ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΜΑΘΗΤΕΣ:ΑΝΤΩΝΙΟΥ ΕΥΑΓΓΕΛΙΑ ,ΔΑΡΑΜΑΡΑ ΑΓΓΕΛΙΚΗ,ΖΑΡΚΑΔΟΥΛΑ ΔΕΣΠΟΙΝΑ ,ΚΑΠΟΥΛΑΣ ΑΠΟΣΤΟΛΟΣ ,ΚΟΛΟΒΟΣ ΠΑΝΑΓΙΩΤΗΣ

ΚΑΘΗΓΗΤΡΙΑ:ΧΑΛΙΜΟΥΡΔΑ ΑΓΓΕΛΙΚΗ

ΕΡΕΥΝΗΤΙΚΗ ΕΡΓΑΣΙΑ ΜΑΙΟΣ 2015

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μορφές ηλεκτρονικού εγκλήματος :

- Κακόβουλα λογισμικά
- Spamming
- Κλοπή ταυτότητας
- Κακόβουλες εισβολές σε δίκτυα
- Επιθέσεις σε διαδικτυακούς τόπους

ΚΑΚΟΒΟΥΛΑ ΛΟΓΙΣΜΙΚΑ

Τα κακόβουλα λογισμικά είναι προγράμματα που έχουν σχεδιαστεί για να βλάψουν έναν Η/Υ , για την υποκλοπή δεδομένων , την σταδιακή επιβράδυνση του και την αποστολή πλαστών μηνυμάτων .

Τα βασικότερα είναι :

- Virus (Ιοί)
- Worms (Σκουλήκια)
- Trojan Horses (Δούρειος Ίππος)
- Rootkit (Ριζικό Εργαλείο)
- Logic Bombs (Λογισμικές Βόμβες)
- Trapdoor/Backdoor (Πόρτα Παγίδα/Παράνομη Πρόσβαση)
- Adware (Λογισμικό Προσεταιρισμού)
- Spyware (Λογισμικό Κατασκοπίας)

Βασικοί τρόποι διάδοσης κακόβουλων λογισμικών

- Λήψη δωρεάν λογισμικού από το διαδίκτυο
- Λήψη νόμιμου λογισμικού
- Επίσκεψη σε παράνομους η μη εμπίστους ισότοπους
- Αναπαραγωγή ψεύτικου μηνύματος
- Άνοιγμα συνημμένου η κανονικού μηνύματος ηλεκτρονικού ταχυδρομείου

Βασικοί τρόποι αποφυγής και πρόληψης από κακόβουλα λογισμικά

- Απαραίτητη χρήση λογισμικού προστασίας
- Συχνή ενημέρωση λογισμικού προστασίας
- Όταν είναι εφικτό να μην χρησιμοποιούμε τον λογαριασμό διαχείρισης
- Αποφυγή λήψεων μη εμπίστων προγραμμάτων
- Αναπαραγωγή συνημμένων η κανονικών μηνυμάτων μόνο από εμπίστους χρηστές
- να μην εμπιστευόμαστε αναδυόμενα παράθυρα και να μην τα αναπαράγουμε η τα εκτελούμε
- Περιορισμός κοινοποίησης αρχείων

SPAMMING

Spam είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου χωρίς αυτοί να το επιθυμούν και χωρίς να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον εν λόγω αποστολέα. Η αλληλογραφία αυτή λοιπόν μπορεί να χαρακτηριστεί ως **απρόκλητη** ή **ανεπιθύμητη αλληλογραφία,** δύο όρους που χρησιμοποιούμε για την απόδοση στη γλώσσα μας του όρου Spam.

