

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Σοφία Π. & Ροδούλα Μ.

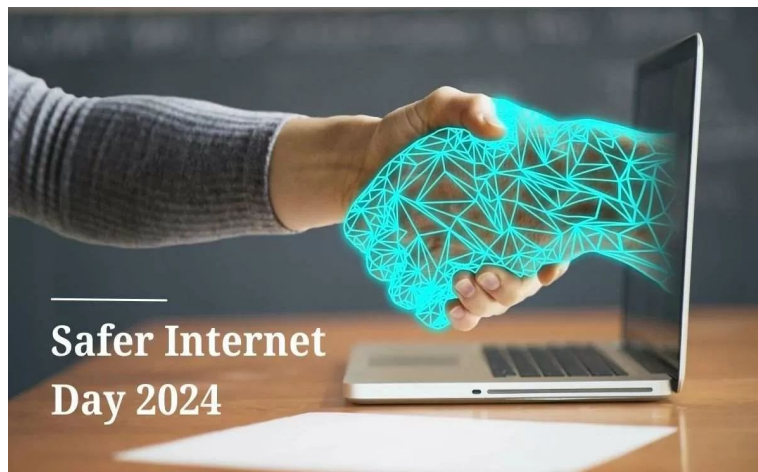
ΓΕΝΙΚΗ ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ



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 την αυτοπροστασία από το ηλεκτρονικό έγκλημα. 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.

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 εισάγει τις προσωπικές του πληροφορίες.



**Safer Internet
Day 2024**

Αυτές οι ψεύτικες ιστοσελίδες είναι συχνά σχεδιασμένες ώστε να φαίνονται όμοιοι με τους νόμιμους ομολόγους τους, για να αποφεύγεται η υποψία. Το ηλεκτρονικό “φαρμακείο” 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.



Προσωπικές πληροφορίες

Προσωπικές πληροφορίες μπορεί να είναι:

1. το όνομά μας (και το επίθετο)
2. την ημερομηνία γέννησης
3. που μένουμε
4. τηλέφωνα και e-mail
5. φωτογραφίες μας
6. τραπεζικούς λογαριασμούς
7. κωδικούς ασφαλείας



Διαδικτυακές απάτες

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



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.

Σε μια μελέτη του 2012 με περισσότερους από 11.925 φοιτητές στις Ηνωμένες Πολιτείες, αναφέρθηκε ότι το 23% των εφήβων ανέφερε ότι ήταν θύμα της παρενόχλησης στον κυβερνοχώρο, το 30% των οποίων ανέφερε ότι αντιμετωπίζει αυτοκτονική συμπεριφορά.



ΠΡΟΣΕΧΟΥΜΕ ΠΟΥ ΠΑΙΖΟΥΜΕ

Πολλές φορές όταν παίζουμε στο διαδίκτυο πρέπει προσέχουμε:

1. σε τι παιχνίδια μπαίνουμε
2. να μην βάζουμε τις προσωπικές πληροφορίες μας ακόμα κι αν τις ζητάν
3. να ρωτάμε τους γονείς μας πριν κατεβάσουμε



GOOGLE FAMILY LINK

Η ιστοσελίδα αυτή υπάρχει για να σας προστατέψει:

1. να μην κάθεστε πολλές ώρες μπροστά σε μια οθόνη
2. να μην βλέπετε πράγματα-video ακατάλληλα για την ηλικία σας
3. μην παίζετε παιχνίδια που δεν σας επιτρέπουν οι γονείς σας

**ΟΙ ΓΟΝΕΙΣ ΣΑΣ ΜΠΟΡΟΥΝ ΝΑ ΕΛΕΓΧΟΥΝ
ΤΙΣ ΣΥΣΚΕΥΕΣ ΣΑΣ ΚΑΙ ΝΑ ΤΙΣ
ΚΛΕΙΔΩΣΟΥΝ ΑΝΑ ΠΑΣΑ ΣΤΙΓΜΗ ΓΙΑ ΤΟΝ
ΟΠΟΙΟΔΗΠΟΤΕ ΛΟΓΟ !!!**

