Τ.Ε.Ι. ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

(ΠΡΩΗΝ Δ.Ι.Κ.Σ.Ε.Ο)

Η ΑΣΦΑΛΗΣ ΧΡΗΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ – SAFERINTERNET.GR

Επώνυμο: Μαραβέγια **Κωτσέτα**

Όνομα: Αικατερίνη **Αναστασία**

Α.Μ.: 15654 **15641**

ΕΙΣΗΓΗΤΗΣ: ΤΣΟΥΡΑΜΑΝΗΣ ΧΡΉΣΤΟΣ

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Το διαδίκτυο είναι ένα παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών για να εξυπηρετεί εκατομμύρια χρήστες καθημερινά σε ολόκληρο τον κόσμο.
Σκοπός της εργασίας μας είναι να παρουσιάσουμε στο ευρύ κοινό την ασφαλή χρήση του διαδικτύου μέσω τριών ιστοσελίδων (site). Αυτά είναι το safeline, saferinternet.gr και το e-crime.

Η παρουσίαση χωρίζεται σε τρία κεφάλαια:

Στο πρώτο κεφάλαιο γίνεται λόγος για το saferinternet.gr και χωρίζεται σε τρείς υποενότητες:

Στο κεφάλαιο 1.1 αναφερόμαστε στο έργο του saferinternet.gr, στους κύριους στόχους της δράσης του και το συμβουλευτικό του όργανο.

Στο κεφάλαιο 1.2 αναφερόμαστε στο Δίκτυο Insafe, στην δημιουργία και διοργάνωση της Ημέρας Ασφαλούς Διαδικτύου καθώς και τους στόχους της.

Στο κεφάλαιο 1.3 αναφερόμαστε στις δραστηριότητες του saferinternet.gr και στις τρεις κατηγορίες του, που είναι οι μεγάλοι, οι έφηβοι και τα παιδιά.

Το δεύτερο κεφάλαιο αναφέρεται στο e-crime (ηλεκτρονικό έγκλημα) και χωρίζεται σε 4 υποενότητες:

Στο κεφάλαιο 2.1 αναφερόμαστε πρώτα στο τι είναι έγκλημα για την πλήρη κατανόηση του.
Στο κεφάλαιο 2.2 αναφερόμαστε στον ορισμό του ηλεκτρονικού εγκλήματος και την χρήση των ψηφιακών αποδείξεων.

Στο κεφάλαιο 2.3 αναφερόμαστε στα χαρακτηριστικά του ηλεκτρονικού εγκλήματος που το διαχωρίζουν από το παραδοσιακό έγκλημα.

Στο κεφάλαιο 2.4 αναφερόμαστε στις διάφορες μορφές ηλεκτρονικού εγκλήματος που υπάρχουν.

Στο κεφάλαιο 2.5 αναφερόμαστε στα μέτρα πρόληψης του διαδικτύου μέσω βασικών εννοιών που αφορούν την ασφάλεια και τις τακτικές αποφυγής θυματοποίησης με την χρήση του ηλεκτρονικού υπολογιστή.

Στο κεφάλαιο 2.6 αναφερόμαστε για το πώς μπορεί να γίνει η ασφαλής χρήση του διαδικτύου.

Στο κεφάλαιο 2.7 αναφερόμαστε στα βασικά προληπτικά εργαλεία και την λειτουργία τους.

Στο κεφάλαιο 2.8 αναφερόμαστε στην κρυπτογραφία και την ασφάλεια.

Στο κεφάλαιο 2.9 αναφερόμαστε στην πρόληψη για την ασφαλή χρήση του διαδικτύου μέσα από συμβουλές.

Στο κεφάλαιο 2.10 αναφερόμαστε στην εξακρίβωση της εισβολής και το πώς είναι δυνατό να γίνει η αποκατάσταση του συστήματος.

Το τρίτο κεφάλαιο αναφέρεται στο safeline.gr και χωρίζεται σε τρείς υποενότητες:

Στο κεφάλαιο 3.1 αναφερόμαστε σε μια μικρή ιστορική εξέλιξη του safeline.gr και στο πρωταρχικό μέλημα του που μας οδηγεί στο σκοπό του.

Στο κεφάλαιο 3.2 αναφερόμαστε στις παράνομες δραστηριότητες του διαδικτύου.

Στο κεφάλαιο 3.3 αναφερόμαστε στην καταγγελία και στην ανωνυμία κάθε χρήστη.

Στο τέταρτο κεφάλαιο γίνεται η σύγκριση και των τριών ιστοσελίδων (site) ανακαλύπτοντας στην πορεία ομοιότητες και διαφορές που υπάρχουν μεταξύ τους, όπως επίσης και πλεονεκτήματα μειονεκτήματα.

Στο πέμπτο κεφάλαιο παραθέτουμε τα συμπεράσματα μας για το Διαδίκτυο και για τις τρείς ιστοσελίδες (sites), που έχουν κυρίαρχο ρόλο στην εργασία μας διότι αποσκοπούν στην ασφαλή χρήση του διαδικτύου.

Φτάνοντας στο τέλος της παρουσίασης, παραθέτουμε σχεδιαγράμματα – γραφήματα, όπου σας δείχνουμε ορισμένα στατιστικά στοιχεία που αφορούν την κάθε ιστοσελίδα (site), καθώς και φωτογραφικό υλικό που παρατίθεται μέσα στο κύριο τμήμα της εργασίας.

ΚΕΦΑΛΑΙΟ 1^{Ο}

www.saferinternet.gr

Στο κεφάλαιο αυτό θα σας μιλήσουμε για τις δυνατότητες που έχει το saferinternet.gr, ποιός είναι ο σκοπός του και εν τέλει για ποιό λόγο θα έπρεπε οι χρήστες του διαδικτύου να το εμπιστεύονται και να το συμβουλεύονται μέσω της περιήγησης μας.

1.1 ΤΟ ΕΡΓΟ - ΟΙ ΚΥΡΙΟΙ ΣΤΟΧΟΙ ΔΡΑΣΗΣ ΤΟΥ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΕΥΤΙΚΟ ΟΡΓΑΝΟ

Η Δράση Ενημέρωσης Saferinternet.gr του Ελληνικού Κέντρου Ασφαλούς Διαδυκτύου και η εκστρατεία ενημέρωσης και επαγρύπνησης που φέρνεται εις πέρας στην χώρα τα από το 2004, πραγματοποιούνται υπό την αιγίδα τα Ευρωπαϊκής Επιτροπής στο πλαίσιο του προγράμματος Safer Internet.

Οι κύριοι στόχοι τα δράσης του είναι:

- Η προστασία των ανήλικων χρηστών του Διαδικτύου από ακατάλληλα ή επιζήμια συμπεριφόρα και περιεχόμενα.
- Η ενημέρωση των γονέων για τους τρόπους προστασιάς τους, αλλά και την επιτυχή ασφάλεια των παιδιών τους από τους κινδύνους που προκύπτουν λόγω της λάθος χρήσης των διαδραστικών τεχνολογιών (π.χ. Διαδίκτυο, κινητό τηλέφωνο).
- Η προώθηση των διαδραστικών τεχνολογιών.
- Η εκπαιδευση των εκπαιδευτικών για την ασφαλή χρήση του Διαδικτύου και του κινητού τηλεφώνου, πληροφορώντας τους για τα θετικά και τα αρνητικά, με αντίκτυπο τη δημιουργία πολλαπλασιαστικής δράσης μέσα στην τάξη.

- Η εμψύχωση του διαλόγου ανάμεσα στους ανήλικους και τους γονείς όσον αφορά την χρήση του Διαδικτύου την προώθηση του ψηφιακού αλφαβητισμού και της κριτικής σκέψης.
- Και η υποστήριξη γονέων, εκπαιδευτικών και ανήλικων χρηστών με το πρέπων ενημερωτικό υλικό.

Για την αποτελεσματική λειτουργία των στόχων που προαναφέρθηκαν, το Saferinternet.gr πραγματοποιεί μια σειρά δραστηριοτήτων, ενημερωτικές εκδηλώσεις, σεμινάρια, τηλεοπτικές και ραδιοφωνικές καμπάνιες, δημιουργία πολυμορφικού online και έντυπου ενημερωτικού υλικού κ.τ.λ. Επίσης, συνεργάζεται με αντιπροσώπους του κράτους, με την βιομηχανία των νέων τεχνολογιών, με Μη Κυβερνητικές Οργανώσεις στην Ελλάδα και το εξωτερικό με κύριο σκοπό την αποκατάσταση του ασφαλέστερου διαδικτυακού περιβάλλοντος

Το Συμβουλευτικό Όργανο του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου συγκροτείται από εκπροσώπους δημοσίων και ιδιωτικών φορέων που δραστηριοποιούνται στο πεδίο των νέων τεχνολογιών, της εκπαίδευσης, της έρευνας και των Μ.Μ.Ε.. Έχει ως στόχο να συμβουλεύει το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου, να προτάσσει νέες δραστηριότητες μέσα από την πείρα του και να δρα πολλαπλά μέσα από τα δικά του κανάλια πρόωθησης και ενημέρωσης. Μερικοί από τους φορείς που αποτελούν το Συμβουλευτικό Όργανο είναι το Πανελλήνιο Σχολικό Δίκτυο, ο Οργανισμός Πολιτισμού, Αθλητισμού και Νεολαίας του Δήμου Αθηναίων, η cosmote, η google κ.τ.λ.

1.2 ΤΟ ΔΙΚΤΥΟ INSAFE

Το Insafe είναι το Πανευρωπαϊκό Δίκτυο Εθνικών Κέντρων Ενημέρωσης και Επαγρύπνησης για ένα ασφαλέστερο διαδίκτυο, στο πλαίσιο Safer Internet της Ε.Ε..
Οργανώνει από κοντά τις συναντήσεις των μελών του σε καθορισμένα χρονικά διαστήματα, όπου ανταλλάσσονται απόψεις και αποφασίζονται μελλοντικές δράσεις του Δικτύου. Επιπλέον, μέσω αρμόδιων ομάδων εργασίας, αλλά και ειδικής online πλατφόρμας, ανταλλάσσονται διαρκώς εμπειρίες, άριστες πρακτικές και ενημερωτικό υλικό.

1.3 ΗΜΕΡΑ ΑΣΦΑΛΟΥΣ ΔΙΑΔΙΚΤΥΟΥ

Η δράση Saferinternet.gr κανονίζει και διοργανώνει σε ετήσια βάση όλες τις επίσημες εθνικές εκδηλωσεις για την « Ημέρα Ασφαλούς Διαδικτύου » (Safer Internet Day), ως ο αντιπρόσωπος του Δικτύου Insafe και ως ο μοναδικός διοργανωτής της Ημέρας Ασφαλούς Διαδικτύου σε παγκόσμιο επίπεδο.

Η Ημέρα Ασφαλούς Διαδικτύου έχει ως στόχο:

- Να ευαισθητοποιήσει όλους τους αναμεμιγμένους αναφορικά με την προώθηση ενός ασφάλεστερου διαδικτύου για τα παιδιά μας.
- Να κινητοποιήσει όλους (μικρούς και μεγάλους) γύρω από την ασφάλεια του διαδικτύου, πληροφορώντας για τη σημασία και τα συμφέροντα που πηγάζουν από μια σωστή και υπεύθυνη χρήση του μέσου.
- Να παροτρύνει το ενδιαφέρον της Πολιτείας και των Μ.Μ.Ε., ως σημαντικούς πυλώνες στη σωστή ενημέρωση, ευαισθητοποίηση και εκπαίδευση.
- Να δραστηριοποιήσει όλους τους φορείς (σχολεία, δημοτικές αρχές, κέντρα νέων εταιρίες κ.τ.λ.)