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

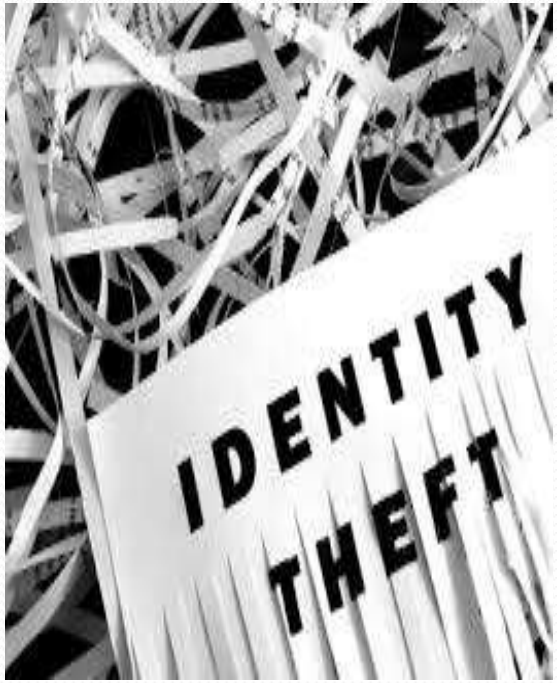
- Απρόκλητο
- Εμπορικό
- Μαζικό

Τι μπορούμε να κάνουμε για να αποφύγουμε το Spam

- Μη δημοσιεύετε την διεύθυνση ηλεκτρονικού ταχυδρομείου σας.
- Μη δίνετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας, σε οργανισμούς που δεν εμπιστεύεστε.
- Μην απαντάτε στο spam.
- Αναφέρετε κάθε μήνυμα Spam που λαμβάνετε.
- Διαδώστε την γνώση σας και την εμπειρία σας σε σχέση με το Spam. Ελέγξτε τα συστήματα σας ώστε να είναι σωστά διαμορφωμένα και ασφαλή.

ΚΛΟΠΗ ΤΑΥΤΟΤΗΤΑΣ

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



Καταπολεμήστε την απάτη

- Βάλε τη φαντασία σου να δουλέψει όταν δημιουργείς κωδικούς πρόσβασης. Μη χρησιμοποιείς κωδικούς που εύκολα μπορεί κανείς να φανταστεί
- Επικοινώνησε με τον πάροχο της υπηρεσίας όπου έχει γίνει η κλοπή ταυτότητας
- Δημιούργησε νέο e-mail, προφίλ
- Μπορείς να κάνεις μια ανώνυμη καταγγελία του περιστατικού στη Safeline.

ΠΡΟΣΤΑΣΙΑ ΣΤΟΙΧΕΙΩΝ

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

ΕΠΙΘΕΣΕΙΣ ΣΕ ΔΙΑΔΙΚΤΥΑΚΟΥΣ ΤΟΠΟΥΣ

Η επίθεση μπορεί να γίνει στο περιεχόμενο μια σελίδας, το οποίο οι βάνδαλοι θα αλλοιώσουν. Παρόλα αυτά, η παραποίηση αυτή μπορεί να εντοπιστεί και στη συνέχεια να διορθωθεί. Το πρόβλημα είναι πως αν το μέγεθος της παρεμβολής είναι μεγάλο, τότε η διόρθωση θα διαρκέσει τόσο ώστε να χρειαστεί μερικές φόρες ο δικτυακός τόπος να παραμείνει κλειστός

Ένα πληροφοριακό σύστημα για να θεωρείται ασφαλές πρέπει να διαθέτει:

- Διαθεσιμότητα
- Ακεραιότητα
- Εμπιστευτικότητα

ΚΑΚΟΒΟΥΛΕΣ ΕΙΣΒΟΛΕΣ ΣΕ ΔΙΚΤΥΑ (HACKING & CRACKING)

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

- Hacker: Τεχνικά καταρτισμένος χρήστης Η/Υ που, με αρνητικά ή θετικά κίνητρα, θα παραβιάσει συστήματα υπολογιστών. Κάποιες φορές, η εισβολή σε κάποιο «στόχο» γίνεται για καλό σκοπό. Μπορεί να είναι επίσης κακό και άδικο για κλοπές και βανδαλισμό.

ΔΙΑΦΟΡΑ HACKER & CRACKER

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

Οι πιο γνωστοί «hackers» όλων των εποχών

- Kevin Mitnick
- Adrian Lamo
- Jonathan James
- Robert Tappan Morris
- Kevin Poulsen

Ευχαριστούμε θερμά για την προσοχή σας!!!