Γραμματισμός Μέσων στον Ψηφιακό Κόσμο: Υποστήριξη των Εκπαιδευτικών μέσω μιας ολιστικής σχολικής προσέγγισης

MeLDE

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union

Emphasys CENTRE

UNIVERSITY OF WOLVERHAMPTON

ANT

BÜRGERHAUS ENNOHAUS

DEMOKRITOS

Ενότητα 4: Διαδικτυακή Ασφάλεια

ΠΕΡΙΓΡΑΦΗ

Η θεματική ενότητα αυτή αποσκοπεί να εισάγει τους εκπαιδευτικούς σε ένα ευρύ φάσμα περιπτώσεων και τρόπων για να παραμείνουν ασφαλείς στο διαδίκτυο. Θα συζητηθούν θέματα, όπως κίνδυνοι και υποχρεώσεις στο διαδίκτυο, προστασία προσωπικών δεδομένων, διαδικτυακή παραπληροφόρηση και επιβλαβές περιεχόμενο, ψηφιακά πνευματικά δικαιώματα και αποτελεσματικές και αναποτελεσματικές πρακτικές για το διαδικτυακό εκφοβισμό.

Ενότητα 4: Διαδικτυακή Ασφάλεια

MeLDE

ΛΙΣΤΑ ΜΕ ΤΑ ΘΕΜΑΤΑ

ΘΕΜΑ 1 ΔΙΑΔΙΚΤΥΑΚΟΙ ΚΙΝΔΥΝΟΙ ΚΑΙ ΕΥΘΥΝΕΣ

ΘΕΜΑ 2 ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΘΕΜΑ 3 ΨΗΦΙΑΚΑ ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ

ΘΕΜΑ 4 ΔΙΑΔΙΚΤΥΑΚΗ ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗ ΚΑΙ ΕΠΙΒΛΑΒΕΣ ΠΕΡΙΕΧΟΜΕΝΟ

ΘΕΜΑ 5 ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΦΟΒΙΣΜΟΣ

Ενότητα 4: Διαδικτυακή Ασφάλεια

ΠΕΡΙΕΧΟΜΕΝΑ

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις
- Πιθανές απειλές για το υλικό και το λογισμικό
- Απειλές για τα Δεδομένα και τις Πληροφορίες
- Τρόποι αναφοράς Διαδικτυακών απατεώνων
- Διαδικτυακά δικαιώματα και υποχρεώσεις

Θέμα 2: Προστασία προσωπικών δεδομένων
- Δημιουργία και Διατήρηση ισχυρών κωδικών
- Η σημασία ενός ενημερωμένου λειτουργικού συστήματος και ενός ενημερωμένου λογισμικού, ενάντια σε κακόβουλα λογισμικά
- Ευαλωτότητα των Κινητών Συνσκευών και Τρόποι να τις διατηρήσεις Ασφαλείς
- Κακόβουλη ηλεκτρονική Αλληλογραφία
- Τρόποι πραστασίας Προσωπικών Δεδομένων στις σελίδες Κοινωνικού Δικτύου

Θέμα 3: Ψηφιακά πνευματικά δικαιώματα
- Συζήτηση νέων νομικών και πολιτικών εξελίξεων του νόμου περί πνευματικών δικαιωμάτων και κατανόηση της υιοθέτησής του στην ψηφιακή εποχή
- Κατανόηση της προστασίας του ψηφιακού περιεχομένου που δημιουργήθηκε και δημοσιεύτηκε από τους μαθητές σου
- Κατανόηση της λογοκλοπής και αποφυγή της στην εποχή της υπερφορτωμένης πληροφορίας, όπου το περιεχόμενο μπορεί να χρησιμοποιηθεί και να επαναχρησιμοποιηθεί με ποικίλους τρόπους από αναρίθμητες πηγές.
- Εξερεύνηση μιας σειράς πηγών ελέυθερων σε πρόσβαση και κατανόηση του γιατί και του πότε μπορεί να χρησιμοποιηθεί και να επαναχρησιμοποιηθεί το ψηφιακό υλικό για εκπαιδευτικούς σκοπούς
- Εργασία σε ομάδες για παραγωγή μικρού και ευανάγνωστου εγχειριδίου σχετικά με τα πνευματικά δικαιώματα για τα σχολεία των ομάδων αυτών.

Ενότητα 4: Διαδικτυακή Ασφάλεια

MeLDE

ΠΕΡΙΕΧΟΜΕΝΑ

Θέμα 4: Διαδικτυακή παραπληροφόρηση και επιβλαβές περιεχόμενο

- Η διαφορά ανάμεσα σε μια γνήσια ιστοσελίδα και σε ένα αντίγραφο
- Αξιολόγηση και αναφορά ιστοσελίδων απάτης
- Η έννοια της 'ψεύτικης είδησης' και πώς να την αξιολογήσεις και να την αναγνωρίσεις
- Γιατί είναι σημαντικό να αναφέρεις τις ιστοσελίδες απάτης και ο επιβλαβής αντίκτυπος τους στη δημοκρατία, την κοινωνία, αλλά και σε ατομικό επίπεδο

Θέμα 5: Διαδικτυακός Εκφοβισμός

- Τι είναι διαδικτυακός εκφοβισμός και γιατί είναι σημαντικός
- Διαφορετικές μορφές διαδικτυακού εκφοβισμού
- Αναγνώριση μαθητών που έπεσαν θύματα διαδικτυακού εκφοβισμού με πολλαπλούς τρόπους
- Δράσεις που θα βοηθήσουν τους μαθητές που έπεσαν θύματα διαδικτυακού εκφοβισμού
- Η σημασία της παρεμβατικής και αποτρεπτικής στρατηγικής στα σχολεία σε σχέση με το διαδικτυακό εκφοβισμό

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ ΚΑΙ ΥΠΟΚΑΤΗΓΟΡΙΕΣ

Σε αυτή τη θεματική ενότητα οι εκπαιδευτικοί θα γνωρίσουν μια σειρά από κινδύνους που μπορούν να συναντήσουν στο διαδίκτυο και θα συζητηθούν οι κίνδυνοι και οι υποχρεώσεις γενικότερα στον ψηφιακό κόσμο. Η ενότητα αυτή θα καλύψει διαφορετικές απειλές για το υλικό και το λογισμικό, αλλά και για τα Δεδομένα και τις Πληροφορίες, όπως τύποι διαδικτυακού εγκλήματος, κακόβουλο λογισμικό, οικονομικές απώλειες, πλαστοπροσωπία και διαδικτυακοί απατεώνες και θα μάθει στον κάθε ένα, πώς να προστατεύεται απέναντι σε αυτούς τους κινδύνους και πώς να μάθει αυτός με τη σειρά του στους μαθητές του τους κινδύνους αυτούς.