- Να δράσουν ως « Πρεσβευτές » της ημέρας αυτής, μεταδίδοντας και αυξάνοντας κατά ποσότητα τα μηνύματα της.
- Και να πληροφορήσει το κοινό για τις απόπειρες της Ευρωπαϊκής Επιτροπής σχετικά με την προστασία των ανηλίκων στο διαδίκτυο και την αντιμετώπιση του απρεπούς και έκνομου διαδικτυακού περιεχομένου.

Στο πλαίσιο του έργου της παίρνει μέρος σε δραστηριότητες εθνικής αλλά και διεθνούς εμβέλειας που αποσκοπούν στη δημιουργία πολλαπλής δράσης των στόχων της, όπως σε συνέδρια, ημερίδες και workshops στην Ελλάδα και το εξωτερικό. Επίσης, υποστηρίζει ενεργά δράσεις μη κερδοσκοπικών φορέων που έχουν να κάνουν με την ισχυροποίηση των ανήλικων σχετικά με την σωστή και ασφαλή χρήση του διαδικτύου, επομένως συμφωνούν με την φιλοσοφία του προγράμματος Safer Internet της Ευρωπαϊκής Επιτροπής.

1.4 ΟΙ ΤΡΕΙΣ ΜΕΓΑΛΕΣ ΚΑΤΗΓΟΡΙΕΣ

Στην ιστοσελίδα αυτή υπάρχουν τρείς κατηγορίες, που είναι οι μεγάλοι, οι έφηβοι και τα παιδιά. Σε κάθε κατηγορία γίνεται πλήρης αναφορά ως προς την προστασία και την ασφαλέστερη πλοήγηση στο διαδίκτυο, με την διαφορά ότι κάθε κατηγορία έχει την ιδιαιτερότητα της.

ΜΕΓΑΛΟΙ

Η ενότητα αυτή απευθύνεται σε εκπαιδευτικούς, σε γονείς και σε ενήλικους που επιζητούν να μάθουν πολάκεις πληροφορίες για την δυνατότερη αντιμετώπιση των προκλήσεων του ψηφιακού κόσμου.

Υπάρχουν κάποιες επιμέρους θεματικές ενότητες που αναφέρονται στις διάφορες πτυχές του διαδικτύου για την ασφαλέστερη χρήση τους.

Ως πρώτη θεματική ενότητα, είναι η επικοινωνία και η ιδιωτικότητα, στην οποία υπάγονται κάποιες μορφές επικοινωνίας που παρέχονται από το διαδίκτυο. Όπως, επίσης παρέχονται οι προκλήσεις όσον αφορά σε σχέση με την ιδωτική ζωή του ατόμου, αλλά και σε σχέση με την ασφάλεια των ανήλικων χρηστών.

Έτσι, η πρώτη μορφή επικονωνίας είναι τα chat / άμεσα μηνύματα, όπου προσφέρει απευθείας επικοινωνία σε πραγματικό χρόνο, διότι είναι εικονικά μέρη στα όποια μπορούν να « συναντηθούν » και να « συζητήσουν », μέσω μηνυμάτων που γράφουν στο πληκτρολόγιο τους. Όμως, τα άμεσα μηνύματα ανταλλαγής μέσω προγραμμάτων « Instant Messaging Programs » παίρνουν και αυτά το ρόλο τους, καθώς τους δείνεται η δυνατότητα να γνωρίζουν πότε συνδέεται ο χρήστης που θέλουν να καλέσουν σε συνομιλία.

Μολοταύτα, η μορφή αυτής της επικοινωνίας μπορεί να αποβεί επικίνδυνη, καθώς μπορεί να υπάρξει grooming /αποπλάνηση, γιατί δεν μπορεί να ξέρει ένας συνομιλήτής εάν αυτός στον οποίο απευθύνεται του έχει δώσει τα αληθή στοιχεία και όχι τα ψευδή. Μια τέτοια κίνηση θα την έκανε ένας παιδόφιλος, όπου θα μπορούσε να έχει συνομιλίες με τα υποψήφια θύματα του, δίνοντας του την ευκαιρία να τα εξοικειώση μέσω αυτών των συζητήσεων για τις σεξουαλικές του προτιμήσεις και με φωτογραφίες πορνογραφικού υλικού (παιδιών και ενηλίκων), έτσι ώστε να μην επιζητήσουν την προστασία των γονιών τους ή και από τον δάσκαλο κάθως πλέον θα αισθάνονται ένοχα λόγω των ανταλλαγών και συνομιλιών που είχαν προηγηθεί.
Στη συνέχεια, εκτός από την αποπλάνηση, υπάρχει και η παρενόχληση, όπου κάποιος μπορεί να επιχειρήσει να ενοχλήσει, να κοροιδέψει, να προσβάλλει ένα παιδί ή και ακόμα να απειλήσει.
Εν τέλει, φτάνουμε στα προσωπικά δεδομένα, όπου μπορούν να δοθούν μέσω της συνομιλίας chat room προσωπικά στοιχεία ενός ατόμου (παιδιού, μεγάλου) με αποτέλεσμα να είναι ευκολότερος ο εντοπισμός του στον πραγματικό κόσμο ή και να γίνει δέκτης παραπλανητικών διαφημίσεων.

Ύστερα, ως δεύτερη μορφή είναι η κοινωνική δικτύωση ή « social networking sites », όπου στις ιστοσελίδες αυτές χρήστες διαφόρων ηλικιών μέσα από τα εικονικά προφίλ τους, τους δίνεται η δυνατότητα να δημιουργούν οι ίδιοι χωρίς εξειδικευμένες τεχνικές γνώσεις περιεχόμενο στο διαδίκτυο (ομάδες κονωνικών ενδιαφερόντων, δημοσίευση φωτογραφιών και βίντεο κ.τ.λ.) και να το μοιράζονται με άλλους χρήστες
Όσον αφορά τα προσωπικά δεδομένα οι περισσότεροι νεαροί χρήστες δεν δίνουν βάση και δεν διαβάζουν τους « Όρους Χρήσης » και την « Πολιτική Απορρήτου » για να διαπιστώσουν εάν όντος τα στοιχεία τους παραμένουν ιδιωτικά ή όχι στους εικονικούς κόσμους όπου πλοηγούνται.
Στη συνέχεια, η αποπλάνηση ανηλίκων στις σελίδες κοινωνικής δικτύωσης με βάση την ανωνυμία που παρέχεται στους χρήστες μπορεί να είναι επιζήμια στα παιδιά με αντίκτυπο το λεγόμενο « grooming », να είναι ένας μεγάλος κίνδυνος, καθώς οι τρόποι επιστράτευσης είναι πολλαπλοί.
Προχωρόντας παρακάτω, η παρενόχληση / κλοπή ταυτότητας στην μορφή αυτή είναι πιο έντονη, καθώς γίνεται δημόσια ενώπιον του δικτύου των φίλων

του θύματος και όχι μόνο. Έχει υπάρξει όμως και κλοπή ταυτότητας με σκοπό την προσβολή ή και την γελοιοποίηση άλλων ατόμων ή και γνωστών εταιριών με σκοπό το κέρδος από την επωφελής χρησιμοποίηση της φήμης τους.
Παρατηρούμε, ότι οι φωτογραφίες είναι πιο επικύνδυνες στα εικονικά προφίλ καθώς υπάρχουν τα λεγόμενα tags με τα οποία γίνεται η ανεπιθύμητη διασύνδεση των φωτογραφίων με προσωπικά δεδομένα και όχι πάντα με την εξουσιοδότηση του κάθε χρήστη.
Τέλος, η μορφή αυτή κλείνει με το spam / phising / ιοί, όπου ένα άτομο με την εγγραφή του σε μια σελίδα ή σε ένα group δίνει το δικαίωμα να υπάρχουν σχόλια διαφημιστικού περιεχομένου ή σύνδεσμοι προς ιστοσελίδες με πορνογραφικό υλικό στο προφίλ του από διάφορους μηχανισμούς.

Η τρίτη μορφή αφορά την αποπλάνηση ανηλίκου, δηλαδή το λεγόμενο grooming που έχουμε αναφερθεί για αυτό στις προηγούμενες θεματικές ενότητες. Εδώ, θα δώσουμε τον κύριο τελικό ορισμό του grooming, που είναι η διαδικασία κατά την οποία, παιδόφιλοι παριστάνοντας τους έφηβους μέσω των διάφορων μορφών επικοινωνίας (chat rooms) έχουν σκοπό να προσελκύσουν τα παιδία με μοναδικό αποτέλεσμα να τα κακοποιήσουν.

Η τέταρτη μορφή αναφέρεται στην ηλεκτρονική παρενόχληση, δηλαδή την βίαιη συμπεριφορά με τη χρήση ηλεκτρονικών μέσων, δημιουργώντας εσκεμμένα ανασφάλεια, φόβο, μοναξιά, έλλειψη εμπιστοσύνης στον εαυτό τους, απομόνωση από τον έξω κόσμο και στο τέλος μπορεί και αυτοκτονία. Τα είδη ηλεκτρονικής παρενόχλησης είναι πολλαπλά, όπως μέσω μηνυμάτων, ανάρτηση κοροϊδευτικών ή και προσβλητικών φωτογραφιών, βίντεο και άλλων υλικών σε ιστοσελίδες, η διάδοση κακόβουλων φημών στο περιβάλλον του θύματος μέσω κινητού, ηλεκτρονικού ταχυδρομείου (e-mail) και μέσω διάφορων μορφών ηλεκτρονικής επικοινωνίας και κλοπή ταυτότητας.

Η πέμπτη μορφή μας παραθέτει τον ορισμό της λέξης « Netiqutte » (Network Etiquette). Είναι ένα σύνολο κανόνων για την ειρηνική και φιλική συμβίωση στους πλασματικούς κόσμους. Μερικοί από τους βασικούς κανόνες είναι ο σεβασμός στον ιδιωτικό χώρο των άλλων, η αποφυγή της δημοσίευσης της διεύθυνσης κάθε παραλήπτη σε άλλους χρησιμοποιόντας στο e-mail το bcc (

blind carbon copy, κρυμμένο αντίγραφο), η αποστολή junk ή spam απαγορεύεται κ.τ.λ.

Στην έκτη μορφή γίνεται λόγος για την ηλεκτρονική γλώσσα των νέων, δηλαδή το λεγόμενο greeklish, που μπορεί να είναι ορθογραφικά σωστά ακολουθώντας τους κανόνες της ελληνικής ορθογραφίας, όπως είναι στο πληκτρολόγιο ή φωνητικά όπου έχουν ως σκοπό στην φωνητική απόδοση των ελληνικών. Υπάρχουν βέβαια και τα λεγόμενα ακρώνυμα, δηλαδή συντομογραφίες στην αγγλική γλώσσα και τα emoticons που χρησιμοποιούνται για οποιοδήποτε σημαντικό συναίσθημα.

Τέλος, ως έβδομη εδώ μορφή είναι το google yourself, όπου γίνεται λόγος ότι εάν πάμε στην μηχανή αναζήτησης του google και πληκτρολογίσουμε το ονοματεπώνυμο μας θα ανακαλύψουμε με λίγη υπομονή πως υπάρχουν στο internet προσωπικά στοίχεια μας και πως εάν δεν πάρουμε τα κατάλληλα μέτρα προστασίας μπορεί να χρησιμοποιηθούν κακόβουλα εναντίον μας.