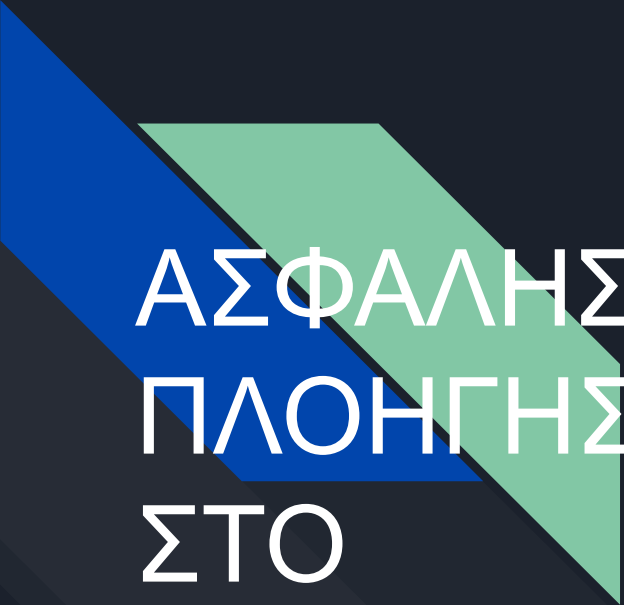


Google Family Link


ΕΥΧΑΡΙΣΤΟΥΜΕ ΠΟΛΥ!!

Πηγές:

ΒΙΚΙΠΑΙΔΙΑ



ΑΣΦΑΛΗΣ
ΠΛΟΗΓΗΣΗ
ΣΤΟ
ΔΙΑΔΙΚΤΥΟ



Το διαδίκτυο έχει έντονη παρουσία στη ζωή μας, ιδιαίτερα δε στη ζωή των νέων λόγω της ευρέως διαδεδομένης χρήσης τους. Ωστόσο, είναι γνωστό ότι αυτή η ενασχόληση ενδεχομένως να αποτελεί απειλή. Οι κίνδυνοι που ελλοχεύουν στη χρήση του διαδικτύου θα μπορούσαν να κατηγοριοποιηθούν σε δύο σκέλη. Το πρώτο και πιο ανώδυνο, σχετικά, είναι η παραβίαση της προσωπικής ζωής των χρηστών παρά την θέλησή τους. Το δεύτερο και πιο επικίνδυνο σκέλος αφορά στην εμμονή των χρηστών για συνεχή απασχόλησή τους, με αυτού του είδους την επικοινωνία. Όμως για τους παραπάνω κινδύνους υπάρχουν μέτρα προφύλαξης ώστε να έχουμε μια συνετή χρήση του διαδικτύου.





ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΠΑΤΕΣ

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



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.



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. 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. Οι κοινές απειλές για την προσωπική ασφάλεια περιλαμβάνουν: phishing, ηλεκτρονικές απάτες, κακόβουλο λογισμικό, cyberstalking, ηλεκτρονική παρενόχληση, online προσθήκες και σεξουαλικότητα.





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. Σε μια μελέτη του 2012 με περισσότερους από 11.925 φοιτητές στις Ηνωμένες Πολιτείες, αναφέρθηκε ότι το 23% των εφήβων ανέφερε ότι ήταν θύμα της παρενόχλησης στον κυβερνοχώρο, το 30% των οποίων ανέφερε ότι αντιμετώπιζε αυτοκτονική συμπεριφορά.



