου Χριστίνα</td></tr>
<tr><td>4</td><td>Κοταπίτας Γρηγόρης</td></tr>
<tr><td>5</td><td>Μαγγόγιας Παναγιώτης</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3">Ομάδα 4η: Ενημέρωση - Προστασία - Αντιμετώπιση</td></tr>
<tr><td>1</td><td>Αποστόλου Παρασκευή</td><td rowspan="5">Τρόποι προστασίας - αντιμετώπισης
Υπεύθυνες υπηρεσίες
Διαδικτυακοί τόποι ενημέρωσης και υπηρεσίες</td></tr>
<tr><td>2</td><td>Καρανάσος Άγγελος</td></tr>
<tr><td>3</td><td>Κουτρομάνου Ευαγγελία</td></tr>
<tr><td>4</td><td>Κυρίτσης Κωνσταντίνος</td></tr>
<tr><td>5</td><td>Κωστακοπούλου Έλενα</td></tr>
</table>

Υπεύθυνη καθηγήτρια: ΧΑΛΙΜΟΥΡΔΑ ΑΓΓΕΛΙΚΗ – ΠΕ19 - Πληροφορικός

ΠΕΡΙΛΗΨΗ

Ομάδα 1η : Σε αυτό το τετράμηνο το θέμα μας ήταν το Ηλεκτρονικό Έγκλημα Στη συνέχεια για να επιτευχθεί ο σκοπός της έρευνας μας χωρίσαμε το θέμα μας σε επιμέρους ενότητες. Τα ερωτήματα με τα οποία ασχοληθήκαμε είναι τα ακόλουθα: τι είναι ηλεκτρονικό έγκλημα, τα χαρακτηριστικά γνωρίσματά του στον Κυβερνοχώρο, την διαδικασία έρευνας γενικώς αλλά και από το τμήμα Δ.Η.Ε της ΕΛΑΣ, η νομοθεσία εξωτερικού, Ελλάδας και οι αδυναμίες της σε σχέση με αυτό. Σε κάθε μέλος της ομάδας είχε ανατεθεί να διερευνήσει ένα ή περισσότερα ερωτήματα. Στο τέλος συγκεντρώσαμε όλα μας τα στοιχεία, επεξεργαστήκαμε, ενώσαμε και διορθώσαμε και προέκυψε η παρακάτω εργασία.

Ομάδα 2η : Η ομάδα μας ασχολήθηκε με τις μορφές ηλεκτρονικού εγκλήματος, τις κακόβουλες εισβολές σε δίκτυα, τα κακόβουλα λογισμικά, το spamming, την κλοπή ταυτότητας και την επίθεση σε δικτυακούς τόπους. Κάθε μαθητής της ομάδας ανέλαβε να ερευνήσει από ένα θέμα ψάχνοντας σε ανάλογες ιστοσελίδες.

Ομάδα 3η : Σε αυτό το τετράμηνο η ερευνητική μας εργασία είχε θέμα το Ηλεκτρονικό Έγκλημα. Η ομάδα μας ασχολήθηκε με τις μορφές εγκλήματος στον Κυβερνοχώρο. Συγκεκριμένα αναλάβαμε το ηλεκτρονικό ψάρεμα (phising), την πειρατεία λογισμικού, την απάτη στο διαδίκτυο, τη διακίνηση παιδικού πορνογραφικού υλικού, το ξέπλυμα χρήματος, τη διαδικτυακή τρομοκρατία και τις επιθέσεις παρενόχλησης (cyberbulling). Συλλέξαμε πληροφορίες και αφού τις ενώσαμε, προέκυψε η τελική διαμορφωμένη εργασία αλλά και η παρουσίαση της.

Ομάδα 4η: Το ηλεκτρονικό έγκλημα είναι ένα συχνό φαινόμενο της σύγχρονης εποχής, εξαιτίας της ραγδαίας ανάπτυξης της τεχνολογίας και της συμμετοχής ολοένα και περισσότερων ατόμων, κυρίως νέων, στον κυβερνοχώρο. Για να μην εξαπλωθεί όμως το παραπάνω πρόβλημα ακόμη περισσότερο, είναι απαραίτητο να ληφθούν ορισμένα μέτρα για την άμεση αντιμετώπιση του. Η ομάδα μας έχει αναλάβει την παρουσίαση των υπηρεσιών που είναι υπεύθυνες και αρμόδιες για θέματα προστασίας από το ηλεκτρονικό έγκλημα.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. ΘΕΩΡΗΤΙΚΟ ΜΕΡΟΣ

ΚΕΦ. 1^{ο} : Ηλεκτρονικό έγκλημα

1.1. Ορισμός

Ως ηλεκτρονικό έγκλημα ορίζονται οι αξιόποινες πράξεις που τελούνται με την χρήση ηλεκτρονικών υπολογιστών και γενικότερα με διάφορα ηλεκτρονικά μέσα. Οι πράξεις αυτές τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία ανάλογα με τον τρόπο τέλεσης. Διαχωρίζονται σε εγκλήματα τελούμενα με την χρήση ηλεκτρονικών υπολογιστών (computer crime) και σε κυβερνοεγκλήματα (cyber crime) εάν τελέσθηκαν μέσω του διαδικτύου.
Το ηλεκτρονικό έγκλημα θεωρείται ως:

α) μια νέα μορφή εγκλήματος

β) μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων

γ) μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθοιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής

1.2. Χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο

- Το έγκλημα στον Κυβερνοχώρο είναι γρήγορο (σε χρόνο δευτερολέπτων).
- Γι’ αυτούς που γνωρίζουν είναι εύκολο στην διάπραξη του.
- Για την τέλεση του απαιτούνται άριστες και εξειδικευμένες γνώσεις.
- Μπορεί να διαπραχθεί χωρίς μετακίνηση.
- Δίνει τη δυνατότητα σε άτομα με ιδιαιτερότητες όπως οι παιδόφιλοι, να επικοινωνούν γρήγορα, σε πραγματικό χρόνο, χωρίς μετακίνηση και εύκολα.
- Οι ¨εγκληματίες του Κυβερνοχώρου¨ πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα.
- Είναι έγκλημα διασυνοριακό και τα αποτελέσματα μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους.
- Είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τελέσεως του και επίσης είναι δύσκολη η διερεύνηση και ο εντοπισμός του δράστη.

- Η έρευνα απαιτεί κατά κανόνα συνεργασία δυο τουλάχιστον κρατών (του κράτους στο οποίο έγινε αντιληπτό το αποτέλεσμα της εγκληματικής συμπεριφοράς και του κράτους όπου βρίσκονται τα αποδεικτικά στοιχεία).
- Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα διότι ελάχιστες περιπτώσεις εγκλημάτων του Κυβερνοχώρου καταγγέλλονται διεθνώς.

1.3. Διαδικασία έρευνας

Η έρευνα ηλεκτρονικών εγκλημάτων είναι σε μεγάλο επίπεδο δύσκολη και χρονοβόρα, όπως και ο εντοπισμός των ηλεκτρονικών ιχνών, τα οποία είναι ένα από τα πιο σημαντικά αποδεικτικά στοιχεία. Συγκεκριμένα μια έρευνα μπορεί να διαρκέσει από έναν μήνα έως και δύο χρόνια. Και ο λόγος αυτής της μεγάλης διάρκειας είναι πως οι χρήστες που έχουν καταγγείλει (οι πολίτες) παίρνουν διάφορα διαδικτυακά μέτρα προστασίας.

Επισημαίνεται πως ο τέλειος συνδυασμός για την επίλυση τέτοιων εγκλημάτων είναι η κατάλληλη εξειδίκευση του αστυνομικού προσωπικού αλλά και τα κατάλληλα τεχνολογικά μέσα. Αν κάτι από αυτά τα δύο δεν είναι αρκετό τότε δεν θα υπάρχουν τα θεμιτά αποτελέσματα ποτέ.

Μετά τη διεξαγωγή του ηλεκτρονικού εγκλήματος θα πρέπει να ληφθούν άμεσα μέτρα. Αρχικά, κρίνεται επιβεβλημένο να εγκαθιδρυθεί περίμετρος ασφαλείας στο χώρο που έλαβε χώρα το έγκλημα. Πολλές φορές μπορεί το μέγεθος αυτής να είναι μεγάλο, λόγω της ύπαρξης δικτύων σε αρκετά κτιριακά συγκροτήματα. Έπειτα επιβάλλεται η προστασία των συσκευών που βρίσκονται εντός της περιμέτρου. Επόμενο βήμα είναι η προστασία των προσωρινών στοιχείων. Εάν αυτά δε δύναται να αποθηκευθούν εξ' αιτίας των προαναφερθέντων προϋποθέσεων, θα πρέπει να φωτογραφίζονται και να καταγράφονται γραπτώς. Τέλος λαμβάνει χώρα η αποσύνδεση των συσκευών από κάθε δικτυακό πόρο. Στις συγκεκριμένες διαδικασίες προκύπτει το δίλημμα της απενεργοποίησης των συσκευών, με δύο σχολές δράσης να κυριαρχούν. Η μία είναι υπέρ της άμεσης αποσύνδεσης των συσκευών από την ηλεκτρική τροφοδοσία για την αποφυγή ηθελημένης καταστροφής δεδομένων κατά τη διαδικασία απενεργοποίησης, ενώ η άλλη συνιστά την ασφαλή απενεργοποίηση για αποφυγή σφαλμάτων υλικού και λογισμικού.

Οι επόμενες κινήσεις αφορούν του ρόλους των εξερευνώντων. Οι τελευταίοι καλούνται να θεσμοθετήσουν μια ιεραρχία ρόλων μεταξύ των εμπλεκομένων μέχρι την ασφαλή περισυλλογή των στοιχείων. Επίσης, είθισται να συντονίζουν έρευνες για ανεύρεση και άλλων φυσικών μέσων αποθήκευσης εντός της περιμέτρου που μπορεί να βοηθήσουν στη διαλεύκανση της εγκληματικής

πράξης. Τέλος, για τη διατήρηση της ακεραιότητας των συλλεχθέντων δεδομένων, κρίνεται επιβεβλημένο να δημιουργούνται διπλά αντίγραφα ασφαλείας.

Εξίσου σημαντικός είναι και ο ρόλος των τεχνικών. Καλούνται να διασφαλίσουν την προστασία «πτητικών» δεδομένων από wipe on startup (σβήσιμο κατά την εκκίνηση) με τη δημιουργία διπλοτύπων. Επόμενο βήμα θεωρείται η ασφαλής απενεργοποίηση των συστημάτων για μεταφορά. Μεγάλη σπουδαιότητα έχει και η οργάνωση των στοιχείων που έχουν ανακαλυφθεί. Συνεπώς οι τεχνικοί τα τοποθετούν σε μη-στατικές θήκες και σε φυσιολογικές κλιματικές συνθήκες, με ετικέτες για την αποσαφήνιση του περιεχομένου. Κατά τη μελέτη των δεδομένων είναι αναγκαίο να γίνεται χρήση ειδικών εργαλείων εγκληματολογίας (forensics). Όταν έρθει εις πέρας η ασφαλής μεταφορά των στοιχείων στους κατάλληλους χώρους αρχίζει η προσεκτική εξέτασή τους, για την οποία ακολουθείται η παρακάτω μεθοδολογία.

1. Προστασία του υποκείμενου σε έρευνα συστήματος από οποιαδήποτε επίθεση, εκούσια ή ακούσια
2. Ανακάλυψη όλων των αρχείων στο σύστημα
3. Επαναφορά διαγραμμένων αρχείων
4. Αποκάλυψη περιεχομένου κρυμμένων και προσωρινών αρχείων
5. Απόκτηση πρόσβασης σε προστατευμένα αρχεία με νόμιμο τρόπο αν αυτό είναι δυνατό
6. Ανάλυση των δεδομένων που βρίσκονται σε ειδικές περιοχές του δίσκου
7. Εκτύπωση του τελικού αποτελέσματος της έρευνας
8. Εξέταση της ανάλυσης από πραγματογνώμονες

- **Οι διαδικασίες έρευνας της Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος της ΕΛΑΣ**

Το βασικότερο είναι ο εντοπισμός των ηλεκτρονικών ιχνών, των ψηφιακών αρχείων για τα οποία γίνεται έρευνα μέσω ειδικών προγραμμάτων έρευνας και ανάλυσης. Σε κάθε διαδικτυακή έρευνα γίνεται προσπάθεια εντοπισμού του ηλεκτρονικού ίχνους του δράστη, το οποίο για κάθε χρήστη του internet είναι μοναδικό και αποτελεί σημαντικό στοιχείο για την αποδεικτική διαδικασία στο δικαστήριο. Με δύο λόγια από τη στιγμή που ο χρήστης συνδέεται στο διαδίκτυο έχει ένα μοναδικό ηλεκτρονικό ίχνος. Δεν υπάρχει καμία περίπτωση δύο άτομα να έχουν τα ίδια ίχνη σε όλο τον κόσμο. Άρα, εδώ μιλάμε για «δακτυλικό» αποτύπωμα. Όπως έχουμε μοναδικό δακτυλικό αποτύπωμα, έτσι έχουμε και μοναδικό ηλεκτρονικό αποτύπωμα.

Εφόσον εντοπιστεί το ηλεκτρονικό ίχνος, μετά η διαδικασία εντοπισμού είναι μονόδρομος. Ανάλυση ηλεκτρονικών ιχνών μέσω ISP. ISP είναι τα internet services providers. Δηλαδή τα ίχνη που θα βρούμε αντιστοιχούν σε κάποιο φυσικό πρόσωπο ή σε εταιρεία. Στην Ελλάδα ISP είναι η OTENET, η Forthnet, η HOL κλπ. Αυτά τα ίχνη ανήκουν σε μία από τις εταιρείες αυτές. Άρα, από τη στιγμή που θα έχει γίνει άρση απορρήτου μέσω του Δικαστικού Συμβουλίου, τότε με την άρση απορρήτου και με τα ίχνη μαζί απευθυνόμαστε στην OTENET ή FORTHNET, η οποία θα μας «πει», ότι αυτά τα ηλεκτρονικά ίχνη αντιστοιχούν στο τάδε φυσικό πρόσωπο. Δεν υφίσταται ακόμη νομοθεσία στη χώρα μας που να υποχρεώνει τους ISP στη χρονική διάρκεια τήρησης ψηφιακών αρχείων που απαιτούνται για τη διαλεύκανση ηλεκτρονικών εγκλημάτων που διαπράττονται μέσω του διαδικτύου.

Επίσης, οποιεσδήποτε πληροφορίες από τους φορείς, παρέχονται κατόπιν δικαστικού βουλεύματος, σύμφωνα με το π.δ.47/2005. Άρα, δεν τους υποχρεώνει κάποιος νόμος να κρατούν τα αρχεία. Είθισται, όμως, να τηρούνται για ένα χρόνο.

Το βασικότερο είναι ο εντοπισμός των ηλεκτρονικών ιχνών, των ψηφιακών αρχείων για τα οποία γίνεται έρευνα μέσω ειδικών προγραμμάτων έρευνας και ανάλυσης. Σε κάθε διαδικτυακή έρευνα γίνεται προσπάθεια εντοπισμού του ηλεκτρονικού ίχνους του δράστη, το οποίο για κάθε χρήστη του internet είναι μοναδικό και αποτελεί σημαντικό στοιχείο για την αποδεικτική διαδικασία στο δικαστήριο. Με δύο λόγια από τη στιγμή που ο χρήστης συνδέεται στο διαδίκτυο έχει ένα μοναδικό ηλεκτρονικό ίχνος. Δεν υπάρχει καμία περίπτωση δύο άτομα να έχουν τα ίδια ίχνη σε όλο τον κόσμο. Άρα, εδώ μιλάμε για «δακτυλικό» αποτύπωμα. Όπως έχουμε μοναδικό δακτυλικό αποτύπωμα, έτσι έχουμε και μοναδικό ηλεκτρονικό αποτύπωμα.

1.4. Νομοθεσία

Η Συνθήκη της Βουδαπέστης: Οι μορφές του ηλεκτρονικού εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του διαδικτύου πολλαπλασιάζονται. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η διακρατική συνεννόηση και η εκπόνηση μιας αναλυτικής και αποτελεσματικής στρατηγικής. Ο στόχος αυτός επετεύχθη στο Συνέδριο για το Ηλεκτρονικό Έγκλημα που έγινε το 2001 στη Βουδαπέστη, όπου υπέγραψαν 26 υπουργοί Ευρωπαϊκών κρατών, μέσα σε αυτούς και της Ελλάδας.

- **Νομοθεσία Διαδικτυακών Εγκλημάτων στο εξωτερικό**

Στην Αγγλία από το 2001 αναλόγως του επιπέδου του χτυπήματος μπορεί να θεωρηθεί ως τρομοκρατία. Επιπλέον, στην Αμερική θεωρούνται όλες οι πράξεις χωρίς εξουσιοδότηση πρόσβασης

σε Η/Υ τρομοκρατικές και τιμωρούνται με φυλάκιση μέχρι και ισόβια χωρίς να μπορεί να μειωθεί η ποινή.

- **Νομοθεσία στην Ελλάδα**

Στην Ελληνική νομοθεσία δεν υπάρχουν νόμοι που να αναφέρονται στα θέματα Διαδικτύου και στην ρύθμιση συμπεριφοράς χρηστών. Όμως υπάρχει συνεργασία με τα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου Ευρώπης και άλλων Εθνικών Οργανισμών. Σίγουρα όμως όλη αυτή η συνεργασία δεν επαρκεί για την τέλεια αντιμετώπιση των εγκλημάτων Διαδικτύου.

- **Αδυναμίες Νομοθεσίας**

Επειδή το ηλεκτρονικό έγκλημα είναι εξειδικευμένο και ανεπτυγμένο ηλεκτρονικά υπάρχουν κάποια προβλήματα:

1. παρουσιάζονται προβλήματα για την οριοθέτηση των πράξεων που πρέπει να διώκονται ποινικά.
2. οι νομοθέτες πρέπει συνεχώς να ενημερώνονται για τις εξελίξεις της τεχνολογίας των υπολογιστών ώστε να εξοικειωθούν με τον τρόπο διάπραξής τους.

Σύμφωνα με έρευνα στη Βρετανία από επιτροπή πρόβλεψης και πρόληψης εγκλήματος το 2020 οι κακοποιοί θα μπορούν να γνωρίζουν σε υψηλό επίπεδο την λειτουργία των συστημάτων ασφαλείας τραπεζικών κωδικών, δηλαδή θα μπορούν να ξεπεράσουν κάθε ηλεκτρονικό εμπόδιο.

ΚΕΦ.2ο : Μορφές εγκλήματος στον Κυβερνοχώρο

2.1. Κακόβουλες εισβολές σε δίκτυα (Hacking και Cracking)

Hacking: Η χωρίς δικαίωμα πρόσβαση σε ένα δίκτυο υπολογιστών. Όταν ο επιτιθέμενος έχει ως σκοπό να προκαλέσει ζημιά ή να αποκομίσει οικονομικό όφελος αναφέρεται ως «hacker» ενώ στην αντίθετη περίπτωση ως «cracker».

Hacker: Τεχνικά καταρτισμένος χρήστης Η/Υ που, με αρνητικά ή θετικά κίνητρα, θα παραβιάσει («σπάζοντας» την ασφάλεια, γι' αυτό κολλάει εδώ ο όρος «cracker») συστήματα υπολογιστών. Κάποιες φορές, η εισβολή σε κάποιο «στόχο» γίνεται για καλό σκοπό, είναι ευγενής κι ευεργετική. Μπορεί να είναι επίσης κακό και άδικο για κλοπές και βανδαλισμό.

Ο όρος «hacker», στη διαδικτυακή αργκό, γράφεται και ως «haxor», «Hax0r» ή «h4x0r».

- **Ιστορική αναδρομή**

Ένας «hacker» της δεκαετίας του 80' ήταν απολύτως κακός κι ανέντιμος. Ένας εγκληματίας ο οποίος αναλάμβανε παράνομα και ανήθικα τον έλεγχο των Η/Υ και δικτύων. Ο ορισμός «hacker» λοιπόν, ακόμη και στις μέρες μας, παραπέμπει σε κάτι παράνομο.Ωστόσο, ο όρος αυτός έχει διευρυνθεί και συμπεριλαμβάνει μη ποινικούς, ακόμη και ευγενείς χρήστες Η/Υ. Σήμερα, ο όρος «hacker» διακρίνεται σε τέσσερις κατηγορίες χρηστών Η/Υ:

- ☺ «Black Hat»
- ☺ «White Hat» (στην οποία συμπεριλαμβάνεται και η συμπαθής κατηγορία των Χακτιβιστών)
- ☺ «Grey Hat»
- ☺ «Script Kiddie».

1) Κλασσικοί «Black Hat» Hackers - εγκληματίες-παραβάτες

Ο κλασικός ορισμός ενός «hacker»: ένας χρήστης Η/Υ που εσκεμμένα επιδιώκει να βλάψει, ή να διαπράξει κλοπές σε δίκτυα άλλων ατόμων. Είναι γνωστός και ως «Black Hat hacker», εξαιτίας των κακόβουλων κινήτρων του. Οι «Black Hat» είναι προικισμένοι τεχνικά χρήστες, αλλά με κακές προθέσεις και τα κίνητρά τους υποκινούνται από συναισθήματα δύναμης και μικροαστικής εκδίκησης. Θεωρούνται ηλεκτρονικοί κακοποιοί, και έχουν τα ίδια χαρακτηριστικά προσωπικότητας με τους εφήβους που σπάνε τα παράθυρα ενός λεωφορείου για προσωπική ικανοποίηση. Είναι γνωστοί για τα παρακάτω εγκλήματα στον κυβερνοχώρο: α) Επιθέσεις DOS/DDOS που επιβαρύνουν τους διακομιστές στο Διαδίκτυο β) Παραμόρφωση ιστοσελίδων με ανάληψη ελέγχου και αντικατάσταση των κύριων φωτογραφιών της σελίδας με αγενή συνθήματα γ) Κλοπή ταυτότητας και προσωπικών πληροφοριών δ) «Botnetting»: τηλεχειρισμός δεκάδων προσωπικών υπολογιστών, και προγραμματισμός των «ζόμπι» για εκτέλεση «spam».

2) White Hat «Ethical Hackers» Ειδικοί Ασφαλείας «Network Security»

Μια διαφορετική κατηγορία «hackers» με έντιμα, ή τουλάχιστον καλοήθη κίνητρα. Ένας τέτοιου είδους χρήστης είναι ταλαντούχος στην ασφάλεια του Η/Υ που χρησιμοποιείται ως βοηθός στην προστασία δικτύων υπολογιστών. Οι «White Hat Ethical Hackers» μπορεί να είναι και πρώην « black hat» που αναλαμβάνουν εργασία ως φρουροί ασφαλείας μιας εταιρίας. Συνήθως υποκινούνται από κάποιο σταθερό μισθό, υπάρχουν όμως κι αυτοί που το κάνουν μόνο από χόμπι χωρίς μίσθωση. Κάτι παραπλήσιο με αυτούς είναι και οι «Ακαδημαϊκοί Hackers»= Οι «Creative Artists» Υπολογιστών.

Ένα άλλο είδος «White Hat» είναι ο «academic hacker»: ένας τεχνικός Η/Υ που ενδιαφέρεται για την δημιουργία έξυπνων προγραμμάτων, κι όχι για την προστασία συστημάτων. Ένας τέτοιος «hacker» για παράδειγμα, θα πάρει έναν κώδικα για να τον βελτιώσει με έξυπνες προσθήκες και μετατροπές. Το Ακαδημαϊκό «hacking» δεν επιδιώκει να βλάψει δίκτυα άλλων ατόμων. Οι ακαδημαϊκοί «White Hathackers» είναι συχνά μεταπτυχιακοί φοιτητές στον προγραμματισμό Η/Υ.

3) Grey Hat Hackers:

Είναι συχνά χομπίστες, χρήστες με βασικές και ενδιάμεσες δεξιότητες τεχνολογίας στους οποίους αρέσει να αποσυναρμολογούν και να τροποποιούν δικά τους συστήματα, απλά και μόνο από χόμπι. Συχνά ανακατεύονται με μικροεγκλήματα, όπως την κοινή χρήση αρχείων ταινιών ή παράνομου (σπασμένου) λογισμικού. Τα εκατομμύρια «p2p downloaders» θεωρούνται χόμπι «hackers». Η τροποποίηση ας πούμε «router» και «firewall» για μεγαλύτερη ταχύτητα στα «p2p downloads» είναι ενέργειες ενός «Grey Hat χόμπι Hacker».Μόνο ένα μικρό ποσοστό αυτών θα γίνουν κάποια στιγμή «Black Hat».

4) «Script Kiddie»:

Ένας «Script Kiddie» χρησιμοποιεί δουλειά άλλων για να αποδείξει στους φίλους ή στην κοπέλα του τις υποτιθέμενες ικανότητές του. Ένας «Wannabe Hacker» θα λέγαμε.

- **Ποιες όμως είναι οι λεπτές διαφορές**;

Εάν κάποιος πειραματίζεται μανιωδώς με το υλικό του υπολογιστή του και το λογισμικό του, είναι ένας «White Hat χόμπι hacker». Αν πάλι πειραματίζεται μανιωδώς και του αρέσει να σπάει λογισμικά και γενικότερα να παραβιάζει πνευματικά δικαιώματα αρχείων, τότε είναι ένας «Grey Hat χόμπι hacker».