Η δεύτερη θεματική ενότητα έχει να κάνει με την πληροφορία στο διαδίκτυο, όπου μπορούμε εύκολα και γρήγορα να ανακτύσουμε οποιαδήποτε πληροφορία μας ενδιαφέρει να μάθουμε. Όμως, για να ξέρουμε εάν οι πληροφόριες που αναζητούμε είναι αξιόπιστες πρέπει να είναι εξαιρετικά εύστοχες. Μπορούμε, επίσης να αναζητήσουμε και χρήσιμο υλικό (βιβλία, άρθρα). Όμως, στην αναζήτηση βιβλίων ή και άρθρων υπάρχει η πνευματική ιδιοκτησία για την προστασία της γνήσιας εργασίας των συντακτών, συγγραφέων κ.τ.λ. Τέλος, τα λεγόμενα blogs (ιστολόγια) είναι πλασματικά σημειωματάρια που δημιουργούνται στο διαδίκτυο εύκολα και ταχύτατα από οποιονδήποτε χρήστη καθώς δεν χρειάζονται πλήρης και έμπειρες γνώσεις.

Η τρίτη θεματική ενότητα αναφέρεται στα παιχνίδια και στην διασκέδαση. Ειδικότερα δίνεται βάση στα ηλεκτρονικά παιχνίδια που μπορεί να είναι μέσω παιχνιδομηχανών (κονσόλες), μέσω φορητών συσκευών ή και online μέσω του διαδικτύου. Αυτό γιατί όλο και πιο πολύ

στην σημερινή εποχή κάθε είδος παιχνιδιού, κυριότερα τα online παιχνιδία γίνονται περισσότερο δημοφιλή και παρατηρούνται οι εξής μορφές, που είναι τα παιχνίδια browser, διαφημιστικά, δικτύου και MMORPG (Massively Multiplayer Online Role Playing Games). Τα προβλήματα που ενδέχεται να προκύψουν είναι η διαταραχή συμπεριφοράς, η υπερβολική ενασχόληση, δηλαδή ο εθισμός, η διαδραστικότητα, η έκθεση σε διαφημιστικό υλικό και το ακατάλληλο περιεχόμενο Ύστερα, είναι το φαίνομενο του τζόγου στο διαδίκτυο, όπου γίνονται στοιχήματα με σκοπό την απόκτηση χρημάτων ανάμεσα σε δύο άτομα ή και σε μια μεγάλη ομάδα ατόμων. Το βασικότερο και μοναδικό πρόβλημα είναι ο κίνδυνος και ο φόβος της χρηματικής απώλειας με αποτέλεσμα να χάσει κάνεις όλα τα περουσιακά του στοιχεία. Τέλος, δίνονται ορισμένες ιστοσελίδες ψυχαγωγίας και μάθησης, όπου οι γονείς μαζί με τα παιδιά τους μπορούν να χρησιμοποιήσουν την ψυχαγωγική πλευρά του διαδικτύου σωστά και με ασφάλεια. Μερικές από αυτές τις ιστοσελίδες είναι η εγκυκλοπαίδεια μείζονος ελληνισμού, national geographic for kids, η Βουλή για τα παιδιά, ΕΡΤ – οπτικοακουστικά στοιχεία κ.τ.λ.

Η τέταρτη θεματική ενότητα αφορά την υπερβολική ενασχόληση. Οι γονείς υποδέχτηκαν το διαδίκτυο μέσα στα σπίτια τους με σκοπό ότι θα άνοιγε νέους ορίζοντες και γνώσεις στα παιδιά τους μολονότι προσφέρε το ακριβώς αντίθετο. Αντί να ασχολούνται με την μαθησιακή γνώση και έρευνα έδιναν βάση σε ηλεκτρονικές συνομιλίες με τους φίλους τους παίζοντας παιχνίδα ή μιλώντας με αγνώστους σε chat rooms. Είναι σημαντικό να αναφέρουμε πως ως πρώτη εμφάνιση και περίπτωση του φαινομένου του « εθισμού » έλαβε χώρα στις Η.Π.Α. το 1997 και το πρώτο κέντρο απεξάρτησης ιδρύθηκε και λειτούργησε το 1995 στην Πενσυλβάνια των Η.Π.Α.

Η πέμπτη θεματική ενότητα μιλάει για το επιβλαβές περιεχόμενο που κάνει την εμφάνιση του στο κυβερνοχώρο. Τα πιο σοβαρά είδη ακατάλληλου, κακόβουλου ή παράνομου περιεχομένου είναι τα σεξουαλικής φύσεως περιεχόμενα (παράνομη παιδική πορνογραφία ή και νόμιμη πορνογραφία ενηλίκων), η ανορεξία – παρότρυνση σε αυτοκτονία, η βία, ο ρατσισμός, η ξενοφοβία και το παράνομο περιεχόμενο, όπου είναι τα είδη που μόλις προαναφέρθηκαν αλλά και το οικονομικό έγκλημα, απάτες, το hacking,

cracking, ο εκφοβισμός, η εξύβριση, συκοφαντική δυσφήμιση και η παραβίαση προσωπικών δεδομένων, πνευματικής ιδιοκτησίας και απορρήτου των επικοινωνιών. Ως βοήθεια σε όλα αυτά είναι τα φίλτρα – εργαλεία γονικού ελέγχου. Είναι προγράμματα που ρυθμίζουν την πρόσβαση σε πληροφορίες ή υπηρεσίες στο διαδίκτυο σύμφωνα με συγκεκριμένα κριτήρια εγκαθυστόντας τα σε οποιονδήποτε υπολογιστή που μπορεί να είναι του χρήστη, σε κεντρικό υπολογιστή ενός συγκεκριμένου φορέα ή σε υπηρεσίες που παρέχει το διαδίκτυο. Τα κριτήρια μπορούν να προειδοποιήσουν για προβληματικές σελίδες, να καταγράψουν λεπτομερώς τις κινήσεις ενός χρήστη στο διαδίκτυο, να μπλοκάρουν ύποπτους ιστοχώρους, να επηρεάσουν την πρόσβαση συγκεκριμένες ώρες και ημέρες άκομα και να κλείσουν τελείως τον υπολογιστή.

Η έκτη θεματική ενότητα αφορά της ηλεκτρονικές συναλλαγές που μπορεί να γίνουν με το δημόσιο, με τις τράπεζες ή και με τις επιχειρήσεις. Επικρατεί η απόψη όμως ότι οι συναλλαγές αυτές μόνο προβλήματα μπορεί να δημιουργήσουν παρά να βοηθήσουν. Αυτό όμως δεν ίσχυει στην περίπτωση που δίνονται σημαντικές πληροφορίες, όπως και συμβαίνει, για την αναγνώριση των αξιόπιστων σελίδων που αφορούν τις ηλεκτρονικές συναλλαγές, αλλά και για την προσοχή σε ορισμένα σημεία ώστε να μην υπάρξουν στενάχωρες εκπλήξεις. Οι πληροφορίες αυτές έχουν να κάνουν με τις ασφαλείς συναλλαγές, όπου γίνεται έλεγχος κάποιων στοιχείων (ασφαλής τρόπος πληρωμής, πολιτική απορρήτου, εξακρίβωση όλων των στοιχείων της εταιρίας κ.τ.λ.) για την εγκυρότητα της σελίδας, με τις ηλεκτρονικές απάτες, όπου υπάρχουν οι πιο διαδεδομένες ηλεκτρονικές μορφές οικονομικής εξαπάτησης που είναι το phising (ψάρεμα προσωπικών δεδομένων και ιδιαίτερα των οικονομικών συναλλαγών), το pharming (αυταπάτη ότι βρίσκονται σε γνήσια ιστοσελίδα, ενώ είναι σε ψεύτικη που είναι ακριβώς ίδια με την γνήσια) και τα scams (απάτες με σκοπό το θύμα – παραλήπτης να πρέπει να πληρώσει για να ολοκληρωθεί η συναλλαγή χωρίς στο τέλος

να αποκτά τα προσφερόμενα ανταλλάγματα), και με τις διαφημίσεις στο διαδίκτυο, καθώς στον κυβερνοχώρο όλο και πίο πολύ είναι μια κερδοφορία επιτυχημένη για πολλάκεις εταιρίες, διότι κερδίζει μεγάλο έδαφος σε αντίθεση με τις παραδοσιακές μεθόδους.

Η έβδομη θεματική ενότητα αναφέρεται στο κινητό τηλέφωνο. Είναι ιδιαίτερα ελκυστικό προς τα παιδιά σε σχέση με τον ηλεκτρονικό υπολογιστή που τον θεωρούν πλέον παραδοσιακό και παλιομοδίτικο, γιατί τους παρέχει περισσότερη προσωπική και ιδωτική φύση, δηλαδή η δυνατότητα ελέγχου από τους γονείς καθιστάται σχεδόν αδύνατη. Μέσω όμως, της κινητής τηλεφωνίας είναι αναμενόμενο ότι μπορεί να υπάρχει ακατάλληλο ή παράνομο υλικό (πορνογραφικό υλικό), επικίνδυνες επαφές και παρενόχληση (με μηνύματα ή και με συνομιλίες chat συνδεόμενοι στο internet από το κινητό), κλοπή κινητού τηλεφώνου, φωτογραφίες, προηγμένες υπηρεσίες / διαφημιστικό υλικό (παίρνουν μέρος σε παιχνίδια, κουίζ, διαγωνισμούς και άλλες νέες εφαρμογές προσιτές προς τα παιδιά – νέους) και η υπεύθυνη χρήση του κινητού.

Τέλος, η όγδοη θεματική ενότητα αφορά τα τεχνικά θέματα.
Γίνεται ο διαχωρισμός δύο εννοιών, πρώτον το safety είναι η ασφάλεια του χρήστη στο διαδίκτυο και δεύτερον το security είναι τα τεχνικά προβλήματα που μπορεί να αντιμετωπίσει ένας ηλεκτρονικός υπολογιστής.

Υπάρχει όμως και μια τρίτη έννοια, αυτή του βλαβερού λογισμικού, δηλαδή αναφέρεται σε λογισμικό και σε προγράμματα που περιλαμβάνουν τους ιούς - viruses (προγράμματα που εισβάλλουν στον υπολογιστή και φτιάχνουν ανεπιθύμητες παρενέργειες), τα σκουλήκια - worms (ιοί που αναπλάθωνται δημιουργώντας αντίγραφα του εαυτού τους μέσω των δικτύων ηλεκτρονικών υπολογιστών), οι δούρειοι ίπποι – trojan horse (προγράμματα που μπορούν να προκαλέσουν αρκετές βλάβες) και τα spyware (προγράμματα που κολλάνε κρυφά σε αρχεία που κατεβάζουμε από το διαδίκτυο). Για αυτό το λόγο και για την αποφυγή όσον προαναφέραμε δίνονται οδηγοί που βοηθούν για την ασφαλή χρήση και πλοήγηση του διαδικτύου.

ΕΦΗΒΟΙ

Η ενότητα αυτή είναι ειδικά αφιερωμένη στους νέους και παρέχει πληροφορίες για θέματα που αφορούν την τεχνολογία στις μέρες μας, χρήσιμες συμβουλές για διάφορα προβλήματα που μπορεί να αντιμετωπίζουν, αλλά και ενδιαφέρουσες πληροφορίες για το διαδίκτυο που μπορεί να μην ξέρουν. Αυτές τις πληροφορίες θα τις ανακαλύψουμε μέσω των θεματικών ενοτήτων που θα παραθέσουμε και θα αναλύσουμε σε αυτήν την ενότητα.