Θα συζητηθούν τα ακόλουθα:

- Πιθανές απειλές για το υλικό και το λογισμικό
- Απειλές για τα Δεδομένα και τις Πληροφορίες
- Τρόποι αναφοράς Διαδικτυακών απατεώνων
- Διαδικτυακά δικαιώματα και υποχρεώσεις

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΠΙΘΑΝΕΣ ΑΠΕΙΛΕΣ ΓΙΑ ΤΟ ΥΛΙΚΟ ΚΑΙ ΤΟ ΛΟΓΙΣΜΙΚΟ

ΑΠΕΙΛΕΣ ΓΙΑ ΤΟ ΥΛΙΚΟ

Meltdown

Το Meltdown αποτελεί ένα πρόγραμμα εκμετάλλευσης της ευπάθειας των σύγχρονων επεξεργαστών του Η/Υ, επιτρέποντας την πρόσβαση στη μνήμη του συστήματος, παρακάμπτοντας την πιο βασική απομόνωση μεταξύ των χρηστών εφαρμογών και του λειτουργικού συστήματος. Ένα χαρακτηριστικό της κεντρικής μονάδας του επεξεργαστή είναι ότι μπορεί να εκτελέσει οδηγίες και διαδικασίες εκτός λειτουργίας. Αυτό είναι μεν χρήσιμο για την επιτάχυνση της επεξεργασίας του κώδικα, αλλά ανοίγει κι ένα παράθυρο προσωρινής εκτέλεσης, στο οποίο επιτρέπεται μη εξουσιοδοτημένη πρόσβαση στο χώρο του πυρήνα.

Row hammer

Οι επιθέσεις Row hammer εκμεταλλεύονται τις ηλεκτρικές αλληλεπιδράσεις μεταξύ των γειτονικών κελιών μνήμης, σε υψηλής πυκνότητας καρτών Δυναμικής Μνήμης Τυχαίας Προσπέλασης (DRAM), για να προκαλέσει σφάλματα μνήμης. Εάν κάποιος εχθρός με περιορισμένα δικαιώματα, αποκτήσει πρόσβαση στη Δυναμική κάρτα μνήμης τυχαίας προσπέλασης της μηχανής που στοχεύει, με συγκεκριμένα μοτίβα, μπορεί να προκαλέσει αλλαγές των bits σε περιοχές της μνήμης, στις οποίες διαφορετικά δε θα είχε πρόσβαση. Το πρόβλημα αυτό δε μπορεί να λυθεί με κανένα λογισμικό επιδιόρθωσης. Η μόνη εφικτή λύση, είναι η αντικατάσταση όλων των μονάδων Δυναμικής μνήμης τυχαίας προσπέλασης.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

ΠΙΘΑΝΕΣ ΑΠΕΙΛΕΣ ΓΙΑ ΤΟ ΥΛΙΚΟ ΚΑΙ ΤΟ ΛΟΓΙΣΜΙΚΟ

Ηλεκτρονικοί Υπολογιστές με συμβατικά BIOS (Βασικό Σύστημα Εισόδου-Εξόδου)

Οι παλαιότεροι Η/Υ με συμβατικά BIOS, δεν είναι συμβατοί με το μηχανισμό Secure Boot. Αυτός ο μηχανισμός υποστηρίζεται από το UEFI (Unified Extensible Firmware Interface), και αποτελεί μια πιο εκσυγχρονισμένη λύση για τα χαμηλού επιπέδου λογισμικά σε πρόσφατες μητρικές κάρτες, ο οποίος ξεκινά με την έναρξη του Η/Υ, πριν μπει σε λειτουργία το λειτουργικό σύστημα. Το Secure Boot αποτρέπει το κοκόβουλο λογισμικό να φορτώσει σε έναν Η/Υ κατά τη διάρκεια της εκκίνησης, ελέγχοντας την εγκυρότητα του συστήματος. Το UEFI υποστηρίζει και λειτουργίες δικτύωσης κατευθείαν στα μόνιμα προγράμματα του λογισμικού της ROM, οι οποίες βοηθούν στη διαχείριση της επίλυσης προβλημάτων και της ρύθμισης παραμέτρων.

Παλιά routers

Πολλά routers που δόθηκαν σε καταναλωτές από την Internet Service Providers (ISP) ανά τον κόσμο, περιέχουν σοβαρές ατέλειες, οι οποίες επιτρέπουν στους hackers να τα ελέγχουν. Τα περισσότερα routers έχουν ένα ευάλωτο σημείο (“directory traversal”), ως προς την ασφάλεια, σε ένα σημείο των μόνιμων προγραμμάτων του λογισμικού της ROM, το λεγόμενο webproc.cgi, το οποίο επιτρέπει στους hackers να εξάγουν ευαίσθητα δεδομένα ρύθμισης παραμέτρων, συμπεριλαμβανομένων των διαπιστευτηρίων διαχειριστή. Μόλις παραβιαστεί το router, μπορεί να χρησιμοποιηθεί για Denial of Service attacks (DDoS)- *Επιθέσεις άρνησης εξυπηρέτησης* ή για πιστοποίηση των διαπιστευτηρίων. Μπορούν επίσης να χρησιμοποιηθούν για να κρύψουν πηγές παράνομων δραστηριοτήτων, αφού οι κινήσεις θα φαίνεται ότι γίνονται από τυχαίες διευθύνσεις και όχι από αυτές που προέρχονται στην πραγματικότητα.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