Αν όμως παραβιάζει συνεχώς πνευματικά δικαιώματα λογισμικού (ξεκλειδώνοντας προγράμματα και παιχνίδια), τότε είναι «Cracker».

Οι υποκατηγορίες και οι ορισμοί του όρου αυτού είναι οι εξής:

1) «Cracker» or «Hacker» (computer security), ένα άτομο που πραγματοποιεί «exploits» σε ευπάθειες «computer» ή «network».

2) «Cracker, a person who uses password cracking».

3) «Cracker, a person who uses software cracking to modify a program».

Οι «crackers» συχνάζουν στη σκηνή (ή «Scene») και παραβιάζουν πνευματικά δικαιώματα κατ' εξακολούθηση κι όχι για ιδία χρήση. Αυτή η εξειδίκευση όμως κάνει τη διαφορά των όρων.

Τα όρια βέβαια είναι πολύ λεπτά, μπορεί ας πούμε ένας «Black Hacker» να αλλάξει καπέλο και να φορέσει ένα λευκό, ή ένας «Cracker» να σταματήσει να σπάει προγράμματα και να ασχοληθεί αποκλειστικά με τη συγγραφή λογισμικού, εφόσον κατέχει προγραμματισμό.

Οι πιο γνωστοί «hackers» όλων των εποχών

- **Kevin Mitnick:** Είναι μάλλον το συνώνυμο του «Hacker». Το Υπουργείο Δικαιοσύνης των Η.Π.Α ακόμα αναφέρεται σε αυτόν χαρακτηρίζοντας τον ως «τον νούμερο ένα καταζητούμενο για ηλεκτρονικά εγκλήματα στην ιστορία των Η.Π.Α.». Ξεκίνησε την δραστηριότητα του από το σύστημα καρτών λεωφορείων του Los Angeles όπου μπορούσε να εκτυπώνει κάρτες για δωρεάν διαδρομές. Μετά από εκεί το ενδιαφέρον του στράφηκε στα κινητά τηλέφωνα και μπήκε στο σύστημα της «Digital Equipment Corporation» κλέβοντας πολύτιμο «software». Από εκεί και μετά ξεκίνησε μια διαδρομή δυόμιση χρόνων περίπου με τον Mitnick να παραβιάζει υπολογιστές, δίκτυα τηλεφώνων, κυβερνητικά έγγραφα και δημόσια συστήματα. Αυτό που έδωσε τέλος στην πορεία του ήταν η προσπάθεια του να παραβιάσει τον προσωπικό υπολογιστή ενός άλλου «hacker», του Tsutomu Shimomura. Αυτή την στιγμή εργάζεται ως υπεύθυνος ασφαλείας υπολογιστών, σχολιαστής και σύμβουλος.
- **Adrian Lamo:** Έχει μείνει στην ιστορία ως ένας από τους μεγαλύτερους χάκερς γιατί εισέβαλε σε συστήματα εταιριών όπως η «Microsoft» και η «New York Times». Χρησιμοποιούσε ως επί το πλείστον δημόσιες συνδέσεις «internet» σε καφετέριες για να είναι πιο δύσκολο να εντοπιστεί, κάτι που του έδωσε το παρατσούκλι «άστεγος hacker». Η λίστα των εταιριών που απέκτησε πρόσβαση περιέχει επίσης τις: Yahoo!, Citigroup, Bank of America και Cingular, βέβαια στα πλαίσια της ομάδας «White Hat Hackers» οι οποίοι προσλαμβάνονται από τις ίδιες τις εταιρίες για να βρουν λάθη στο σύστημα προστασίας τους ο Lamo δεν διέπραξε κανένα έγκλημα αλλά παρέβη το νόμο όταν μπήκε στο ιδιωτικό σύστημα επικοινωνίας των «New York Times». Αυτή την στιγμή έχει εκτίσει την διετή ποινή περιορισμού που του είχε επιβληθεί και είναι βραβευμένος δημοσιογράφος.
- **Jonathan James:** Στα 16 του χρόνια έγινε ο πρώτος ανήλικος που καταδικάζεται για ηλεκτρονικά εγκλήματα με ποινή φυλάκισης. Αργότερα παραδέχτηκε ο ίδιος ότι το έκανε για πλάκα και απολάμβανε τις προκλήσεις. Εισέβαλε σε δημόσιους οργανισμούς όπως ένα

παράρτημα του Υπουργείου Δικαιοσύνης και έπαιρνε κωδικούς για να έχει πρόσβαση σε απόρρητους λογαριασμούς «e-mail». Εκτός από αυτά, απέκτησε ακόμη πρόσβαση στους υπολογιστές της NASA και έκλεψε πολύτιμα «software» συνολικής αξίας 1,7 εκατ. δολαρίων!

- **Robert Tappan Morris:** Είναι γιος ενός πράκτορα της NASA και δημιουργός του «Morris worm». Είναι ένα είδος ιού που εξαπλώνεται και αυτό-αντιγράφεται ανεξέλεγκτα σε χιλιάδες μηχανήματα. Το συγκεκριμένο «worm» ήταν το πρώτο που αναπτύχθηκε και διαδόθηκε μέσω του internet.[5] Ο Morris το δημιούργησε ενώ ήταν φοιτητής στο «Cornell» και ισχυρίστηκε ότι το έκανε απλά για να δει πόσο μεγάλο ήταν το internet εκείνη την στιγμή. Το «worm» ωστόσο άρχισε να διαδίδεται ανεξέλεγκτα προκαλώντας πρόβλημα σε χιλιάδες υπολογιστές κάτι που του κόστισε 3 χρόνια με αναστολή, ένα πρόστιμο αξίας 10.500 δολαρίων και 400 ώρες κοινωνικής εργασίας. Σήμερα ο Morris είναι καθηγητής στο πανεπιστήμιο MIT στο τμήμα «Computer Science» και ο τομέας έρευνας του είναι η αρχιτεκτονική των δικτύων υπολογιστών.
- **Kevin Poulsen:** Πιο γνωστός με το παρατσούκλι του, «Dark Dante», ο Kevin Poulsen έγινε γνωστός εισβάλοντας στο τηλεφωνικό κέντρο του ραδιοφωνικού σταθμού «KISS-FM» του Los Angeles παρεμβαίνοντας στις κληρώσεις και κερδίζοντας μεγάλα δώρα μεταξύ των οποίων και μια «Porsche». Το FBI άρχισε να ασχολείται μαζί του αφού απέκτησε πρόσβαση στα αρχεία της και αποσπούσε σημαντικές και απόρρητες πληροφορίες. Η ειδικότητά του ήταν οι τηλεφωνικές γραμμές και αποκτούσε πρόσβαση σε μεγάλα δίκτυα, όπως το «Los Angeles Radio» και τον «KIIS-FM» προκαλώντας το χάος. Αφού συνελήφθη σε ένα σουπερμάρκετ, καταδικάστηκε σε πέντε χρόνια φυλάκισης, και ενώ ήταν στην φυλακή δούλευε ως δημοσιογράφος και αργότερα εκδότης των «Wired News».

2.2. Κακόβουλο λογισμικό (Malicious/Malware Software)

Τα κακόβουλα λογισμικά είναι προγράμματα τα όποια έχουν σχεδιαστεί για να βλάψουν έναν Η/Υ, για την υποκλοπή δεδομένων, την σταδιακή επιβράδυνση του Η/Υ και την αποστολή πλαστών μηνυμάτων. Με την τεχνολογία να προχωρά με ταχυτάτους ρυθμούς έχουν σχεδιαστεί πολλά κακόβουλα λογισμικά αλλά τα βασικότερα είναι :

1. Virus (Ιοί)
2. Worms (Σκουλήκια)
3. Trojan Horses (Δούρειος Ίππος)
4. Rootkit (Ριζικό Εργαλείο)
5. Logic Bombs (Λογισμικές Βόμβες)
6. Trapdoor/Backdoor (Πόρτα Παγίδα/Παράνομη Πρόσβαση)
7. Adware (Λογισμικό Προσεταιρισμού)

8. Spyware (Λογισμικό Κατασκοπίας)

Τα κακόβουλα λογισμικά χωρίζονται σε δυο (2) κατηγορίες σε αυτά που χρειάζονται ξενιστή και σε αυτά που δεν χρειάζονται ξενιστή. Άλλος τρόπος χωρισμού είναι σε ιομορφικά και μη ιομορφικά.

- **Βασικοί τρόποι διάδοσης κακόβουλων λογισμικών**
    a. Λήψη δωρεάν λογισμικού από το διαδίκτυο
    b. Λήψη μη-νομίμου λογισμικού
    c. Επίσκεψη σε παράνομους ή μη έμπιστους ιστότοπους
    d. Αναπαραγωγή ψεύτικου μηνύματος
    e. Άνοιγμα συνημμένου η κανονικού μηνύματος ηλεκτρονικού ταχυδρομείου

- **Βασικοί τρόποι αποφυγής και πρόληψης από κακόβουλα λογισμικά**
    a. Απαραίτητη χρήση λογισμικού προστασίας
    b. Συχνή ενημέρωση λογισμικού προστασίας
    c. Αποφυγή λήψεων μη έμπιστων προγραμμάτων
    d. Αναπαραγωγή συνημμένων η κανονικών μηνυμάτων μόνο από έμπιστους χρήστες
    e. Να μην εμπιστευόμαστε αναδυόμενα παράθυρα και να μην τα αναπαράγουμε η τα εκτελούμε
    f. Περιορισμός κοινοποίησης αρχείων

- **Τι πρέπει να γνωρίζουμε για το κάθε κακόβουλο λογισμικό ξεχωριστά**

1. Virus (Ιός)

Το πιο εύκολο μέσο διάδοσης του ιού είναι τα USB (Εξωτερικοί Δίσκοι). Η εξάπλωση του είναι εύκολη και κατευθύνεται κυρίως σε χρήσιμα προγράμματα. Οι κύριες επιπτώσεις του είναι η διαγραφή δεδομένων έως και η κατάρρευση ολοκλήρου του συστήματος.

2. Worms (Σκουλήκια)

Εξαπλώνεται μόνο μέσω διαδικτύου και μπορεί εύκολα να μεταδοθεί σε τοπικά δίκτυα. Έχει την ικανότητα να πολλαπλασιάζεται αυτόματα στο σύστημα και αποκτά δεδομένα και κωδικούς πρόσβασης ώστε ο Hacker που κάνει την επίθεση να έχει πλήρη πρόσβαση στην σύνδεση δικτύου. Τέλος επιβαρύνει το σύστημα με άχρηστα προγράμματα και δραστηριότητες και προκαλεί επιβράδυνση του συστήματος.

3. Trojan Horses (Δουρειος Ιππος)

Θεωρείται ένα από τα πιο δυνατά κακόβουλα λογισμικά και όχι άδικα. Πήρε την ονομασία του από την κατασκευή του Οδυσσέα στην Τροία, τον Δούρειο Ίππο (Ελληνική Μυθολογία) διότι χρησιμοποίει το στοιχείο της παραπλάνησης. Ο Δούρειος Ίππος παριστάνεται ως χρήσιμο για το σύστημα ενώ στην πραγματικότητα υποκλέβει στοιχεία η αποκτά πλήρη έλεγχο του συστήματος. Το συγκεκριμένο λογισμικό δεν έχει σκοπό την μόλυνση του Η/Υ, δεν αναπαράγεται και δεν χαρακτηρίζεται σαν ιός.

4. Rootkit (Ριζικό Εργαλείο)

Αυτό το λογισμικό χρησιμοποιείται σε όλα τα παραπάνω με συνδυασμό ώστε τα κακόβουλα λογισμικά να μην γίνονται ορατά στα λογισμικά ασφαλείας. Έχει την δυνατότητα να διαγράφει τις πληροφορίες του Hacker .

5. Logic Bombs (Λογισμικές Βόμβες)

Μικρό πρόγραμμα η αλυσίδα προγραμμάτων. Μπορεί να διαγράψει μικρά αρχεία που δεν επιτρέπουν την λειτουργία προγραμμάτων. Η χρήση του δεν είναι απαραίτητα κακόβουλη, απομακρύνει προγράμματα που έχουν λήξει ή δεν λειτουργούν πια ή και το αντίθετο δηλαδή να λειτουργήσει ελαττωματικό πρόγραμμα. Βασικός σκοπός σχεδίασης του είναι η παράταση ζωής των προγραμμάτων ασφαλείας.

6. Trapdoor/Backdoor (Πόρτα Παγίδα/ Παράνομη Πρόσβαση)

Είναι μικρά προγράμματα τα οποία εγκαθίστανται στο σύστημα αλλά με σκοπό την χρησιμοποίηση τους αργότερα όποτε χρειαστεί. Η μόνη διαφορά τους είναι ότι τα Backdoor διαγράφονται μόνα τους όταν δεν είναι πλέον χρήσιμα ενώ τα Trapdoor δεν διαγράφονται αυτόματα..

7. Adware (Λογισμικό Προσεταιρισμού)

Παρουσιάζεται σαν ιός , προσεταιρίζει γνωστές ιστοσελίδες επί πληρωμή με σκοπό την απόσπαση χρημάτων.

8. Spyware (Λογισμικό Κατασκοπίας)

Συλλέγει πληροφορίες παρακολούθησης. Εξαπλώνεται άμεσα , υποκλέβει τοποθεσίες , κωδικούς πρόσβασης, πληροφορίες Marketing έως δυνατότητα διαχείρισης κάμερας ασφαλείας. Εγκαθίσταται μέσω ιού ή εξωτερικής μονάδας. Αν το σύστημα σας αλλάξει Broswer, τροποποιήσει

λίστες αγαπημένων και απενεργοποιήσει το τοίχος ασφαλείας (Firewall) τότε έχετε πέσει θύμα Hijacking (Έμπειρος Hacker με δυνατότητες μη αντιμετώπισης του).

- **Ιστορικη Αναδρομη**

1. Virus

Ο πρώτος ιός κατασκευάστηκε το 1982 από τον δεκαπεντάχρονο τότε Ριτσαρντ Σκρεντα και κατασκευάστηκε για υπολογιστές Apple.

2. Worms

Ο όρος "σκουλήκι"(worm) χρησιμοποιήθηκε για πρώτη φορά στο μυθιστόρημα του John Brunner, το 1975, με τίτλο "The Shockwave Rider". Σε αυτό το μυθιστόρημα ο Nichlas Halfinger σχεδίασε και εξαπέλυσε ένα σκουλήκι συλλογής δεδομένων σε μία πράξη εκδίκησης εναντίον κάποιων ισχυρών ανθρώπων οι οποίοι λειτουργούσαν έναν εθνικό ηλεκτρονικό ιστό πληροφοριών που παρακινούσε συμμόρφωση μάζας. Στις 2 Νοεμβρίου του 1988, ο Robert Tappan Morris, μεταπτυχιακός φοιτητής της επιστήμης υπολογιστών του πανεπιστημίου Κορνέλ, εξαπέλυσε ένα σκουλήκι που έγινε γνωστό ως "σκουλήκι Morris", διαταράσσοντας ίσως και το 10% των υπολογιστών του Διαδικτύου τότε. Το 1989 ο Morris ήταν ο πρώτος άνθρωπος που κατηγορήθηκε με βάση νόμο των ΗΠΑ περί Ηλεκτρονικής Απάτης και Κατάχρησης.

3. Trojan Horses

Ο όρος "δούρειος ίππος" χρησιμοποιήθηκε αρχικά από τον Κεν Τόμσον στην ομιλία του το 1983 κατά την τελετή απονομής των βραβείων Turing. Ο Τόμσον παρατήρησε ότι είναι δυνατόν να προστεθεί κακόβουλος κώδικας στην εντολή login του Unix για την υποκλοπή κωδικών πρόσβασης. Αυτήν του την ανακάλυψη την ονόμασε "δούρειο ίππο". Επιπροσθέτως υποστήριξε ότι οποιοσδήποτε μεταγλωττιστής C μπορεί να μετατραπεί κατάλληλα ούτως ώστε να προσθέτει αυτόματα κακόβουλο κώδικα στα προγράμματα που δημιουργεί. Με τον τρόπο αυτό ο εντοπισμός του κακόβουλου κώδικα γίνεται ακόμη πιο δύσκολος.

4. Rootkit

Στις αρχές του 1990 φημολογείται η πρώτη γνωστή χρήση των Rootkits από τους Lance Davis και Steve Dake οι οποίοι πρόσθεσαν ένα Rootkit σε Sun Microsystems μια έκδοση του λειτουργικού συστήματος "Sun", αν και καμία δημόσια εγγραφή δεν έχει βρεθεί. Πριν συμβεί αυτό ο

Ken Thompson έστειλε μια root-kitted έκδοση του GNU C compiler στα εργαστήρια Bell για να το χρησιμοποιήσουν στο λειτουργικό Unix . Ο όρος αναφερόταν αρχικά σε κακόβουλα προγράμματα τα οποία αντικαθιστούσαν βασικά διαχειριστικά εργαλεία για λειτουργικά συστήματα τύπου Unix. Αν κάποιος κατάφερνε να αντικαταστήσει κάποιο από αυτά σε έναν υπολογιστή αποκτούσε τον πλήρη έλεγχο αλλά, παράλληλα, έχοντας δικαιώματα υπερχρήστη μπορούσε να κρύβει και τα ίχνη του. Η πιο γνωστή χρήση των Rootkit έχει γίνει από την Sony/BMG.

5. Logic Bombs

Τον Φεβρουάριο του 2000 στον Tony Xiaotong απαγγέλθηκαν σοβαρές κατηγορίες για τοποθέτηση Logic Bomb στην εταιρία που εργαζόταν την Deutch Morgan Grenfell. Η τοποθέτηση έγινε το 1996 και το 2003 κατάφεραν να βγει από το σύστημα τους. Στις 20 Μαρτίου του 2013 βρέθηκε logic bomb σε Attack Launcher (πύραυλοι στρατού) στην Νότιο Κορέα, ευτυχώς δεν χρησιμοποιήθηκαν.

6. Trapdoor/Backdoor

Κατασκευάστηκαν για πρώτη φορά από τον Κεν Τομσον το 1983 και χρησιμοποιήθηκαν για την παράταση χρονοδιαγραμμάτων του Λευκού Οίκου.

7. Adware

Γερμανικής προέλευσης και αγνώστου κατασκευαστή. Φήμες λένε ότι κατασκευάστηκε περίπου το 2000.

8. Spyware

Πρόγραμμα Ρωσικής καταγωγής άγνωστου κατασκευαστή. Δημιουργήθηκε περίπου το 1990 και χρησιμοποιήθηκε δοκιμαστικά από μυστικές κρατικές υπηρεσίες.

2.3. Ανεπιθύμητη Αλληλογραφία (Spamming)

- **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,** δύο όρους που χρησιμοποιούμε για την απόδοση στη γλώσσα μας του όρου Spam.

Τα κυριότερα χαρακτηριστικά του Spam μπορούν να συνοψιστούν στα ακόλουθα σημεία:

- **Απρόκλητο:** Η επικοινωνία που επιχειρείται είναι απρόκλητη, με την έννοια ότι δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα που θα δικαιολογούσε ή θα προκαλούσε την επικοινωνία αυτή.
- **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.

➢ **Τι μπορούμε να κάνουμε για να αποφύγουμε το Spam**

<u>Οι απλοί χρήστες:</u>

- **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 να 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 (Open Relay), αλλά ακόμα και από συστήματα χρηστών.

<u>Οι διαχειριστές εξυπηρετητών ηλεκτρονικού ταχυδρομείου (mail servers):</u>

- Θα πρέπει να έχουν κατάλληλο DNS όνομα και διεύθυνση IP
- Το λογισμικό του εξυπηρετητή ηλεκτρονικού ταχυδρομείου θα πρέπει να είναι ασφαλές, εκπληρώνοντας τα διεθνή standards και σωστά ρυθμισμένο.
- Παρακολουθείστε τα μηνύματα καταγραφής στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου, για να δείτε ποιος τον χρησιμοποιεί για την αποστολή μηνυμάτων και ελέγξετε την πιθανότητα να χρησιμοποιηθεί από χρήστες εκτός του δικτύου σας (το δίκτυο της σχολικής ή διοικητικής μονάδα σας) για την αποστολή μηνυμάτων. (περίπτωση Open Relay Server)

<u>Για όλα τα συστήματα:</u>

- Χρησιμοποιείτε πάντα λογισμικό προστασίας από τους ιούς (Antivirus) με δυνατότητα αυτόματης ανανέωσης από τον κατασκευαστή για τους τελευταίους ιούς.
- Ενεργοποιείστε τις δυνατότητες προστασίας των συστημάτων σας που διαθέτουν τα σύγχρονα συστήματα.
- Τέλος μπορείτε να χρησιμοποιήσετε ειδικό λογισμικό τύπου firewall για την προστασία του δικτύου σας ή του μεμονωμένου υπολογιστή σας.

Εναλλακτικοί τρόποι δημοσίευσης e-mail διευθύνσεων σε ιστοσελίδες

Η δημοσίευση e-mail διευθύνσεων σε ιστοσελίδες παρόλο που είναι πολύ χρήσιμη, αποτελεί παράλληλα και κακή πρακτική. Βάζοντας μία e-mail διεύθυνση σε μια ιστοσελίδα είναι σίγουρο ότι σύντομα, ο ιδιοκτήτης της, θα λάβει μηνύματα ενοχλητικής αλληλογραφίας (spam) στο γραμματοκιβώτιο.

Η δημοσίευση e-mail διευθύνσεων μπορεί να προκαλέσει την μαζική αποστολή μεγάλου αριθμού μηνυμάτων (spam) που απευθύνονται στους συγκεκριμένους χρήστες χωρίς αυτοί να το επιθυμούν και χωρίς να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον άγνωστο αποστολέα. Προσπαθήστε λοιπόν, όσο το δυνατόν να αποφεύγετε τη δημοσίευση e-mail διευθύνσεων ή εφαρμόστε κάποιο εναλλακτικό τρόπο γραφής τους, ώστε αυτές να μην μπορούν να ανιχνευτούν από τις μηχανές αναζήτησης των spammers.

Κάποιοι εναλλακτικοί τρόποι γραφής e-mail διευθύνσεων σε ιστοσελίδα είναι οι εξής:

1. Αποτύπωση των e-mail διευθύνσεων ως εικόνα.
2. Χρησιμοποίηση ειδικού τύπου γραφής των e-mail διευθύνσεων.
3. Χρήση κώδικα JavaScript για την αποτύπωση των e-mail διευθύνσεων

2.4. Επιθέσεις σε δικτυακούς τόπους (sites)

Στην κατηγορία των «γνήσιων» ηλεκτρονικών εγκλημάτων εντάσσονται και οι επιθέσεις στους δικτυακούς τόπους που στοχεύουν κυρίως σε κυβερνητικούς οργανισμούς και υπηρεσίες. Η επίθεση μπορεί να γίνει στο περιεχόμενο μια σελίδας, το οποίο οι βάνδαλοι θα αλλοιώσουν. Παρόλα αυτά, η παραποίηση αυτή μπορεί να εντοπιστεί και στη συνέχεια να διορθωθεί. Το πρόβλημα είναι πως αν το μέγεθος της παρεμβολής είναι μεγάλο, τότε η διόρθωση θα διαρκέσει τόσο ώστε να χρειαστεί μερικές φόρες ο δικτυακός τόπος να παραμείνει κλειστός.

Η αλματώδης εξέλιξη του διαδικτύου μέσα στην τελευταία δεκαετία έχει ανοίξει νέους ορίζοντες στις έννοιες πολιτισμός και κοινωνία και μας έχει φέρει αντιμέτωπους με νέες προκλήσεις αλλά και με την ανάγκη της προσαρμογής των συμβάσεων και των κανόνων συμπεριφοράς που ισχύουν στον πραγματικό κόσμο, στο νέο καθεστώς της ψηφιακής κοινωνίας. Μια από τις κοινώς αποδεκτές ως θεμελιώδεις αξίες της ανθρώπινης κοινωνίας είναι η προστασία του απαραβίαστου της προσωπικής ζωής, των προσωπικών δεδομένων και του απόρρητου της αλληλογραφίας, που είναι κατοχυρωμένες συνταγματικά στα περισσότερα κράτη του κόσμου

και προστατεύονται από διεθνείς οργανισμούς. Το διαδίκτυο, που αυτή τη στιγμή «στεγάζει» δεκάδες εκατομμύρια χρήστες και είναι χώρος επικοινωνίας, κοινωνικοποίησης, εκπαίδευσης και οικονομικής δραστηριότητας με μια διαρκώς αυξανόμενη δύναμη , είναι η νέα ψηφιακή κοινωνία στην οποία ο κάθε χρήστης πρέπει να αισθάνεται ασφαλής.

Ένα πληροφοριακό σύστημα για να θεωρείται ασφαλές θα πρέπει να διαθέτει :

α) Εμπιστευτικότητα (Confidentiality), δηλαδή τα διακινούμενα δεδομένα να αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα,

β) Ακεραιότητα (Integrity), δηλαδή πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων και

γ) Διαθεσιμότητα (Availability) δηλαδή οι εξουσιοδοτημένοι χρήστες να μην αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης όταν επιθυμούν να προσπελάσουν τους πόρους του συστήματος.