Ως πρώτη θεματική ενότητα είναι το gaming and sharing. Βλέπουμε πρώτα τα είδη των παιχνιδιών.
Είναι τα online παιχνίδια (stand – alone, local and wide network games, δηλαδή παιχνίδια τοπικού δικτύου κ.τ.λ.) και τα offline παιχνίδια (αθλήματα, δράσης, πάλης, στρατηγικής κ.τ.λ.).
Μετά γίνεται λόγος για τις ταινίες και την μουσική, όπου οι νέοι μέσω του διαδικτύου μπορούν και κατεβάζουν εύκολα και γρήγορα χωρίς να ξέρουν ότι υπάρχουν και οι ανάλογες επιπτώσεις, καθώς αυτή η χρήση του διαδικτύου είναι παράνομη. Οι επιπτώσεις αυτές μπορεί να οδηγήσουν σε ποινικές διώξεις και σε φυλάκιση, με βάση το πόσο μεγάλα είναι τα αρχεία που κυκλοφόρησαν για ένα εκτενές χρονικό διάστημα, το κίνητρο για κέρδος κ.τ.λ. Αξίζει να σημειωθεί ότι διαφέρουν οι επιπτώσεις των παραβιάσεων και οι νόμοι περί πνευματικής ιδιοκτησίας από χώρα σε χώρα.

Ως δεύτερη θεματική ενότητα είναι η παρενόχληση.

Έχει γίνει αναφορά στην ενότητα των μεγάλων, εδώ ομώς θα αναφέρουμε δύο άλλες πτυχές της παρενόχλησης που είναι η κλοπή ταυτότητας και ο ρατσισμός – λογοκρισία στο διαδίκτυο. Η κλοπή ταυτότητας στον διαδικτυακό χώρο ονομάζεται η πρακτική του να χρησιμοποιεί ένα άτομο την εικονική ταυτότητα ενός άλλου ατόμου εκμεταλλεύοντας τα στοιχεία του για να έχει πρόσβαση σε διάφορες

διαδικτυακές υπηρεσίες, με σκοπό την οικονομική εξαπάτηση, τον εξευτελισμό ή και την διάδοση φημών στο διαδικτυακό περιβάλλον του ατόμου. Όσον αφορά το ρατσισμό και την λογοκρισία στο διαδίκτυο περισσότερο παραμονεύει το φαινόμενο της λογοκρισίας, διότι ξεκινά από την πλήρη απαγόρευση των διαδικτυακών τόπων με βάση το θέμα τους και φτάνει μέχρι τον αποκλεισμό επιλεγμένου περιεχομένου.Εν ολίγοις, ακόμα και εάν τίθεται αυστηρά με τις καλύτερες προθέσεις έχει ως αντίκτυπο νέους πιο επίπονους και άσχημους περιορισμούς στην ελευθερία της βούλησης και της έκφρασης.

Ως τρίτη θεματική ενότητα είναι οι πληροφορίες που εκτυλίσονται στην εκπαίδευση και την διασκέδαση. Δίνεται για αρχή η αξιοπιστία των πληροφοριών που συναντάμε στο διαδίκτυο, δηλαδή η ιδιότητα του να διασταυρώνουμαι τις πληροφορίες που συναντάμε στο διαδίκτυο με άλλες πηγές, ώστε να ανακαλύψουμε την εγκυρότητα τους. Μετά είναι τα blogs ή αλλιώς ιστολόγια (βλέπε σελίδα), τα χρήσιμα links που προτείνονται για περιήγηση για όποιον ενδιαφέρεται (σπουδαστήριο του νέου ελληνισμού, εθνική βιβλιοθήκη της Ελλάδας, κέντρο ελληνικής γλώσσας κ.τ.λ.), και η πνευματική ιδιοκτησία που αποτελεί μια μορφή προστασίας που παρέχεται από τον νόμο στους συντάκτες και τους δημιουργούς γνήσιας εργασίας.

Ως τέταρτη θεματική ενότητα είναι οι αγορές που μας εξηγούν πώς να μην πιανομάστε κορόιδα από τις απάτες – μηνύματα που έχουν ως σκοπό να αποσπάσουν χρήματα και στοιχεία τραπεζικών λογαριασμών από τα υποψήφια θύματα που είναι γνωστά ως phising και scams, όπως και η άλλη μορφή απάτης το social networking phising. Για τις απάτες που μόλις αναφέραμε συνοπτικά αλλά και η διαφήμιση έχουν αναφερθεί προηγουμένος στην ενότητα των μεγάλων (βλέπε σελίδα 16 – 17).

Η πέμπτη, η έκτη και η έβδομη θεματική ενότητα, δηλαδή η επικοινωνία, τα τεχνικά θέματα και το κινητό τηλέφωνο έχουν αναλυθεί πλήρως και αυτά στην ενότητα των μεγάλων.

Τέλος, όσον αφορά την ασφάλεια σας εάν νιώθετε άβολα, σοκαρισμένα ή προσβεβλημένα μπορείτε να κάνετε καταγγελία στη Safeline με μήνυμα, με

ηλεκτρονική κατάθεση, με το ταχυδρομείο ή το ηλεκτρονικό ταχυδρομείο, και τηλεφωνικά. Εάν από την άλλη χρείαζεσται βοήθεια μπορείτε να καλέσετε στην γραμμή βοήθειας Υποστηρίζω χωρίς χρέωση που είναι ειδικά αφιερωμένη στους έφηβους.

ΠΑΙΔΙΑ

Η ενότητα αυτή μας καλοσωρίζει στο νησί του saferinternet.gr. Τα παιδιά εδώ πρέπει να ανακαλύψουν όλες τις πληροφορίες που είναι κρυμμένες μέσα στο νησί που αναφέρονται στους καλούς τρόπους, στο κινητό τηλέφωνο, στους « κακούς » του διαδικτύου, στην επικοινωνία, στην καταγγελία και στην βοήθεια. Ύστερα, αφού μελετήσουν προσεκτικά τις πληροφορίες τους δίνεται η δυνατότητα να πάνε με ένα κλικ μέσα στο νησί και να απαντήσουν στα τέσσερα πρώτα κουίζ που έχουν κάνουν με το netiquette, το κινητό, τις γενικές γνώσεις και το chat. Εάν απαντήσουν σε όλα σωστά κερδίζουν τα διπλώματα του καλού θαλασσοπόρου του saferinternet.gr και τους δίνεται η ευκαιρία να σερφάρουν ελεύθερα με ασφάλεια στο διαδικτυακό πέλαγος.

Υπάρχουν όμως και άλλες δραστηριότητες μέσα στο νησί, όπως το eSafetyKit, δηλαδή παίζουν και μαθαίνουν συγχρόνως πώς είναι να είναι συνδεδεμένοι στο διαδίκτυο ή αλλιώς online, το ιντερνετοδάσος που στοχεύει στην προώθηση των δικαιωμάτων των παιδιών και της προστασίας τους από κάθε είδους βία, τα παιχνίδια που μπορεί να είναι διαφόρων ειδών, όπως κρυπτόλεξο, λαβύρινθος, βρες τις διαφορές, ένωσε τις τελίτσες κ.τ.λ. και οι χειροτεχνίες, όπως ένας ανεμόμυλος, ένα ταμπελάκι για πόρτα και δύο σελιδοδείκτες.

ΚΕΦΑΛΑΙΟ 2^{Ο}

E - CRIME

Σε αυτό το κεφαλαίο θα αναλυθεί το εγκληματικό φαινόμενο. Στη συνέχεια θα αναφερθούμε στην έννοια του διαδικτύου και πως η είσοδος του στην καθημερινότητα μας έχει φέρει τεράστιες αλλαγές με αποτέλεσμα να υπάρχουν πολλά πλεονεκτήματα και μειονεκτήματα. Τέλος η αναφορά γίνεται στη νέα μορφή προβατικής συμπεριφοράς που καλείται «ηλεκτρονικό» ή αλλιώς «ψηφιακό» έγκλημα. Παρατίθενται ιστορικά στοιχεία καθώς και τα κυριότερα χαρακτηριστικά του.

2.1 ΤΙ ΕΙΝΑΙ ΕΓΚΛΗΜΑ

Το έγκλημα έχει φύση σύνθετη, γιατί σε αυτήν συναντώνται και την καθορίζουν από τη μια μεριά η κοινωνική, βιολογική και ψυχολογική πραγματικότητα του ανθρώπου και από την άλλη η δεοντολογία που διέπει στο πλαίσιο ορισμένης κοινωνικής συμπεριφορά του. Έτσι το έγκλημα είναι αξεχώριστα τόσο ως οντολογικό όσο και ως αξιολογικό φαινόμενο. Δεν είναι ούτε μόνο το ένα ούτε μόνο το άλλο. Η σύνθετη φύση του εγκλήματος μπορεί να αποδοθεί από τον χαρακτηρισμό του, ως ορισμένου αρνητικά αξιολογούμενου φαινομένου της πραγματικότητας.

Μολοταύτα, το έγκλημα είναι αναπόσπαστο κομμάτι κάθε κοινωνίας και συμπεριφέρεται, ως ένας οργανισμός που συνεχώς μεταβάλλονται οι εκφάνσεις, τα μέσα τέλεσης καθώς και το νομικό πλαίσιο που το διέπει. Με διαφορετική μάσκα αλλά και περιεχόμενο πολλές φορές ανάλογα με τις κοινωνικοπολιτικές και ηθικές τάσεις κάθε εποχής και τόπου το έγκλημα παραμένει παρόν και κινούμενο πάντα με τρεις βασικούς άξονες. Τα απαραίτητα συστατικά στοιχεία του αυτό που το ορίζουν. Το ουσιαστικότερο

περιεχόμενο του εγκλήματος συνιστάται στο ότι, είναι η πράξη εκείνη που θίγει τις αξίες της κοινωνικής ζωής στην γενικότερη αποδοχή της πλευράς της και που η τέλεση της εκφράζει την έλλειψη σεβασμού του δράστη προς τις αξίες αυτές, έτσι ώστε η ποινική καταστολή της να κρίνεται κοινωνικά απόλυτα αναγκαία.

Το εγκληματικό φαινόμενο αποτελεί ιστορικό-κοινωνικό φαινόμενο, καθώς ακολουθεί την εξέλιξη των ανθρωπίνων κοινωνιών. Εδώ έχει ιδιαίτερη σημασία να επισημάνουμε την διαχρονικότητα του στο πλαίσιο των αιώνων. Καμία κοινωνία δεν έχει απαλλαχτεί από αυτό, αν και σε κάθε έγκλημα υπήρχε, υπάρχει και θα υπάρχει ποινή. Αντίθετα, αυτό που παρατηρείται είναι η αύξηση του εγκληματικού φαινομένου και συγχρόνως εμφάνιση νέων μορφών εγκληματικής συμπεριφοράς.

Τα πλεονεκτήματα του Διαδικτύου είναι πολλά. Αυτά που έχουν μπει στις ζωές μας είναι η ταχύτητα και η άνεση, διότι όλα γίνονται πλέον με ένα πάτημα ενός κουμπιού, τα δίκτυα είναι ενσύρματα και κυρίως ασύρματα με αποτέλεσμα να κυριαρχούν παντού, η φυσική παρουσία πλέον για αγορά, μάθηση, πληροφόρηση και συνομιλία δεν είναι απαραίτητη, το internet πετυχαίνει πολλά μέσα σε λίγα δευτερόλεπτα λόγω του παγκόσμιου ιστού (world wide web), και αποτελεί μια μεγάλη γκάμα πληροφοριών με χρήσιμες πηγές.