ΠΙΘΑΝΕΣ ΑΠΕΙΛΕΣ ΓΙΑ ΤΟ ΥΛΙΚΟ ΚΑΙ ΤΟ ΛΟΓΙΣΜΙΚΟ

ΑΠΕΙΛΕΣ ΣΤΟ ΛΟΓΙΣΜΙΚΟ

Ιός Η/Υ

Οι ιοί στους Η/Υ είναι μία από τις πιο κοινές απειλές απέναντι στη διαδικτυακή ασφάλεια. Ένας τέτοιος ιός, είναι ένας επιβλαβής κωδικός ή ένα επιβλαβές πρόγραμμα που δημιουργείται για να αλλάξει τον τρόπο με τον οποίο λειτουργεί ένας Η/Υ, σχεδιάζεται για να μεταδοθεί από τον έναν εξυπηρετητή στον άλλο και έχει τη δυνατότητα να κάνει αντίγραφα του εαυτού του. Συνήθως στέλνεται ως συνημμένο αρχείο σε κάποιο email ή κατεβαίνει από μια συγκεκριμένη ιστοσελίδα, με σκοπό να μολύνει τον Η/Υ, αυτού που τον κατεβάζει. Μόλις οι συνθήκες προκαλέσουν ένα υπολογιστή ή μια συσκευή να εκτελέσει τον κώδικα του ιού, μπορεί να αρχίσει να στέλνει ανεπιθύμητη αλληλογραφία, να απενεργοποιεί τις ρυθμίσεις ασφαλείας της συσκευής, να διεφθείρει ή να κλέψει δεδομένα, συμπεριλαμβανομένων των προσωπικών δεδομένων, όπως είναι οι κωδικοί. Οι ιοί μπορούν επίσης να διαγράψουν τα πάντα από τις κάρτες HDD, SSD , SD της συσκευής που παραβιάστηκε.

Adware – Λογισμικό για διαφημίσεις

Ως Adware θεωρείται κάθε λογισμικό, το οποίο έχει σχεδιαστεί για να εντοπίζει τα δεδομένα ή τις πιο συνηθισμένες περιηγήσεις των χρηστών και με βάση αυτό, να τους εμφανίζει διαφημίσεις και αναδυόμενα παράθυρα. Τα Adware μαζεύουν δεδομένα με τη συγκατάθεση των χρηστών και αποτελούν μια νόμιμη πηγή εισοδήματος για τις εταιρείες που επιτρέπουν στους χρήστες να δοκιμάζουν το λογισμικό τους δωρεάν, αλλά με την ταυτόχρονη παρουσία διαφημίσεων. Ο σκοπός των adware είναι συνήθως κρυμμένος στα έγγραφα που σχετίζονται με τη Αποδοχή Χρήσης (User Agreement), αλλά μπορεί να ελεγχθεί με μια καλή ανάγνωση των όρων που αποδεχόμαστε, όταν εγκαθιστούμε ένα λογισμικό στη συσκευή μας. Η παρουσία του adware σε έναν Η/Υ παρατηρείται μόνο μέσα από τα αναδυόμενα παράθυρα και μερικές φορές μπορεί να επιβραδύνει τον επεξεργαστή και την ταχύτητα του διαδικτύου. Όταν το adware κατεβαίνει χωρίς να υπάρχει συγκατάθεση, πρόκειται για επιβλαβές περιεχόμενο.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΠΙΘΑΝΕΣ ΑΠΕΙΛΕΣ ΓΙΑ ΤΟ ΥΛΙΚΟ ΚΑΙ ΤΟ ΛΟΓΙΣΜΙΚΟ

Spyware- Λογισμικό κατασκοπίας

Το Spyware λειτουργεί παρόμοια με το adware, αλλά εγκαθίσταται στον Η/Υ σου εν αγνοία σου. Θεωρείται ένα λογισμικό, το οποίο αλλάζει τον υπολογιστή του χρήστη με κάποιον τρόπο, κάνοντας από μόνο του εγκατάσταση ή αποθηκεύοντας δεδομένα στον υπολογιστή για μεταγενέστερη ανάκτηση. Μπορεί να περιέχει keyloggers (καταγραφή πληκτρολόγησης) που κρατάει προσωπικές πληροφορίες, συμπεριλαμβανομένων των διευθύνσεων email, κωδικών, ακόμα και κωδικούς πιστωτικών καρτών, κάνοντάς το πολύ επικίνδυνο εξαιτίας του υψηλού κινδύνου πλαστοπροσωπίας.

Μη ενημερωμένα ή ξεπερασμένα λειτουργικά συστήματα/λογισμικά/προγράμματα περιήγησης

Τα λογισμικά έχουν μικρό κύκλο ζωής, διατηρούνται μέσω συνεχών ενημερώσεων και αναβαθμίσεων. Τα μη ενημερωμένα ή ξεπερασμένα λειτουργικά συστήματα/ λογισμικά/ προγράμματα περιήγησης θέτουν πιθανώς την ασφάλεια του χρήστη σε κίνδυνο, μέσω των ατελειών και των κενών που δημιουργούνται στο σύστημα και δεν έχουν ανακαλυφθεί και επιδιορθωθεί ακόμα. Τα μη ενημερωμένα ή ξεπερασμένα συστήματα είναι εύκολα προσβάσιμα για τους hackers και έτσι μπορούν να εκμεταλλευτούν την ευπάθεια του επιπέδου ασφαλείας του συστήματος. Επίσης, τα ξεπερασμένα συστήματα είναι εκτεθειμένα σε επιθέσεις εκβιασμού, με την έννοια ότι μια μορφή κακόβουλου λογισμικού μπορεί να χτυπήσει το σύστημα, να κρυπτογραφήσει τα αρχεία του χρήστη και να απαιτεί έπειτα χρήματα για να επιδιορθώσει τα δεδομένα μέσω πληρωμής.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΠΙΘΑΝΕΣ ΑΠΕΙΛΕΣ ΓΙΑ ΤΟ ΥΛΙΚΟ ΚΑΙ ΤΟ ΛΟΓΙΣΜΙΚΟ

ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ Η/Υ ΣΟΥ

- Κράτα το πρόγραμμα προστασίας ανοικτό
- Κάνε εγκατάσταση ή ενημέρωσε το λογισμικό antivirus (αντιιικό)
- Κάνε εγκατάσταση ή ενημέρωσε τα αντικατασκοπευτικά σου προγράμματα
- Κράτα ενημερωμένο και έγκυρο το λειτουργικό σου σύστημα
- Να είσαι προσεκτικός στο κατέβασμα υλικού
- Κλείνε τον Η/Υ σου
- Κάνε συχνά επιδιορθώσεις στο σύστημα και το λογισμικό, ώστε να αποτρέψεις τους διαδικτυακούς εγκληματίες να εκμεταλλευτούν τα κενά και τις ευπάθειες του συτήματός σου και έτσι να κάνουν επιθέσεις
- Κατέβασε αρχεία και λογισμικό μόνο από αξιόπιστες ιστοσελίδες
- Μην ανοίγεις συνδέσμους, emails ή συνημμένα αρχεία από άγνωστους ή ύποπτους αποστολείς

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

ΑΠΕΙΛΕΣ ΣΕ ΔΕΔΟΜΕΝΑ ΚΑΙ ΠΛΗΡΟΦΟΡΙΕΣ

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Hacking – Ηλεκτρονική πειρατεία

Οι hackers των Η/Υ είναι μη εξουσιοδοτημένοι χρήστες, οι οποίοι μπαίνουν στο σύστημα των υπολογιστών, με σκοπό να κλέψουν, να αλλάξουν, να υφαρπάξουν ή να καταστρέψουν πληροφορίες, εγκαθιστώντας συνήθως επιβλαβές υλικό, χωρίς την ενημέρωση ή τη συγκατάθεση του χρήστη. Οποιοσδήποτε χρησιμοποιεί ένα ηλεκτρονικό υπολογιστή συνδεδεμένο με το διαδίκτυο, είναι ευάλωτος σε αυτή την απειλή. Όσο ο Η/Υ είναι συνδεδεμένος στο διαδίκτυο, το κοκόβουλο υλικό που έχει εγκαταστήσει ο hacker θα μεταφέρει μυστικά προσωπικές και οικονομικές πληροφορίες εν αγνοία του χρήστη και φυσικά χωρίς να συναινέσει.

Keylogging – Καταγραφή πληκτρολόγησης

Μια από τις καλύτερες τεχνικές λήψης κωδικών είναι η καταγραφή απομακρυσμένης πληκτρολόγησης, γνωστή ως keylogging, η οποία ουσιαστικά είναι η χρήση λογιμικού ή υλικού για να καταγράψεις, ποιά πλήκτρα πατιούνται κατά την πληκτρολόγηση στον Η/Υ. Η καταγραφή της πληκτρολόγησης είναι μία λειτουργία, η οποία αποθηκεύει ή πλητρολογεί σε έναν Η/Υ. Αν το δεις σε αρχικό το επίπεδο, κάτι τέτοιο φαίνεται εντελώς άκακο. Στα χέρια ενός hacker ή ενός ηλεκτρονικού απατεώνα όμως, το keylogger αποτελεί ένα ισχυρό εργαλείο για να κλέψουν πληροφορίες. Οι καταγραφείς πληκτρολόγησης είναι μια σοβαρή απειλή για τους χρήστες και τα δεδομένα τους, καθώς παρακολουθούν την πληκτρολόγηση για να εκμαιεύσουν κωδικούς και άλλα ευαίσθητα δεδομένα. Αυτό δίνει στους hackers το προνόμιο, να έχουν πρόσβαση σε κωδικούς PIN και νούμερα λογαριασμών, κωδικούς σε ιστοσελίδες ηλεκτρονικών μαγαζιών, ονόματα χρηστών και ταυτότητες ηλεκτρονικής αλληλογραφίας και άλλες εμπιστευτικές πληροφορίες.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΑΠΕΙΛΕΣ ΣΕ ΔΕΔΟΜΕΝΑ ΚΑΙ ΠΛΗΡΟΦΟΡΙΕΣ

Pharming

Ο όρος Pharming είναι μια σύνθετη λέξη από το "phishing" (ψαρεύω) και το "farming" (καλλιεργώ) και είναι μια πρακτική απάτης, με την οποία επιβλαβής κωδικός εγκαθίσταται σε έναν Η/Υ και έπειτα ο χρήστης οδηγείται παραπλανητικά σε ιστοσελίδες που δραστηριοποιούνται απατεώνες, χωρίς να λάβει γνώση και να συναινέσει. Το Pharming εκμεταλλεύεται τη βάση του τρόπου με τον οποίο λειτουργούν τα προγράμματα περιήγησης στο διαδίκτυο. Η σειρά των γραμμάτων που διαμορφώνουν μια διαδικτυακή διεύθυνση, όπως το www.google.com, πρέπει να μετατραπεί σε μία διεύθυνση IP από έναν DNS server, για να μπορέσει να γίνει η σύνδεση. Οι επιθέσεις του Pharming εκμεταλλεύονται αυτή τη διαδικασία μέσω της εγκατάστασης ενός ιού ή ενός Trojan (εξηγείται παρακάτω) από κάποιον hacker στον Η/Υ ενός χρήστη, για να αλλάξει τα αρχεία του εξυπηρετητή και συνεπώς και την πορεία του μακριά από το στόχο του και έτσι να καταλήξει σε μια ιστοσελίδα απάτης. Οι παράνομες ιστοσελίδες μπορούν να χρησιμοποιηθούν για να εγκαταστήσουν ιούς ή Trojans στον Η/Υ του χρήστη, ή μπορούν να προσπαθήσουν να συλλέξουν προσωπικές και οικονομικές πληροφορίες, για πλαστοπροσωπία.