Με την απουσία αυτών των ιδιοτήτων ένα πληροφοριακό σύστημα καθίσταται ανασφαλές, με αποτέλεσμα να σχετίζεται με την εγκληματικότητα που αναπτύσσεται στους κόλπους του. Μερικές από τις βασικότερες αρχές του Δικαίου, αποτελούν η ελεύθερη διακίνηση των ιδεών, ο σεβασμός της αξίας και η προστασία του ατόμου, η ελεύθερη ανάπτυξη της προσωπικότητας, το απόρρητο και το απαραβίαστο των επικοινωνιών. Έτσι, κάθε άτομο έχει το δικαίωμα να απαιτήσει την μη διαρροή των στοιχείων αυτών σε τρίτα πρόσωπα και απαιτεί τα στοιχεία αυτά να κινούνται με ασφάλεια και μυστικότητα. η εφαρμογή, όμως, των αρχών αυτών στο διαδίκτυο είναι ένα από τα πλέον δύσκολα και περίπλοκα θέματα, τόσο από τεχνικής όσο και από νομικής άποψης.

2.5. Κλοπή ταυτότητας

- **Ορισμός**

"Κλοπή ταυτότητας" (identity theft) στο Διαδίκτυο ονομάζεται η πρακτική του να χρησιμοποιεί κανείς την εικονική ταυτότητα ενός άλλου ατόμου χρησιμοποιώντας το όνομα χρήστη και τον κωδικό πρόσβασής του σε διάφορες διαδικτυακές υπηρεσίες. Σκοπός όσων επιχειρούν κλοπή ταυτότητας μπορεί να είναι η οικονομική εξαπάτηση αλλά και ο εξευτελισμός ή η διάδοση φημών για ένα άτομο στο διαδικτυακό του περιβάλλον.

Χαρακτηριστικό παράδειγμα είναι τα ψεύτικα προφίλ σε ιστοσελίδες κοινωνικής δικτύωσης που χρησιμοποιούνται για να εξευτελίσουν κάποιο άτομο στους πραγματικούς και εικονικούς του φίλους.

- **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 άμυνες σας και στα δύο επίπεδα.

- **Καταπολεμήστε την απάτη**

Ενέργειες που πρέπει να γίνουν αν κλαπούν οι κωδικοί facebook:

- Βάλε τη φαντασία σου να δουλέψει όταν δημιουργείς κωδικούς πρόσβασης. Μη χρησιμοποιείς κωδικούς που εύκολα μπορεί κανείς να φανταστεί (ημερομηνία γέννησης κ.α.)
- «Google yourself!» Χρησιμοποίησε μια μηχανή αναζήτησης ανά τακτά διαστήματα και πραγματοποίησε αναζήτηση με το όνομά σου ή το ψευδώνυμο που χρησιμοποιείς στο Διαδίκτυο. Έτσι θα μπορείς να εποπτεύεις την εικονική σου παρουσία.
- Σε περίπτωση που έρθεις αντιμέτωπος / η με περιστατικό κλοπής ταυτότητας και γνωρίζεις το δράστη ζήτησέ του να σβήσει τα μηνύματα και να αποκαταστήσει την αλήθεια σε περίπτωση διάδοσης φημών.
- Επικοινώνησε με τον πάροχο της υπηρεσίας όπου έχει γίνει η κλοπή ταυτότητας και ενημέρωσέ τον για το περιστατικό.
- Δημιούργησε νέο e-mail, προφίλ, κ.λπ.
- Μπορείς να κάνεις μια ανώνυμη καταγγελία του περιστατικού στη Safeline.
- Κάνε μια αναφορά για το περιστατικό στους διαχειριστές της ιστοσελίδας που χρησιμοποιείς, π.χ. για το Facebook

Αυτό το πρόβλημα έχει γίνει ήδη οξύτατο στις ΗΠΑ και σε μερικά χρόνια θα είναι το ίδιο και εδώ. Δείτε αυτήν την ανταπόκριση:

Διαστάσεις επιδημίας λαμβάνουν οι κλοπές της ιατρικής ταυτότητας στις ΗΠΑ. Σύμφωνα με τα τελευταία δεδομένα, μια ομοσπονδιακή έκθεση του 2007, περισσότεροι από 250.000 Αμερικανοί κάθε χρόνο πέφτουν θύματα κακοποιών, οι οποίοι οικειοποιούνται το όνομα και την ασφάλιση υγείας των θυμάτων τους και τους φορτώνουν με χρέη δεκάδων χιλιάδων δολαρίων. Ο *αριθμός αυτός έχει αναμφίβολα αυξηθεί από το 2007, λόγω της αυξημένης χρήσης ηλεκτρονικών συστημάτων ιατρικής αρχειοθέτησης, τα οποία έχουν αναπτυχθεί χωρίς εκτεταμένες προστατευτικές δικλείδες, αναφέρει η Pam Dixon, διευθύντρια ενός μη κερδοσκοπικού φόρουμ για την προστασία των ιδιωτικών δεδομένων. Επιπλέον, εκτός από τα καταγεγραμμένα περιστατικά, αναρίθμητοι είναι εκείνοι που δεν γνωρίζουν καν ότι έχουν πέσει θύματα τέτοιας κλοπής, προσθέτει η κ. Dixon*

Η πιο απλή μορφή αυτού του εγκλήματος είναι να μάθει κάποιος το όνομά σου και τον αριθμό κοινωνικής ασφάλισης και να τα χρησιμοποιήσει για επείγουσες ιατρικές υπηρεσίες, τις οποίες πολλά νοσοκομεία υποχρεούνται να παρέχουν ανεξάρτητα από το αν ο ασθενής έχει ασφάλιση υγείας ή όχι. Στη συνέχεια, όμως, οι υπηρεσίες αυτές χρεώνονται. Σε πρόσφατο άρθρο στους New York Times αναφέρεται η περίπτωση 37χρονου μάνατζερ, ο οποίος ανακάλυψε ότι χρωστάει υπέρογκα ποσά για ιατρικές υπηρεσίες που δεν είχε λάβει ποτέ, όταν θέλησε να αγοράσει σπίτι και κατέθεσε αίτηση για υποθήκη. Εκτός από πολλαπλές επισκέψεις σε τμήματα επειγόντων σε νοσοκομεία σε όλη τη χώρα, είχε χρεωθεί ακόμη και με έναν λογαριασμό 19.000 δολαρίων για χρήση ιατρικού ελικοπτέρου σε απομακρυσμένη τοποθεσία στην οποία δεν είχε πάει ποτέ.
Μια άλλη παραλλαγή του εγκλήματος είναι να μάθει κάποιος τον αριθμό της ιδιωτικής σου ασφάλισης και να χρεώσει το ασφαλιστικό σου πρόγραμμα με οποιαδήποτε υπηρεσία, από μια απλή φυσική εξέταση έως μια δύσκολη χειρουργική επέμβαση. Κάτι τέτοιο είναι εκπληκτικά εύκολο να γίνει, καθώς πολλοί ιατροί και νοσοκομεία δεν ζητάνε αποδεικτικά στοιχεία ταυτότητας, παρά μόνο τα βασικά στοιχεία της ασφάλισης.

Ακόμη πιο συχνά είναι τα περιστατικά κατά τα οποία υπάλληλοι ενός ιατρείου ή νοσοκομείου «κατεβάζουν» ζωτικά προσωπικά δεδομένα από το ηλεκτρονικό σύστημα αρχειοθέτησης και τα πωλούν στη μαύρη αγορά ή τα χρησιμοποιούν οι ίδιοι για ψεύτικες απαιτήσεις προς ασφαλιστικές εταιρείες.

Χαρακτηριστική είναι η περίπτωση υπαλλήλου της Cleveland Clinic, ο οποίος το 2006 κατέβασε τα αρχεία 1.100 ασφαλισμένων του κρατικού προγράμματος Medicare και έδωσε τις πληροφορίες στον ξάδελφο του, ο οποίος στη συνέχεια κέρδισε ψεύτικες αποζημιώσεις υγείας ύψους 2,8 εκατομμυρίων δολαρίων.

Όταν τα θύματα δεν γνωρίζουν ότι η ιατρική τους ταυτότητα έχει κλαπεί, οι ασφαλιστικές εταιρείες απλά συνεχίζουν να πληρώνουν τις ψεύτικες απαιτήσεις, έως ότου τα ίδια τα θύματα θελήσουν να χρησιμοποιήσουν την ασφάλιση υγείας τους και ανακαλύψουν ότι το όριό τους έχει εξαντληθεί.

Για την κλοπή της ιατρικής ταυτότητας δεν υπάρχει καμία από τις προστασίες που υπάρχουν για την παραδοσιακή κλοπή ταυτότητας. Βάσει της νομοθεσίας για τις πιστωτικές κάρτες, μπορείς να ζητήσεις δωρεάν αναφορά της πιστωτικής σου κατάστασης και, σε περίπτωση κλοπής, χρεώνεσαι μόνο με 50 δολάρια από το ποσό που έχει κλαπεί. Στην περίπτωση της ιατρικής ταυτότητας, δικαιούσαι μεν να λάβεις αντίγραφο των ιατρικών σου αρχείων, αλλά το πληρώνεις με ένα διόλου ευκαταφρόνητο ποσό.

Ακόμη χειρότερα, αν τα ιατρικά σου δεδομένα μπερδευτούν με τα ιατρικά δεδομένα κάποιου άλλου, είναι σχεδόν αδύνατο να τα ξεμπλέξεις, καθώς τα ιατρικά δεδομένα του κλέφτη προστατεύονται από το ιατρικό απόρρητο

- **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.

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.

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.

2.6. Ηλεκτρονικό ψάρεμα (Phising)

Το **Phishing** είναι ενέργεια εξαπάτησης των χρηστών του διαδικτύου, κατά την οποία ο 'θύτης' υποδύεται μία αξιόπιστη οντότητα, καταχρώμενος την ελλιπή προστασία που παρέχουν τα ηλεκτρονικά εργαλεία, και την άγνοια του χρήστη-'θύματος', με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων, όπως είναι ευαίσθητα ιδιωτικά στοιχεία και κωδικοί. 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.

Αν ήταν εφικτό να αποδώσουμε τον όρο στα Ελληνικά, θα μπορούσαμε κάλλιστα να το αποκαλέσουμε 'Ηλεκτρονικό Ψάρεμα'. Ο όρος Phishing, που πρωτοχρησιμοποιήθηκε από τον χάκερ Khan C Smith και υιοθετήθηκε στη συνέχεια από όλη την κοινότητα των χάκερς, προέρχεται από το αγγλικό 'fishing' (ψάρεμα) , καθώς η διαδικασία με την οποία ο θύτης παρουσιάζεται ως η αξιόπιστη οντότητα ώστε να προσελκύσει τους χρήστες, θυμίζει την διαδικασία του δολώματος στο ψάρεμα.

- **Πώς ξεκίνησε το Phishing;**

Η πρώτη περιγραφή της τεχνικής Phishing έγινε το 1987 σε μία παρουσίαση στο διεθνές συνέδριο χρηστών της Hewlett-Packard, από την Interex. Στην πράξη όμως, οι πρώτες καταγεγραμμένες ενέργειες Phishing ήρθαν πολύ αργότερα, για να πλήξουν την τότε μεγαλύτερη διαδικτυακή υπηρεσία επικοινωνίας AOL, το 1995, που την περίοδο εκείνη εξυπηρετούσε 3.5 εκατομμύρια λογαριασμούς. Οι phishers, δημιουργώντας ψεύτικους λογαριασμούς, επικοινωνούσαν με τους χρήστες της υπηρεσίας υποδυόμενοι υπαλλήλους της ίδιας της εταιρίας, ζητώντας απροκάλυπτα από τους χρήστες τους προσωπικούς τους κωδικούς και τους αριθμούς τραπεζικών λογαριασμών, συνήθως με την πρόφαση πως υπάρχει κάποιο πρόβλημα με τον λογαριασμό τους.

Το Phishing έγινε πλέον εύκολο ακόμα και για άπειρους χρήστες, με την είσοδο του προγράμματος AOHell, το οποίο εξαπατούσε τους χρήστες με αυτοματοποιημένο τρόπο, μετατρέποντας το Phishing από ένα απλό αστείο σε μία από τις μεγαλύτερες διαδικτυακές απειλές. Όπως ήταν φυσικό, η εταιρία αναγκάστηκε να προβεί στην ενίσχυση των εργαλείων ασφάλειας της υπηρεσίας, τοποθέτησε προειδοποιητικά μηνύματα σε διάφορα σημεία του εργαλείου, ενώ ταυτόχρονα ανακοίνωσε και επίσημη προειδοποίηση προς τους χρήστες της πως θα πρέπει να πάρουν και οι ίδιοι μέτρα, αποφεύγοντας ύποπτους χρήστες και αλλάζοντας συχνά τον κωδικό τους. Η AOL ανέπτυξε ένα σύστημα απενεργοποίησης λογαριασμών που σχετίζονταν με phishing, πριν ανταποκριθούν οι χρήστες.

Με την πάροδο του χρόνου και τις συνεχείς τεχνολογικές εξελίξεις το Phishing πήρε άλλη έκταση αφού χρησιμοποιήθηκε κατά κόρον, για μαζικές επιθέσεις σε τραπεζικούς λογαριασμούς αλλά φημολογηθήκαν ακόμα και στοχευόμενες επιθέσεις προς κυβερνήσεις.

- **Πώς λειτουργεί το phishing;**

Το phishing όπως προαναφέρθηκε ξεκινάει λίγο παλαιότερα, με το phone phreaking, όταν ακόμα οι hackers έκαναν επιθέσεις στα τηλεφωνικά δίκτυα, επεμβαίνοντας στις γραμμές και αποσπώντας κρίσιμες πληροφορίες από προσωπικές συζητήσεις. Στην διαδικτυακή του μορφή πρωτοεμφανίστηκε το 1995 μέσω της υπηρεσίας e-mail, και στη συνέχεια με άμεσο μήνυμα (instant

messaging). Ο hacker στέλνει ένα e-mail ή άμεσο μήνυμα στο 'θύμα', στο οποίο συστήνεται ως αξιόπιστο πρόσωπο που ανήκει σε κάποια εταιρία ή οργανισμό, πολλές φορές και την ίδια την υπηρεσία του e-mail, και ζητά από το θύμα κάποια προσωπικά στοιχεία. Βασικό εργαλείο του phishing είναι οι αποπλανητικοί σύνδεσμοι (link manipulation). Γενικά το "Ψάρεμα" είναι κάτι περισσότερο από ανεπιθύμητα και ενοχλητικά ηλεκτρονικά μηνύματα. Μπορούν να οδηγήσουν στην κλοπή των αριθμών πιστωτικών καρτών, των κωδικών πρόσβασης, των πληροφοριών λογαριασμών ή άλλων προσωπικών δεδομένων. Ο χρήστης βρίσκεται σε μία ιστοσελίδα, e-mail ή άμεσο μήνυμα, που τον παραπέμπουν σε έναν σύνδεσμο επιφανειακά αξιόπιστο, αλλά είναι φτιαγμένος έτσι ώστε να τον οδηγεί σε διαφορετική ιστοσελίδα από αυτή που προβλέπεται. Αυτό είναι κάτι πολύ κρίσιμο αλλά ταυτόχρονα και πολύ εύκολο στη δημιουργία του, αφού σε έναν απλό html κώδικα δίνεται η δυνατότητα να μετατρέψει κανείς τον τίτλο του συνδέσμου όπως θέλει. Κάπως έτσι λειτουργούν και οι ψεύτικες ιστοσελίδες (fake websites), που μέσω παραπλανητικών συνδέσμων, οδηγούν τους χρήστες σε σελίδες οπτικά πανομοιότυπες με τις αυθεντικές ιστοσελίδες, ανήκουν όμως στον server του hacker.

Το Phishing μπορεί να γίνει ακόμα πιο επίφοβο, όταν χρησιμοποιούνται μέθοδοι ακόμα πιο δύσκολοι στην ανίχνευση τους. Το λεγόμενο IDN spoofing, μέσω του οποίου με κακό χειρισμό των International Domain Names (IDN), πανομοιότυπα URL μπορούν να οδηγούν σε διαφορετικές ιστοσελίδες, δεν λύνεται ούτε με τα υπάρχοντα πιστοποιητικά αφού είναι πλέον πολύ εύκολο ακόμα και για τους hackers να αποκτήσουν πιστοποιητικό αυθεντικότητας. Πολλές φορές οι phishers εξαπατούν ακόμα και τα anti-phishing προγράμματα ή καλύπτουν τα ίχνη τους με χρήση φίλτρων, όπως εικόνες ή flashplayer αντί για κείμενο ή την αξιοποίηση JavaScript για την κάλυψη του URL με κάποιο άλλο. Στη δεύτερη περίπτωση είτε τοποθετείται μία εικόνα πάνω στο πραγματικό URL, η οποία δείχνει το πλαστό, είτε το πραγματικό URL κρύβεται πλήρως και στη θέση του μπαίνει το ψεύτικο. Ο θύτης μπορεί επίσης να εκμεταλλευτεί προβλήματα στον κώδικα της αυθεντικής ιστοσελίδας και προκαλέσει την επίθεση μέσω αυτής.

Άλλες τεχνικές Phishing χρησιμοποιούν αναδυόμενα παράθυρα (pop-up windows), πολλαπλές καρτέλες (tab-nabbing) ή ακόμα και τη δημιουργία ψεύτικων δημοσίων δικτύων σε αεροδρόμια, ξενοδοχεία και καφετέρειες.

- **Πώς να διακρίνετε μία απάτη ψαρέματος;**

Δεν είναι ασφαλές να εισάγετε προσωπικές ή οικονομικές πληροφορίες σε pop up windows (αναδυόμενα παράθυρα). Μια κοινή τεχνική ψαρέματος είναι το άνοιγμα ενός ψεύτικου αναδυόμενου παραθύρου όταν κάποιος κάνει κλικ σε ένα ηλεκτρονικό μήνυμα ψαρέματος. Μπορεί να φαίνεται πολύ πειστικό ή μπορεί να εμφανίζεται πάνω από ένα παράθυρο που εμπιστεύεστε.

Ακόμη και εάν το αναδυόμενο παράθυρο φαίνεται πολύ επίσημο ή διακηρύσσει πως είναι ασφαλές, θα πρέπει να αποφεύγετε να εισάγετε ευαίσθητα προσωπικά δεδομένα γιατί δεν υπάρχει τρόπος να ελέγξετε την πιστοποίηση ασφάλειας.

- **Ποιος τρόπος υπάρχει να διαπιστώσετε εάν μία τοποθεσία Web προσφέρει ασφάλεια για να προστατέψετε τα ευαίσθητα προσωπικά σας δεδομένα;**

Το πιστοποιητικό ασφαλείας της τοποθεσίας αντιστοιχεί στο όνομα της τοποθεσίας. Η εμφάνιση του εικονιδίου με το κίτρινο λουκέτο είναι ένα σημάδι, επειδή το κλειστό λουκέτο υποδεικνύει πως η τοποθεσία Web χρησιμοποιεί κρυπτογράφηση για την προστασία των ευαίσθητων προσωπικών πληροφοριών που εισάγετε (όπως ο αριθμός της πιστωτικής σας κάρτας ή άλλη πληροφορία ταυτοποίησης). Όμως, το εικονίδιο με το κίτρινο λουκέτο μπορεί να είναι ψεύτικο. Για να διασφαλίσετε τη γνησιότητά του κάντε διπλό κλικ για να διαπιστώσετε το πιστοποιητικό ασφαλείας της τοποθεσίας. Το όνομα που ακολουθεί το "Issued to" (Εκδόθηκε για), θα πρέπει να αντιστοιχεί με το όνομα της τοποθεσίας. Εάν το όνομα διαφέρει, πιθανόν να βρίσκεστε σε μια ψεύτικη τοποθεσία, γνωστή και ως "spoofed" (πλαστή) τοποθεσία. Εάν δεν είστε σίγουροι εάν το πιστοποιητικό είναι νόμιμο, μην εισαγάγετε προσωπικά δεδομένα.

- **Η εκτέλεση λογισμικού προστασίας από ιούς μπορεί να βοηθήσει στην προστασία σας από απάτες ψαρέματος. Αληθεύει;**

Αν και το λογισμικό προστασίας από ιούς δεν μπορεί να σας αποτρέψει να ανοίξετε ένα πλαστό ηλεκτρονικό μήνυμα ή να κάνετε κλικ σε επικίνδυνους συνδέσμους, μπορεί εντούτοις να σταματήσει ιούς ή λογισμικό υποκλοπής που θα προέλθει από τέτοιες ενέργειες. Κάποιο πλαστό ηλεκτρονικό μήνυμα μπορεί να σας οδηγήσει σε τοποθεσίες Web που εγκαθιστούν στον υπολογιστή σας λογισμικό το οποίο συνεχίζει να καταγράφει τις πληροφορίες που εισάγετε όπως τον κωδικό πρόσβασης, πληροφορίες σύνδεσης και δεδομένα του λογαριασμού. Αυτού του είδους το ανεπιθύμητο λογισμικό συχνά καλείται spyware (λογισμικό υποκλοπής) ενώ μπορεί να περιέχει ακόμη και ιό.

- **Ενδείξεις πως ένα ηλεκτρονικό μήνυμα πιθανόν να είναι πλαστό.**

Στις απάτες ψαρέματος συνηθίζονται οι γενικές προσφωνήσεις όπως "Αγαπητέ πελάτη" αντί για το όνομά σας. Σας ζητούν να κάνετε κλικ σε κάποιο σύνδεσμο, με φρασεολογία που δίνει την εντύπωση του επείγοντος ή σας ζητούν να επιβεβαιώσετε κάποιες προσωπικές σας πληροφορίες.

- **Τι να κάνετε εάν πέσετε θύμα απάτης με την πιστωτική σας κάρτα.**

Εάν πιστεύετε πως πέσατε θύμα απάτης με την πιστωτική σας κάρτα, μπορείτε να ακολουθήσετε αυτά τα βήματα ώστε να ελαχιστοποιήσετε τη ζημιά που μπορεί να προκαλέσει ένας απατεώνας στο λογαριασμό της ταυτότητας, της πιστωτικής κάρτας ή του τραπεζικού λογαριασμού σας. Όταν χρησιμοποιείτε πιστωτική κάρτα, μπορεί να γίνετε ευάλωτοι σε πιθανή απάτη πληρώνοντας μέσω Διαδικτύου, μέσω τηλεφώνου ή ακόμη και αυτοπροσώπως στο μανάβικο της γειτονιάς σας. Γι' αυτό κάθε φορά που πληρώνετε με πιστωτική κάρτα, οι επιχειρήσεις θα πρέπει να επιβεβαιώνουν τα στοιχεία του λογαριασμού σας πριν σας παρέχουν αγαθά και υπηρεσίες. Δυστυχώς, επειδή τα στοιχεία της πιστωτικής σας κάρτας αποθηκεύονται σε μεγάλους υπολογιστές, οι διακομιστές μπορούν να γίνουν στόχος χάκερ οι οποίοι αναζητούν τρόπους για να εισχωρήσουν στο σύστημα και να ανακτήσουν στοιχεία τα οποία κατόπιν, θα τα χρησιμοποιήσουν για να διαπράξουν κάποια απάτη.