Υπάρχουν, όμως και τα μειονεκτήματα ως αντίβαρο, διότι το διαδίκτυο συμβάλλει στις κοινωνικές διακρίσεις με το χωρισμό των μελών σε αυτούς που έχουν την δυνατότητα να το χρησιμοποιούν και σε αυτούς που δεν μπορούν (οικονομικό πρόβλημα, ηλικίας κ.τ.λ.), στην κοινωνική αποξένωση του ανθρώπου από τον πραγματικό κόσμο με αποτέλεσμα να υπάρχει όλο και λιγότερη κοινωνικοποίηση και στην ασφάλεια των πληροφοριών του.

2.3 ΤΙ ΕΙΝΑΙ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η ηλεκτρονική εγκληματολογία (Computer Forensic Science) είναι η επιστήμη που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό.

Για την επιτυχή εξιχνίαση μιας υπόθεσης ηλεκτρονικού εγκλήματος χρησιμοποιούνται οι ψηφιακές αποδείξεις οι οποίες διαχωρίζονται σε:

- Ψηφιακές αποδείξεις (digital evidence) : πληροφορίες που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και μπορούν να αποθηκευτούν ή να μεταδοθούν σε ψηφιακή μορφή.
- Αντικείμενα δεδομένων (data objects) : αντικείμενα ή πληροφορίες που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και σχετίζονται με φυσικά αντικείμενα.
- Φυσικά αντικείμενα (physical items) : τα φυσικά μέσα, όπου αποθηκεύονται ή μέσω τον οποίων μεταδίδονται πληροφορίες και αντικείμενα δεδομένων.
- Γνήσιες ψηφιακές αποδείξεις (original digital evidence) : φυσικά αντικείμενα δεδομένων τη στιγμή που συλλέγονται από την σκηνή του εγκλήματος.
- Διπλότυπες ψηφιακές αποδείξεις (duplicate digital evidence) : φυσικά αντικείμενα και αντικείμενα δεδομένων που περιέχονται σε ένα γνήσιο ψηφιακό αντικείμενο.
- Αντίγραφο (copy) : μια ακριβής αναπαραγωγή των πληροφοριών που περιέχονται σε ένα γνήσιο φυσικό, ανεξάρτητα από το αντικείμενο αυτό.

2.4 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Το ηλεκτρονικό έγκλημα ανεξάρτητα από το εάν προσεγγιστεί από την στενή ή την ευρεία έννοια που εμπεριέχει, έχει ορισμένα χαρακτηριστικά γνωρίσματα που το διαχωρίζουν από το παραδοσιακό έγκλημα.

Τέτοια είναι τα εξής:

- Το έγκλημα στον κυβερνοχώρο είναι γρήγορο, διαπράττεται σε πραγματικό χρόνο, ακόμα και σε δευτερόλεπτα, και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.
- Είναι εύκολο στη διάπραξη του για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά.
- Για την εκτέλεση του απαιτούνται άριστες και εξιδανικευμένες γνώσεις.
- Οι κυβερνο-εγκληματίες πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα, αποστέλλοντας ηλεκτρονικά μηνύματα (e-mails) με ψευδή στοιχεία.
- Μπορεί να διαπραχθεί από οποιοδήποτε μέρος, καθώς δεν απαιτείται η μετακίνηση του δράστη και τα αποτελέσματα του μπορούν να γίνονται ταυτόχρονα αισθητά σε πολλούς στόχους ανεξάρτητα εδαφικού περιορισμού .
- Ο εντοπισμός ενός ψηφιακού εγκληματία κατά κανόνα είναι πολύ δύσκολος (αλλά όχι ακατόρθωτος) να προσδιοριστεί, καθώς επίσης και ο (πραγματικός) τόπος τέλεσης του και αυτό, γιατί μπορεί ο δράστης να εντοπιστεί σε συγκεκριμένο τόπο, τα αποδεικτικά στοιχεία όμως να βρίσκονται σε διαφορετική και απομακρυσμένη χώρα ή να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες.
- Ο κίνδυνος ανακάλυψης του ηλεκτρονικού δράστη είναι μικρός, καθώς το ηλεκτρονικό έγκλημα αποδίδει μεγάλα κέρδη.
- Ο αριθμός των θυμάτων τους συγκρινόμενος με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος.

- Για τη διερεύνηση του απαιτείται συνεργασία τουλάχιστον δυο κρατών, του κράτους που γίνεται αντιληπτή ή εξωτερίκευση του εγκλήματος και του κράτους, όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία.
- Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα, γιατί ελάχιστες περιπτώσεις κυβερνο-εγκλημάτων καταγγέλλονται διεθνώς με άμεση συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του διαδικτύου να χαρακτηρίζεται ακόμα πιο «σκοτεινό» από ότι το έγκλημα.

2.5 ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Οι μορφές ηλεκτρονικού εγκλήματος διαφέρουν μεταξύ τους, καθώς καποιές μορφές έχουν να κάνουν με τα ηλεκτρονικά ή ψηφιακά εγκλήματα (hacking, κλοπή ταυτότητας, πειρατεία λογισμικού, κακόβουλο λογισμικό κ.τ.λ.) και άλλες με τα παραδοσιακά εγκλήματα (απάτες, κατασκοπεία, υποκλοπές).

Οι πιο πασίγνωστες μορφές είναι οι παρακάτω:

- Οι κακόβουλες εισβολές σε δίκτυα (Hacking και cracking) , δηλαδή η χωρίς δικαίωμα πρόσβαση σε ένα δίκτυο υπολογιστών. Όταν ο επιτιθέμενος έχει ως σκοπό να προκαλέσει ζημία ή να αποκομίσει οικονομικό όφελος, αναφέρεται ως hacker ενώ σε αντίθετη περιπτώση ως cracker.

- Οι επιθέσεις άρνησης εξυπηρέτησης (denial of service attack – DOS) , αποσκοπούν στην εξάντληση των πόρων ενός υπολογιστή, ώστε να μην μπορεί να εξυπηρέτησει άλλους υπολογιστές. Αυτό συχνά ισοδυναμεί με διακοπή λειτουργίας μιας κρίσιμης υπηρεσίας ή συνόλου υπηρεσιών που προφέρονται από ένα ή περισσότερους διακομιστές με απρόβλεπτες συνέπειες για την εταιρεία ή τον οργανισμό. Επίσης, μια άλλη μορφή επίθεσης είναι το « θανατηφόρο

πινγκ » κατά την οποία ο ψηφιακός δράστης στέλνει μια διαταγή πινγκ με ένα τεράστιο πακέτο IP, με αντίκτυπο το πάγωμα ή την αναγκαστική επανεκκίνηση του διακομιστή του θύματος του.

- Το κακόβουλο λογισμικό, είναι προγράμματα ηλεκτρονικού υπολογιστή που δημιουργούνται με σκοπό να προκαλέσουν ζημία σε Η/Υ ή να εισχωρήσουν σε έναν Η/Υ για την υποκλοπή, αλλοίωση ή διαγραφή δεδομένων και προγραμμάτων. Το κακόβουλο λογισμικό διακρίνεται σε τρείς βασικές κατηγορίες, τους ιούς (viruses), τα σκουλήκια (worms) και τους Δούρειους ίππους (trojan horses) . Πρωταρχικά, οι ιοί διακρίνονται σε πολλές μορφές, όπως (boot viruses) που μολύνει τον τομέα εκκίνησης ενός σκληρού δίσκου που περιέχει εντολές εκκίνησης του υπολογιστη, (system cluster viruses) που μολύνει το σύστημα και κολλά σε τμήματα του λειτουργικού ή στο πρόγραμμα ελέγχου των εφαρμογών, (software viruses) που προσβάλλουν προγράμματα υπολογιστών και τρέχουν μόλις ξεκινήσει το πρόγραμμα που έχουν μολύνει, (polymorphous viruses) που αναπαράγονται με ποικίλλους τρόπους, ώστε να αντέχουν στα anti – virus προγράμματα, (stealth viruses) που υποκρύπτουν τις αλλαγές στον τομέα εκκίνησης του συστήματος, (retroviruses) που προσπαθούν να καταστρέψουν ή να σβήσουν εντελώς προγράμματα anti – virus και (data viruses) που προσβάλλουν τις μακρο – εντολές σύγχρονων προγραμμάτων εφαρμογών. Δευτερεύον, τα σκουλήκια (worms) είναι προγράμματα Η/Υ που χρησιμοποιούνται σαν μηχανισμός μεταφοράς άλλων προγραμμάτων, είναι όπως οι ιοί με μόνη διαφορά ότι δεν είναι αναγκαία η ανθρώπινη παρεμβολή τους για την ενεργοποίηση τους. Τρίτον, οι Δούρειοι ίπποι (Trojan horses) είναι όπως τους ιούς (viruses) και τα σκουλήκια (worms) , μόνο που εμφανίζεται συνήθως με την μορφή παιχνιδιού με σκοπό να κλέψει τα ονόματα (usernames) και τους κωδικούς (passwords) των ανυποψίαστων χρηστών του διαδικτύου.

- Ανεπιθύμητη Αλληλογραφία (Spamming) , είναι η χρήση οποιουδήποτε ηλεκτρονικού μέσου για την αποστολή ανεπιθύμητων μηνυμάτων σε πολύ μεγάλες ποσότητες. Αν και όρος αναφέρεται περισσότερο στην αποστολή μεγάλης ποσότητας μηνυμάτων, με διαφημιστικό περιεχόμενο χρησιμοποιείται, επίσης για να καταδείξει την αποστολή οποιουδήποτε μηνύματος, το οποίο μπορεί να χαρακτηριστεί ενοχλητικό, από αυτόν που το λαμβάνει.

- Επιθέσεις σε δικτυακούς τόπους (sites) , που αποσκοπούν στην αλλοίωση του περιεχομένου ενός δικτυακού τόπου, κατά τρόπο χιουμοριστικό, προπαγανδιστικό ή προσβλητικό.

- Ηλεκτρονικό ψάρεμα (Phising) , όπου επιχειρείται η απόσταση προσωπικών πληροφοριών του θύματος, όπως ο αριθμός της πιστωτικής του κάρτας, κωδικοί πρόσβασης κ.τ.λ.

- Πειρατεία λογισμικού, αναφέρεται στην αναπαραγωγή και την διάθεση προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων χωρίς τη γραπτή συναίνεση του δημιουργού της.

- Απάτη στο διαδίκτυο, αποτελεί ηλεκτρονική έκφανση της συμβατικής απάτης. Κυρίως οι επιτιθέμενοι χρησιμοποιούν παραπλανητικά e-mail, αποστέλλοντας Νιγηριανές επιστολές ή ενημέρωση για κέρδη στο Ισπανικό Λόττο, επίσης πολλές απάτες πραγματοποιούνται με τη χρήση πιστωτικών καρτών.

- Κλοπή ταυτότητας, η υποκλοπή στοιχείων ταυτότητας ανυποψίαστων και η χρήση τους για παράνομες δραστηριότητες.

- Ξέπλυμα χρήματος, η προσπάθεια εξαφάνισης χρήματος που προέρχεται από παράνομες δραστηριότητες. Χαρακτηριστικό παράδειγμα, αποτελεί η ασυνήθιστη αγορά μεγάλων ποσοτήτων αγαθών μέσω του διαδικτύου.

- Διακίνηση παιδικού πορνογραφικού υλικού, αναφέρεται στη διακίνηση παιδικού πορνογραφικού υλικού μέσω του διαδικτύου, που μπορεί να είναι σε μορφή φωτογραφιών, βίντεο ή οποιαδήποτε άλλη μορφή πολυμέσων.