ΕΥΧΑΡΙΣΤΟΥΜΕ ΓΙΑ ΤΗΝ ΠΑΡΟΥΣΙΑ ΣΑΣ

ΠΗΓΕΣ: WIKIPEDIA \ GOOGLE \ ΕΙΚΟΝΕΣ

ΑΣΦΑΛΕΙΑ ΔΙΑΔΙΚΤΥΟΥ





Ασφάλεια στο διαδίκτυο

→ ΣΕΡΦΑΡΟΥΜΕ ΑΣΦΑΛΕΙΣ

● ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

● Ηλεκτρονικό "ψάρεμα"

1. 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.
2. Το ηλεκτρονικό "ψάρεμα" (phishing) συμβαίνει συχνά μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου και άμεσων μηνυμάτων και μπορεί να περιέχει συνδέσμους σε ιστότοπους που κατευθύνουν εμάς να εισάγουμε τις προσωπικές μας πληροφορίες.
3. Αυτές οι ψεύτικες ιστοσελίδες είναι συχνά σχεδιασμένες ώστε να φαίνονται όμοιοι με τους νόμιμους ιστότοπους τους, για να αποφεύγεται η υποψία μας.



● ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

● Διαδικτυακές απάτες

- Πρόκειται για προγράμματα ή ανθρώπους που εξαπατούν εμάς με διάφορους τρόπους, προσπαθώντας να πάρουν τις πληροφορίες μας.
- Οι απάτες στο Διαδίκτυο προσπαθούν να εξαπατήσουν το θύμα με πράγματα της προσωπικής ιδιοκτησίας με μέσω ψευδών υποσχέσεων

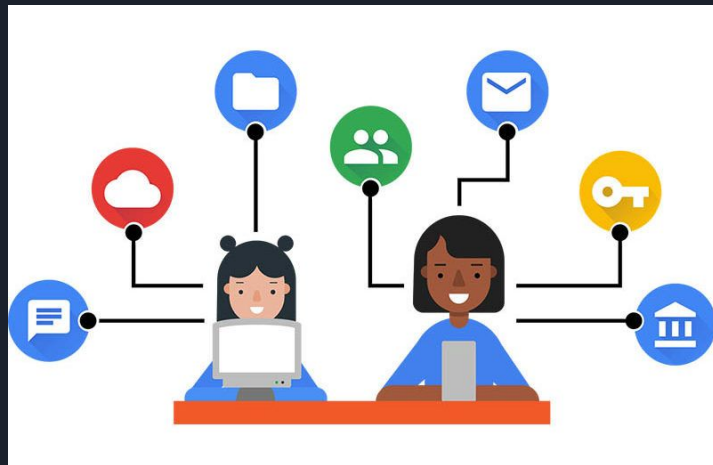


- ΘΥΜΗΘΕΪΤΕ ΔΕΝ ΜΟΙΡΑΖΟΥΜΕ ΤΙΣ ΠΡΟΣΩΠΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΜΑΣ ΣΕ ΑΓΝΩΣΤΟΥΣ

• ΠΩΣ ΜΕΝΟΥΜΕ ΑΣΦΑΛΕΙΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Υπάρχουν πολλές επιλογές για να μειούμε ασφάλεις στο διαδίκτυο και να απολαμβάνουμε τον χρόνο μας σερφαροντας χωρίς απειλες.Εδω μπορείτε να βρειτε μερικες επιλογες...

- ★ ad blocker
- ★ family link
- ★ antivirus



- Για περισσότερες πληροφορίες μπορείτε να επισκεφτείτε το saferinternet4kids



....ΣΑΣ ΕΥΧΑΡΙΣΤΩ ΓΙΑ ΤΗΝ ΠΑΡΑΚΟΛΟΥΘΗΣΗ

Πηγές

- Google Safety
- saferinternet4kids
- wikipedia

Παναγιώτα Ανθή Κατσαβρέα

Ασφάλεια Στο Διαδίκτυο

nektony



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.



Κακόβουλο λογισμικό

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. 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.



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.

Σε μια μελέτη του 2012 με περισσότερους από 11.925 φοιτητές στις Ηνωμένες Πολιτείες, αναφέρθηκε ότι το 23% των εφήβων ανέφερε ότι ήταν θύμα της παρενόχλησης στον κυβερνοχώρο, το 30% των οποίων ανέφερε ότι αντιμετώπιζε αυτοκτονική συμπεριφορά.