Εάν πιστεύετε πως πέσατε θύμα απάτης ή δόλου, ακολουθήστε αμέσως τα παρακάτω βήματα:

- Όσο ταχύτερα επικοινωνήσετε με τις αρμόδιες αρχές, τόσο πιθανότερο είναι να μειώσετε τη ζημιά που μπορεί να κάνει ο απατεώνας με τα στοιχεία σας, την πιστωτική σας κάρτα και τον τραπεζικό σας λογαριασμό.
- Κλείστε όλους τους λογαριασμούς που επηρεάζονται.
- Επικοινωνήστε με την πραγματική εταιρεία ή τον οργανισμό εάν πιστεύετε πως δώσατε ευαίσθητες πληροφορίες σε άγνωστη πηγή, η οποία προσποιήθηκε πώς ήταν η πραγματική εταιρεία ή οργανισμός. Εάν επικοινωνήσετε αμέσως με την πραγματική εταιρεία, ίσως μπορέσουν να περιορίσουν τη ζημιά προς εσάς και προς τους υπολοίπους.
- Επικοινωνήστε με το τμήμα ασφάλειας ή απάτης κάθε τράπεζας ή πιστωτικού ιδρύματος με το οποίο συνεργάζεστε, συμπεριλαμβανομένων των εταιριών πιστωτικών καρτών, εργαλείων, παροχών υπηρεσιών Διαδικτύου και άλλων τοποθεσιών όπου χρησιμοποιείτε την πιστωτική σας κάρτα, για κάθε ύποπτη πρόσβαση ή άνοιγμα λογαριασμού.
- Στη συνέχεια στείλτε μία επιστολή και κρατήστε και ένα αντίγραφο για εσάς.
- Όταν ανοίξετε νέους λογαριασμούς χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης, όχι δηλαδή το όνομα της μητέρας σας μαζί με αριθμό λογαριασμού.
- Αλλάξτε τους κωδικούς πρόσβασης σε όλους τους διαδικτυακούς λογαριασμούς και αρχίστε από αυτούς που έχουν σχέση με χρηματοπιστωτικά ιδρύματα ή πληροφορίες.
- Προσθέστε ειδοποίηση απάτης στους πιστωτικούς λογαριασμούς

- Ζητήστε ένα αντίγραφο της αναλυτικής κατάστασης του λογαριασμού σας (τα θύματα κλοπής στοιχείων ταυτότητας μπορούν να λάβουν αντίγραφα των αναλυτικών καταστάσεων των πιστωτικών τους λογαριασμών δωρεάν) και ζητήστε να μην γίνει καμία νέα πίστωση του λογαριασμού χωρίς την έγκριση σας.
- Βεβαιωθείτε πως ο λογαριασμός σας διαθέτει επισήμανση "ειδοποίησης απάτης" και "δήλωση θύματος" και επιμείνετε ώστε η προειδοποίηση να παραμείνει ενεργή το πολύ για εφτά χρόνια.
- Στείλτε τις αιτήσεις γραπτώς και φυλάξτε αντίγραφα για εσάς.
- Όταν λάβετε τις αναλυτικές καταστάσεις εξετάστε τις προσεκτικά.
- Ψάξτε για ερωτήσεις που δεν κάνατε, λογαριασμούς που δεν ανοίξατε και ανεξήγητες χρεώσεις.
- Καταθέστε μια καταγγελία.
- Κάντε αναφορά στο τοπικό αστυνομικό τμήμα.
- Ζητήστε αντίγραφο της αναφοράς της αστυνομίας για να ενημερώσετε την τράπεζα, την εταιρεία της πιστωτικής κάρτας και τους υπόλοιπους πιστωτές ότι είστε θύμα απάτης και όχι καταχραστής της πίστωσης.
- Να καταχωρίζετε και να αποθηκεύετε τα πάντα
- Μόλις ολοκληρώσετε όλα τα βήματα, καλό είναι αφού δημιουργήσετε εκτυπωμένα αντίγραφα των εγγράφων για σας, περιλαμβανομένων των ηλεκτρονικών μηνυμάτων και γραπτών απαντήσεων και αφού καταγράψετε τις τηλεφωνικές σας κλήσεις, να τα φυλάξετε σε κάποιο ασφαλές μέρος.
- Για τηλεφωνικές ή κατ' ιδίαν συνομιλίες, επανέλθετε με επιστολές επιβεβαίωσης προς τους οργανισμούς και φυλάξτε ένα αντίγραφο για τον εαυτό σας.
- Αναφέρετε στην επιστολή ό,τι ειπώθηκε κατά τη συνομιλία και καταγράψτε κάθε στοιχείο που ακολουθεί και για το οποίο δεσμευτήκατε εσείς ή ο αντιπρόσωπός σας κατά την συζήτηση.

➢ **Πληροφορίες για την Προστασία από ηλεκτρονικό ψάρεμα**

Η Προστασία από ηλεκτρονικό ψάρεμα σάς προστατεύει από επικίνδυνους ιστότοπους. Όταν η Προστασία από ηλεκτρονικό "ψάρεμα" είναι ενεργοποιημένη, το αντίστοιχο στοιχείο αναλύει το επίπεδο ασφαλείας των ιστότοπων που επισκέπτεστε. Στη συνέχεια, εμφανίζει τα αποτελέσματα στο αναδυόμενο παράθυρο **Ασφάλεια τοποθεσίας**. Η λειτουργία Προστασίας από ηλεκτρονικό ψάρεμα αποκλείει επίσης και την πλοήγηση σε ιστότοπους που έχουν αποδειχθεί κακόβουλοι.

Η λειτουργία Προστασίας από ηλεκτρονικό ψάρεμα παρέχει τις παρακάτω πληροφορίες για τους ιστότοπους που επισκέπτεστε:

- Εάν ο ιστότοπος είναι ασφαλής για εισαγωγή εμπιστευτικών πληροφοριών
- Εάν ο ιστότοπος είναι κακόβουλος
- Εάν ο ιστότοπος είναι ύποπτος
- Εάν είναι γνωστό ότι ο ιστότοπος περιλαμβάνει ενοχλητικό περιεχόμενο

Το αναδυόμενο παράθυρο Ασφάλεια τοποθεσίας στα προγράμματα περιήγησης Web Internet Explorer, Firefox ή Chrome, σας επιτρέπει να προβάλλετε περισσότερες λεπτομέρειες σχετικά με την κατάσταση ασφαλείας των ιστότοπων που επισκέπτεστε.

Επιπλέον, το αναδυόμενο παράθυρο Ασφάλεια τοποθεσίας του περιλαμβάνει πληροφορίες σχετικά με τους ιστότοπους με ασφάλεια Norton. Οι εισβολείς ιστότοπων συχνά μιμούνται ιστοσελίδες εταιρειών για να δημιουργήσουν κακόβουλους ιστότοπους. Το Norton 360 Online εντοπίζει τους κακόβουλους ιστότοπους.

Η Symantec αναλύει τις σελίδες σε αυτές τις τοποθεσίες και επαληθεύει εάν ανήκουν στην εταιρεία που αντιπροσωπεύουν. Μπορείτε να είστε βέβαιοι ότι οι πληροφορίες που παρέχετε καταλήγουν στην εταιρεία με την οποία θέλετε να έχετε συναλλαγές.

Μπορείτε να αναφέρετε την αξιολόγηση ενός ιστότοπου που υποπτεύεστε ότι είναι κακόβουλος στη Symantec για περαιτέρω αξιολόγηση. Χρησιμοποιήστε την επιλογή Αναφορά ιστότοπου από τη Γραμμή εργαλείων του Norton για να αναφέρετε έναν ιστότοπο.

Ακόμα και εάν απενεργοποιήσετε την επιλογή Προστασία από ηλεκτρονικό ψάρεμα, το Norton 360 Online σας προστατεύει από απειλές στο Internet μέσω των λειτουργιών του Norton Safe Web. Όταν είναι απενεργοποιημένη η λειτουργία Προστασία από ηλεκτρονικό ψάρεμα, δεν μπορείτε να χρησιμοποιήσετε την επιλογή Αναφορά ιστότοπου, στο μενού Norton, για να υποβάλετε αξιολόγηση του ιστότοπου στη Symantec.

Το αναδυόμενο παράθυρο Ασφάλεια τοποθεσίας εμφανίζει τα παρακάτω μηνύματα:

- Η τοποθεσία είναι ασφαλής
- Η τοποθεσία δεν είναι ασφαλής
- Μη ελεγμένη τοποθεσία
- Norton Secured
- Προσοχή
- Η τοποθεσία είναι κακόβουλη
- Ύποπτη τοποθεσία

- Η σελίδα δεν έχει αναλυθεί
- Απενεργοποίηση ή ενεργοποίηση της λειτουργίας Προστασία από ηλεκτρονικό ψάρεμα
- Αναφορά εσφαλμένης αξιολόγησης ενός ιστότοπου

➢ **Ειδοποιήσεις για ηλεκτρονικό ψάρεμα (phishing) και κακόβουλα προγράμματα (malware)**

Το Google Chrome σάς προειδοποιεί, αν ο ιστότοπος που επιχειρείτε να επισκεφτείτε είναι ύποπτος για ηλεκτρονικό ψάρεμα (phishing) ή κακόβουλο πρόγραμμα (malware), χρησιμοποιώντας την τεχνολογία Ασφαλούς περιήγησης της Google.

➢ **Ειδοποιήσεις για ηλεκτρονικό ψάρεμα (phishing) και κακόβουλα προγράμματα (malware)**

Όταν είναι ενεργοποιημένος ο εντοπισμός ηλεκτρονικού ψαρέματος (phishing) και κακόβουλων προγραμμάτων (malware) ενδέχεται να εμφανιστούν τα ακόλουθα μηνύματα:

- **Ο παρακάτω ιστότοπος περιέχει κακόβουλο πρόγραμμα (malware)!** - Ο ιστότοπος που επιχειρείτε να επισκεφτείτε μπορεί να εγκαταστήσει κακόβουλο πρόγραμμα (malware) στον υπολογιστή σας.
- **Κίνδυνος: Κακόβουλο πρόγραμμα (malware)!** - Η ιστοσελίδα που επιχειρείτε να επισκεφτείτε μπορεί να περιέχει κακόβουλο πρόγραμμα (malware).
- **Έγιναν αναφορές ηλεκτρονικού ψαρέματος (phishing) στον παρακάτω ιστότοπο!** - Ο ιστότοπος που επιχειρείτε να επισκεφτείτε είναι ύποπτος ως ιστότοπος ηλεκτρονικού ψαρέματος (phishing).
- **Ο παρακάτω ιστότοπος περιέχει επιβλαβή προγράμματα** - Ο ιστότοπος που επιχειρείτε να επισκεφτείτε ενδέχεται να προσπαθήσει να σας εξαπατήσει έτσι ώστε να εγκαταστήσετε προγράμματα που βλάπτουν την εμπειρία περιήγησής σας.

➢ **Απενεργοποίηση ειδοποιήσεων για ηλεκτρονικό ψάρεμα (phishing) και κακόβουλα προγράμματα (malware)**

Ακολουθώντας τα παρακάτω βήματα μπορείτε να απενεργοποιήσετε τις ειδοποιήσεις για ηλεκτρονικό ψάρεμα (phishing) και κακόβουλα προγράμματα (malware), καθώς και τις προειδοποιήσεις λήψεων.

1. Στην επάνω δεξιά γωνία του παραθύρου του προγράμματος περιήγησης, κάντε κλικ στο μενού Chrome .
2. Κάντε κλικ στις **Ρυθμίσεις**.

3. Κάντε κλικ στην **Εμφάνιση σύνθετων ρυθμίσεων**.
4. Στην περιοχή "Απόρρητο", καταργήστε το πλαίσιο "Ενεργοποίηση προστασίας από ηλεκτρονικό ψάρεμα (phishing) και κακόβουλα προγράμματα (malware)".

- **Πού στηρίζεται η επιτυχία του Phishing;**

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

Ακόμα και σε περιπτώσεις που ο χρήστης έχει τις κατάλληλες γνώσεις για να ανιχνεύσει τα κακόβουλα στοιχεία, πολλές φορές δεν θα προσέξει τα σημάδια, αφού μπορεί να είναι αφηρημένος ή απασχολημένος με κάτι άλλο. Σύμφωνα με μία αναφορά της εταιρίας Symantec το 2006, οι επιθέσεις Phishing αυξήθηκαν κατά 30% σε σημαντικές μέρες όπως ήταν τα Χριστούγεννα, η Πρωτοχρονία και το Κύπελλο του Ποδοσφαίρου. Έτσι ο χρήστης μπορεί είτε να μην δίνει αρκετή σημασία στις υπάρχουσες προειδοποιήσεις ασφάλειας ή στην έλλειψη αυτών.

Άλλωστε η σωστή τεχνική phishing κρύβει τα περισσότερα από τα σημάδια. Πώς; Και εκεί κρίνεται ο πιο σημαντικός παράγοντας για μία επιτυχημένη επίθεση phishing: Η οπτική εξαπάτηση. Στόχος του hacker είναι να πείσει το θύμα για την αυθεντικότητα και την αξιοπιστία του. Αυτό το επιτυγχάνει με:

- ***Παραπλανητικό κειμένο.*** Το κείμενο αυτό, που συνήθως είναι οι παραπλανητικοί σύνδεσμοι, μπορεί να χρησιμοποιεί λάθος σύνταξη ή ορθογραφία (π.χ. www.fasebook.com), αναγραμματισμούς (π.χ. www.yutoube.com) ή να αντικαθιστά παρόμοια γράμματα όπως το αγγλικό μικρό l (L) με το κεφαλαίο I (i), κλπ.
- ***Παραπλανητικές εικόνες.*** Οι εικόνες αυτές, μπορεί να είναι οι ίδιες οπτικά με τις εικόνες που χρησιμοποιεί κάποια ιστοσελίδα, για παράδειγμα το logo της google, αλλά όταν πατάς σε αυτές να σε οδηγούν αλλού. Μία εξίσου κοινή μέθοδος είναι εικόνος που μιμούνται το λειτουργικό σύστημα του υπολογιστή.
- ***Παραπλανητικό design.*** Με τη βοήθεια του παραπλανητικού κειμένου και εικόνων, αλλά και την επεξεργασία του κώδικα της αυθεντικής ιστοσελίδας, ο hacker μπορεί να φτιάξει μία ολόκληρη ιστοσελίδα με το ίδιο ακριβώς design που έχει η αυθεντική.

Εάν ένα phishing website καταφέρει να συνδυάσει όλα τα παραπάνω, στις περισσότερες περιπτώσεις έχει κατα 90% επιτυχημένες επιθέσεις.

- **Ποιοι είναι οι στόχοι των Phishers και οι κίνδυνοι;**

Οι hackers έχουν συνήθως οικονομικούς σκοπούς, για αυτό το λόγο στοχεύουν στις περισσότερες περιπτώσεις σε τραπεζικούς λογαριασμούς, ή λογαριασμούς στους οποίους οι χρήστες εμπιστεύονται τα προσωπικά τους δεδομένα για να κάνουν συναλλαγές. Σε άλλες περιπτώσεις, το phishing γίνεται εργαλείο για spamming, προώθηση κακόβουλου λογισμικού, διαφημιστικά.

- **Ηλεκτρονικό «ψάρεμα» και Facebook**

Ενίοτε, οι αποστολείς ανεπιθύμητων μηνυμάτων (spam) δημιουργούν ιστοτόπους που μοιάζουν με τη σελίδα σύνδεσης του Facebook. Αν πληκτρολογήσετε τη διεύθυνση email και τον κωδικό πρόσβασής σας σε μία από αυτές τις σελίδες, οι πληροφορίες σας καταγράφονται και διατηρούνται από τον αποστολέα ανεπιθύμητων μηνυμάτων (spam). Αυτό ονομάζεται **ηλεκτρονικό ψάρεμα**.

Όταν ένας χρήστης πέσει θύμα ηλεκτρονικού ψαρέματος, συχνά ο λογαριασμός του αρχίζει να στέλνει αυτόματα μηνύματα ή συνδέσμους σε πολλούς φίλους του. Τα μηνύματα αυτά ή οι σύνδεσμοι είναι συνήθως διαφημίσεις που ζητούν από τους φίλους του χρήστη να δουν βίντεο ή προϊόντα.

Αν ο λογαριασμός σας στέλνει αυτόματα ανεπιθύμητα μηνύματα ή συνδέσμους, ασφαλίστε τον. Αν πιστεύετε ότι ο λογαριασμός ενός φίλου σας έχει πέσει θύμα ηλεκτρονικού ψαρέματος, πείτε στο φίλο σας να αλλάξει τον κωδικό πρόσβασής του και να χρησιμοποιήσει στον υπολογιστή του λογισμικό προστασίας από ιούς.

Πολλοί ψηφιακοί απατεώνες λοιπόν προσπαθούν να ξεγελάσουν τους χρήστες με ψεύτικες προσφορές για δωρεάν, σπάνια, μυστικά ή αποκλειστικά ψηφιακά αγαθά (όπως νομίσματα, μάρκες, δώρα κτλ.).

Να είστε επιφυλακτικοί με:

- ✓ Μηνύματα που περιέχουν ορθογραφικά και τυπογραφικά λάθη, πολλές γραμματοσειρές ή τόνους σε περίεργα σημεία.
- ✓ Μηνύματα που ισχυρίζονται ότι περιλαμβάνουν τον κωδικό πρόσβασής σας ως συνημμένο αρχείο. Το Facebook δεν θα σας στείλει ποτέ τον κωδικό πρόσβασής σας ως συνημμένο. Για τα παραπλανητικά email (spam) δείτε παρακάτω.

- ✓ Συνδέσμους που δεν συμφωνούν με τη διεύθυνση στην οποία παραπέμπουν: Τοποθετείτε πάντοτε το ποντίκι πάνω από κάθε σύνδεσμο και ελέγχετε τη γραμμή κατάστασης (στο κάτω μέρος του παραθύρου του προγράμματος περιήγησης) για να βεβαιωθείτε ότι ο σύνδεσμος όντως παραπέμπει στη διεύθυνση που εμφανίζεται στο email.
- ✓ Μηνύματα που σας ζητούν προσωπικές πληροφορίες. Το Facebook δεν θα σας ζητήσει ποτέ:

  Τον κωδικό πρόσβασης του λογαριασμού σας

  Τον αριθμό κοινωνικής ασφάλισης ή το ΑΦΜ σας

  Τον πλήρη αριθμό της πιστωτικής σας κάρτας ή το PIN σας
- ✓ Μηνύματα που ισχυρίζονται ότι ο λογαριασμός σας θα διαγραφεί ή θα κλειδωθεί αν δεν κάνετε άμεσα κάποια ενέργεια.

Οι αποστολείς ανεπιθύμητης αλληλογραφίας (spam) και οι απατεώνες δημιουργούν ορισμένες φορές μηνύματα email που φαίνεται ότι προέρχονται από το Facebook. Τα μηνύματα αυτά μπορεί να είναι πολύ πειστικά. Ακόμη και το πεδίο "Από:" μπορεί να πλαστογραφηθεί για να συμπεριλάβει ως αποστολέα το «Facebook» ή την «Ομάδα του Facebook».

Αυτά τα μηνύματα email μπορεί να μοιάζουν με:

- ✓ Ειδοποιήσεις για αιτήματα φιλίας, μηνύματα, εκδηλώσεις, φωτογραφίες και βίντεο
- ✓ Ψευδείς κατηγορίες για κατάχρηση του ιστοτόπου
- ✓ Προειδοποιήσεις ότι κάτι θα συμβεί στο λογαριασμό σας αν δεν τον ενημερώσετε ή αν δεν κάνετε άμεσα κάποια άλλη ενέργεια

Ένας τρόπος για να ελέγξετε αν ένα μήνυμα email προέρχεται πραγματικά από το Facebook είναι να βρείτε ένα σύνδεσμο στο κάτω μέρος του μηνύματος που σας δίνει τη δυνατότητα να διαγραφείτε από τις ενημερώσεις ή να επεξεργαστείτε τις ρυθμίσεις ειδοποιήσεων μέσω email που λαμβάνετε από το Facebook. Για να ελέγξετε αυτό τον σύνδεσμο:

- ✓ Κάντε δεξί κλικ στο σύνδεσμο και αντιγράψτε τη διεύθυνση URL
- ✓ Επικολλήστε τη διεύθυνση στο πρόγραμμα περιήγησης που χρησιμοποιείτε.
- ✓ Βεβαιωθείτε ότι η διεύθυνση αρχίζει με το «www.facebook.com»

Λάβετε υπόψη ότι αυτός ο σύνδεσμος δεν συμπεριλαμβάνεται σε όλη την αλληλογραφία που λαμβάνετε από το Facebook. Για παράδειγμα, αν επικοινωνήσετε με το Facebook για κάποιο θέμα, η απάντηση email που θα λάβετε δεν θα συμπεριλαμβάνει το σύνδεσμο διαγραφής από τις ενημερώσεις. Αν ένα μήνυμα email σάς φαίνεται περίεργο, μην πατήσετε κανέναν από τους συνδέσμους που περιέχει και μην ανοίξετε κανένα συνημμένο αρχείο.

Σημείωση: Το Facebook δεν θα σας στείλει ποτέ οποιονδήποτε κωδικό πρόσβασης ως συνημμένο αρχείο.

Συμπερασματικά, το Phising πρόκειται για ιδιαίτερα διαδεδομένη τεχνική οικονομικής εξαπάτησης μέσω του «ψαρέματος» προσωπικών δεδομένων και ειδικότερα στοιχείων που αφορούν οικονομικές συναλλαγές (αριθμό λογαριασμού, κωδικό πιστωτικής κάρτας κ.λπ.).

Κάποια γνωστή τράπεζα, οργανισμός, τηλεπικοινωνιακός πάροχος ή άλλη νόμιμη εταιρεία εμφανίζεται ως αποστολέας ηλεκτρονικού μηνύματος που ενημερώνει τους παραλήπτες του για την ύπαρξη κενών ασφαλείας σε κάποιο λογαριασμό ή συνδρομή.

Μέσα στο κείμενο παρατίθεται και ένας σύνδεσμος προς πλαστή ιστοσελίδα, η οποία πλασάρεται ως η επίσημη ιστοσελίδα του αποστολέα. Πηγαίνοντας στην ιστοσελίδα αυτή, το θύμα καλείται να συμπληρώσει τα στοιχεία του π.χ. για να μην κλειστεί ο λογαριασμός του. Την ίδια ώρα αυτοί που κρύβονται πίσω από το ψεύτικο μήνυμα αποκτούν πρόσβαση στα στοιχεία αυτά και στη συνέχεια μπορούν να κάνουν ηλεκτρονικές απάτες εις βάρος του πραγματικού ιδιοκτήτη αυτών των στοιχείων.

Δείτε παρακάτω ένα παράδειγμα τέτοιου μηνύματος που φαινόταν πως προέρχεται από το Υπουργείο Οικονομικών, όπου ο παραλήπτης ενημερωνόταν ότι δικαιούται κάποιο ποσό ως επιστροφή φόρου και για να το παραλάβει άμεσα θα έπρεπε να συμπληρώσει τα στοιχεία του στην ηλεκτρονική φόρμα που του δίδονταν. Εκεί ζητούνταν τα προσωπικά δεδομένα του παραλήπτη (ονοματεπώνυμο, διεύθυνση κατοικίας, ΑΦΜ, κ.α), στοιχεία πρόσβασης σε τραπεζικό λογαριασμό (όνομα χρήστη- **username** και συνθηματικό- **password**), καθώς και όλα τα στοιχεία πιστωτικής του κάρτας.

Μετά από τον τελευταίο ετήσιο υπολογισμό της φορολογικής
δραστηριότητας σας έχουμε καθορίσει ότι είστε επιλέξιμοι για να λάβετε μια επιστροφή
φόρου 568.24 ευρω. Παρακαλω συμπληρωστε το εντυπο.

Ο τραπεζικός χρήστης Διαδικτύου σας - ταυτότητα:
Ο αριθμός τραπεζικού λογαριασμού σας:
Ο τραπεζικός κωδικός πρόσβασης Διαδικτύου σας:
Ο αριθμός δρομολόγησης τράπεζάς σας:
Το ονομά σας: - (Τυπώστε το πλήρες όνομα σας)
Ο εύχων αριθμός ταυτότητάς σας:
Η διεύθυνση κατοικίας σας
Κράτος:
Ο αριθμός Α.Φ.Μ σας:
Ταχυδρομικός κώδικας:
Πόλη:
Το ποσό 568.24 ευρω θα είναι στείλει στην κάρτα μου
Επιλέξτε το οικονομικό όργανο σας:
ή γράψτε το οικονομικό όργανο σας
Αριθμός καρτών:
Ο απολογισμός απου θέλετε να λάβετε την επιστροφή φόρου 568.24
Ημερομηνία λήξης:
CVV:
- 3 ψηφία στο πίσω μέρος της κάρτας σας.
Καρφίτσα:
- Εκτάσεις τον ψηφιακό αριθμό αναγνώρισης του ATM προσωπικό για την επεξεργασία και την επαλήθευση τραπεζών

Σημαντικός: Ο φορολογικός νόμος επιβάλλει τις βαριές ποινικές ρήτρες για το δέσιμο των ψεύτικων ή παραπλανητικών πληροφοριών

Δηλώνω ότι: όλες οι πληροφορίες που έχω δώσει σε αυτήν την φορολογική επιστροφή, συμπεριλαμβανομένων οποιωνδήποτε οι συνδέσεις, είναι αληθείς και σωστές

- **Εναλλακτικές μορφές**

Spear Phishing: Πρόκειται για στοχευόμενα μηνύματα που μοιάζουν αυθεντικά για κάποιες ομάδες ανθρώπων. Για παράδειγμα, στους υπαλλήλους μιας εταιρίας μπορεί να φτάσει μήνυμα με αποστολέα τον εργοδότη τους, στο οποίο τους απευθύνεται προσωπικά και τους ζητά όνομα χρήστη και κωδικούς πρόσβασης. Απαντώντας κανείς σε ένα μήνυμα spear phishing θέτει προσωπικές και συχνά απόρρητες πληροφορίες στη διάθεση των απατεώνων.

Vishing: Σε αυτή την εκδοχή του phishing, για να πειστεί ευκολότερα το θύμα, του δίνεται τηλεφωνικός αριθμός εξυπηρέτησης ή του ζητείται το δικό του τηλέφωνο ώστε να μπορούν να επικοινωνήσουν μαζί του οι υποτιθέμενοι εκπρόσωποι της εταιρίας. Η πρακτική αυτή στηρίζεται στις τεχνολογίες **VoIP** που προσφέρει το Διαδίκτυο.

Social Networking Phishing: Αντλώντας πληροφορίες και πολλά προσωπικά δεδομένα από τα προφίλ των χρηστών των ιστοσελίδων κοινωνικής δικτύωσης, οι απατεώνες στέλνουν εξατομικευμένα μηνύματα. Η επιτυχία της μεθόδου είναι μεγάλη. Σε πρόσφατο πείραμα που πραγματοποιήθηκε στις Ηνωμένες Πολιτείες, το 70% όσων έλαβαν εξατομικευμένο παραπλανητικό μήνυμα πάτησε το σύνδεσμο που περιέχετο σε αυτό και συμπλήρωσε τα στοιχεία του στην εικονική ιστοσελίδα - απάτη.