- Διαδικτυακή τρομοκρατία, αναφέρεται στη χρήση της τεχνολογίας των ηλεκτρικών υπολογιστών και δικτύων για την πραγματοποίηση της τρομοκρατικής επιθέσεις.

- Επιθέσεις παρενόχλησης (cyberbulling) , είναι μια εγκληματική συμπεριφορά, όπου ο επιτιθέμενος με τη χρήση ηλεκτρονικών μέσων επικοινωνίας, όπως το διαδίκτυο και τα κινητά τηλέφωνα , εκφοβίζει, απειλή, εκβιάζει και γενικότερα παρενοχλεί τα θύματα του για διάφορους λόγους, όπως η εκδίκηση, επίλυση προσωπικών διαφορών κ.α.

- Κατασκοπεία που μπορεί να είναι βιομηχανική, κρατική ή και πολιτική. Επίσης υπάρχουν τα κατασκοπευτικά προγράμματα (spyware) , οι οποίες είναι μικρές εφαρμογές που μπαίνουν σε έναν ηλεκτρονικό υπολογιστή χωρίς να γίνονται αντιληπτά από τον χρήστη του.

- Υποκλοπές τηλεφωνικών συνομιλιών με αποτέλεσμα την προσβολή του προσωπικού απορρήτου των συνομιλούντων.

2.6 ΜΕΤΡΑ ΠΡΟΛΗΨΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Σε αυτό το κεφάλαιο αναφέρονται οι βασικότερες έννοιες που αφορούν την ασφάλεια, την πρόληψη καθώς και κάποιες από τις πλέον διαδεδομένες τακτικές προς την αποφυγή της θυματοποίησης του πολίτη με τη χρήση ηλεκτρονικού υπολογιστή.

Βασικές έννοιες της ασφάλειας είναι:

- Η εμπιστευτικότητα, η οποία αναφέρεται στην προστασία δεδομένων από την πρόσβαση μη εξουσιοδοτημένων χρηστών. Για την επίτευξη της εμπιστευτικότητας απαιτείται περιορισμός της πρόσβασης στο σύστημα και δεδομένα από νόμιμους χρήστες.

- Η ακεραιότητα, που συνδέεται με την προστασία των δεδομένων από τυχόν τροποποίηση (προσθήκη, διαγραφή) . Η αλλοίωση της ακεραιότητας μπορεί να προκύψει εξαιτίας κάποιου αλλού στο σύστημα ή ακόμα να είναι αποτέλεσμα δόλιας ενέργειας.

- Η διαθεσιμότητα, η οποία σχετίζεται με τη δυνατότητα άμεσης όταν ή όποτε απαιτείται. Στις επιθέσεις άρνησης εξυπηρέτησης υπάρχει παραβίαση της διαθεσιμότητας, όταν δεν επιτρέπεται στους εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στους πόρους τους συστήμα.

2.7 ΤΑ ΒΑΣΙΚΑ ΠΡΟΛΗΠΤΙΚΑ ΕΡΓΑΛΕΙΑ ΚΑΙ Η ΛΕΙΤΟΥΡΓΙΑ ΤΟΥΣ

Για την καλύτερη ασφάλεια ενός χρήστη και του ηλεκτρονικού υπολογιστή του από το διαδίκτυο υπάρχουν βασικά προληπτικά εργαλεία στα οποία θα εξηγήσουμε την λειτουργία τους.

Είναι η χρήση λογισμικού ασφαλείας – λογισμικού / antivirus, όπου η διασπορά των ιών είναι μια από τις πιο διαδομένες μορφές επίθεσης στο διαδίκτυο. Η χρήση λογισμικού αντιβιοτικού είναι η πιο συνηθισμένη μέθοδος αντιμετώπισης τους. Ένα τέτοιο πρόγραμμα που πρέπει να είναι εγκατεστημένο σε κάθε ηλεκτρονικό υπολογιστή επιτελεί τρείς βασικές λειτουργίες. Αυτές είναι:

- Η ανίχνευση των ιών, όπου η λειτουργία αυτή πραγματοποιείται κατόπιν ενέργειας του χρήση (έλεγχος από το antivirus λογισμικού) ή μπορεί να γίνει και αυτόματα (έλεγχος από το antivirus λογισμικού που είναι φορτωμένο στη μνήμα RAM του ηλεκτρονικού υπολογιστή) .

- Ο προσδιορισμός ταυτότητας των ιών, στο οποίο αφού έχει προηγηθεί ο εντοπισμός του ιού ακολουθεί η αφαίρεση του. Το λογισμικό antivirus επιδιορθώνει το μολυσμένο από το ιό πρόγραμμα ή ακόμα μπορεί και να το διαγράψει.

- Η πιστοποίηση του χρήστη, είναι η πιο συνηθισμένη τεχνική πιστοποίησης της ταυτότητας ενός χρήστη, μέσω της δημιουργίας και της χρήσης συνθηματικών λέξεων ή συμβόλων. Έτσι, το όνομα του χρήστη (user id) και ο κωδικός πρόσβασης (password) είναι απαραίτητα στοιχεία προκείμενου να επιτραπεί η είσοδος του εξουσιοδοτημένου χρήστη στο σύστημα.

- Το firewalls – τείχος προστασίας, στην επιστήμη των υπολογιστών χρησιμοποιείται για να δηλώσει κάποια συσκευή ή προγράμματα και είναι ρυθμισμένο, ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.

Η κύρια λειτουργία ενός firewall – τείχος προστασίας, είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα στα δυο δίκτυα υπολογιστών. Συνήθως, τα δύο αυτά δίκτυα είναι το διαδίκτυο και το τοπικό / εταιρικό δίκτυο. Ένα firewall – τείχος προστασίας παρεμβάλλεται ανάμεσα σε δυο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης, ενώ το εταιρικό έχει το δίκτυο ή το οικιακό δίκτυο, τα οποία διαθέτουν το μέγιστο βαθμό εμπιστοσύνης. Ο σκοπός της τοποθέτησης ενός firewall – τείχος προστασίας, είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπιση τους. Η σωστή πρακτική είναι το firewall – τείχος προστασίας να ρυθμίζεται, έτσι ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστείς του δικτύου. Για να ρυθμιστεί σωστά ένα firewall – τείχος προστασίας θα πρέπει ο διαχειριστείς του δικτύου να έχει μια ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα των υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίζουν το firewall – τείχος προστασίας, ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει. Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες. Το firewall – τείχος προστασίας, λειτουργεί ως φράκτης ανάμεσα στο ιντερνέτ και στο εσωτερικό δίκτυο ή έναν υπολογιστή και σταματάει διάφορους κινδύνους και επιθέσεις, συμπεριλαμβανομένων και ορισμένων ιών (viruses) . Το firewall – τείχος προστασίας, μπορεί να είναι λογισμικό που τρέχει στον υπολογιστή (π.χ. Microsoft ISA server) ή συσκευή hardware συνδεμένη στο δίκτυο. Το firewall – τείχος προστασίας φιλτράρουν την πληροφορία που εισέρχεται στο δίκτυο ή εξέρχεται από αυτό, με βάση τους κανόνες τους οποίους έχουμε θέσει. Με αυτό τον τρόπο προστατεύεται το δίκτυο από εισβολείς (hackers, ορισμένους ιούς κ.λ.π.) . Επιπλέον, απαγορεύεται η αποστολή πληροφορίας από τους υπολογιστές του δικτύου,

όπως παραδείγματος χάριν ποιοί είναι οι τύποι αρχείων που επιτρέπεται να αποστέλλονται.
Στα μειονεκτήματα του firewall – τείχους προστασίας, καταλογίζεται το υψηλό οικονομικό κόστος, η δυσκολία να ρυθμιστούν με τρόπο αποτελεσματικό για την εκπλήρωση της αποστολή τους και τέλος το γεγονός ότι η προστασία που παρέχουν είναι εντελώς σχετική. Είναι γνωστό ότι τα modems αποτελούν ένα σημείο εισόδου στο δίκτυο το όποιο υπερφαλαγγίζει κάθε firewall – τείχος προστασίας.

Ένας σημαντικός τρόπος για την προστασία από πολλά είδη επιθέσεων είναι η σχεδίαση τοπολογίας του δικτύου, ώστε να είναι δύσκολη να γίνει η εισβολή. Ένα firewall – τείχος προστασίας είναι ένα επιπλέον επίπεδο προστασίας τοποθετημένο γύρω από ένα δίκτυο ή από μια συγκεκριμένη εφαρμογή. Ένα firewall – τείχος προστασίας που προστατεύει ένα δίκτυο θα περιλαμβάνει συνήθως ένα δρομολογητή (router) που μπορεί να προγραμματιστεί έτσι ώστε να γίνεται επιλεκτικά η πρόσβαση σε ένα δίκτυο, για παράδειγμα θα απορρίπτει πακέτα που δεν στέλνονται σε συγκεκριμένες επιτρεπόμενες θύρες. Όταν ένα πακέτο φτάνει στον δρομολογητή του firewall – τείχος προστασίας αυτός επεξεργάζεται και αποφασίζει αν θα το αφήσει αν περάσει στο δίκτυο που προστατεύει ή όχι. Μια ακόμη ισχυρότερη χρήση του firewall – τείχος προστασίας είναι σε ένα σενάριο δυο επιπέδων προστασίας, όπου χρησιμοποιείται ένας δρομολογητής που παρακολουθεί την επικοινωνία με το ιντερνέτ και ένας ακόμη που παρακολουθεί την επικοινωνία στο εσωτερικό δίκτυο.

2.8 ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ

Κρυπτογράφηση καλείται η διαδικασία της επεξεργασίας κωδικοποίησης της ψηφιακής πληροφορίας κατά τέτοιο τρόπο, ώστε αυτή να παραμένει αναγνωρίσιμη και κατανοητή μορφή μόνο από τους εξουσιοδοτημένους παραλήπτες που διαθέτουν το κατάλληλο «κλειδί» - κώδικα, δηλαδή η πληροφορία καθίσταται εμπιστευτική. Αρχικά, η τεχνολογία της κρυπτογράφησης δημιουργήθηκε με σκοπό την προστασία του απορρήτου του μηνύματος. Στην πορεία η εξέλιξη της κρυπτογράφησης προσφέρει στον αποστολέα του μηνύματος κατά την αποστολή του ένα κρυπτογραφικό σύστημα, το οποίο αποτελεί ένα σύνολο λειτουργιών που είναι παραμετροποιημένες από κλειδιά που χρησιμοποιούνται για τη διατήρηση της εχεμύθειας στην επικοινωνία. Με τις ενσωματωμένες λειτουργιές της ένκρυψης και της απόκρυψης το σύστημα παρέχει ασφάλεια και προστασία στην ιδιωτικότητα αποκλίνοντας έτσι την χωρίς εξουσιοδότηση πρόσβαση σε υλικό που ορίστηκε να παραμείνει απόρρητο. Το κρυπτογραφικό περιεχόμενο δεν μπορεί να γίνει προσβάσιμο από οποιανδήποτε που θα προσπαθήσει να προσπελάσει χωρίς να γνωρίζει τι περιέχει. Συνεπώς, αποκλείεται η έκθεση σε βλαπτικό υλικό για όποιον θα μπορούσε να προσβληθεί ακόμα και εάν αυτό συνέβαινε τυχαία.

Ένα σύγχρονο σύστημα κρυπτογράφησης αποτελείται από τέσσερα σημεία.