Social Engineering

Social Engineering, στο πλαίσιο της ασφάλειας της πληροφορίας, είναι η απάτη μέσω της οποίας οι χρήστες χειραγωγούνται, ώστε να γνωστοποιήσουν εμπιστευτικές ή προσωπικές πληροφορίες, οι οποίες μπορούν να χρησιμοποιηθούν για δόλιους σκοπούς. Χρησιμοποιείται ψυχολογική χειραγώγηση για να ξεγελαστούν οι χρήστες και να κάνουν λάθη ως προς την ασφάλεια ή να φανερώσουν ευαίσθητες πληροφορίες. Ο δράστης αρχικά ερευνά το θύμα του, για να μαζέψει χρήσιμες πληροφορίες, όπως πιθανά σημεία εισόδου και αδύναμα πρωτόκολλα ασφάλειας, αναγκαία για την επίθεση. Έπειτα, προσπαθεί να κερδίσει την εμπιστοσύνη του θύματος και να του δώσει το κίνητρο να ακολουθήσει ενέργειες που σπάνε την ασφάλεια, όπως το να αποκαλύψει ευαίσθητες πληροφορίες ή να δώσει πρόσβαση σε κρίσιμες πηγές. Αυτό που κάνει την τεχνική του social engineering ιδιαίτερα επικίνδυνη, είναι ότι ποντάρει στο ανθρώπινο λάθος, αντί να ψάχνει πού είναι ευάλωτα το λογισμικό και το λειτουργικό σύστημα. Λάθη που γίνονται από νόμιμους χρήστες δεν προβλέπονται εύκολα, κάνοντας την αναγνώριση και την αποτροπή τους πολύ πιο δύσκολη από ότι μια εισβολή βασισμένη σε κακόβουλο υλικό.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΑΠΕΙΛΕΣ ΣΕ ΔΕΔΟΜΕΝΑ ΚΑΙ ΠΛΗΡΟΦΟΡΙΕΣ

DOS and DDOS attack

Μία επίθεση Denial of Service (DoS) γίνεται σε μια μηχανή και στη σύνδεση της με το διαδίκτυο, κατακλύζοντας μια ιστοσελίδα με αιτήσεις για εξυπηρέτηση και κάνοντας ακατόρθωτο για τους νόμιμους χρήστες να έχουν πρόσβαση στις υπηρεσίες της σελίδας αυτής.

Οι επιθέσεις Distributed Denial of Service (DDoS) attack είναι παρόμοιες με τις DOS, αλλά είναι πιο ισχυρές. Είναι πολύ πιο δύσκολο να αντικρούσεις μια επίθεση DDoS. Εξαπολύεται από πολλούς Η/Υ, με τον αριθμό των υπολογιστών να ανέρχεται από δυο-τρεις μέχρι και χιλιάδες και ακόμα περισσότερους. Εφόσον είναι πιθανό, να μην ανήκουν όλες οι συσκευές στον απατεώνα, ενώνονται και προσθέτονται και αυτές στο δίκτυο αυτού που κάνει την επίθεση, με κακόβουλο λογισμικό. Αυτοί οι Η/Υ μπορεί να διανεμηθούν σε όλο τον κόσμο και το δίκτυο που δημιουργείται μεταξύ τους, ονομάζεται botnet. Επειδή η επίθεση γίνεται από τόσες πολλές και διαφορετικές διευθύνσεις IP ταυτόχρονα, μία επίθεση DDoS κάνει πολύ πιο δύσκολο για το θύμα, να ανιχνεύσει το δράστη και να αμυνθεί.

Phishing

Το Phishing είναι μια μέθοδος κοινωνικής μηχανής, με σκοπό την απόκτηση ευαίσθητων δεδομένων, όπως κωδικοί, ονόματα χρηστών και νούμερα πιστωτικών καρτών. Οι επιθέσεις γίνονται συνήθως με τη μορφή άμεσου μηνύματος ή ηλεκτρονικής αλληλογραφίας, που αρχικά φαίνονται νόμιμα. Ο παραλήπτης του email παραπλανάται τότε, ώστε να ανοίξει έναν επιβλαβή σύνδεσμο, ο οποίος οδηγεί στην εγκατάσταση κακόβουλου λογισμικού στον Η/Υ του. Μπορεί επίσης να λάβει προσωπικές πληροφορίες, στέλνοντας ένα email, το οποίο φαίνεται πως εστάλη από τράπεζα, ζητώντας από το χρήστη να πιστοποιήσει την ταυτότητα του, δίνοντας προσωπικές πληροφορίες.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΑΠΕΙΛΕΣ ΣΕ ΔΕΔΟΜΕΝΑ ΚΑΙ ΠΛΗΡΟΦΟΡΙΕΣ

Spamming – Αποστολή ανεπιθύμητων μηνυμάτων

Ο κατακλυσμός του διαδικτύου με αυθαίρετα και παραπλανητικά μηνύματα, μπορεί να οριστεί ως spamming. Ο όρος Spam χρησιμοποιείται ως επι το πλείστον για επιθετική εμπορική διαφήμιση. Η πιο κοινή μορφή του είναι η ανεπιθύμητη αλληλογραφία και ακολουθούν τα ανεπιθύμητα αποτελέσματα στη μηχανή αναζήτησης. Η πρώτη αναφέρεται στην πρακτική αποστολής ανεπιθύμητων μηνυμάτων μέσω email σε μια αδιάκριτη ομάδα παραληπτών. Η δεύτερη, στην πρακτική τροποποίησης των σελίδων HTML, για να αυξήσουν τις πιθανότητες να τοποθετηθούν στις πρώτες θέσεις των αποτελεσμάτων της μηχανής αναζήτησης.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΑΠΕΙΛΕΣ ΣΕ ΔΕΔΟΜΕΝΑ ΚΑΙ ΠΛΗΡΟΦΟΡΙΕΣ

MALWARE (ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ)

Rogue security software

Το Rogue security software είναι ένα κακόβουλο λογισμικό που παραπλανητικά κάνει τους χρήστες να πιστεύουν, πως κάποιος ιός έχει εγκατασταθεί στον Η/Υ τους ή πως τα μέτρα ασφαλείας τους δεν είναι σωστά ενημερωμένα. Έτσι, προσφέρονται προς εγκατάσταση ή προς ενημέρωση των ρυθμίσεων ασφαλείας του χρήστη. Θα ζητήσουν από το χρήστη είτε να καταβάσει το πρόγραμμά τους για να απομακρύνει τους υποτιθέμενους ιούς, ή να πληρώσει για ένα εργαλείο. Και οι δυο περιπτώσεις, οδηγούν σε κακόβουλο υλικό, που εγκαθίσταται στον Η/Υ του θύματος.