- **Λύσεις**

Οι προσπάθειες για την αντιμετώπιση του αυξανόμενου αριθμού των αναφερόμενων περιστατικών phishing περιλαμβάνουν τη νομοθεσία, την εκπαίδευση των χρηστών, την ευαισθητοποίηση του κοινού, και τεχνικά μέτρα ασφαλείας. Η λύση στο πρόβλημα του phishing δεν είναι απλή. Είναι ένα πρόβλημα που συνεχώς θα υπάρχει και θα πρέπει να αντιμετωπίζεται κάθε φορά με συνεχή ενίσχυση των παραπάνω.

- **Υπάρχουσες νομοθεσίες**

Το Διαδίκτυο είναι μη ελεγχόμενο, με την έννοια ότι δεν υπάρχει κάποια ενιαία κυβερνητική ή άλλη αντίστοιχη αρχή, η οποία θα ελέγχει το περιεχόμενό του πριν αυτό δημοσιευθεί. Ωστόσο οι κρατικές υπηρεσίες και η αστυνομία κάθε χώρας, καθώς και οι αντίστοιχες νομοθετικές ρυθμίσεις, παρεμβαίνουν για την αναστολή των αξιόποινων πράξεων που διαπράττονται μέσω Διαδικτύου. Από το 2004 έως σήμερα έχει καταγραφεί μεγάλος αριθμός συλλήψεων ανά τον κόσμο για ηλεκτρονικά εγκλήματα που έχουν διαπραχθεί μέσω της μεθόδου phishing. Επιπλέον, πρέπει να σημειώσουμε πως το 2006 θεσπίστηκε η «Fraud Act» στο Ηνωμένο Βασίλειο η οποία ορίζει την ηλεκτρονική απάτη ως αδίκημα το οποίο τιμωρείται με ποινή φυλάκισης έως και 10 ετών και απαγορεύει ρητά τη

δημιουργία ή κατοχή εργαλείων ηλεκτρονικού ψαρέματος. Ακόμη, το 2005 θεσπίστηκε στις Ηνωμένες πολιτείες η «Anti-Phishing Act», νομοθεσία που καταδικάζει σε ποινή φυλάκισης 5 ετών την κλοπή ταυτότητας μέσω παραποιημένων εταιρικών ιστοσελίδων ή μυνημάτων ηλεκτρονικού ταχυδρομείου. Όσον αφορά την ελληνική νομοθεσία δηλώνεται ρητά πως εφόσον 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 προκλήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών».

- **Ενημέρωση του κοινού**

Η ενημέρωση του κοινού είναι κρίσιμη, καθώς η αποτελεσματικότερη αντιμετώπιση του προβλήματος είναι η ίδια η πρόληψη του. Κάποιες πολύ καλές ιστοσελίδες για την ενημέρωση του κοινού είναι οι εξής: Antiphishing Web. Παρέχει πολύ σημαντικές πληροφορίες, στατιστικές, λίστες με αναφορές σε εντοπισμένα phishing websites, λίστες με ποσοστά επιθέσεων σε γνωστές σελίδες κλπ. Fraudwatch International's Web site. Καθημερινά καταγράφει χιλιάδες επιθέσεις phishing και δημιουργεί ανάλογα προειδοποιητικά, ενώ παρέχει στους χρήστες μαζί με το antivirus, εφαρμογές anti-phishing. Anti-Phishing Working Group. Κάνει πολύ σημαντικές μελέτες και δημιουργεί κάθε χρόνο στατιστικές σε σχέση με τις επιθέσεις phishing.

- **Τεχνική Αντιμετώπιση**

Μερικές τεχνικές αντιμετώπισης του Phishing είναι:

- Λήψη προγραμμάτων περιήγησης που αναγνωρίζουν τους ιστοτόπους στους οποίους παραπέμπουν τα παραπλανητικά μηνύματα μέσω διαφορετικού URL
- Χρήση λογισμικού προστασίας ενάντια σε ιούς και προγράμματα κατασκοπείας (Anti-spyware).
- Λήψη προγραμμάτων anti-spam για προστασία email
- Λήψη πρόσθετων (add-ons) για τον εντοπισμό phishing script στις ιστοσελίδες
- Λήψη antivirus με safe browsing advisor όπου υπάρχουν αξιολογήσεις για κάθε σελίδα που αναζητάτε μέσω Google.

2.7. Πειρατεία λογισμικού

- **Τι είναι η πειρατεία λογισμικού**

Ως πειρατεία λογισμικού ορίζεται η μη εξουσιοδοτημένη αντιγραφή ή η διανομή λογισμικού, η οποία πραγματοποιείται με την, λήψη, αντιγραφή, κοινή χρήση, πώληση ή εγκατάσταση πολλαπλών αντιγράφων σε προσωπικούς ή εταιρικούς υπολογιστές. Αυτό που οι περισσότεροι δεν κατανοούν όταν αγοράζουν λογισμικό, είναι ότι στην πραγματικότητα αγοράζουν την άδεια χρήσης του και όχι το ίδιο το λογισμικό. Η άδεια θα πρέπει να διαβάζεται πολύ προσεκτικά γιατί καθορίζει σε πόσους υπολογιστές επιτρέπεται η εγκατάσταση του λογισμικού. Επομένως, η δημιουργία περισσοτέρων αντιγράφων από όσα ορίζει η άδεια αποτελεί πειρατεία.

Ας ξεκινήσουμε από το πιο βασικό κίνητρο. Το βασικό κίνητρο λοιπόν των περισσότερων αν όχι όλων αυτών που ασχολούνται με την πειρατεία είναι το γρήγορο και χωρίς ιδιαίτερο κόπο κέρδος. Η δραστηριότητα αυτή ονομάζεται πειρατεία. Ας δούμε τις βασικές περιπτώσεις πειρατείας :

- ✓ Η δημιουργία παράνομων αντιγράφων προγράμματος από το αυθεντικό και η χρήση τους.
- ✓ Η παράνομη εγκατάσταση προγραμμάτων χωρίς την άδεια του δημιουργού.
- ✓ Η παράνομη αναπαραγωγή και διάθεση αντιγράφων προγραμμάτων με κίνητρο το οικονομικό όφελος.

- **Πλεονεκτήματα από τη χρήση νόμιμου λογισμικού**

Κάθε φορά που προμηθευόμαστε ένα λογισμικό (πρόγραμμα, ηλεκτρονικό παιχνίδι), αυτό πρέπει να συνοδεύεται από ένα έγγραφο άδειας χρήσης. Το έγγραφο αυτό ονομάζεται Πιστοποιητικό Αυθεντικότητας και αναφέρει όλους τους όρους που πρέπει να τηρήσουμε. Αυτό αποτελεί απόδειξη νομιμότητας ως προς την προμήθεια και τη γνησιότητα του προϊόντος. Την άδεια χρήσης του λογισμικού την έχει μόνο ο αγοραστής του και αυτή την άδεια δεν μπορεί να τη δανείσει ούτε να τη μεταπωλήσει. Άραγε τι κέρδος έχουμε εμείς από τη χρήση Νόμιμου Λογισμικού, που συνοδεύεται από πιστοποιητικό αυθεντικότητας;

- ✓ Είμαστε βέβαιοι ότι το CD ή DVD που κρατάμε στα χέρια μας δεν περιέχει ιούς ή άλλα κακόβουλα προγράμματα.
- ✓ Το προϊόν που παίρνουμε είναι ελεγμένο και δοκιμασμένο.
- ✓ Μας παρέχονται τα απαραίτητα εγχειρίδια χρήσης, για να μάθουμε να χρησιμοποιούμε σωστά το νέο πρόγραμμα.
- ✓ Έχουμε τεχνική υποστήριξη από τους κατασκευαστές.
- ✓ Μπορούμε να το χρησιμοποιήσουμε νόμιμα, για να παράγουμε και εμείς με τη σειρά μας τη

δική μας πνευματική εργασία.

- **Κίνδυνοι από πειρατεία λογισμικού**

Η πειρατεία λογισμικού είναι ένα πολύ σοβαρό θέμα. Εκτός από την παραβίαση του νόμου και των δικαιωμάτων πνευματικής ιδιοκτησίας των δημιουργών λογισμικού, το πλαστό λογισμικό μπορεί να βλάψει σοβαρά το Η/Υ σας και να υπονομεύσει την ασφάλεια του. Το πλαστό λογισμικό πωλείται συνήθως σε ψεύτικες ιστοσελίδες ή μέσω ταξινομημένων διαφημίσεων. Το πλαστό μπορεί να είναι καλό αντίγραφο του πρωτοτύπου, είναι όμως περισσότερο πιθανό να είναι ελαττωματικό, ακόμα και επικίνδυνο. Το πειρατικό λογισμικό μπορεί να φαίνεται καλή περίπτωση, αλλά μπορεί να αποβεί ιδιαίτερα δαπανηρό. Ορίστε μερικοί από τους λόγους:

- ✓ Το πειρατικό λογισμικό μπορεί να προκαλέσει ολικές βλάβες του υπολογιστή σας. Χάνετε χρόνο. Μπορεί να χάσετε αναντικατάστατα αρχεία ή δεδομένα. Μπορεί ακόμα και να καταστρέψετε το PC σας και όλο σας το άλλο λογισμικό.
- ✓ Το πλαστό λογισμικό μπορεί να περιέχει spyware που φορτώνεται στον υπολογιστή σας και αναφέρει προσωπικά δεδομένα χωρίς να το γνωρίζετε, όπως αριθμούς πιστωτικών καρτών και τραπεζικών λογαριασμών, κωδικούς πρόσβασης και βιβλία διευθύνσεων. Οι κλεμμένες πληροφορίες μπορεί να γίνουν αμέσως αντικείμενο εκμετάλλευσης από κλέφτες ταυτότητας.
- ✓ Οι κυβερνοκλέφτες ανακαλύπτουν κατά περιόδους ευπάθειες σε λογισμικό και οι προμηθευτές λογισμικού παρέχουν διορθωτικές εκδόσεις που αντιμετωπίζουν την ευπάθεια. Αν έχετε πλαστό λογισμικό, δεν θα μπορείτε να του ενσωματώνετε τις νομότυπες ενημερώσεις κι έτσι θα είστε ευάλωτοι σε επιθέσεις.
- ✓ Ένας πωλητής που προτείνει να παραβιάσετε το νόμο ίσως να μη σταματήσει στο πειρατικό λογισμικό. Οποιαδήποτε δεδομένα πιστωτικών καρτών ή προσωπικά δεδομένα που παρέχετε μπορεί να τύχουν εκμετάλλευσης από κλέφτες ταυτότητας.

- **Πως να αποφύγετε την πειρατεία λογισμικού**

- ✓ Αγοράζετε λογισμικό μόνο από αξιόπιστες εταιρείες.
- ✓ Όταν κάνετε αγορές online, να βεβαιώνεστε ότι η ιστοσελίδα είναι νομότυπη. Στη σελίδα πραγματοποίησης αγοράς της ιστοσελίδας, κάντε κλικ στο εικονίδιο με το λουκέτο στο παράθυρο του προγράμματος περιήγησης και δείτε το πιστοποιητικό ασφαλείας. Αν δεν υπάρχει λουκέτο, πιθανότατα η ιστοσελίδα δεν είναι ασφαλής.
- ✓ Πριν δώσετε στοιχεία πιστωτικής κάρτας, ελέγξτε τη διεύθυνση URL της ιστοσελίδας. Πρέπει να περιλαμβάνει την ένδειξη "https:" όχι μόνο "http:". Αν δεν υπάρχει "s" από τη λέξη secure, μην κάνετε την αγορά. (Το γράμμα "s" σημαίνει μόνο ότι οι πληροφορίες είναι

κρυπτογραφημένες όταν στέλνονται μέσω του Internet. Δεν σημαίνει ότι η ιστοσελίδα είναι νομότυπη.)

- ✓ Αν σας φαίνεται ότι μια τιμή φαίνεται πολύ καλή για να είναι αληθινή, μάλλον έτσι είναι. Προσέχετε τις εξαιρετικά μειωμένες τιμές και διπλό ελέγξτε τη γνησιότητα της ιστοσελίδας.
- ✓ Αν το λογισμικό σας καταφθάσει σε μια λευκή θήκη ή σε έναν απλό φάκελο, πιθανότατα είναι πλαστό. Το νομότυπο λογισμικό διατίθεται σε συσκευασίες με πλαστικό κάλυμμα, με τυπωμένες οδηγίες και κάρτες δήλωσης στοιχείων.

- **Συνέπειες πειρατείας λογισμικού**

Ένα μέρος από τα χρήματα που δαπανούνται για την αγορά αυθεντικού λογισμικού διοχετεύεται πίσω στην έρευνα και την ανάπτυξη λογισμικού, ώστε να παραχθούν νεότερα και πιο εξελιγμένα προγράμματα, και στο κράτος ως φορολόγηση από την πώληση του προϊόντος. Όταν όμως αγοράζουμε παράνομα αντίγραφα, τα χρήματά μας πηγαίνουν κατευθείαν στις τσέπες των παραβατών. Το γεγονός αυτό έχει σαν συνέπεια να δημιουργούνται σημαντικά προβλήματα στη βιομηχανία λογισμικού, στην οικονομία του κράτους καθώς και σε εμάς τους ίδιους. Η πειρατεία λογισμικού είναι εχθρός της γενικότερης ανάπτυξης και οικονομικής ευημερίας κάθε χώρας. Επενεργεί ανασταλτικά στην επένδυση κεφαλαίων από εθνικούς και ξένους επενδυτές. Στερεί τα κράτη από φορολογικούς πόρους αλλά και θέσεις απασχόλησης σε τομείς που σχετίζονται άμεσα ή έμμεσα με την ανάπτυξη λογισμικού. Δημιουργεί μία ανεξέλεγκτη παραοικονομία με υψηλά αφορολόγητα εισοδήματα. Εθίζει ορισμένους στην εγκληματική δράση.

- **Ποινικές διώξεις για πειρατεία λογισμικού**

Σύμφωνα με το άρθρο 2 του νόμου 3524/2007, όποιος έχει εγκατεστημένο στον ηλεκτρονικό υπολογιστή ή τον server πειρατικό λογισμικό (δηλαδή χωρίς άδεια χρήσης), σε περίπτωση ελέγχου θα πρέπει να πληρώσει πρόστιμο €1000 για κάθε πειρατικό πρόγραμμα. Το ίδιο ισχύει για όποιον διακινεί, πουλά ή αναπαράγει πειρατικά προγράμματα. Πιο συγκεκριμένα, αν σε περίπτωση ελέγχου εντοπιστούν σε έναν υπολογιστή εγκατεστημένα 3 πειρατικά προγράμματα, ο παραβάτης είναι υποχρεωμένος να πληρώσει πρόστιμο €3,000 - δηλαδή €1000 για κάθε ένα πειρατικό πρόγραμμα.

Οι αρμόδιες υπηρεσίες για την επιβολή του προστίμου είναι η Υπηρεσία Ειδικών Ελέγχων (πρώην ΣΔΟΕ) του υπουργείου οικονομικών, οι Αστυνομικές Αρχές και οι Τελωνιακές Αρχές. Το πρόστιμο επιβάλλεται στο νόμιμο εκπρόσωπο της εταιρίας και στον προϊστάμενο η υπευθυνο της μηχανογράφησης. Αν μέσα στο ίδιο οικονομικό έτος εντοπιστούν ξανά πειρατικά λογισμικά το πρόστιμο διπλασιάζεται, δηλαδή γίνεται 2000 ευρώ για κάθε πειρατικό λογισμικό. Η εξόφληση των προστυμμάτων γίνεται στα γραφεία των αρμόδιων Δ.Ο.Υ η στα τελωνεία. Σε περίπτωση που κάποιος αρνηθεί να πληρώσει το διοικητικό πρόστιμο η ποινική διαδικασία συνεχίζεται κανονικά

από τις αρμόδιες υπηρεσίες ελέγχου, οι οποίες υποβάλλουν μήνυση και στην μηνυτήρια αναφορά αναφέρεται το ακριβές ποσό του διοικητικού προστίμου καθώς και η άρνηση από την πλευρά του παραβάτη να καταβάλλει άμεσα και ανεπιφύλακτα το πρόστιμο, το οποίο αποτελεί έσοδο του κράτους.

2.8. Απάτη στο Διαδίκτυο

Κάποιες από τις πιο συχνές ηλεκτρονικές απάτες στο διαδίκτυο είναι:

1) Pharming
2) Scam
3) Blog
4) Διαδικτυακός τζόγος

1. PHARMING

Το Pharming είναι μια μορφή απάτης της ηλεκτρονικής διεύθυνσης που έχει ως αποτέλεσμα να πιστεύουν οι χρήστες ότι βρίσκονται σε μια γνήσια ιστοσελίδα με το σωστό URL. Ωστόσο, στην πραγματικότητα έχουν παραπεμφθεί σε μια ψεύτικη, η οποία όμως μοιάζει πανομοιότυπη με τη γνήσια.

"Pharming" σημαίνει ότι εγκληματίες χάκερ ανακατευθύνουν την κίνηση του Διαδικτύου από μία ιστοσελίδα σε μια άλλη, πανομοιότυπη έτσι ώστε να σας ξεγελάσουν και να καταχωρήσετε το όνομα χρήστη και τον κωδικό χρήστη στη βάση δεδομένων της πλαστής ιστοσελίδας. Ιστοσελίδες τραπεζών ή αντίστοιχων οικονομικών οργανισμών είναι συχνά στόχοι τέτοιων επιθέσεων, κατά τις οποίες εγκληματίες προσπαθούν να αποσπάσουν προσωπικά δεδομένα, με σκοπό να βρουν πρόσβαση στον τραπεζικό σας λογαριασμό, να κλέψουν την ταυτότητά σας ή να διαπράξουν άλλου είδους απάτη στο όνομά σας.

Εκμεταλλευόμενοι κάποια κενά στην ασφάλεια μιας ιστοσελίδας στην οποία οι χρήστες μπαίνουν για να πραγματοποιήσουν διάφορες συναλλαγές, οι απατεώνες καταφέρνουν να εκτρέψουν την ροή των επισκεπτών σε άλλο ιστοχώρο, όπου τα στοιχεία των συναλλαγών που καταχωρούνται χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών.

Τέτοιου είδους εκτροπή δεν μπορεί να γίνει σε ιστοσελίδες που χρησιμοποιούν το πρωτόκολλο SSL. Για να διαπιστώσετε αν οι συναλλαγές που κάνετε είναι ασφαλείς, δείτε στο πεδίο της διεύθυνσης αν υπάρχει η ένδειξη https:// αντί για το συμβατικό http://.

Το Pharming (παραπλάνηση), η χρήση δηλαδή ψεύτικων ιστοσελίδων πιθανόν να θυμίζει τις απάτες ψαρέματος από ηλεκτρονικά μηνύματα, όμως η παραπλάνηση είναι πιο ύπουλη, αφού

μπορεί να κατευθυνθείτε σε μία ψεύτικη ιστοσελίδα χωρίς να το γνωρίζετε. Έως σήμερα έχουν γίνει αρκετές επιθέσεις, γεγονός που έχει αρχίσει να ανησυχεί αρκετά κυβερνήσεις και επιχειρήσεις. Είναι επίσης σημαντικό να θυμάστε πως το Διαδίκτυο είναι μια δωρεάν και ανεξάρτητη πηγή, όπως μία βιβλιοθήκη ή άλλες δημόσιες υπηρεσίες, στον τόπο όπου ζείτε. Εάν παρατηρήσετε κάτι ύποπτο σχετικά με μία ιστοσελίδα που εμπιστεύεστε, αναφέρετέ το —τηλεφωνικά εάν είναι δυνατόν—στην επιχείρηση ή στον ιδιοκτήτη της ιστοσελίδας.

- **Πώς μπορεί κάποιος απατεώνας που θέλει να με παραπλανήσει, να κατευθύνει το browser μου σε κάποια άλλη ιστοσελίδα;**

Με τη χρήση μιας διαδικασίας που ονομάζεται "δηλητηρίαση DNS" κατά την οποία κάποιος εισβολέας αποκτά πρόσβαση στις τεράστιες βάσεις δεδομένων που χρησιμοποιούν οι πάροχοι υπηρεσιών Διαδικτύου για να δρομολογήσουν τη διαδικτυακή κίνηση και μπορεί να κάνει τροποποιήσεις σε κάποιο σημείο έτσι ώστε να εκτρέπεστε στην ψεύτικη ιστοσελίδα πριν αποκτήσετε πρόσβαση σε αυτή που τελικά επιθυμούσατε. Κάποιες εταιρίες υποστηρίζουν πως το λογισμικό firewall (τείχος προστασίας) που χρησιμοποιούν προστατεύει και από την παραπλάνηση (pharming).

Κάποιοι πάροχοι υπηρεσιών διαδικτυακής ασφάλειας πιστεύουν πως οι πελάτες τους που καθοδηγούν όλη τους την διαδικτυακή κίνηση μέσω των δικών τους, ασφαλών, διακομιστών είναι και προστατευμένοι από επιθέσεις παραπλανήσεις.

Η φύση της παραπλάνησης υποδεικνύει το αντίθετο αλλά, ανεξάρτητα από το τι υποστηρίζει η κάθε εταιρεία, είναι καλή ιδέα να αναζητάτε προσεκτικά τα προϊόντα ασφαλείας πριν επενδύσετε και εμπιστευτείτε κάποιες λύσεις λογισμικού.

2. SCAM

Μέχρι πρόσφατα, οι επαγγελματίες απατεώνες περιορίστηκαν στη χρήση αργών και αναποτελεσματικών τηλεφωνημάτων και έντυπων αγγελιών για να προωθήσουν τις απάτες τους. Σήμερα, τα ίδια χαρακτηριστικά που κάνουν το Διαδίκτυο τόσο βολικό για όσους αναζητούν εργασία, δηλαδή η παγκοσμιότητα, η ευχρηστία και η ταχύτητα, διευκολύνουν τους εγκληματίες να επιδίδονται σε απάτες με θέμα την απασχόληση, διατρέχοντας μικρότερο κίνδυνο.

Σε γενικές γραμμές οι απάτες που είναι γνωστές με τον όρο «scam» αφορούν κάποια συναλλαγή που για να ολοκληρωθεί χρειάζεται κάποια χρήματα από το υποψήφιο θύμα - παραλήπτη του παραπλανητικού μηνύματος. Ωστόσο, το θύμα δεν παραλαμβάνει ποτέ τα προσφερόμενα ανταλλάγματα.

Παραδείγματα scams:

Νιγηριανά scam ή απάτη 419: Μέσω ηλεκτρονικού ταχυδρομείου αποστέλλεται μήνυμα που ζητάει με συγκινησιακά φορτισμένο τόνο από τον παραλήπτη να βοηθήσει στην διεκπεραίωση κάποιας οικονομικής συναλλαγής, η οποία συνήθως αφορά ποσό πολλών εκατομμυρίων. Ως αποτέλεσμα της βοήθειάς του θα έχει προμήθεια ένα σημαντικό ποσοστό του ποσού αυτού.

Οι συναλλαγές που εμφανίζονται συχνότερα είναι: η διεκδίκηση ανύπαρκτων κληρονομιών, η αποδέσμευση χρημάτων από τραπεζικούς λογαριασμούς, η παραλαβή και αποθήκευση των χρημάτων του αποστολέα σε ασφαλές μέρος και η επένδυση των χρημάτων αυτών στη χώρα του θύματος. Η συντριπτική πλειοψηφία τέτοιων μηνυμάτων προέρχεται από τη Νιγηρία. Για το λόγο αυτό η πρακτική αυτή αποκαλείται «νιγηριανό scam» αλλά και «απάτη 419» από το άρθρο του ποινικού κώδικα της Νιγηρίας που αφορά στις οικονομικές απάτες.

Οι απατεώνες διατηρούν την επικοινωνία και στέλνουν μάλιστα και αποδεικτικά στοιχεία της ταυτότητάς τους (φυσικά πλαστά), ώστε το θύμα να μην έχει την παραμικρή αμφιβολία. Κάποια στιγμή ζητούν χρήματα από τον παραλήπτη για τα έξοδα της συναλλαγής, φόρους κ.λπ. Από τη στιγμή που θα παραλάβουν τα χρήματα, κάθε δίοδος επικοινωνίας διακόπτεται και φυσικά το θύμα δεν καταφέρνει να αποκτήσει το αστρονομικό ποσό που του είχαν τάξει.

Διεθνή Λαχεία: «Διεθνή» λαχεία αποστέλλουν e-mails, ανακοινώνοντας κέρδη. Στη συνέχεια και αφού τα θύματα έχουν πεισθεί για τα κέρδη, ζητούν απ' αυτούς να καταβάλλουν χρήματα για διαδικαστικά έξοδα. Με αυτό τον τρόπο κατορθώνουν να αποσπούν σημαντικά χρηματικά ποσά.

Δημοπρασίες: Σε μη αξιόπιστες ιστοσελίδες δημοπρασιών ενδέχεται να γίνεται πλειστηριασμός ανύπαρκτων αντικειμένων. Τα θύματα πληρώνουν προκαταβολές και διαδικαστικά έξοδα, ωστόσο δεν παραλαμβάνουν ποτέ το αντικείμενο για το οποίο πλειοδότησαν.

