Ασφάλεια Διαδικτύου

Δημοτικό Σχολείο Λόφου

Σχολικό έτος 2021-2022

Τι είναι ασφάλεια διαδικτύου

Η ασφάλεια στο Διαδίκτυο ή η **διαδικτυακή ασφάλεια** είναι η γνώση των κινδύνων προσωπικής ασφάλειας και ασφάλειας του χρήστη σε ιδιωτικές πληροφορίες και περιουσίες που σχετίζονται με τη χρήση του Διαδικτύου και την αυτοπροστασία από το ηλεκτρονικό έγκλημα.

Δεδομένου ότι ο αριθμός των χρηστών του Διαδικτύου συνεχίζει να αυξάνεται παγκοσμίως, διαδικτυακοί οργανισμοί, κυβερνήσεις και οι οργανισμοί εξέφρασαν ανησυχίες για την ασφάλεια των παιδιών που χρησιμοποιούν το Διαδίκτυο.

Η Ημέρα Ασφαλέστερου Διαδικτύου γιορτάζεται παγκοσμίως τον Φεβρουάριο για να ευαισθητοποιήσει την ασφάλεια στο Διαδίκτυο Στο Ηνωμένο Βασίλειο, η καμπάνια <<Get Safe Online>> έχει λάβει χορηγίες από την κυβερνητική υπηρεσία Serious Organized Crime Agency (SOCA) και τις μεγάλες εταιρείες του Διαδικτύου όπως η Microsoft και το eBay .

Ασφάλεια πληροφοριών

Οι ευαίσθητες πληροφορίες όπως οι προσωπικές και η ταυτότητα του χρήστη , οι κωδικοί πρόσβασης συνδέονται συχνά με προσωπικά είδη (π.χ. τραπεζικοί λογαριασμοί) και με την ιδιωτική τους ζωή και ενδέχεται να παρουσιάζουν ανησυχία σχετικά με την ασφάλεια των χρηστών εάν διαρρεύσουν.

Η μη εξουσιοδοτημένη πρόσβαση και η χρήση ιδιωτικών πληροφοριών μπορεί να έχει ως συνέπεια την κλοπή ταυτότητας , καθώς και την κλοπή ιδιοκτησίας. Κοινές αιτίες παραβιάσεων της ασφάλειας των πληροφοριών περιλαμβάνουν:

Πηγή: Wikipedia

- Ηλεκτρονικό '' ψάρεμα ''
- Διαδικτυακές απάτες
- Κακόβουλο λογισμικό

Πηγή: Wikipedia

Το ηλεκτρονικό ψάρεμα

Το ηλεκτρονικό "ψάρεμα" είναι ένας τύπος απάτης στον οποίο οι απατεώνες εμφανίζονται με ψεύτικα στοιχεία για την απόκτηση ιδιωτικών πληροφοριών, όπως κωδικών πρόσβασης, πληροφοριών πιστωτικών καρτών κ.λπ. μέσω του διαδικτύου.

Το ηλεκτρονικό "ψάρεμα" (phishing) συμβαίνει συχνά μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου και άμεσων μηνυμάτων και μπορεί να περιέχει συνδέσμους σε ιστότοπους που κατευθύνουν τον χρήστη να εισαγάγει τις προσωπικές του πληροφορίες. Αυτές οι ψεύτικες ιστοσελίδες είναι συχνά σχεδιασμένες ώστε να φαίνονται όμοιοι με τους νόμιμους ομολόγους τους, για να αποφεύγεται η υποψία από τον χρήστη.

Πηγή: Wikipedia


Personal
Data

Διαδικτυακές απάτες

- Πρόκειται για προγράμματα που εξαπατούν τον χρήστη με διάφορους τρόπους, προσπαθώντας να εκμεταλλευτούν πληροφορίες του χρήστη.

Πηγή: Wikipedia

- Οι απάτες στο Διαδίκτυο προσπαθούν να εξαπατήσουν το θύμα με πράγματα της προσωπικής ιδιοκτησίας παρά με προσωπικές πληροφορίες μέσω ψευδών υποσχέσεων, τεχνάσματα εμπιστοσύνης και πολλά άλλα.

Κακόβουλο λογισμικό

Το κακόβουλο λογισμικό , ιδιαίτερα το λογισμικό υποκλοπής spyware , είναι κακόβουλο λογισμικό που μεταμφιέζεται ως λογισμικό που έχει σχεδιαστεί για τη συλλογή και τη μετάδοση ιδιωτικών πληροφοριών, όπως κωδικών πρόσβασης, χωρίς τη συγκατάθεση ή τη γνώση του χρήστη.