Trojan horse

Το Trojan horse, or “Trojan”, είναι ένα κακόβουλο κομμάτι ενός επιτιθέμενου κωδικού, που παραπλανά τους χρήστες να το τρέξουν οικειοθελώς, ενώ είναι κρυμμένο πίσω από ένα νόμιμο πρόγραμμα. Συνήθως μεταδίδεται μέσω email, το οποίο φαίνεται να είναι από κάποιον γνωστό σου, και όταν κλικάρεις πάνω του και στο συνημμένο του αρχείο, κατεβάζεις αμέσως κακόβουλο λογισμικό στον Η/Υ. Τα Trojans ματαδίδονται επίσης όταν κλικάρεις σε διαφήμιση που είναι απάτη. Αν μπει στον υπολογιστή σου, το Trojan horse μπορεί να καταγράψει τους κωδικούς σου από αποθήκευση πληκτρολόγησης, να οικειοποιηθεί τη διαδικτυακή κάμερα και να κλέψει ευαίσθητα δεδομένα που πιθανώς έχεις στον Η/Υ.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΑΠΕΙΛΕΣ ΣΕ ΔΕΔΟΜΕΝΑ ΚΑΙ ΠΛΗΡΟΦΟΡΙΕΣ

Computer worm

Τα Computer worms είναι κομμάτια κακόβουλων προγραμμάτων, τα οποία αυτοαναπαράγονται γρήγορα και διαδίδονται από τον ένα Η/Υ στον άλλο. Ένα τέτοιο ‘’σκουλήκι’’, μεταδίδεται από έναν μολυσμένο υπολογιστή στέλνοντας αντίγραφο του εαυτού του σε όλες τις επαφές του υπολογιστή και έπειτα στις επαφές και των υπολογιστών που μόλυνε. Τέτοιες μεταδόσεις γίνονται συχνά εφικτές λόγω της εκμετάλλευσης της ευαλωτότητας του λογισμικού. Όλως παραδόξως, δε σχεδιάζονται πάντοτε για να κάνουν κακό. Αποτελούν απλώς σκουλήκια που δημιουργούνται για να μεταδίδονται.

Rootkit

Το Rootkit είναι μια συλλογή εργαλείων λογισμικού που επιτρέπει τον απομακρυσμένο έλεγχο και την πρόσβαση ενός επιπέδου διαχείρισης κάποιου Η/Υ ή κάποιου δικτύου υπολογιστών. Με το που αποκτηθεί η απομακρυσμένη πρόσβαση, το rootkit μπορεί να πετύχει πολλές κακόβουλες πράξεις. Είναι εξοπλισμένο με καταγραφή πληκτρολόγησης, κλοπή κωδικών και απενεργοποιητές αντιιικών προγραμμάτων. Τα Rootkits εγκαθίστανται κρυφά σε νόμιμο λογισμικό, οπότε όταν δώσεις άδεια σε αυτό το λογισμικό να κάνει αλλαγές στο λειτουργικό σύστημα, το rootkit εγκαθίσταται από μόνο του στον Η/Υ και περιμένει τον hacker να το ενεργοποιήσει. Άλλοι τρόποι διανομής του rootkit περιέχουν τα ‘’emails ηλεκτρονικού ψαρέματος’’, συνδέσμους ή αρχεία με κακόβουλο υλικό και κατέβασμα λογισμικού από ύποπτες ιστοσελίδες.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΑΠΕΙΛΕΣ ΣΕ ΔΕΔΟΜΕΝΑ ΚΑΙ ΠΛΗΡΟΦΟΡΙΕΣ

ΟΙΚΟΝΟΜΙΚΕΣ ΑΠΩΛΕΙΕΣ

Η ασφάλεια των πληροφοριών είναι κρίσιμο ζήτημα για τα άτομα και τους οργανισμούς, γιατί οδηγούν σε τεράστια απώλεια οικονομικών. Κλεμμένες πληροφορίες καρτών πληρωμής, όπως το όνομα του κατόχου της κάρτας, το νούμερο και η ημερομηνία λήξης της, μπορούν να χρησιμοποιηθούν για απάτη σε διαδικτυακές αγορές. Η προοπτική αρνητικών επιπτώσεων μπορεί να γίνει πολύ μεγαλύτερη με τη δόλια χρήση πληροφοριών μιας κάρτας πληρωμής, ιδίως όταν τα δεδομένα είναι ίδια με την πιστωτική κάρτα του θύματος.

ΠΛΑΣΤΟΠΡΟΣΩΠΙΑ

Η πλαστοπροσωπία, γνωστή και ως εξαπάτηση ταυτότητας, είναι ένα έγκλημα, κατά το οποίο ο απατεώνας αποκτά βασικά κομμάτια αναγνωρίσιμων προσωπικών πληροφοριών, όπως τα νούμερα κοινωνικής ασφάλισης ή του διπλώματος οδήγησης, με σκοπό να παριστάνει κάποιον άλλο. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για απόκτηση πιστοληπτικής ικανότητας, εμπορευμάτων και υπηρεσιών στο όνομα του θύματος, ή για να παρέχει στον κλέφτη πλαστά πιστοποιητικά. Εκτός από τη δημιουργία χρέους, σε σπάνιες περιπτώσεις, ένας απατεώνας θα μπορούσε να παράσχει ψευδή ταυτότητα στην αστυνομία, δημιουργώντας ποινικό μητρώο ή αφήνοντας εκκρεμή εντάλματα σύλληψης για το πρόσωπο του οποίου η ταυτότητα έχει κλαπεί.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΤΡΟΠΟΙ ΑΝΑΦΟΡΑΣ ΔΙΑΔΙΚΤΥΑΚΩΝ ΑΠΑΤΕΩΝΩΝ