Loser

Stupid

😈😈😈

😡😡😡

😏😏😏

😡

👎👎👎

😏

Διαδικτυακές απάτες

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

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.

SCAM



Ευχαριστούμε πολύ που μας παρακολουθήσατε!

Πηγή:wikipedia

google/εικόνες/Ασφάλεια διαδικτύου

Την παρουσίαση επιμελήθηκαν οι
μαθητές:Βασίλης Κηπόπουλος,
Μιχαήλ Λιονάκης,Ανδρέας Αναστασιάδης,
Θοδωρής Μπίλλας.Της Ε'1 τάξης



ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Ε1 ΑΝΕΛΙΑ ΧΡΥΣΑΝΘΗ



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.

A photograph of a laptop computer. The screen displays the text "IS IT SAFE?" in large, bold, black capital letters. In the foreground, a heavy metal padlock is attached to a chain, symbolizing security or a barrier. The background is a soft, out-of-focus blue light.

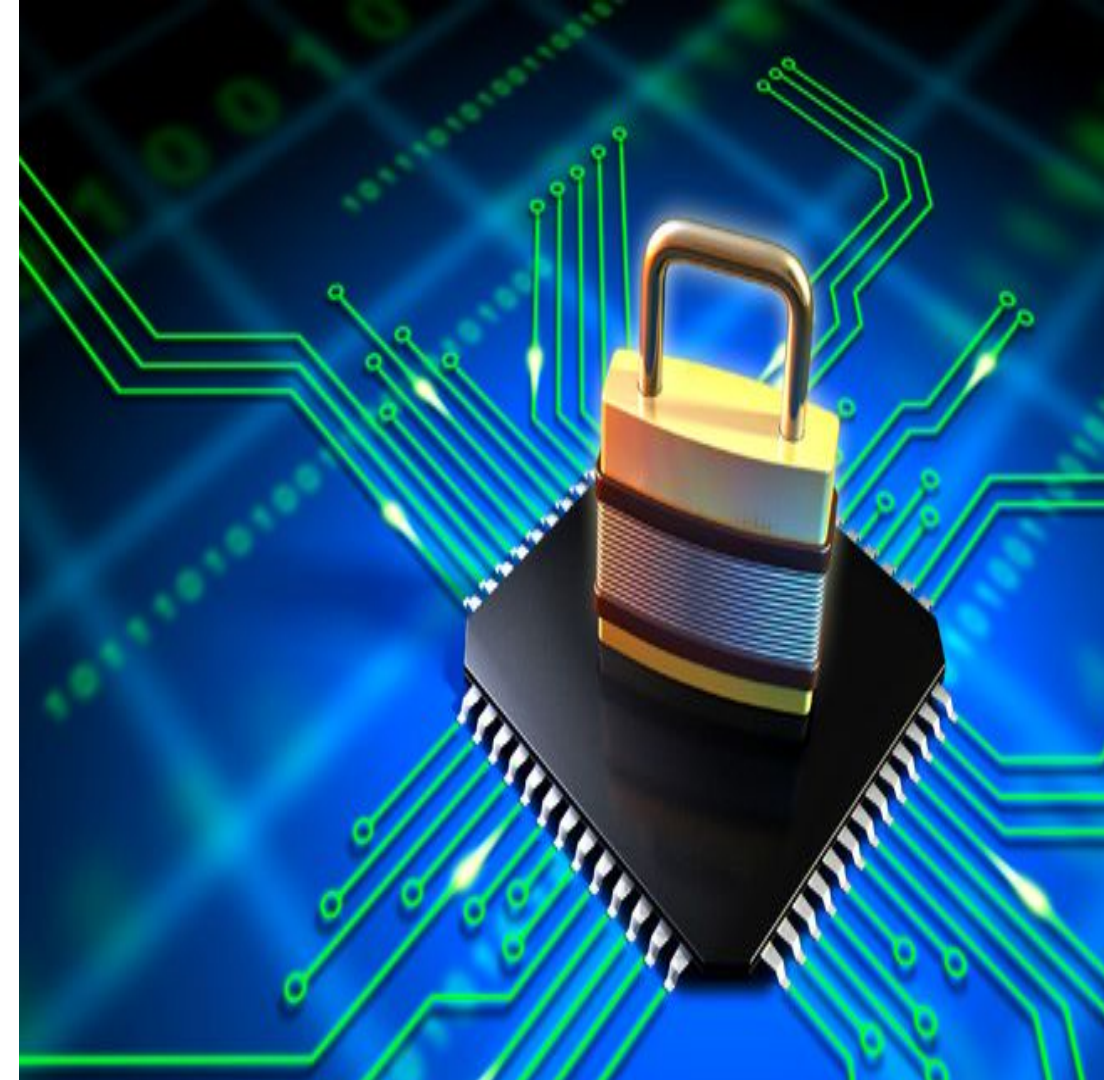
IS IT SAFE?