Αυτά είναι:

- Το αρχικό μήνυμα.
- Το κρυπτογραφικό σύστημα αποτελούμενο από ένα αλγόριθμο κρυπτογράφησης και ένα αλγόριθμο αποκρυπτογράφησης.
- Το κρυπτογραφημένο μήνυμα. Πρόκειται για το αποτέλεσμα της εφαρμογής του αλγόριθμου της κρυπτογράφησης στο αρχικό μήνυμα πριν αυτό σταλεί στον παραλήπτη.
- Το κλειδί το οποίο είναι σύμβολο –σειρά.

- Η σύμβολο-σειρά αυτή χρησιμοποιείται στη διαδικασία της κρυπτογράφησης με αλγόριθμο και αποκρυπτογράφησης με τον αντίστροφο αλγόριθμο.

2.9 ΣΥΜΒΟΥΛΕΣ ΚΑΙ ΠΡΟΛΗΨΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΗ ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Εκτός από την κρυπτογράφηση και ασφάλεια που αναφέραμε πιο πάνω υπάρχουν οι συμβουλές για την ασφαλή χρήση του διαδικτύου και η πρόληψη για την προστασία του συστήματος.
Οι συμβουλές για την ασφαλή χρήση του διαδικτύου είναι οι εξής:

- Η προστασία κατά την περιήγηση στο Διαδίκτυο, όπου χωρίζεται σε δύο κλάδους, των γονιών και των νέων. Στους γονείς δίνονται βασικές συμβουλές όσον αφορά την ασφάλεια και την προστασία την δική τους, αλλά πιο πολύ των παιδιών τους. Ύστερα στους νέους δίνονται συμβουλές για την ασφάλεια τους στις διάφορες τους περιήγησεις στο διαδίκτυο (συνομιλίες) και πώς να μην φοβούνται να μιλήσουν με τους γονείς τους για οτιδήποτε πρόβλημα προκύψει μέσω του διαδικτύου.
- Οι συμβουλές για τις ασφαλείς οικονομικές συναλλαγές, περιέχουν πληροφορίες συγκεκριμένα για τις ασφαλείς διαδικτυακές συναλλαγές που χρησιμοποιούν πλέον οι περισσότεροι χρήστες του διαδικτύου, όσον αφορά το τι πρέπει να αποφεύγουν, τι πρέπει να φροντίσουν, πώς να προστατεύονται και πως εάν είναι κάτοχοι ηλεκτρονικού ταχυδρομείου (e-mail) να προσέχουν τι μηνύματα αποδέχονται και ποια πρέπει να απορρίπτουν.
- Οι συμβουλές για τους χρήστες Αυτόματων Τραπεζικών Μηχανών (Α.Τ.Μ.), αφορούν ως προς τον τρόπο χρήσης των Α.Τ.Μ. και πώς να προστατεύσουν τους λογαριασμούς τους.

- Η προστασία από το spam δίνει συμβουλές όσον αφορά την προστασία των χρηστών από δελεαστικά μηνύματα που μπορεί να δέχονται στα e – mails τους και πως μπορούν πολύ εύκολα να τα αποφύγουν με ειδικά προγράμματα.
- Η προστασία από το κακόβουλο λογισμικό, αφορά την προστασία των χρήστων που έχουν ηλεκτρονικούς υπολογιστές πώς να τους προσέχουν, ώστε να μην έχουν προβλήματα με ιούς και τα λεγόμενα « third party cookies » που τοποθετούνται από τριτογενείς φορείς.
- Τέλος, η προστασία από παρενοχλήσεις, έχει συμβουλές για το πώς να προστατεύονται οι χρήστες από ανθρώπους που τους ενοχλούν και σημαντικότερο από όλα να μην δίνουν χωρίς κανένα δισταγμό προσωπικές πληροφορίες είτε σε δικτυακό τόπο, είτε σε άγνωστο όπου συνομιλούνε μέσω των chat room.

Η πρόληψη για την προστασία του συστήματος μπορεί να γίνει μόνο εάν ο χρήστης του ηλεκτρονικού υπολογιστή:

- Προστατεύσει με κάθε τρόπο που περνάει από το χέρι του τη διαρροή σε τρίτους πληροφοριών, που αφορούν εκείνον, τους ανθρώπους που το χρησιμοποιούν και τα ανάλογα προγράμματα που τρέχουν στον υπολογιστή.
- Περιορίζει την ελεύθερη πρόσβαση στο σύστημα ανεξαιρέτως διακρίσεων.
- Ανανεώνει τη λειτουργία του συστήματος με σύγχρονο λογισμικό (windows updates).
- Διαγράψει κάθε αρχείο, πρόγραμμα, φωτογραφικό υλικό κ.τ.λ., το οποίο δεν χρησιμοποιείται πλέον.
- Χρησιμοποιήσει αντιϊκά προγράμματα (anti – virus), τα τείχη προστασίας (firewalls) που έχουν ως σκοπό τους την προστασία δεδομένων του χρήστη από κάθε ανεπιθύμητη επέμβαση και την χρησιμοποίηση ειδικών προγραμμάτων για την προστασία ευαίσθητων δεδομένων με την μέθοδο της κρυπτογράφησης.

2.10 Η ΕΞΑΚΡΙΒΩΣΗ ΤΗΣ ΕΙΣΒΟΛΗΣ ΚΑΙ Η ΑΠΟΚΑΤΑΣΤΑΣΗ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

Πέρα από τα μέτρα που λαμβάνονται για την ασφάλεια του συστήματος, πάντα υπάρχει η πιθανότητα να πέσει ένας χρήστης « θύμα » ενός χάκερ (hacker) και τις περισσότερες φορές συμβαίνει αυτό χωρίς ο χρήστης να αντιλιφθεί τίποτα για την ενέργεια που ακολούθησε. Για να μπορέσει να γίνει η καταγραφή θα πρέπει να παρακολουθείτε στενά το σύστημα, έτσι ώστε με το κατάλληλο λογισμικό να γίνει η ανίχνευση οποιασδήποτε ανωμαλίας που υπάρχει στο σύστημα.
Μετά την καταγραφή των διάφορων ανωμαλιών θα πρέπει να γίνει ανασυγκρότηση του συστήματος για να επανέλθουν όλα όπως ήταν πριν. Αυτό για να συμβεί θα πρέπει:

- Να γίνει επαναφόρα των άρχειων που καταστράφηκαν πριν μολυνθούν.
- Να γίνει επαναλειτουργία όλων των υπηρεσίων του συστημάτος προς τους χρήστες του.
- Να γίνει γνωμάτευση και διόρθωση του προβλήματος για την αποφυγή επανάληψης στο μέλλον.
- Να γίνει προσπάθεια για τον εντοπισμό των « hackers » για να παραδοθούν στις διωκτίκες αρχές και ύστερα στην δικαιοσύνη.
- Να γίνει λόγος για το όλο συμβάν, έτσι ώστε να μην επιβαρυνθεί η εικόνα του χρήστη, ειδικά εάν πρόκειται για επιχείρηση.
- Και να γίνει μελέτη όσων στοιχείων έχουν μαζέψει, έτσι ώστε να γνωρίζουν στο μέλλον εάν υπάρξει ανάλογη κατάσταση τι να κάνουν και πώς να το αντιμετωπίσουν.

Εν τέλει πρέπει να σημειωθεί ότι οι « hackers » μπορούν να γίνουν αντιληπτοί αναλόγα με το κίνητρο τους, το οποίο μπορεί να είναι κοινωνικό (προσπάθεια αλλαγής του κόσμου), επιστημονικό (υπόδειξη των δυνατοτήτων τους και βελτίωση της ασφάλειας), πολιτικό (άκουσμα της φωνής τους μέσω δικτύου και ύστερα των Μ.Μ.Ε.), και κοινωνικό (οικονομικό κέρδος)

ΚΕΦΑΛΑΙΟ 3^{Ο} :
SAFELINE
3.1 ΙΣΤΟΡΙΚΗ ΕΞΕΛΙΞΗ

Η safeline αποτελεί μια από τις τρεις δράσεις του ελληνικού κέντρου ασφαλούς διαδικτύου, το οποίο υλοποιείται υπό την αιγίδα της Ευρωπαϊκής Επιτροπής στα πλαίσια του προγράμματος Safer internet.

Ξεκίνησε τη λειτουργία της στις 14 Απριλίου 2003 και είναι η μοναδική ανοιχτή γραμμή καταγγελιών παράνομου περιεχομένου στο διαδίκτυο και επίσημο μέλος της Inhope (Διεθνής Σύνδεσμος Ανοικτών Γραμμών Διαδικτύου) από τις 18 Οκτωμβρίου 2005.

Βασική μέριμνα της Safeline είναι η εξάλειψη φωτογραφιών και βίντεο που απεικονίζουν την κακοποίηση ανηλίκων, καθώς και η προάσπιση του δικαιώματος της ασφαλούς πλοήγησης του παιδιού στο διαδίκτυο. Στα παραπάνω προστίθεται και η αντιμετώπιση της παρενόχλησης μέσω του Κυβερνοχώρου ή του κινητού τηλεφώνου, αλλά και η αντιμετώπιση περιεχομένου που αφορά την βία, το ρατσισμό, την ξενοφοβία και γενικά καθετί το οποίο αντιβαίνει στην ελληνική νομοθεσία.
Στην μετέπειτα πορεία ένωσε τις δυνάμεις της με τον Ελληνικό Κόμβο Επαγρύπνησης, παράλληλα δημιουργήθηκε η γραμμή βοήθειας Υποστηρίζω της μονάδας εφηβικής υγείας. Οι τρείς δράσεις δημιούργησαν τον Ελληνικό Κόμβο Ασφαλούς Διαδικτύου με στόχο μια πιο πολύπλευρη και οργανωμένη προσπάθεια που ενσωματώνει την ενημέρωση και την αφύπνιση του κοινού, την καταγγελία καθώς και την πρόληψη και βοήθεια κάτω από το ίδιο κοινό έργο.

Πρωταρχικό μέλημα της safeline είναι η εξάλειψη από το διαδικτυακό περιεχόμενο της παιδικής πορνογραφίας με αποτέλεσμα σκοπός της να είναι η καταπολέμηση κάθε είδους παράνομου περιεχομένου στο διαδίκτυο.

Δέχεται καταγγελίες για περιεχόμενο που εντοπίζεται στο διαδίκτυο και περιέχει εικόνες κακοποίησης παιδιών σε οποιδήποτε άλλο σημείο του κόσμου, ρατσισμό και ξενοφοβικό υλικό που προβαίνει την ελληνική νομοθεσία και οτιδήποτε άλλο θεωρείτε ότι είναι παράνομο.
Επίσης, συνεργάζεται με φορείς παροχής υπηρεσιών διαδικτύου, όπως το ακαδημαϊκό δίκτυο ΕΔΕΤ και το σχολικό δίκτυο, τα ερευνητικά και πολιτιστικά ιδρύματα και με ενώσεις καταναλώτων και την ελληνική αστυνομία για τον περιορισμό της ροής του παράνομου περιεχομένου στο διαδίκτυο.
Τέλος, υλοποιείται από τους οργανισμούς (Ινστιτούτο πληροφορικής, ίδρυμα τεχνολογίας και έρευνας και το ελληνικό όργανο αυτορύθμισης για το περιεχόμενο του internet) και υποστηρίζεται από το safer internet programme της Ευρωπαϊκής Ένωσης.