- **Αναφορά Διαδικτυακού Εγκλήματος**

https://www.europol.europa.eu/report-a-crime/report-cybercrime-online

- **Αναφορά Περιστατικού Ασφάλειας Πληροφοριών**

https://ec.europa.eu/growth/tools-databases/security-incidents_en

- **Αναφορά Διεθνούς Απάτης διαδικτυκά**

https://www.econsumer.gov/#crnt

- **Αναφορά Διαδικτυακού Εγκλήματος στο Ηνωμένο Βασίλειο**

https://www.actionfraudalert.co.uk/Contact

- **Αναφορά Διαδικτυακού Εγκλήματος στην Κύπρο**

https://cybercrime.police.gov.cy/police/CyberCrime.nsf/subscribe_en/subscribe_en?OpenForm

- **Αναφορά Διαδικτυακού Εγκλήματος στην Ελλάδα**

http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang=

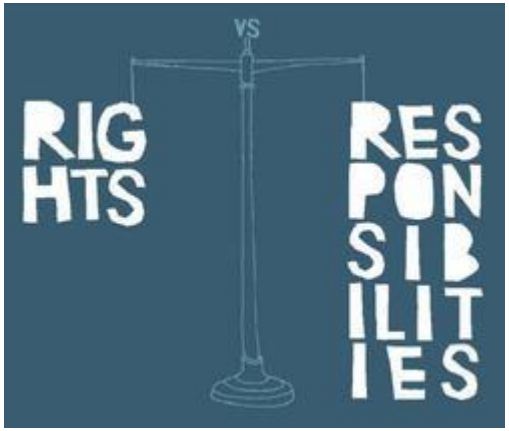
Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΔΙΑΔΙΚΤΥΑΚΑ ΔΙΚΑΙΩΜΑΤΑ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ

ΔΙΑΔΙΚΤΥΑΚΑ ΔΙΚΑΙΩΜΑΤΑ

- Πρόσβαση στη γνώση του τρόπου λειτουργίας του Διαδικτύου
- Πρόσβαση στη γνώση του τρόπου αξιολόγησης της πληροφορίας
- Πρόσβαση στη γνώση του τι είναι γεγονός και τι όχι
- Πρόσβαση στη γνώση του τι είναι υλικό και τι διαφήμιση
- Προστασία της ιδιωτικότητας
- Προστασία ενάντια στον εκφοβισμό/ την παρενόχληση/ τη βία
- Αίσθημα ασφάλειας σωματική/ διανοητική και συναισθηματική
- Έλεγχος των προσωπικών δεδομένων
- Εύκολη αναφορά ανησυχητικού/ ενοχλητικού/ βίαιου διαδικτυακού περιεχομένου στους παρόχους του διαδικτύου
- Δυνατότητα να παίξεις/ να μιλήσεις με φίλους
- Συμμετοχή σε συζητήσεις/forums
- Δυνατότητα δημιουργίας νέου περιεχομένου



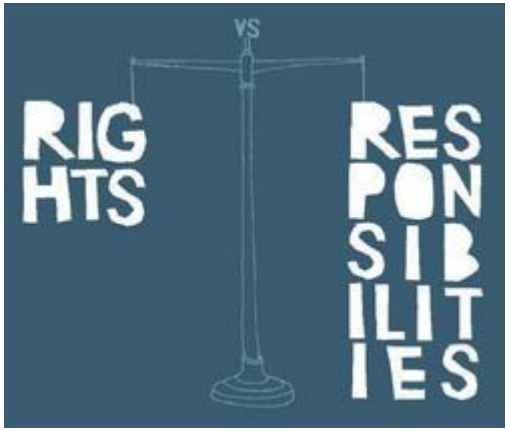
Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΔΙΑΔΙΚΤΥΑΚΑ ΔΙΚΑΙΩΜΑΤΑ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ

ΔΙΑΔΙΚΤΥΑΚΕΣ ΥΠΟΧΡΕΩΣΕΙΣ

- Σεβάσου τα προσωπικά δεδομένα των άλλων χρηστών και την πνευματική ιδιοκτησία και μη δημοσιεύεις δικά τους δεδομένα χωρίς τη συγκατάθεσή τους
- Κράτα τους κωδικούς σου κρυφούς και επίλεξε δύσκολους κωδικούς για το σκοπό αυτό
- Μην παρενοχλείς/ εκφοβίζεις άλλους
- Απόφυγε τους ξένους και ανάφερε τη βίαιη ή ύποπτη συμπεριφορά
- Σεβάσου την ταυτότητα και τις αξίες των άλλων χρηστών
- Να είσαι ενήμερος για το ψηφιακό αποτύπωμα κάποιου και πώς αυτό επηρεάζει τον τρόπο με τον οποίο γίνεται αντιληπτός και ποιον και τι αντιπροσωπεύει
- Βοήθησε τους άλλους και κυρίως τα νέα παιδιά να πλοηγούν με ασφάλεια στο Διαδίκτυο
- Πάντα να ελέγχεις την αξιοπιστία των διαδικτυακών πληροφοριών
- Πλοηγήσου μόνο σε ιστοσελίδες κατάλληλες για την ηλικία σου, σεβάσου κάθε ηλικιακό περιορισμό και διάβασε τους ‘Όρους’ και την ‘Πολιτική’ των ιστοσελίδων



Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΠΕΡΙΛΗΨΗ

- Οι κωδικοί και τα ευαίσθητα δεδομένα μπορούν να διαρρεύσουν από πολλά σημεία ευαλωτότητας στο υλικό και το λογισμικό των σύγχρονων Η/Υ.
- Είναι σημαντικό να κάνεις ό,τι μπορείς για να προστατέψεις τον Η/Υ σου και τα δεδομένα σου.
- Οι πιο σημαντικές απειλές για τα δεδομένα και τις πληροφορίες είναι το ηλεκτρονικό έγκλημα, το κακόβουλο-επιβλαβές λογισμικό (malware) , οι οικονομικές απώλειες και η πλαστοπροσωπία.
- Υπάρχουν πολλοί τρόποι αναφοράς της διαδικτυακής απάτης και είναι ευθύνη μας να το κάνουμε.
- Είμαστε υποχρεωμένοι ως χρήστες του διαδικτύου να προστατεύουμε και να διεκδικούμε τα δικαιώματα μας και να αποδεχόμαστε τις διαδικτυακές μας ευθύνες.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΠΑΡΑΠΟΜΠΕΣ