Ransomware: Μέσω ηλεκτρονικού ταχυδρομείου το θύμα λαμβάνει μήνυμα με ένα συνημμένο αρχείο ή πρόγραμμα. Μόλις το ανοίξει αρχίζει διαδικασία κρυπτογράφησης των αρχείων που είναι αποθηκευμένα στον υπολογιστή του. Ως συνέπεια, το θύμα δεν μπορεί να ανοίξει κανένα αρχείο του εκτός από το μήνυμα που του άφησαν οι «scammers» στο οποίο του εξηγούν ότι μόνο αφού πληρώσει ένα συγκεκριμένο ποσό θα του αποσταλεί ο κωδικός πρόσβασης. Πρόκειται ουσιαστικά για απαγωγή των αρχείων μας, για την ανάκτηση των οποίων πρέπει να καταβάλουμε λύτρα!

Ψεύτικες ευκαιρίες απασχόλησης: Δημιουργώντας ψεύτικες αγγελίες θέσεων εργασίας που μοιάζουν με τις αληθινές και, συχνά, δημοσιεύοντάς τις σε νόμιμες ιστοσελίδες εύρεσης εργασίας, οι

απατεώνες ελπίζουν να παραπλανήσουν τους πρόθυμους και ανυποψίαστους που αναζητούν εργασία και να τους πείσουν να στείλουν τα προσωπικά τους στοιχεία (το γνωστό ψάρεμα). Αυτές οι ψεύτικες αγγελίες εύρεσης εργασίας γίνονται όλο και πιο κομψές και, συχνά, χρησιμοποιούν συνηθισμένη εικόνα ή πειστικά εταιρικά λογότυπα και φρασεολογία. Πολλές φορές, διαθέτουν και συνδέσμους προς πλαστές ιστοσελίδες που εμφανίζονται ως τοποθεσίες πραγματικών εταιρειών. Κάποιες φορές ακόμα χρεώνουν για υπηρεσίες που δεν θα παράσχουν ποτέ. Τυπικά, μετά από μερικές μέρες, οι κλέφτες κλείνουν το scam και εξαφανίζονται.

Παράνομα γραφεία ευρέσεως εργασίας: Ακόμα, εκτός από τη σάρωση προσωπικών ιστοσελίδων και τη δημοσίευση ανακοινώσεων σε δημόσιες ιστοσελίδες, οι επαγγελματίες απατεώνες συχνά εμφανίζονται ως γραφεία ευρέσεως εργασίας που διαθέτουν ευκαιρίες απασχόλησης και στέλνουν ανεπιθύμητη αλληλογραφία (ή spam) σε πιθανούς υποψηφίους ή νόμιμα γραφεία ευρέσεως εργασίας. Ένας επαγγελματίας απατεώνας τέτοιου είδους θα προσπαθήσει να κερδίσει την εμπιστοσύνη του θύματος, χρησιμοποιώντας ψεύτικο προσωπικό για να αποσπάσει προσωπικά στοιχεία, ακόμη και από το τηλέφωνο. Είναι σημαντικό να θυμάστε ότι τέτοια στοιχεία θα σας ζητηθούν μόνον σε προσωπική συνέντευξη

3. BLOG

Η πρακτική του blogging, η τήρηση προσωπικού ημερολογίου στο Διαδίκτυο, μεγαλώνει δραματικά— ειδικά ανάμεσα στους έφηβους, οι οποίοι ορισμένες φορές διατηρούν ημερολόγια blog χωρίς να το γνωρίζουν οι γονείς ή οι κηδεμόνες τους.

Σύμφωνα με κάποιες πρόσφατες μελέτες έδειξαν πως τα μισά από τα ημερολόγια blog σήμερα δημιουργούνται από εφήβους με δύο στους τρεις να δημοσιοποιούν την ηλικία τους, τρεις στους πέντε να αποκαλύπτουν την τοποθεσία τους και έναν στους πέντε να αποκαλύπτει το πλήρες όνομα του. Αυτό συμβαίνει χωρίς να λέγεται ότι υπάρχουν πιθανοί κίνδυνοι από τη δημοσιοποίηση αυτού του τύπου προσωπικών λεπτομερειών. Και καθώς πολλά νεαρά παιδιά δημιουργούν όλο και περισσότερα ημερολόγια blog, οδηγούνται σε έναν αυξανόμενο ανταγωνισμό μεταξύ τους για να τραβήξουν την προσοχή. Μερικές φορές αυτό μπορεί να οδηγήσει τα παιδιά να δημοσιεύσουν ακατάλληλο υλικό όπως προκλητικές εικόνες των εαυτών τους ή των φίλων τους.

Αν και η διατήρηση ενός ημερολογίου blog προσφέρει πιθανά οφέλη, όπως την βελτίωση των ικανοτήτων στη γραφή και στην επικοινωνία, είναι σημαντικό να εκπαιδεύσετε τα παιδιά σας σχετικά με το Διαδίκτυο και τη δημιουργία ημερολογίων πριν ακόμη ξεκινήσουν.

Να μερικές προτάσεις για να ξεκινήσετε:

• Καθιερώστε κανόνες για τη χρήση του Διαδικτύου με τα παιδιά σας και να είστε επιμελής.

• Δείτε τι πρόκειται να δημοσιεύσουν τα παιδιά σας πριν το δημοσιεύσουν. Πληροφορίες που πιθανόν φαίνονται ακίνδυνες όπως το σήμα ή το όνομα του σχολείου ή φωτογραφίες της πόλης μπορούν, αν τοποθετηθούν μαζί να αποκαλύψουν που πηγαίνουν σχολείο τα παιδιά.

• Αναρωτηθείτε (και καθοδηγήστε τα παιδιά σας ώστε να πράξουν το ίδιο) εάν είστε άνετοι δείχνοντας το σε κάποιο ξένο. Εάν αμφιβάλλετε, υποχρεώστε τα να το διαγράψουν.

• Δοκιμάστε την υπηρεσία δημιουργίας ημερολόγιων blog και βρείτε εάν προσφέρει ιδιωτικά ημερολόγια με προστασία κωδικού πρόσβασης.

• Επισκεφθείτε το ημερολόγιο του παιδιού σας συχνά και επιθεωρήστε το. Επισκεφθείτε άλλα ημερολόγια για να βρείτε καλά παραδείγματα ώστε να τα υιοθετήσουν τα παιδιά σας.

Βασικές οδηγίες για δημιουργούς ημερολογίων blog

Οι ακόλουθες συμβουλές είναι ένα καλό σημείο εκκίνησης για παιδιά που ενδιαφέρονται να δημιουργήσουν ημερολόγια blog.

• Μην παρέχετε ποτέ προσωπικές πληροφορίες όπως επώνυμο, πληροφορίες επικοινωνίας, διεύθυνση κατοικίας, αριθμούς τηλεφώνων, όνομα σχολείου, ηλεκτρονική διεύθυνση, επώνυμο φίλων ή συγγενών, όνομα άμεσης επικοινωνίας, ηλικία ή ημερομηνία γέννησης.

• Μην δημοσιεύετε ποτέ προκλητικές φωτογραφίες του εαυτού σας ή κάποιον άλλο και βεβαιωθείτε πως όποια φωτογραφία δημοσιεύεται δεν αποκαλύπτει κάποιες προσωπικές πληροφορίες.

• Επίσης να θυμάστε να κοιτάτε πάντα στο background της φωτογραφίας.

• Θεωρείστε πως ό,τι δημοσιεύεται στο Διαδίκτυο είναι μόνιμο. Οποιοσδήποτε μπορεί στο Διαδίκτυο να εκτυπώσει ένα ημερολόγιο ή να το αποθηκεύσει στον υπολογιστή του.

• Χρησιμοποιήστε τοποθεσίες παροχής ημερολογίων blog με ξεκάθαρους όρους χρήσης, και βεβαιωθείτε πως μπορείτε να προστατέψετε με κωδικό πρόσβασης και τα ενεργά ημερολόγια blog και όχι μόνο τους λογαριασμούς. (Εάν όχι, είναι καλύτερο να θεωρήσετε πως οποιοσδήποτε μπορεί να το δει).

• Αποφεύγετε να υπερβάλετε ή να ανταγωνίζεστε με άλλους δημιουργούς ημερολογίων (bloggers).

• Διατηρήστε τα ημερολόγια blog θετικά και μην τα χρησιμοποιείτε για να δυσφημήσετε ή να επιτεθείτε σε άλλους.

4. ΔΙΑΔΙΚΤΥΑΚΟΣ ΤΖΟΓΟΣ

Πολλά παιδιά απολαμβάνουν να χρησιμοποιούν το Internet για να ανακαλύπτουν δραστηριότητες ψυχαγωγίας, όπως τα διαδικτυακά παιχνίδια. Πολλές φορές, ενώ αναζητούν μια νέα ιστοσελίδα με παιχνίδια μπορεί να βρουν ιστοσελίδες με στοιχήματα και τυχερά παιχνίδια. Ενώ η χρήση των περισσότερων παιχνιδιών και δραστηριοτήτων από ανηλίκους είναι νόμιμη, η χρήση των τυχερών παιχνιδιών δεν είναι.

- **Ποιά είναι η διαφορά ανάμεσα στις τοποθεσίες παιχνιδιών και τις τοποθεσίες τυχερών παιχνιδιών;**

Οι κυριότερες διαφορές μεταξύ των τύπων των ιστοσελίδων είναι οι εξής:

• Οι τοποθεσίες παιχνιδιών συνήθως περιέχουν παιχνίδια με κάρτες, πίνακες, λέξεις, arcade ή παζλ, με αυτόματη παρακολούθηση και προβολή του σκορ.

• Δεν γίνεται ανταλλαγή χρημάτων, αληθινών ή ψεύτικων. Οι τοποθεσίες τυχερών παιχνιδιών μπορούν να περιέχουν σενάρια, στα οποία οι άνθρωποι κερδίζουν ή χάνουν κάποιο τεχνητό νόμισμα. Οι τοποθεσίες Τζόγου συνήθως αφορούν το κέρδος ή την απώλεια αληθινών χρημάτων.

Οι γονείς θα πρέπει να αποφασίσουν ποιοι τύποι παιχνιδιών ή τοποθεσιών παιχνιδιών είναι κατάλληλοι για τα παιδιά τους. Για παράδειγμα, μπορείτε να βασίσετε τα κριτήριά σας στον τύπο του παιχνιδιού (μόνον παιχνίδια με κάρτες και πίνακα ή μόνον παιχνίδια στρατηγικής και φαντασίας), καθώς και στο εάν το παιχνίδι παίζεται διαδραστικά με άλλους στο Διαδίκτυο, εάν η τοποθεσία προσφέρει το παιχνίδι δωρεάν ή και κατά περίπτωση.

Μπορείτε επίσης να κάνετε και τα εξής:

- Μάθετε ποιές τοποθεσίες επισκέπτονται τα παιδιά σας στο Διαδίκτυο και τι κάνουν.
- Καθιερώστε σαφείς κανόνες σχετικά με τα διαδικτυακά παιχνίδια που μπορούν να παίξουν τα παιδιά σας και τοποθετήστε τους υπολογιστές που έχουν πρόσβαση στο Διαδίκτυο σε ανοικτό χώρο, όχι στο παιδικό δωμάτιο.
- Υπενθυμίστε στα παιδιά σας πώς είναι παράνομο να συμμετέχουν σε τυχερά παιχνίδια στο Διαδίκτυο. (Σε πολλές χώρες η συμμετοχή ανηλίκων σε τυχερά παιχνίδια απαγορεύεται, γι' αυτό ενημερωθείτε για την τοπική νομοθεσία).

2.9. Διακίνηση παιδικού πορνογραφικού υλικού

- **Τι είναι παιδική πορνογραφία;**

Η παιδική πορνογραφία ορίζεται διαφορετικά από τη νομοθεσία της κάθε χώρας. Ο κοινός παρανομαστής είναι 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 ή και καρτούν. Είναι ευρέως γνωστό ότι η παιδική πορνογραφία είναι παράνομη και υπόκειται σε ποινικές κυρώσεις. Επιπλέον υπάρχουν σημαντικές διαφορές στην αντιμετώπιση της παιδικής πορνογραφίας από χώρα σε χώρα. Σε ορισμένες χώρες για παράδειγμα, ακόμη και η εν γνώση κατοχή παιδικής πορνογραφίας είναι έγκλημα (όπως στην Ισπανία). Σύμφωνα με τη Σύμβαση για τα Διαδικτυακά Εγκλήματα του Συμβουλίου της Ευρώπης η παιδική πορνογραφία έχει τις εξής μορφές:

i. Ένας ανήλικος που συμμετέχει σε σεξουαλική δραστηριότητα.
ii. Ένα άτομο που συμμετέχει σε σεξουαλική δραστηριότητα προσποιούμενο ότι είναι ανήλικο
iii. Ρεαλιστικές εικόνες που αναπαριστούν ένα ανήλικο να συμμετέχει σε σεξουαλικές δραστηριότητες

Η πορνογραφία ως υλικό μπορεί να περιλαμβάνει κυρίως περιοδικά, βιντεοταινίες, κινηματογραφικές ταινίες ή φωτογραφίες. Αν και η διαφήμιση του υλικού αυτού συχνά είναι καλυμμένη και κωδικοποιημένη , οι αστυνομικές εκθέσεις δείχνουν αύξηση των περιπτώσεων ανταλλαγής υλικού και παιδιών μεταξύ παιδεραστών. Η παραγωγή και εμπορία πορνογραφικού υλικού με πρωταγωνιστές μικρά παιδιά και η σεξουαλική εκμετάλλευση των παιδιών κρίνεται ότι είναι πράξεις που κακοποιούν, εκμεταλλεύονται και προκαλούν σοβαρές ζημιές στα παιδιά.Επομένως, η ύπαρξη παιδικής πορνογραφίας αποτελεί, σαφές και κατηγορηματικό στοιχείο παιδικής κακοποίησης.

- **Παιδόφιλοι**

Είναι σημαντικό να γνωρίζουμε τι είναι ακριβώς ο παιδόφιλος. Γενικά, παιδόφιλος είναι εκείνος ο ενήλικας (αν και υπάρχουν και έφηβοι με αυτό το χαρακτηρισμό) που σεξουαλικά προσελκύεται από παιδιά. Πιο επίσημα, η τέταρτη έκδοση του Διαγνωστικού και Στατιστικού Εγχειριδίου Διανοητικών Διαταραχών (Diagnostic and statistical Manual of Mental Disorders, Fourth Edition),(APA 1994) ορίζει την παιδοφιλία. Ο παιδόφιλος πρέπει να είναι τουλάχιστον δεκαέξι ετών και τουλάχιστον πέντε χρόνια μεγαλύτερος από το θύμα. Για τους εφηβικούς

παιδόφιλους, δεν δίνεται καμία συγκεκριμένη διαφορά ηλικίας μεταξύ κακοποιού και θύματος. Οι τεχνικές γνώσεις των παιδόφιλων δεν μπορούν να λύσουν άμεσα τις υποθέσεις, αλλά είναι σημαντικό για τους ανακριτές να έχουν μια αίσθηση του πεδίου στο οποίο λειτουργούν.

Τα διαγνωστικά κριτήρια για ένα παιδόφιλο περιλαμβάνουν :

- επαναλαμβανόμενες και έντονες σεξουαλικά φαντασίες, ωθήσεις ή συμπεριφορές που αφορούν σεξουαλικές πράξεις με ένα προεφηβικό παιδί ή παιδία
- φαντασίες, ωθήσεις ή συμπεριφορά που οδηγεί σε κλινικά σημαντικό κίνδυνο (παραδείγματος χάριν, ανησυχία ή κατάθλιψη), ή την εξασθένιση σε κοινωνική, εργασιακή ή άλλη σημαντική πτυχή της λειτουργίας του ως άνθρωπος
- το άτομο είναι δεκαέξι ετών ή μεγαλύτερο και έχει τουλάχιστον πέντε χρόνων ηλικιακή διαφορά από το παιδί ή τα παιδιά.

Οι περισσότεροι παιδόφιλοι γνωρίζουν την έλξη τους για τα παιδιά γύρω στις αρχές της εφηβείας τους ή προς το τέλος της, αν και υπάρχουν εκθέσεις για παιδόφιλους που η έλξη για ανήλικους εμφανίζεται στη μέση ηλικία. Δεν συναντούν κριτήρια για διάγνωση παιδοφιλίας όλοι οι άνθρωποι που συλλαμβάνονται για παρενόχληση παιδιών. Οι παιδικοί σεξουαλικοί κακοποιοί μπορούν να υποδιαιρεθούν σε τέσσερα κριτήρια :

- Η ηλικία του δράστη (έφηβοι, νέοι και μέσης ηλικίας ενήλικοι, ηλικιωμένα άτομα)
- Το φύλο του παραβάτη (αρσενικό ή θηλυκό)
- Ο σεξουαλικός προσανατολισμός ή η προτίμηση (στο αρσενικό φύλο ή στο θηλυκό)
- Ο τύπος των θυμάτων (αρσενικό ή θηλυκό ή και τα δύο, νήπια, μικρά παιδιά, παιδιά του δημοτικού, έφηβοι ή χωρίς κάποια διάκριση).

Όπως σημειώνεται, οι τέσσερις κατηγορίες δεν είναι αμοιβαία αποκλειστικές. Όσο περισσότερο μαθαίνει κανείς για τους παραβάτες, συμπεριλαμβανομένων αυτών που κακοποιούν σεξουαλικά παιδιά (σημειώστε ότι είναι δυνατό να χαρακτηριστεί κάποιος παιδόφιλος και όμως να μην είναι παραβάτης), τόσο περισσότερο γίνεται εμφανές ότι δεν υπάρχει κανένας εύκολος τρόπος να προσδιορίσει κανείς ποιος είναι πιθανός να σημειώσει μια σεξουαλική παρατυπία.

Οι ενήλικες σεξουαλικές αλληλεπιδράσεις περιλαμβάνουν γενικά ένα από τα ακόλουθα τρία σενάρια: διαπραγμάτευση και συγκατάθεση, πίεση και εκμετάλλευση, δύναμη και επίθεση. Αν και το πρώτο σενάριο (η διαπραγμάτευση και η συγκατάθεση) αποτελεί το κατάλληλο σχέδιο δράσης, ακόμη και αυτή η επιλογή λείπει με τους ανήλικους συνεργάτες. Σίγουρα, τα μικρά παιδιά στερούνται τη δυνατότητα να δώσουν τη συγκατάθεση τους, αλλά ακόμα και τα σεξουαλικά ώριμα

προεφηβικά παιδιά δεν έχουν την ψυχολογική ωριμότητα να διαπραγματευτούν τη σεξουαλική δραστηριότητα με έναν ενήλικο. Οι ενήλικοι μπορούν να επωφεληθούν αυτή την σεξουαλική ανωριμότητα και μπορούν να εκμεταλλευτούν το παιδί με ποικίλους τρόπους. Οι διάφορες τυπολογίες αυτών που κακοποιούν σεξουαλικά παιδιά αναπτύχθηκε με την πρόθεση να βοηθήσει τους ανθρώπους να αναγνωρίζουν τα κοινά γνωρίσματα και συμπεριφορές για διαγνωστικούς, επεξεργασιακούς και ερευνητικούς σκοπούς, οι οποίοι ποικίλλουν στη χρησιμότητα και στους φορείς. Οι παραβάτες διακρίνονται στους σταθερούς και στους παλινδρομικούς. Ο μεν σταθερός παραβάτης ελκύεται αποκλειστικά από έναν ιδιαίτερο τύπο θυμάτων, παραδείγματος χάριν, από ένα δεκάχρονο αγόρι ενώ ο παλινδρομικός παραβάτης έχει ως ένα βαθμό ώριμες και ηλικιακά κατάλληλες σχέσεις, αλλά για κάποιους λόγους έχει προσανατολιστεί προς νεότερους συνεργάτες. Ένας σημαντικός παράγοντας που μπορεί να έχει οδηγήσει προς αυτή τη κατεύθυνση έναν παλινδρομικό παραβάτη θα μπορούσε να είναι ένα διαζύγιο, η απώλεια μιας εργασίας ή οποιοσδήποτε άλλη ενέργεια που πιθανώς να έχει σοβαρές επιπτώσεις στον αυτοσεβασμό του. Κάτι τέτοιο μπορεί να είναι προσωρινό ή και παρατεταμένο.

Οι Taylor, Holland και Quayle (2001), προσπάθησαν να δώσουν μια τυπολογία παιδόφιλων στο διαδίκτυο διακρίνοντας τους χρήστες σε εννέα κατηγορίες:

1. Ο ξεφυλλιστής (Browser). Ο τύπος χρήστη αναφέρεται σε αυτόν που «σερφάρει» στο διαδίκτυο, συναντά ακούσια (επί παραδείγματι μέσω ενοχλητικού ταχυδρομείου «spam») υλικό παιδικής πορνογραφίας και αποφασίζει να το κρατήσει. Το εάν ο συγκεκριμένος χρήστης συνέλεξε το υλικό συμπτωματικά θα φανεί από το κατά πόσο θα συνεχίσει αυτή τη δραστηριότητα που ξεκίνησε τυχαία.

2. Η ιδιωτική φαντασίωση (Private fantasy). Ο τύπος χρήστη αναφέρεται στο άτομο που έχει προσωπικές σεξουαλικές φαντασιώσεις και μόνο με παιδί, τις οποίες αποτυπώνει σε κείμενα ψηφιακής μορφής στον υπολογιστή του ή χρησιμοποιεί ψηφιακές φωτογραφίες για προσωπική του χρήση, χωρίς ωστόσο να έχει την πρόθεση να τις μοιραστεί με άλλους.

3. Το «αλιευτικό πλοιάριο» (Trawler). Ο τύπος χρήστη είναι ο λεγόμενος «αλιευτής», ο οποίος αναζητά ενεργά υλικό παιδικής πορνογραφίας χρησιμοποιώντας και άλλους χρήστες με παρόμοια ενδιαφέροντα.

4. Ο μη ασφαλής συλλέκτης (Non-secure collector).Ο τύπος χρήστη χαρακτηρίζεται ως ο «επισφαλής» συλλέκτης, ο οποίος αγοράζει, συλλέγει και ανταλλάσσει πορνογραφικό υλικό που

διατίθεται σε ιστοσελίδες ή chatrooms, που δεν απαιτούν κωδικούς ασφαλείας, εγγραφές και οτιδήποτε άλλο διασφαλίζει τέτοια δραστηριότητα.

5. Ο ασφαλής συλλέκτης (Secure collector).Ο τύπος αυτός είναι ο αντίθετος του προηγούμενου, δηλαδή αυτός που ενεργά αναζητά, συλλέγει και αγοράζει παιδικό πορνογραφικό υλικό, αλλά χρησιμοποιώντας πάντα αυστηρές δικλείδες ασφαλείας. Για παράδειγμα, κάποια δίκτυα ανταλλαγής υλικού απαιτούν, πριν από την εγγραφή νέων μελών, αυτά να καταθέσουν μέρος των προσωπικών του συλλογών, «κλειδώνοντας» έτσι τα μέλη τους.

6. Ο σε απευθείας σύνδεση «περιποιητής» groomer (online). Ο τύπος αυτός είναι ο λεγόμενος groomer , ο χρήστης δηλαδή που ξεκινά μια διαδικτυακή επικοινωνία με το παιδί με σκοπό να αναπτύξει σεξουαλική σχέση μαζί του, διαδικτυακά ή φυσικά. Η παιδική πορνογραφία χρησιμοποιείται από το συγκεκριμένο χρήστη για προετοιμάσει το παιδί για την ειδική περίσταση και να μειώσει τις αναστολές του.

7. Ο φυσικός καταχραστής (Physical abuser). Ο τύπος αυτός είναι αυτός που διαπράττει φυσικά σεξουαλικά εγκλήματα σε βάρος παιδιών και για τον οποίο η παιδική πορνογραφία πλαισιώνει τη σεξουαλική του δραστηριότητα..

8. Ο παραγωγός (Producer). Ο παραγωγός είναι αυτός που εμπλέκεται φυσικά στη σεξουαλική κακοποίηση του παιδιού και διακινεί έπειτα τις εικόνες αυτές στο διαδίκτυο. Ενδέχεται να παρακινεί παιδιά στο να διαθέτουν τα ίδια τις φωτογραφίες τους

9. Ο διανομέας (Distributor). Ο τύπος αυτός, είναι που διανέμει το πορνογραφικό υλικό σε όλους τους παραπάνω για να κερδίσει χρήμα. Ο ίδιος μπορεί να ενδιαφέρεται σεξουαλικά για παιδιά, μπορεί και όχι

- **Τι είναι τα κυκλώματα παιδοφιλίας;**

Ένα κύκλωμα παιδοφιλίας είναι μια ομάδα ανθρώπων που εργάζονται μαζί μέσω Διαδικτύου σε διαφορετικές χώρες και υπό διαφορετικά νομοθετικά πλαίσια, με σκοπό τη συλλογή και διανομή πορνογραφικού υλικού για τη δική τους ικανοποίηση. Μπορεί επίσης να γίνεται και ανταλλαγή εμπειριών και γνώσεων ως προς την αποφυγή ανίχνευσης και το σχεδιασμό εγκληματικών ενεργειών εις βάρος παιδιών.

- **Πώς τα κυκλώματα παιδοφιλίας χρησιμοποιούν το Διαδίκτυο;**

Υπάρχει μια ισχυρή εντύπωση ότι το Διαδίκτυο έχει γίνει ένας ισχυρός παράγων στην εξέλιξη των παιδοφιλικών κυκλωμάτων παγκοσμίως. Πολλές πρόσφατες καταδίκες στις Ηνωμένες

Πολιτείες Αμερικής και στο Ηνωμένο Βασίλειο απέδειξαν ότι το Διαδίκτυο χρησιμοποιείται ευρέως από τα μέλη τέτοιων κυκλωμάτων, τόσο για να την ανταλλαγή εμπειριών όσο και για την διακίνηση φωτογραφιών παιδικής πορνογραφίας.