Πηγή: Wikipedia

Συχνά διανέμεται μέσω ηλεκτρονικού ταχυδρομείου, από ανεπίσημες τοποθεσίες. Το κακόβουλο λογισμικό είναι ένα από τα πιο διαδεδομένα προβλήματα ασφαλείας, καθώς συχνά είναι αδύνατο να προσδιοριστεί εάν ένα αρχείο έχει μολυνθεί, ακόμα και αν είναι ασφαλής η πηγή του αρχείου.

Προσωπική ασφάλεια

Η ανάπτυξη του Διαδικτύου δημιούργησε πολλές σημαντικές υπηρεσίες προσβάσιμες σε οποιονδήποτε συνδέεται. Μία από αυτές τις σημαντικές υπηρεσίες είναι η ψηφιακή επικοινωνία.

Ενώ η υπηρεσία αυτή επέτρεπε την επικοινωνία με άλλους μέσω του Διαδικτύου, επιτρέπει επίσης την επικοινωνία με κακόβουλους χρήστες.

Ενώ οι κακόβουλοι χρήστες συχνά χρησιμοποιούν το διαδίκτυο για προσωπικό κέρδος, αυτό μπορεί να μην περιορίζεται σε οικονομικό / υλικό κέρδος. Αυτό είναι ιδιαίτερα ανησυχητικό για τους γονείς και τα παιδιά, καθώς τα παιδιά αποτελούν συχνά στόχους αυτών των κακόβουλων χρηστών.

Πηγή: Wikipedia

Οι κοινές απειλές για την προσωπική ασφάλεια περιλαμβάνουν:

- phishing
- ηλεκτρονικές απάτες
- κακόβουλο λογισμικό
- cyberstalking
- ηλεκτρονική παρενόχληση

Cyberstalking είναι η χρήση του Διαδικτύου ή άλλων ηλεκτρονικών μέσων για την καταδίωξη ή την παρενόχληση ενός ατόμου, μιας ομάδας ατόμων ή ενός οργανισμού.

Μπορεί να περιλαμβάνει ψευδείς καταγγελίες ή δηλώσεις (δυσφήμηση), παρακολούθηση, απειλές, κλοπή ταυτότητας, βλάβη δεδομένων ή εξοπλισμού, ή συλλογή πληροφοριών που μπορούν να χρησιμοποιηθούν για παρενόχληση.

Σύμφωνα με μελέτη που έγινε από τους Baum et al. (2009), ο ρυθμός επίθεσης μέσω ηλεκτρονικών μέσων, όπως το ηλεκτρονικό ταχυδρομείο ή η ανταλλαγή άμεσων μηνυμάτων, ήταν πάνω από ένα στα τέσσερα από όλα τα θύματα καταδίωξης στη μελέτη.

Ηλεκτρονική παρενόχληση

Η ηλεκτρονική παρενόχληση είναι η επίθεση εναντίον ενός ατόμου ή μιας ομάδας μέσω της χρήσης ηλεκτρονικών μέσων όπως η άμεση ανταλλαγή μηνυμάτων, τα κοινωνικά δίκτυα, το ηλεκτρονικό ταχυδρομείο και άλλες μορφές ηλεκτρονικής επικοινωνίας με σκοπό την κατάχρηση, τον εκφοβισμό ή την υπερνίκηση.

Αστείο / προσβλητικό περιεχόμενο

Διάφοροι ιστότοποι στο Διαδίκτυο περιέχουν υλικό που κάποιοι θεωρούν προσβλητικό, δυσάρεστο ή ρητό, το οποίο συχνά δεν μπορεί να είναι από τις προτιμήσεις του χρήστη.

Τέτοιες ιστοσελίδες μπορεί να περιλαμβάνουν το διαδίκτυο, ιστοσελίδες σοκ , ομιλία μίσους ή άλλο φλεγμονώδες περιεχόμενο. Ένα τέτοιο περιεχόμενο μπορεί να εκδηλωθεί με πολλούς τρόπους, όπως οι αναδυόμενες διαφημίσεις και οι ανυποψίαστοι σύνδεσμοι.

ΕΥΧΑΡΙΣΤΟΥΜΕ ΠΟΛΥ

ΓΙΑ ΤΗΝ ΠΑΡΑΚΟΛΟΥΘΗΣΗ!

Η παρούσα εργασία πραγματοποιήθηκε στο εργαστήριο Πληροφορικής από τα παιδιά της ΣΤ' Τάξης το σχολικό έτος 2021-2022 με Θέμα την Ασφάλεια Διαδικτύου.

Τα παιδιά εργάστηκαν σε ομάδες των δύο ατόμων όπως και ατομικά για την αναζήτηση πληροφοριών στο διαδίκτυο.

Κύρια πηγή πληροφοριών ήταν η Wikipedia.