- Biryukov, V. (2015, April 1). Deep Dive: 5 Threats Affecting Hardware. Retrieved from https://www.kaspersky.com/blog/hardware-malware/8169/
- Lindros, K. (2016, October 12). 12 hardware and software vulnerabilities you should address now. Retrieved from https://www.computerworld.com/article/3130119/12-hardware-and-software-vulnerabilities-you-should-address-now.html
- Lucian, C. (2015, March 19). At least 700,000 routers given to customers by ISPs are vulnerable to hacking. Retrieved from https://www.cio.com/article/2899734/at-least-700000-routers-given-to-customers-by-isps-are-vulnerable-to-hacking.html
- The security risks of outdated software. Retrieved from https://www.parkersoftware.com/blog/the-security-risks-of-outdated-software/
- SecurityTrails Team. (2018, October 16). Top 10 Common Network Security Threats Explained. Retrieved from https://securitytrails.com/blog/top-10-common-network-security-threats-explained
- Sanchez, M. (2010, December 9). The 10 most common security threats explained. Retrieved from https://blogs.cisco.com/smallbusiness/the-10-most-common-security-threats-explained
- Maina, A. (2017, February 16). What is Spamming? Hint: It Involves More Than Just Email. Retrieved from https://smallbiztrends.com/2017/02/what-is-spamming.html
- Rouse, M. pharming. Retrieved from https://searchsecurity.techtarget.com/definition/pharming
- On the Internet. Retrieved from https://www.fbi.gov/scams-and-safety/on-the-internet

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΠΑΡΑΠΟΜΠΕΣ

- Internet Fraud. Retrieved from https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud
- Rouse, M. identity theft. Retrieved from https://searchsecurity.techtarget.com/definition/identity-theft
- Trend Micro Team. (2018, October 31). Information security: How Hackers Leverage Stolen Data for Profit. Retrieved from https://blog.trendmicro.com/information-security-how-hackers-leverage-stolen-data-for-profit/
- Oglethorpe, M. (2013, February 5). Rights and Responsibilities Online: Safer Internet Day 2013. Retrieved from https://themodernparent.net/rights-and-responsibilities-online-safer-internet-day-2013/

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΓΛΩΣΣΑΡΙ

Όρος	Έννοια
ADWARE	Adware θεωρείται κάθε λογισμικό, το οποίο έχει σχεδιαστεί για να εντοπίζει τα δεδομένα ή τις πιο συνηθισμένες περιηγήσεις των χρηστών και με βάση αυτό, να τους εμφανίζει διαφημίσεις και αναδυόμενα παράθυρα.
COMPUTER VIRUS	A computer virus είναι ένας επιβλαβής κωδικός ή ένα επιβλαβές πρόγραμμα που δημιουργείται για να αλλάξει τον τρόπο με τον οποίο λειτουργεί ένας Η/Υ, σχεδιάζεται για να μεταδοθεί από τον έναν εξυπηρετητή στον άλλο και έχει τη δυνατότητα να κάνει αντίγραφα του εαυτού του.
COMPUTER WORM	Τα Computer worms είναι κομμάτια κακόβουλων προγραμμάτων, τα οποία αυτοαναπαράγονται γρήγορα και διαδίδονται από τον ένα Η/Υ στον άλλο.
HACKING	Hacking είναι όταν μη εξουσιοδοτημένοι χρήστες, μπαίνουν στο σύστημα των υπολογιστών, με σκοπό να κλέψουν, να αλλάξουν, να υφαρπάξουν ή να καταστρέψουν πληροφορίες, εγκαθιστώντας συνήθως επιβλαβές υλικό, χωρίς την ενημέρωση ή τη συγκατάθεση του χρήστη.
KEYLOGGING	Η καταγραφή απομακρυσμένης πληκτρολόγησης είναι η χρήση λογιμικού ή υλικού για να καταγράψεις, ποιά πλήκτρα πατιούνται κατά την πληκτρολόγηση στον Η/Υ.
PHARMING	Το Pharming είναι μια πρακτική απάτης, με την οποία επιβλαβής κωδικός εγκαθιστάται σε έναν Η/Υ και έπειτα ο χρήστης οδηγείται παραπλανητικά σε ιστοσελίδες που δραστηριοποιούνται απατεώνες, χωρίς να λάβει γνώση και να συναινέσει.
PHISHING	Το Phishing είναι μια μέθοδος κοινωνικής μηχανής, με σκοπό την απόκτηση ευαίσθητων δεδομένων, όπως κωδικοί, ονόματα χρηστών και νούμερα πιστωτικών καρτών.

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

MeLDE

ΓΛΩΣΣΑΡΙ

Όρος	Έννοια
ROOTKIT	Το Rootkit είναι μια συλλογή εργαλείων λογισμικού που επιτρέπει τον απομακρυσμένο έλεγχο και την πρόσβαση ενός επιπέδου διαχείρισης κάποιου Η/Υ ή κάποιου δικτύου υπολογιστών.
SPAMMING	Spamming είναι ο κατακλυσμός του διαδικτύου με αυθαίρετα και παραπλανητικά μηνύματα.
SPYWARE	Το Spyware είναι το λογισμικό, που έχει σχεδιαστεί για να εντοπίζει τα δεδομένα ή τις πιο συνηθισμένες περιηγήσεις των χρηστών και με βάση αυτό, να τους εμφανίζει διαφημίσεις και αναδυόμενα παράθυρα και εγκαθίσταται εν αγνοία του χρήστη.
SOCIAL ENGINEERING	Social Engineering, στο πλαίσιο της ασφάλειας των πληροφοριών, είναι η απάτη μέσω της οποίας οι χρήστες χειραγωγούνται, ώστε να γνωστοποιήσουν εμπιστευτικές ή προσωπικές πληροφορίες, οι οποίες μπορούν να χρησιμοποιηθούν για δόλιους σκοπούς.
TROJAN HORSE	A Trojan Horse, είναι ένα κακόβουλο κομμάτι ενός επιτιθέμενου κωδικού ή λογισμικού, που παραπλανά τους χρήστες να το τρέξουν οικειοθελώς, ενώ είναι κρυμμένο πίσω από ένα νόμιμο πρόγραμμα .