Η διάδοση της παιδικής πορνογραφίας προκαλεί μεγάλη ανησυχία στους διεθνείς φορείς που ασχολούνται με την προστασία των ανηλίκων. Ανεξάρτητα από τους τρόπους που χρησιμοποιούνται για την διακίνηση φωτογραφιών παιδικής πορνογραφίας στο Διαδίκτυο, το πρόβλημα εξακολουθεί να είναι σοβαρό στη δυτική Ευρώπη, όπου αποκαλύφθηκαν σημαντικά κυκλώματα παιδικής πορνογραφίας στη Δανία, την Ισπανία, τη Γερμανία, την Ιταλία, την Ολλανδία, τη Σουηδία και το Ηνωμένο Βασίλειο.

Καθώς αυτά τα δίκτυα χρησιμοποιούν εξελιγμένες τεχνολογίες τηλεπικοινωνιών, κάνοντας χρήση κρυπτογράφησης και κωδικών ονομασιών, γίνεται συνεχώς δυσκολότερη η ανακάλυψή τους από τις αρχές.

- **Τι σημαίνει ο όρος grooming;**

Το grooming είναι η διαδικασία κατά την οποία, παιδόφιλοι, προσποιούμενοι ότι είναι έφηβοι, χρησιμοποιούν τα chatrooms για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν. Τα chatrooms φιλοξενούνται στο Διαδίκτυο και σε αυτά μπορεί να έχει πρόσβαση οποιοσδήποτε από οποιοδήποτε σημείο στον κόσμο. Συχνά θεωρούνται από τα παιδιά ασφαλείς τόποι συνομιλίας στο Διαδίκτυο, τόσο εξαιτίας της δημόσιας φύσης της συζήτησης αλλά και της λανθασμένης εκτίμησης των παιδιών ότι διατηρείται η ανωνυμία τους.

Οι παιδόφιλοι ξεκινούν συζητήσεις με τα πιθανά θύματα με σκοπό να αναπτύξουν φιλική σχέση με αυτά και να αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον τόπο διαμονής τους, τα ενδιαφέροντα, τα χόμπι και τις σεξουαλικές τους εμπειρίες.

Μέσα από την σχέση αυτή προκαλούν σιγά - σιγά συζητήσεις σεξουαλικής φύσεως και πολλές φορές οι παιδόφιλοι στέλνουν στα υποψήφια θύματα φωτογραφίες παιδικής πορνογραφίας αλλά και πορνογραφίας ενηλίκων για να δώσουν την αίσθηση ότι αυτό είναι κάτι το αποδεκτό και φυσιολογικό. Η τακτική αυτή χρησιμοποιείται για να υπονομεύσει την απροθυμία των παιδιών στο να λάβουν μέρος σε σεξουαλική επαφή. Χρησιμοποιείται επίσης για να αποτρέψει το θύμα από το να ζητήσει προστασία από τους γονείς και τους δασκάλους του, αφού καταλήγει να νιώθει ένοχο που έχει ανταλλάξει τέτοιου είδους φωτογραφίες.

- **Τρόποι επικοινωνίας μέσω διαδικτύου και η χρήση τους στην διανομή παράνομου πορνογραφικού υλικού**

1. Δωμάτιο Συνομιλίας
2. Στιγμιαίο Μήνυμα (IM)
3. Ηλεκτρονικό ταχυδρομείο (e-mail)
4. Ηλεκτρονικές ομάδες (e-groups)
5. Κατάλογοι ηλεκτρονικών διευθύνσεων
6. Ομάδες πληροφόρησης
7. Πίνακας δελτίων (BBS)

- **Τι είναι τα «chatrooms»**

Είναι κοινωνικά δωμάτια συνομιλίας, όπου κάθονται στη μία μεριά ο ανήλικος και στην άλλη κάποιος άλλος που ίσως του έχει παρουσιαστεί ανήλικος, συνομήλικος κλπ. Μέσα στα chatrooms διακινούνται ναρκωτικά. Έχουμε υποθέσεις σωματεμπορίας, αποπλάνησης και ναρκωτικών. Ο ανήλικος μπορεί ευκολότερα να αποπλανηθεί όταν αυτός εθίζεται στα chat. Υπάρχουν περιπτώσεις μαθητών όπου γονείς δεν μπορούν να κάνουν καλά τα παιδιά τους τα οποία εγκατέλειψαν τα σχολεία τους για να είναι συνέχεια στα chatrooms. Άρα, με λίγα λόγια, ελέγχουμε και βάζουμε χρονικά όρια στα chatrooms. Είναι η τάση της εποχής. Υπάρχει και ένα άλλο φαινόμενο. Παρατηρείτε διακίνηση ερασιτεχνικών ερωτικών videos στο διαδίκτυο με πρωταγωνιστές μαθητές διαφόρων σχολείων. Η Υπηρεσία Ηλεκτρονικού Εγκλήματος με τα σχολικά videos εντόπισε δύο κυκλώματα σε Αθήνα και Λαμία, τα οποία διακινούσαν για κερδοσκοπία τα videos αυτά, που προμηθεύονταν από τους μαθητές.

- **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 φωτογραφίες μας, οι οποίες είναι προκλητικές.

- **Νομικό Πλαίσιο**

1. Όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην Επικράτεια ή εξάγει από αυτή, μεταφέρει, προσφέρει, πωλεί ή με άλλον τρόπο διαθέτει, αγοράζει, προμηθεύεται, αποκτά ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει ή μεταδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.
2. Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων δια συστήματος ηλεκτρονικού υπολογιστή ή με τη χρήση διαδικτύου, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.
3. Υλικό παιδικής πορνογραφίας, κατά την έννοια των προηγούμενων παραγράφων, συνιστά η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα του σώματος ή μέρους του σώματος ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο.
4. Οι πράξεις της πρώτης και δεύτερης παραγράφου τιμωρούνται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή πενήντα χιλιάδων έως εκατό χιλιάδων ευρώ:

   α. αν τελέσθηκαν κατ' επάγγελμα ή κατά συνήθεια»

   β. αν η παραγωγή του υλικού της παιδικής πορνογραφίας συνδέεται με την εκμετάλλευση της ανάγκης, της ψυχικής ή της διανοητικής ασθένειας ή σωματικής δυσλειτουργίας λόγω οργανικής νόσου ανηλίκου ή με την άσκηση ή απειλή χρήσης βίας ανηλίκου ή με τη χρησιμοποίηση ανηλίκου που δεν έχει συμπληρώσει το δέκατο πέμπτο έτος».

   Αν η πράξη της περίπτωσης β' είχε ως αποτέλεσμα τη βαριά σωματική βλάβη του παθόντος, επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή εκατό χιλιάδων έως

πεντακοσίων χιλιάδων ευρώ αν δε αυτή είχε ως αποτέλεσμα το θάνατο, επιβάλλεται ισόβια κάθειρξη.

- **Επιπτώσεις της παιδικής πορνογραφίας – Συνέπειες στην σεξουαλικότητα**

Στην εποχή μας η διάδοση και επιρροή της πορνογραφίας είναι μεγαλύτερη όσο ποτέ άλλοτε. Το διαδίκτυο και οι αναρίθμητοι πλέον τηλεοπτικοί σταθμοί, που προσφέρουν είτε δωρεάν είτε με πληρωμή κάθε μορφής πορνογραφικό περιεχόμενο, βρίσκονται πολύ κοντά σε όλους μας. Οι σύγχρονες τεχνολογίες επιτρέπουν τόσο σε ενήλικες αλλά και σε παιδιά ή έφηβους μια εξαιρετικά εύκολη πρόσβαση σε πορνογραφικές φωτογραφίες, ταινίες ή κείμενα, οποιαδήποτε ώρα ή ημέρα. Το πρόβλημα γίνεται ακόμη σοβαρότερο από το γεγονός, ότι όλα αυτά μπορούν να γίνουν με μεγάλη ευκολία και συστηματικά από το σπίτι, χωρίς να γίνεται εύκολα αντιληπτό από τους άλλους.

Παλαιότερα η πορνογραφία ήταν περιορισμένη. Εκτός από τα περιοδικά που δεν ήταν εύκολο να προμηθευτεί ο οποιοσδήποτε και ιδιαίτερα τα παιδιά, υπήρχαν στους κινηματογράφους οι σχετικές ταινίες. Στις περιπτώσεις αυτές τόσο η πρόσβαση όσο και το περιεχόμενο υπόκειντο σε έλεγχο. Σήμερα το διαδίκτυο επιτρέπει πρακτικά σε όλους την πρόσβαση σε πληθώρα δικτυακών τόπων με πολύμορφο πορνογραφικό περιεχόμενο. Κανείς δεν μπορεί να ελέγξει τη βιομηχανία αυτή στην οποία προβάλλονται καταστάσεις που παλαιότερα ήταν αδύνατο κάποιος να φανταστεί.

Η ποιότητα του περιεχομένου που προβάλλεται από τους πορνογραφικούς δικτυακούς τόπους είναι συχνά επικίνδυνη. Συχνά δεν προβάλλονται κανονικές σεξουαλικές συμπεριφορές αλλά τροποποιημένες καταστάσεις με στόχο την εμπορική εκμετάλλευση. Οι στρεβλωμένες παθολογικές συμπεριφορές, οι ανεπίτρεπτες σεξουαλικές καταστάσεις όπως η παιδεραστία, η ζωοφιλία ή άλλες ασυνήθιστες ή μη κοινωνικά αποδεκτές φαντασιώσεις προβάλλονται με τον ίδιο τρόπο και παράλληλα με φυσιολογικές σεξουαλικές ή ερωτικές συμπεριφορές .

Βλέπουμε λοιπόν ότι η νέα αυτή κατάσταση είναι ιδιαίτερα ανησυχητική. Επηρεάζει σήμερα τεράστιο αριθμό ανθρώπων, είναι δυνατόν να τροποποιεί τις αντιλήψεις, δίνει λανθασμένα μηνύματα στους νέους αλλά και στους ενήλικες. Όλο και περισσότεροι παράγοντες των σύγχρονων κοινωνιών αρχίζουν να αντιλαμβάνονται τα κοινωνικά και ψυχολογικά προβλήματα, που συνεχίζουν να δημιουργούνται και να συσσωρεύονται διαχρονικά λόγω της πρόσφατης εκπληκτικής εξάπλωσης της πορνογραφίας.

Είναι σημαντικό όλοι οι σημαίνοντες κοινωνικοί και πολιτειακοί παράγοντες όπως επίσης και το πλατύ κοινό, να συνειδητοποιήσουν το μέγεθος του προβλήματος και τις επιπτώσεις που

μπορεί να έχει βραχυπρόθεσμα αλλά και μακροπρόθεσμα η ανεπιθύμητη κατάσταση αυτή. Δυστυχώς, η πορνογραφία σήμερα μετατρέπει προς το χειρότερο τη σεξουαλικότητα και τις ανθρώπινες σχέσεις. Ακόμη χειρότερα υπάρχει ο σοβαρός κίνδυνος παροχής κακής και στρεβλωμένης αγωγής για θέματα σεξ στα παιδιά και στους έφηβους λόγω του ότι η πορνογραφία έχει καταστεί σημαντική πηγή πληροφόρησης για αυτούς

Οδηγίες προς τους γονείς

- Να ενημερωθούν για τους κινδύνους που κρύβει η ανεπιτήρητη πλοήγηση των παιδιών στο Internet.
- Να εξοικειωθούν και εκείνοι στη χρήση του διαδικτύου, για να μπορούν να μιλούν την ίδια γλώσσα με τα παιδιά τους.
- Να θεσπίσουν κανόνες στην πρόσβαση στο Internet, όπως:
- Να μην επιτρέπουν στα παιδιά τους να δίνουν πληροφορίες για προσωπικά στοιχεία, δηλαδή ονοματεπώνυμο, διεύθυνση, τηλέφωνο, σχολείο, επάγγελμα γονιών, οικογενειακή κατάσταση, αριθμό πιστωτικής κάρτας.
- Να απαγορεύεται στα παιδιά να συναντηθούν με άτομο που γνώρισαν στο διαδίκτυο, χωρίς την ενημέρωση και άδεια των γονιών.
- Να μη στέλνουν φωτογραφίες σε γνωριμίες από το Internet.

2.10. Ξέπλυμα χρήματος

- **Ορισμός**

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 αποκρύπτεται και το «βρώμικο χρήμα», ή «μαύρο χρήμα» που αποκρύπτεται.

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 αποκρύπτεται, 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 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.

- **Ιστορικό**

Η πρώτη αναφορά στον όρο «ξέπλυμα χρήματος» γίνεται στο περίφημο σκάνδαλο Watergate. Η επιτροπή του τότε Αμερικανού Προέδρου Richard Nixon για την επανεκλογή Προέδρου είχε διοχετεύσει όλα τα έσοδα της προεκλογικής καμπάνιας του στο Μεξικό και τα «επαναπάτρισε» μέσω μίας εταιρίας στο Miami, Florida. Η Βρετανική εφημερίδα “The Guardian” είναι εκείνη που αναφέρθηκε στην κίνηση αυτή με τον όρο “laundering - έσοδα από παράνομες δραστηριότητες”

- **Τρόποι**

Οι εποχές που το ξέπλυμα βρώμικου χρήματος γινόταν σε καζίνο, μέσω ασφαλιστήριων συμβολαίων ή με δελτία Προ-Πο ανήκουν πια στο παρελθόν. Πλέον, οι κακοποιοί 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;

1. **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.

2. **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.

3. 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.

4. 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.

5. Online στοιχηματικές 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 στοιχηματική εταιρεία, η οποία θα "ζητήσει" το ισοζύγιο κερδών και "χασούρας" να είναι αντίστοιχο με τη γκανιότα (προμήθεια) της.

- **Μοντέλα των φάσεων**

Πρωταρχικός στόχος της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες είναι η αποτροπή της αποκάλυψης και κατά συνέπεια της μετατροπής περιουσιακών στοιχείων, κυρίως όσον αφορά την εγκληματική προέλευσή τους. Δεν είναι όμως και ο μοναδικός στόχος. Απλή

απόκρυψη δεν προσφέρει ουσιαστικά κάτι στο δράστη αφού για να τα αξιοποιήσει ή χρησιμοποιήσει ή επενδύσει πρέπει οι πρόσοδοι αυτοί να ενταχθούν ως νόμιμοι πια στην οικονομία. Εμπνευστής των μοντέλων αυτών είναι ο Ελβετός Paolo Bernasconi, ο οποίος και αποτέλεσε πρωτεργάτη της εισαγωγής διατάξεων στον Ελβετικό Ποινικό Κώδικα για την αντιμετώπιση της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες. Το μοντέλο βασικά ξεχωρίζει το ξέπλυμα σε πρώτου και δευτέρου βαθμού. Διακρίνει ακόμη σε χώρες εμπορίου (όπου γίνεται η κύρια πράξη από την οποία προέρχεται το βρώμικο χρήμα) και σε χώρες ξεπλύματος (μεγάλα χρηματοοικονομικά κέντρα, γνωστά και ως φορολογικοί παράδεισοι).

1η Φάση

- Νομιμοποίηση περιουσιακών στοιχείων, άμεσα προερχομένων από ποινικά κολάσιμες πράξεις
- Μετρητό χρήμα (κατά κανόνα)
- Βραχυπρόθεσμες συναλλαγές
- Ο δράστης επιδιώκει να εμποδίσει την αναγνώριση των περιουσιακών στοιχείων. .

2η Φάση

- Νομιμοποίηση περιουσιακών στοιχείων προερχομένων αποκλειστικά από την τέλεση ποινικά κολάσιμων πράξεων
- Μέσο-μακροπρόθεσμες επιχειρήσεις
- Στόχος η απάλειψη του στίγματος της παρανομίας από τα εγκληματικής προέλευσης περιουσιακά στοιχεία, προσδίδοντάς τους τον χαρακτήρα νόμιμης οικονομικής δραστηριότητας.

➢ **Οι τεχνικές ξεπλύματος χρήματος**

Με βάση κάποιες εκτιμήσεις των τελωνιακών υπηρεσιών των Η.Π.Α. καταγράφονται οι κυριότερες τεχνικές που χρησιμοποιούνται διεθνώς για την νομιμοποίηση των εσόδων από εγκληματικές δραστηριότητες και στις τρεις φάσεις που προαναφέρθηκαν.

1. ΤΟΠΟΘΕΤΗΣΗ

❖ Ψευδής παρουσίαση ή απόκρυψη της πραγματικής προέλευσης των δικαιούχων και χρησιμοποίηση εταιριών - βιτρίνα, διατραπεζικές συναλλαγές και εξαιρέσεις από την υποχρέωση αναφοράς και εξακρίβωσης ταυτότητας.

- Μέθοδος του μυρμηγκιού
- Συνεργία από το εσωτερικό κάποιου χρηματοπιστωτικού οργανισμού
- διασυνοριακή λαθραία φυσική μμεταφορά χρημάτων μέσω πλοίων, αεροπλάνων, απεσταλμένων συσκευασμένα ως εμπορεύματα
- Απόκτηση υλικών αντικειμένων (ακίνητα, πολύτιμα κοσμήματα και μέταλλα, πλοία, αυτοκίνητα, αεροπλάνα) ή χρηματιστηριακών τίτλων, επιταγών και άλλων τραπεζογραμματίων.

2. ΣΥΣΣΩΡΕΥΣΗ

- Ηλεκτρονική μεταφορά κεφαλαίων μέσω διαδικτύου
- Μετατροπή χρήματος σε άλλες χρηματοοικονομικές μορφές
- Πώληση ή εξαγωγή περιουσιακών στοιχείων
- Παραποίηση εξαγωγικών και εισαγωγικών εγγράφων

3. ΟΛΟΚΛΗΡΩΣΗ

- Εταιρίες βιτρίνα
- Συνεργία αλλοδαπής τράπεζας
- Απόκτηση περιουσιακών στοιχείων

2.11. Διαδικτυακή τρομοκρατία

Το FBI ορίζει την κυβερνοτρομοκρατία (cyber terrorism) «ως την προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι αμάχων στόχων από ομάδες και μυστικούς πράκτορες»

Η χρήση του διαδικτύου παρέχει στους ιδιοκτήτες μια σειρά από πλεονεκτήματα και ειδικότερα:

1. Είναι φθηνότερο σε σχέση με τις άλλες τρομοκρατικές μεθόδους.
2. Οι ενέργειες τους δύσκολα εντοπίζονται.
3. Μπορούν να εξαπολύσουν την επίθεση τους από οποιοδήποτε σημείο του κόσμου και να επιτεθούν ταυτόχρονα σε πολλούς στόχους.
4. Το διαδίκτυο είναι ένας χώρος όπου προς το παρόν τουλάχιστον υπάρχει ελευθερία της έκφρασης και αυτή μπορεί να ενθαρρύνει κάποιον να μεταδώσει αυτά που θέλει, διατηρώντας την ανωνυμία του.

Με τη χρήση λοιπόν του διαδικτύου οι τρομοκράτες μπορούν να παρακάμψουν τις ασφαλιστικές δικλείδες στις οποίες υπόκεινται τα παραδοσιακά ΜΜΕ και να έχουν παγκόσμια πρόσβαση σε εκατοντάδες εκατομμύρια ανθρώπων. Ένα παράδειγμα είναι το 1999 ένας δεκαεπτάχρονος Αμερικανός που λειτουργούσε με το όνομα Chameleon βρέθηκε να κλέβει δορυφορικές εικόνες από τις στρατιωτικές ιστοσελίδες των Η.Π.Α. Ο Chameleon θεωρήθηκε ότι βρισκόταν στην υπηρεσία του Osama Bin Laden, ο άνθρωπος που είναι ύποπτος ότι βρίσκεται πίσω από τον βομβαρδισμό των Αμερικανικών βάσεων στην Ανατολική Αφρική το 1998 και συνεπώς στην κορυφή του καταλόγου των καταζητούμενων του FBI. Στον Chameleon δόθηκαν 1000 $ προκαταβολικά για την ανταλλαγή με το software και θα έπαιρνε επιπλέον 10.000 $ με την πρόοδο της εργασίας. Ευτυχώς το FBI τον συνέλαβε προτού να έχει την ευκαιρία να διανέμει τα στοιχεία.

2.12. Επιθέσεις παρενόχλησης (cyberbulling)

Ο όρος Διαδικτυακός εκφοβισμός (cyberbullying) αφορά τον εκφοβισμό, την απειλή, την ταπείνωση ή την παρενόχληση παιδιών, προεφήβων και εφήβων που δέχονται μέσω της χρήσης του διαδικτύου, κινητών τηλεφώνων είτε άλλων ψηφιακών τεχνολογιών από συνομηλίκους τους.

- **Αίτια**

Συχνά οι νέοι οδηγούνται στον διαδικτυακό εκφοβισμό εξαιτίας της βίωσης έντονων συναισθημάτων όπως θυμός, απόγνωση είτε πάλι και εκδίκηση, που μπορεί να προέρχεται τόσο από τις προβληματικές σχέσεις που υπάρχουν στο οικογενειακό περιβάλλον όσο και εξαιτίας μιας ευρύτερης κοινωνικής δυσλειτουργίας που παρουσιάζει το άτομο. Σε μερικές περιπτώσεις ο διαδικτυακός εκφοβισμός αποτελεί μορφή ψυχαγωγίας στοχεύοντας στην εκδήλωση ποικίλων αντιδράσεων και στην ικανοποιήση αναγκών που σχετίζονται με την επιβολή εξουσίας και ελέγχου. Σπανιότερα, η αποστολή μηνυμάτων σε λάθος παραλήπτες μπορεί να αποτελέσει αιτία του φαινομένου.

- **Η συχνότητα των απειλών**

1) Η επικοινωνία πραγματοποιείται μόνο μία φορά

2) Η επικοινωνία επαναλαμβάνεται με ίδιο ή διαφορετικό τρόπο

3) Η επικοινωνιακή δραστηριότητα αυξάνεται

4) Τρίτα άτομα εμπλέκονται στην επικοινωνία με αποτέλεσμα το άτομο να λαμβάνει μηνύματα από διαφορετικούς παραλήπτες

- **Μορφές Διαδικτυακού εκφοβισμού**

- Επαναλαμβανόμενη αποστολή ηλεκτρονικών ή τηλεφωνικών μηνυμάτων
- Παρέμβαση και παρενόχληση οποιασδήποτε δραστηριότητας του ατόμου
- Δημιουργία ψεύτικων διαδικτυακών προφίλ
- Είσοδος σε προσωπικούς διαδικτυακούς λογαριασμούς του ατόμου
- Αποστολή φωτογραφιών του ατόμου ή άλλου είδους μαγνητοσκοπημένου υλικού
- Αποστολή προσωπικών πληροφοριών του ατόμου σε πολλαπλούς παραλήπτες
- Αποστολή απειλητικών μηνυμάτων σε άλλα άτομα υποκρινόμενοι το άτομο που εκφοβίζεται
- Υποκίνηση τρίτων για διαδικτυακή παρακολούθηση και παρενόχληση του ατόμου

- **Αντιμετώπιση του Διαδικτυακού εκφοβισμού**

i. Αγνόηση ενοχλητικών μηνυμάτων, σε περίπτωση ωστόσο απειλών συνιστάται αναφορά των μηνυμάτων και λήψη προληπτικών μέτρων
ii. Αποκλεισμός του αποστολέα των απειλητικών μηνυμάτων
iii. Αναφορά της περίστασης στον γονέα ή κηδεμόνα
iv. Αναφορά του περιστατικού στην Αστυνομία είτε σε κάποια αρμόδια υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος

- **ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ**

α. Περίπου 15-35% των νέων έχει πέσει θύμα διαδικτυακού εκφοβισμού

β. 10-20% των νέων παραδέχεται την ανάμειξη του σε κάποιο περιστατικό

γ. Τα κορίτσια ενδέχεται να εμπλακούν συχνότερα από ότι τα αγόρια σε καποιο περιστατικό

δ. Η πλειοψηφία των ατόμων που υφίσταται ή ασκεί cyberbullying είναι ηλικίας 12-16 ετών

- **Είδη παρατηρητών στον διαδικτυακό εκφοβισμό**

Όπως ακριβώς και στον σχολικό εκφοβισμό έτσι και στον διαδικτυακό -που μπορεί να αποτελέσει προέκταση του πρώτου- καταγράφονται κυρίως δύο είδη παρατηρητών (bystanders).

- Στην πρώτη κατηγορία ανήκουν οι επιβλαβείς για το θύμα παρατηρητές, καθώς επιδοκιμάζουν

την συμπεριφορά του θύτη ενισχύοντας έτσι την ένταση του εκφοβιστικού γεγονότος ή άλλοτε παρατηρούν το περιστατικό με απάθεια δίχως να σημειώνουν κάποια αντίδραση ή παρέμβαση για την καταστολή του εκφοβισμού

- Σε αντίθεση με την πρώτη κατηγορία, οι βοηθοί παρατηρητές αντιδρούν άμεσα και ενεργά στο συμβάν του διαδικτυακού εκφοβισμού. Παράλληλα, στοχεύουν στην κινητοποίηση περισσότερων ατόμων για την καταπολέμηση του.