3.2 ΟΙ ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Το διαδίκτυο είναι μια ευρεία γκάμα δραστηριοτήτων (ψυχαγωγία, επικοινωνία, έρευνα κ.τ.λ.) όπου χρησιμοποείται από τον καθένα χωρίς περιορισμούς. Παρόλα αυτά υπάρχουν και χρήστες που χρησιμοποιούν με κακόβουλο τρόπο το διαδίκτυο με αποτέλεσμα οι δραστηριότητες τους αυτές να χαρακτηρίζονται από την Ελληνική Νομοθεσία παράνομες.

Οι δραστηριότητες αυτές είναι:

- Η παιδική πορνογραφία, όπου σε κάποιες χώρες την αποκαλούν και την ορίζουν ως εικονική σεξουαλική κακομεταχείριση των παιδιών. Όμως, η έννοια της ανά χώρα καθορίζεται νομικά με διαφορετικό τρόπο. Ο ελάχιστος προσδιορισμός που δίνεται στον όρο είναι μια φωτογραφία η οποία παριστάνει ένα παιδί να λαμβάνει μέρος ή να παρουσιάζεται ότι λαμβάνει μέρος σε σεξουαλικές δραστηριότητες.

Δημιουργία αντίρρησης ανά χώρα είναι η ηλικία συναίνεσης για σεξουαλική επαφή, όπως επίσης και στις νομοθετικές διαφορές για το εάν η κατοχή παιδικής πορνογραφίας είναι ποινικό αδίκημα ή όχι ή εάν είναι οι πειραγμένες εικόνες μέρος του πορνογραφικού υλικού και τέλος κατά πόσο αληθινά χρησιμοποιήθηκε ένα παιδί στη πορνογραφία.

- Η ξενοφοβία και ο ρατσισμός που δημιουργούν πεποιθήσεις διαφόρων ατόμων σε παγκόσμια κλίμακα, αυτό γιατί το διαδίκτυο δεν μπορεί να λογοκριθεί από κανέναν πράγμα που δίνει την δυνατότητα προώθησης του προβληματικού αυτού φαινομένου.
- Ο ηλεκτρονικός εκφοβισμός (cyber bullying), όπου είναι ένα σύνολο ενεργειών που διαπράττονται από παιδιά με σκοπό να εκφοβίσουν συνομίληκους τους, ώστε να τους τραυματίσουν ψυχολογικά μέσω των νέων τεχνολογιών (κινητή τηλεφωνία, σελίδες κοινωνικής δικτύωσης, ηλεκτρονικό ταχυδρομείο).
- Η επικοινωνία μέσω διαδικτύου με σκοπό την αποπλάνηση (grooming) είναι όλες οι διαδικασίες με τις οποίες ένας ενήλικας προσποιείται ότι είναι μικρότερης ηλικίας για να προσελκύσει παιδία, να τα κάνει να νιώσουν ασφάλεια και εμπιστοσύνη προς αυτόν, έτσι ώστε να έρθει σε κοντινή επαφή μαζί τους στον πραγματικό κόσμο με σκοπό τη σεξουαλίκη εκμετάλλευση ή και κακοποίηση.

3.3 ΚΑΤΑΓΓΕΛΙΑ

Όταν ένας χρήστης του διαδικτύου αισθανθεί ότι απειλείται ή εκφοβίζεται άσχημα από κάποιο συγκεκριμένο άτομο μπορεί να υποβάλει μια ανώνυμη καταγγελία στη Safeline. Αυτό γιατί με την διασφάλιση της ανωνυμίας δίνει θάρρος στους χρήστες να καταγγείλουν ένα περιστατικό και όχι να αισθανθούν δισταγμούς ή ενδυασμούς. Η διεύθυνση IP (Internet Protocol) του υπολογιστή που χρησιμοποιείται για την καταγγελία δεν καταχωρείται από το σύστημα της Safeline και εάν κάποιος χρήστης θελήσει να δώσει τα στοιχεία του, αυτά παραμένουν απόρρητα και χρησιμοποιούνται αποκλειστικά μόνο για την δική του ενημέρωση για την εξέλιξη της καταγγελίας του.
Επίσης, καταγγελία μπορεί να υποβάλει ο χρήστης και μέσω της εφαρμογής Android της Safeline που είναι και αυτή εντελώς ανώνυμη.
Μετέπειτα, η Safeline λαμβάνοντας μια καταγγελία ακολουθεί μια προκαθορισμένη διαδικασία, η οποία αναλόγα με την σοβαρότητα της κάθε καταγγελίας αλλάζει και τις ενέργειες στις οποίες θα προβεί, όπως θα δούμε και στο διάγραμμα που βρίσκεται στα δεξία μας.

Όσον αφορά το περιεχόμενο των καταγγελιών που λαμβάνει η Safeline, το μεγαλύτερο ποσοστό ανηκεί στην κατηγορία των προσωπικων δεδομένων στα 34% καθώς το ένα τρίτο των περιπτώσεων των αναφορών είχαν να κάνουν με την έλλειψη σεβασμού της διαδικτυακής ταυτότητας και της ιδιωτικής ζωής των χρηστών του Διαδικτύου. Η παρανομία αυτή έχει ως χώρα

προέλευσης την Ελλάδα, έτσι οι καταγγελίες που λαμβάνει η Safeline προωθούνται στην Μονάδα Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας και στις δύο ανεξάρτητες αρχές που είναι η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών και η Αρχή Προστασίας Προσωπικών Δεδομένων. Σε οποιαδήποτε περίπτωση που το παράνομο περιεχόμενο έχει χώρα προέλευσης σε άλλη χώρα του εξωτερικού οι καταγγελίες δίδονται στις αντίστοιχες Ανοιχτές Γραμμές του εξωτερικού μέσω της κοινής βάσης του INHOPE.

Η ραγδαία αυτή αύξηση των καταγγελιών που κατά κύριο λόγο αφορούν το facebook είναι δύσκολο να προσδιοριστούν ως αιτία. Μια όμως θα μπορούσε να είναι η αύξηση των χρηστών του διαδικτύου φτιάχνοντας προφίλ στο ευρέως διαδεδομένο κοινωνικό δίκτυο.

Βλέπουμε όμως ότι από το διάγραμμα που μας παρατίθεται υπάρχει μαζική αύξηση της τάξεως του 11% στην κατηγορία της παιδικής πορνογραφίας, ενώ το 2010 ήταν της τάξεως του 6% (Βλέπε σελίδα 47, Στατιστικά Στοιχεία Safeline) .

ΣΥΓΚΡΙΣΕΙΣ

Στο κεφάλαιο αυτό θα σας παραθέσουμε την σύγκριση ανάμεσα στο saferinternet.gr, στο e-crime και στο safeline.gr , δηλαδή τις ομοιότητες – διαφορές και τα πλεονεκτήματα – μειονεκτήματα με στόχο να ανακαλύψουμε την κλίμακα βαρύτητας που δίνεται σε καθέ μια από τις τρείς ιστοσελίδες (sites), για να μπορέσουμε να τα κατατάξουμε σε κατηγορίες ανάλογα με την ιδιαιτερότητα τους και από στατιστική άποψη ανάλογα με το πόσο χρησιμοποιούνται.

Πρωταρχικά, το saferinternet.gr ασχολείτε με δραστηριότητες, με σκοπό την πραγματοποίηση διαφόρων προγραμμάτων, την πλήρη ενημέρωση και καθοδήγηση των τριών μεγάλων κατηγοριών του (μεγάλοι, έφηβοι παιδιά), όμως με συνοπτικές πληροφορίες για το τι θα πρέπει να προσέχουν και τι όχι και το αλφαβητάριο.

Ύστερα, το e – crime ασχολείται με την πλήρης ενημέρωση για το τι είναι έγκλημα αρχικά και μετά φτάνει στον τελικό ορισμό σε συνδυασμό με το διαδίκτυο που είναι το ηλεκτρονικό έγκλημα ή αλλιώς e – crime. Αυτό γιατί μετέπειτα διαχωρίζει το ηλεκτρονικό έγκλημα από το παραδοσιακό έγκλημα αναλύοντας τα χαρακτηριστικά τους. Αναφέρει λεπτομερώς όλες τις μορφές του ηλεκτρονικού εγκλήματος και τα μέτρα πρόληψης. Παρέχει και αυτό αλφαβητάριο.

Τέλος, το safeline.gr ασχολείται εκτενέστερα και βαθύτερα με τα δικαιώματα και την προστασία των χρηστών βάση νόμου, με την καταγγελία και την ανωνυμία και με τις παράνομες δραστηριότητες του διαδικτύου.

Βλέπουμε πως κάθε μια από τις τρεις ιστοσελίδες μπορεί κάπου να κερδίζει σε πληροφορίες και ενημέρωση και κάπου αλλού να χάνει. Αυτό συμβαίνει όμως, διότι η κάθε ιστοσελίδα ασχολείται με ένα συγκεκριμένο θέμα, με αποτέλεσμα το ένα να συμπληρώνει το άλλο.

Επιπρόσθετα, με μια καλύτερη παρατήρηση βλέπουμε ότι saferinternet.gr και το safeline.gr βρίσκονται υπό την ίδια αιγίδα, αυτό γιατί το safeline.gr λειτουργεί με την υποστήριξη του saferinternet.gr. Έτσι καταλαβαίνουμε πως τα δύο αυτά θέματα επικαιρότητας που προκύπτουν από τις δύο ιστοσελίδες που μόλις προαναφέραμε, επειδή χρειάζονται σωστή και προσεγμένη ενημέρωση – μελέτη, για να καλύψουν με ευκρίνεια κάθε στοιχείο έχουν χωριστεί σε αυτές τις δύο ιστοσελίδες για την καλύτερη και μεγαλύτερη απόδοση.

ΕΠΙΛΟΓΟΣ / ΣΥΜΠΕΡΑΣΜΑΤΑ

Φτάνοντας στο τέλος της παρουσίασης παρατηρούμαι ότι οι τρεις ιστοσελίδες (sites) κάνουν ότι είναι δυνατό για να ενημερώσουν, να προστατέψουν και να συμβουλέψουν όλους τους χρήστες του διαδικτύου, έτσι ώστε κάθε πλοήγηση στο διαδίκτυο να είναι αρμονική με ασφάλεια και όχι με την αίσθηση του φόβου να υπάρχει μέσα στο μυαλό.

Παρ' όλα αυτά επειδή είναι ευρέως γνωστό ότι με το διαδίκτυο κυκλοφορεί και παραμονεύει πάντοτε ο κίνδυνος, η κάθε ιστοσελίδα στοχεύει και δρα πάνω στο στοιχείο της, έτσι ώστε με την οποιαδήποτε νέα απειλή του κυβερνοχώρου να ξέρουν να δράσουν άμεσα και σώστα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΗΛΕΚΤΡΟΝΙΚΟΙ ΙΣΤΟΤΟΠΟΙ

- Saferinternet.gr – Για ένα ασφαλέστερο Διαδίκτυο. Internet Version: http://www.saferinternet.gr/
- Ηλεκτρονικό Έγκλημα, απάτη στο διαδίκτυο, ασφάλεια στο διαδίκτυο, παιδική πορνογραφία, phising, κοινωνικά δίκτυα. Internet Version: http://www.e-crime.gr/
- Safeline.gr: Η Ελληνική Ανοιχτή Γραμμή για το παράνομο περιεχόμενο στο διαδίκτυο/ Safeline. Internet Version: http://www.safeline.gr/

ΒΙΒΛΙΑ

- Τσουραμάνης Χρ.Ε.(2010) Οικονομία και εγκληματικότητα, Αθήνα, Εκδόσεις Βας.Ν.Κατσαρού

ΠΑΡΑΡΤΗΜΑ

ΠΑΡΑΡΤΗΜΑ 1^{Ο} :

ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ SAFELINE