➢ **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 τον 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, κυρίως κατά την εφηβική ηλικία η αποχή από το σχολείο και από τις παρέες των συνομηλίκων αποτελεί προσωρινό καταφύγιο, ενώ ταυτόχρονα η αυτοκτονία θεωρείται ως η μοναδική λύση στο πρόβλημα. Άτομα που δέχτηκαν ένοντα διαδικτυακό εκφοβισμό ενδέχεται στο μέλλον να παρουσιάσουν μεγαλύτερη αστάθεια στις διαπροσωπικές τους σχέσεις συνοδευόμενη από την κοινωνική απομόνωση. Από την άλλη, οι εκφοβιστές τείνουν να είναι άτομα με έντονη αντικοινωνική συμπεριφορά, επιρρεπή στο αλκοόλ και απομονωμένα από το κοινωνικό σύνολο. Μακροπρόθεσμα, αντιλαμβάνονται ότι ο εκφοβισμός δεν αποτελεί μορφή ικανοποιήσης και αναγνώρισης, βιώνοντας έτσι έντονη προσωπίκη απογοήτευση.

ΚΕΦ. 3ο: Ενημέρωση - Προστασία - Αντιμετώπιση

Το ηλεκτρονικό έγκλημα είναι ένα συχνό φαινόμενο της σύγχρονης εποχής, εξαιτίας της ραγδαίας ανάπτυξης της τεχνολογίας και της συμμετοχής ολοένα και περισσότερων ατόμων, κυρίως νέων, στον κυβερνοχώρο. Για να μην εξαπλωθεί όμως το παραπάνω πρόβλημα ακόμη περισσότερο, είναι απαραίτητο να ληφθούν ορισμένα μέτρα για την άμεση αντιμετώπιση του. Η ομάδα μας έχει αναλάβει την παρουσίαση των υπηρεσιών που είναι υπεύθυνες και αρμόδιες για θέματα προστασίας από το ηλεκτρονικό έγκλημα.

➢ **Πάταξη του ηλεκτρονικού εγκλήματος – αρμόδιες υπηρεσίες**

1. **Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (http://www.astynomia.gr)**

Η αποστολή της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας.

Η Δίωξη Ηλεκτρονικού Εγκλήματος, στην εσωτερική της δομή, αποτελείται από τέσσερα τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου. Έτσι, στη νέα αναβαθμισμένη δομή της αποτελείται από:

- Το Τμήμα Γενικών Υποθέσεων και Προστασίας Προσωπικών Δεδομένων που ασχολείται με τις εγκληματικές πράξεις που διαπράττονται στα μέσα ηλεκτρονικής επικοινωνίας και ψηφιακής αποθήκευσης ή μέσω αυτών σε ολόκληρη τη χώρα.
- Το Τμήμα Προστασίας Ανηλίκων που ασχολείται με τα εγκλήματα που διαπράττονται κατά των ανηλίκων με τη χρήση του διαδικτύου και των άλλων μέσων ηλεκτρονικής ή ψηφιακής επικοινωνίας και αποθήκευσης.
- Το Τμήμα Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων που ασχολείται με τις υποθέσεις παράνομης διείσδυσης σε υπολογιστικά συστήματα και κλοπής, καταστροφής ή παράνομης διακίνησης λογισμικού υλικού, ψηφιακών δεδομένων και οπτικοακουστικών έργων, που τελούνται σε ολόκληρη τη χώρα.
- Το Τμήμα Ασφάλειας Ηλεκτρονικών Επικοινωνιών, που ασχολείται με την πρόληψη και καταστολή εγκλημάτων παραβίασης του απορρήτου των ηλεκτρονικών επικοινωνιών.

2. Ελληνική ανοιχτή γραμμή επικοινωνίας Safeline (http://www.safeline.gr/)

Η SafeLine είναι μια Ανοικτή Γραμμή (HotLine) που δέχεται καταγγελίες για δικτυακούς τόπους (websites) ή υπηρεσίες νέων (newsgroups) που εσείς βρήκατε στο Ίντερνετ και περιέχουν:

- εικόνες κακομεταχείρισης των παιδιών, οπουδήποτε στον κόσμο ρατσιστικό και ξενοφοβικό περιεχόμενο που, κατά την άποψή σας, παραβαίνει την Ελληνική νομοθεσία και άλλο περιεχόμενο, παράνομο, κατά την άποψή σας.
- Η SafeLine συνεργάζεται με τους Φορείς Παροχής Υπηρεσιών Ίντερνετ, το Ακαδημαϊκό Δίκτυο "ΕΔΕΤ" και το Πανελλήνιο Σχολικό Δίκτυο, Ερευνητικά και Πολιτιστικά Ιδρύματα, Ενώσεις Καταναλωτών και την Ελληνική Αστυνομία για τον περιορισμό της ροής του παράνομου περιεχομένου στο Ίντερνετ.

3. Νέο Ευρωπαϊκό Κέντρο (http://ec.europa.eu/news/justice/120328_el.htm)

Νέο ευρωπαϊκό κέντρο επαγρύπνησης θα προειδοποιεί για νέους κινδύνους και θα βοηθά στον εντοπισμό ηλεκτρονικών εγκλημάτων.

Καθημερινά, ένα εκατομμύριο άτομα πέφτουν θύματα ηλεκτρονικού εγκλήματος. Οι ένοχοι τέτοιων εγκλημάτων είναι αόρατοι και συνήθως μένουν ατιμώρητοι.

Η ΕΕ προτίθεται να αντιμετωπίσει αυτό το πρόβλημα δημιουργώντας ένα Ευρωπαϊκό Κέντρο για την Εγκληματικότητα στον Κυβερνοχώρο, το οποίο θα προειδοποιεί τις χώρες της ΕΕ για τις σοβαρότερες απειλές και θα τους επισημαίνει τις αδυναμίες άμυνας των επιγραμμικών τους εγκαταστάσεων. Θα εντοπίζει επίσης τα εγκληματικά δίκτυα και τους πλέον επικίνδυνους εγκληματίες, και θα παρέχει υποστήριξη κατά τη διάρκεια σχετικών ερευνών.

Το κέντρο αυτό θα συγκεντρώνει πληροφορίες από τον ιδιωτικό τομέα, τη βιομηχανία, την αστυνομία και τον ακαδημαϊκό κόσμο και θα βοηθά τις υπηρεσίες διερεύνησης τέτοιων εγκλημάτων καθώς και τις εισαγγελικές και δικαστικές αρχές.

Ο καθένας μπορεί να πέσει θύμα κάποιας μορφής ηλεκτρονικού εγκλήματος:

- κλοπή επιγραμμικής ταυτότητας
- απάτη μέσω υπολογιστή
- υποκλοπή πιστωτικής κάρτας
- σεξουαλική εκμετάλλευση παιδιών
- πειρατεία ηλεκτρονικών λογαριασμών
- επιθέσεις σε δημόσια ή ιδιωτικά συστήματα ΤΠ

Αυτού του είδους τα εγκλήματα αυξάνονται συνεχώς. Περίπου 600.000 λογαριασμοί Facebook χρειάζεται να κλειδώνονται καθημερινά μετά από απόπειρες πειρατείας. Μόνο στο Βέλγιο, οι υποθέσεις ηλεκτρονικής απάτης αυξήθηκαν από 4.000 το 2008 σε πάνω από 7.000 το 2010. Στο ΗΒ, οι υπεξαιρέσεις τραπεζικών λογαριασμών αυξήθηκαν κατά 207% το διάστημα 2008-2009. Σχετική έρευνα σε πολλά κράτη, μεταξύ των οποίων και στην Ελλάδα, έδειξε ότι λόγω της αύξησης των κρουσμάτων τους τελευταίους 12 μήνες, οι ενδιαφερόμενοι δίνουν περισσότερη προσοχή στο ηλεκτρονικό οικονομικό έγκλημα δεδομένου ότι ενεργοποιείται με απίστευτη ταχύτητα και κρύβει νέους κινδύνους.

Με την πάταξη του ηλεκτρονικού εγκλήματος θα αυξηθεί η εμπιστοσύνη των καταναλωτών προς τα ηλεκτρονικά συστήματα τραπεζικών εργασιών και κρατήσεων, και θα εξοικονομηθούν μεγάλα ποσά, καθώς το κόστος του κυβερνοεγκλήματος παγκοσμίως υπολογίζεται για το 2011 σε 85-291 δισ. Ευρώ!

Η πανευρωπαϊκή μορφή του κέντρου θα διασφαλίσει την ταχεία ανταλλαγή πληροφοριών μεταξύ των χωρών της ΕΕ. Αν, π.χ., στη Λιθουανία κάποιος αναφέρει παράνομη είσοδο στον τραπεζικό του λογαριασμού, θα μπορεί το γεγονός αυτό να συνδυάζεται ταχύτατα με παρόμοια περιστατικά σε άλλα κράτη ώστε το κέντρο να προειδοποιεί έγκαιρα όλες τις χώρες της ΕΕ για τον συγκεκριμένο κίνδυνο.

Το κέντρο θα συνδράμει επίσης ανακριτικές, εισαγγελικές και δικαστικές αρχές στην επίλυση τεχνικών και εγκληματολογικών ζητημάτων που ανακύπτουν κατά τις εργασίες τους.

Το κέντρο θα εγκατασταθεί στη Χάγη, εντός της Ευρωπαϊκής Αστυνομικής Υπηρεσίας – Ευρωπόλ, η οποία θα πρέπει πρώτα να εγκρίνει την πρόταση λειτουργίας του.

4. **Ομάδα Δράσης για την Ψηφιακή Ασφάλεια - D.A.R.T. (Digital Awareness & Response to Threats**) (http://www.dart.gov.gr/)

Η Ομάδα Δράσης για την Ψηφιακή Ασφάλεια D.A.R.T. (Digital Awareness & Response to Threats,) θα συμβάλλει στην πιο τακτική ενημέρωση των πολιτών και των επιχειρήσεων για το ηλεκτρονικό έγκλημα και τους τρόπους αντιμετώπισής του. Πρώτο βήμα της προσπάθειας είναι η δημιουργία της διαδικτυακής πύλης D.A.R.T., η οποία θα λειτουργεί ως κόμβος ενημέρωσης για κάθε πολίτη, με υλικό που σταδιακά θα ενισχύεται.

Κάθε πολίτης θα έχει πρόσβαση σε χρηστικές πληροφορίες είτε μέσα από το κεντρικό μενού «Ενημέρωση - Πρόληψη - Αντιμετώπιση» είτε επιλέγοντας την κατηγορία που τον χαρακτηρίζει: **Γονέας**, **Παιδί**, **Καταναλωτής**, **Απλός Χρήστης**, **Επιχείρηση**.

Η Ομάδα θα στελεχώνεται επίσης με έμπειρα στελέχη από το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος του Υπουργείου Δημόσιας Τάξης. Θα συνεργάζεται παράλληλα με οποιονδήποτε άλλο φορέα επιθυμεί να συνδράμει στο έργο της.

Πιο αναλυτικά, σκοπός της Ομάδας είναι η κατάρτιση προτάσεων για την πρόληψη και προστασία έναντι κινδύνων και απειλών σχετικών με τις νέες τεχνολογίες.

Συγκεκριμένα, η Ομάδα D.A.R.T. θα συντονίζει και θα υλοποιεί τους παρακάτω στόχους:

- Πρόληψη Ψηφιακών Κινδύνων και προτάσεις πολιτικής για την ασφάλεια
- Ενημέρωση για Ψηφιακούς Κινδύνους
- Ανταλλαγή τεχνογνωσίας με φορείς, εμπειρογνώμονες και οργανισμούς, ενώ οι δραστηριότητές της θα απευθύνονται σε όλους τους πολίτες της ελληνικής επικράτειας και τις ελληνικές επιχειρήσεις.

Στο πλαίσιο των ανωτέρω δράσεων, η Ομάδα D.A.R.T. θα λειτουργεί ως κεντρικό σημείο για την ενημέρωση πολιτών και επιχειρήσεων αναφορικά με ζητήματα αντιμετώπισης ψηφιακών κινδύνων και απειλών, αξιοποιώντας κάθε πρόσφορο μέσο. Θα ενημερώνει και θα παρέχει πληροφόρηση σχετικά με ζητήματα ψηφιακής ασφάλειας στο κοινό και σε δημόσιους, ιδιωτικούς και ανεξάρτητους φορείς που δραστηριοποιούνται σε θέματα Τεχνολογιών Πληροφορικής και Επικοινωνιών, με στόχο την ευαισθητοποίηση και τη συνειδητοποίηση των ψηφιακών κινδύνων.

Σημαντική δράση της Ομάδας θα αφορά στην επιμέλεια, συλλογή και διάχυση πληροφοριών μέσα από πολλαπλά δίκτυα για την αύξηση της συνειδητοποίησης των ζητημάτων ψηφιακής ασφάλειας.

Μεταξύ άλλων, η Ομάδα θα συνεργάζεται στενά με οργανώσεις και φορείς, θα διευκολύνει την επικοινωνία μεταξύ εμπειρογνωμόνων στους τομείς της ασφάλειας συστημάτων, θα συμμετέχει σε ερευνητικές δραστηριότητες, εγχώρια και διεθνή forum.

Βασικές δράσεις της Ομάδας αυτής θα είναι:

- να προτείνει πρακτικά μέτρα για την πρόληψη των ψηφιακών κινδύνων από πολίτες, επιχειρήσεις και δημόσιους φορείς,
- να αναπτύσσει τεχνικές που επιτρέπουν την αξιολόγηση και την πρόβλεψη πιθανών ψηφιακών απειλών,
- να ενημερώνει το ευρύ κοινό τακτικά σχετικά με την εξάπλωση ψηφιακών κινδύνων και τους τρόπους έγκαιρης αντιμετώπισης ψηφιακών απειλών και
- να καταρτίζει προτάσεις για την πρόληψη και προστασία έναντι ψηφιακών κινδύνων και απειλών.

5. Saferinternet (http://www.saferinternet.gr/

Μία ακόμη υπηρεσία που προσφέρεται με σκοπό την ενημέρωση για ασφαλέστερη χρήση του διαδικτύου, και την αντιμετώπιση των κινδύνων που ελλοχεύουν στο διαδίκτυο είναι η saferinternet . Η υπηρεσία αυτή αναλαμβάνει την ενημέρωση παιδιών, εφήβων και ενηλίκων για την κατάσταση που επικρατεί σήμερα στον κυβερνοχώρο και πραγματοποιεί διάφορες εκδηλώσεις, ομιλίες και προγράμματα σε σχολεία της χώρας.

2. Βιβλιογραφία – Πηγές :

Βιβλία:

- Εφαρμογές Πληροφορικής Α' Λυκείου
- Η Καινοτομία των Ερευνητικών Εργασιών στο Λύκειο (Ηλίας Γ. Ματσαγγούρας)

Εργασίες:

a. **Ασφάλεια στο Διαδίκτυο: Το αντίδοτο στην «Πληροφορύπανση»**
Α. Π. Λούβρης, Μ. Κοντογιώργης (Περιφερειακή Δ/νση Π/θμιας & Δ/θμιας Εκπ/σης Δυτ. Ελλάδας - Ίδρυμα Ιατροβιολογικών Ερευνών Ακαδημίας)

b. **Ασφάλεια στο Διαδίκτυο και σε άλλες Διαδραστικές Τεχνολογίες**
Ερευνητική Εργασία

Ιστοσελίδες:

- http://www.e-crime.gr
- http://www.astynomia.gr
- http://www.astynomia.gr/asfaliμgr.html
- http://internet-safety.sch.gr/
- http://www.cyberkid.gov.gr/
- http://www.saferinternet.gr
- http://ec.europa.eu/news/justice/120328_el.htm
- http://www.synigoroskatanaloti.gr/docs/info/info-Hlektroniko-Egklima.pdf
- https://www.edmodo.com/?language=el
- http://el.wikipedia.org/wiki/Facebook
- http://blogs.sch.gr/internet-safety
- http://sumstanvoi.blogspot.gr/
- https://dspace.lib.uom.gr/bitstream/2159/.../1/Hatzispyrou_Msc2010.pdf
- www.moneyguru.gr/analyseis/xeplima-vromikou-xrimatos-986
- http://ec.europa.eu/news/justice/120328_el.htm
- http://el.wikipedia.org/wiki/Phishing
- http://www.cnc.uom.gr/services/WEB_DECEPTION.pdf
- https://support.norton.com/sp/el/gr/home/current/solutions/v15610505_N360_N360SOS_2013_el_el
- https://support.google.com/chrome/answer/99020?hl=el
- http://windows.microsoft.com/el-gr/windows-vista/what-is-phishing
- http://blogs.sch.gr/internet-safety/archives/1099
- http://www.saferinternet.gr/index.php?childobjId=Category116&objId=Category37&parentobjId=Page2
- http://www.cnc.uom.gr/services/WEB_DECEPTION.pdf
- http://www.saferinternet.gr/index.php?childobjId=Category116&objId=Category37&parentobjId=Page2
- http://el.wikipedia.org/wiki/Phishing
- http://www.cnc.uom.gr/services/WEB_DECEPTION.pdf
- https://support.norton.com/sp/el/gr/home/current/solutions/v15610505_N360_N360SOS_2013_el_el
- https://support.google.com/chrome/answer/99020?hl=el
- http://windows.microsoft.com/el-gr/windows-vista/what-is-phishing
- http://blogs.sch.gr/internet-safety/archives/1099
- http://www.saferinternet.gr/index.php?childobjId=Category116&objId=Category37&parentobjId=Page2

3. Παράρτημα

Γλωσσάρι

Πρόγραμμα προστασίας από ιούς
Ένα πρόγραμμα σχεδιασμένο να αποτρέπει τα κακόβουλα προγράμματα από το να προσπελαύνουν το σύστημα, εντοπίζοντας τα αρχεία που έχουν προσβληθεί και διαγράφοντας ή καθαρίζοντάς τα.

Ιστολόγιο
Ένα ηλεκτρονικό ημερολόγιο, που δημοσιεύεται στο Διαδίκτυο.

Δωμάτιο συνομιλίας
Ένα φόρουμ συζήτησης σε πραγματικό χρόνο, όπου οι χρήστες γράφουν μηνύματα που εμφανίζονται απευθείας στην οθόνη, το ένα μετά το άλλο. Όταν γράφονται νέα μηνύματα αντικαθιστούν τα παλιά, έτσι ώστε να εμφανίζονται μόνο τα πιο πρόσφατα μηνύματα.

Προστασία δεδομένων
Μια σειρά κανονισμών που διασφαλίζουν ότι τηρείται το απόρρητο των πληροφοριών. Οι κανονισμοί προστασίας δεδομένων καλύπτουν απόρρητες πληροφορίες, όπως είναι τα προσωπικά στοιχεία και εφαρμόζονται μέσω της πολιτικής προστασίας των πληροφοριών ή της δήλωσης περί προστασίας του απορρήτου.

Φόρουμ συνομιλίας
Μια διαδικτυακή τοποθεσία συνομιλίας, συχνά με κάποιο συγκεκριμένο θέμα, όπου οι χρήστες μπορούν να δημοσιεύουν μηνύματα, με τη μορφή που καθορίζεται από τον πάροχο της υπηρεσίας. Ορισμένα φόρουμ συνομιλίας απαιτούν εγγραφή.
Ορισμένα φόρουμ περιέχουν αρχείο, στο οποίο ο χρήστης μπορεί να αναζητήσει κάποιο συγκεκριμένο θέμα. Ορισμένα φόρουμ είναι εποπτευόμενα. Αυτό σημαίνει ότι ο διαχειριστής του φόρουμ έχει το δικαίωμα να διαγράφει ή να τροποποιεί τα μηνύματα που δημοσιεύονται ή να αποκλείει τους χρήστες που συμπεριφέρονται ανάρμοστα.

Λήψη
Αποθήκευση αρχείων από το Διαδίκτυο στον υπολογιστή του χρήστη.

Τείχος προστασίας
Λογισμικό ή συσκευή που έχει σχεδιαστεί για να ελέγχει την επικοινωνία μεταξύ δικτύων ή μεταξύ του δικτύου και κάποιου μεμονωμένου συστήματος υπολογιστή. Για παράδειγμα, ένα τείχος προστασίας μπορεί να περιορίσει την κυκλοφορία δεδομένων με βάση προκαθορισμένους κανόνες, με βάση τους οποίους η επικοινωνία θα επιτρέπεται μόνον μεταξύ καθορισμένων διευθύνσεων.

Χάκερ, κράκερ
Κάποιο άτομο που παραβιάζει το δίκτυο ή σύστημα πληροφοριών μιας εταιρείας ή οργανισμού ή το χρησιμοποιεί χωρίς άδεια. Σημείωση: ο όρος "χάκερ" έχει κι άλλη έννοια: σημαίνει επίσης έναν πολύ ικανό χρήστη υπολογιστή.

Επικίνδυνα προγράμματα: Ιοί, Worm και Δούρειοι ίπποι
Ένα πρόγραμμα ή μέρος προγράμματος που προορίζεται να προκαλέσει προβλήματα σε έναν υπολογιστή ή υπολογιστικό σύστημα, όπως οι ιοί, τα worm ή οι δούρειοι ίπποι.

Ασφάλεια πληροφοριών
Μια πολιτική που εφαρμόζεται προκειμένου να διασφαλιστεί ότι οι κίνδυνοι για την ασφάλεια των πληροφοριών βρίσκονται υπό έλεγχο.

Ανεπιθύμητα ή ενοχλητικά μηνύματα ηλεκτρονικού ταχυδρομείου (spam)
Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου, που συνήθως στέλνονται για σκοπούς μάρκετινγκ. Τα ανεπιθύμητα μηνύματα σχεδόν πάντοτε στέλνονται σε μεγάλο αριθμό αποδεκτών συγχρόνως.

Ηλεκτρονική αλληλογραφία, ηλεκτρονικό ταχυδρομείο, μήνυμα
Ένα μήνυμα ηλεκτρονικού ταχυδρομείου. Η ηλεκτρονική μεταφορά κειμένου ή εικόνων μεταξύ διευθύνσεων εφαρμογών υπολογιστή

Λειτουργικό σύστημα
Ένα κεντρικό πρόγραμμα που λειτουργεί μεταξύ του υπολογιστή και των εφαρμογών λογισμικού. Το λειτουργικό σύστημα επιτρέπει στον υπολογιστή να ελέγχει να επιτηρεί και να χρησιμοποιεί το εγκατεστημένο λογισμικό. Τα συνηθέστερα λειτουργικά συστήματα είναι τα Microsoft® Windows®, Apple® Mac-OS και Linux®.

Αναδυόμενο παράθυρο
Ένα νέο παράθυρο που ανοίγει επάνω από το ενεργό παράθυρο του προγράμματος περιήγησης Διαδικτύου. Αυτό το παράθυρο συνήθως δεν διαθέτει δική του ηλεκτρονική διεύθυνση, σε ορισμένες περιπτώσεις, όμως, μπορεί να συμβαίνει κι αυτό. Τα αναδυόμενα παράθυρα που ανοίγουν χωρίς να το ζητήσει ο χρήστης συνήθως περιέχουν διαφημίσεις.

Διακομιστής
Ένα πρόγραμμα που διανέμει αρχεία στους υπολογιστές ενός δικτύου, με βάση προκαθορισμένους κανόνες. Για παράδειγμα, στο Διαδίκτυο, οι χρήστες λαμβάνουν τα μηνύματα ηλεκτρονικού ταχυδρομείου από το διακομιστή ηλεκτρονικού ταχυδρομείου του δικτύου. Διακομιστής συχνά λέγεται ο υπολογιστής όπου είναι εγκατεστημένο το πρόγραμμα διανομής.

Ιός
Ένα κακόβουλο πρόγραμμα λογισμικού που εξαπλώνεται αντιγράφοντας τον εαυτό του σε άλλα προγράμματα. Ένας ιός μπορεί να εξαπλωθεί μέσω αρχείων, ηλεκτρονικού ταχυδρομείου ή ιστοσελίδων. Ένας υπολογιστής μπορεί να προσβληθεί από ιό όταν ο χρήστης περιηγείται στο Διαδίκτυο ή ανοίξει κάποιο αρχείο συνημμένο σε μήνυμα ηλεκτρονικού ταχυδρομείου. Οι ιοί μπορούν να μειώσουν την ισχύ λειτουργίας του υπολογιστή ή του συστήματος.

Worm
Ένα κακόβουλο πρόγραμμα που μπορεί να εξαπλωθεί ανεξάρτητα, μέσω των δικτύων υπολογιστών. Τα worm μπορούν να εξαπλωθούν μέσω ηλεκτρονικού ταχυδρομείου ή μέσω των κενών στις λειτουργίες ασφάλειας πληροφοριών που ενδεχομένως να έχει το πρόγραμμα περιήγησης Διαδικτύου ή το λειτουργικό σύστημα. Ακόμα κι αν ο χρήστης δεν κάνει τίποτα, τα worm ενδεχομένως να προσπελάσουν τον απροστάτευτο υπολογιστή του όταν συνδεθεί στο Διαδίκτυο. Τα worm εμποδίζουν τη λειτουργία του συστήματος ή του υπολογιστή και ενδεχομένως να μεταφέρουν και άλλα κακόβουλα προγράμματα.