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** . ^[3]:



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

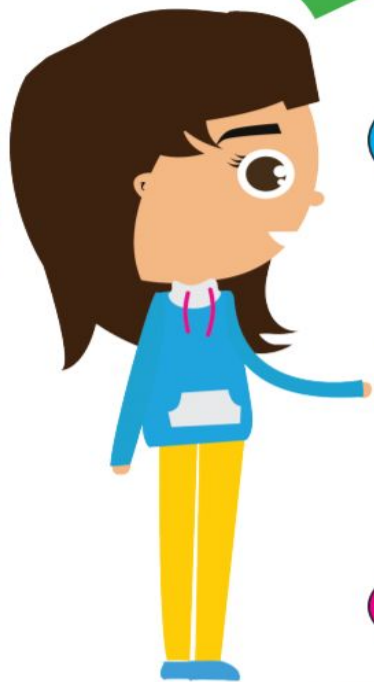
Αν ήταν εφικτό να αποδώσουμε τον όρο στα Ελληνικά, θα μπορούσαμε κάλλιστα να το αποκαλέσουμε 'Ηλεκτρονικό Ψάρεμα', κι αυτό γιατί αγγλικός όρος δεν απέχει πολύ από αυτό.

Ο όρος Phishing, που πρωτοχρησιμοποιήθηκε από τον [χάκερ Khan C Smith](#) και υιοθετήθηκε στη συνέχεια από όλη την κοινότητα.





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:



Παιδιά
βοηθήστε με να
ξεχωρίσω ποιές από
αυτές τις πληροφορίες
είναι προσωπικά μου
δεδομένα!

Οι φωτογραφίες μου

Το όνομά μου

Το τηλέφωνό μου

Τι καιρό κάνει
σήμερα;

Το όνομα του
σκύλου μου

Προσωπικά
Δεδομένα

Το βιβλίο
που διαβάζω

Η διεύθυνση μου

Ο παιδότοπος
που συχνάζω

Το πολίτευμα
της Ελλάδας

Το σχολείο που πηγαίνω

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

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.








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

Σας ευχαριστούμε για την παρακολούθησή σας!

Πηγές

1. [google/εικόνες/Ασφάλεια στο διαδίκτυο](#)
2. [wikipedia/Ασφάλεια στο διαδίκτυο](#)



ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΣΤΑΜΑΤΙΑ Ι. ΚΑΙ ΛΥΔΙΑ Κ.

ΠΑΜΕ ΝΑ ΔΟΥΜΕ ΜΑΖΙ ΤΙ ΠΡΕΠΕΙ ΝΑ ΠΡΟΣΕΧΟΥΜΕ




- ΟΤΑΝ ΣΕ ΕΝΑ ΠΑΙΧΝΙΔΙ ΜΑΣ ΛΕΕΙ ΟΤΙ ΚΕΡΔΙΣΑΜΕ ΚΑΤΙ ΑΛΛΑ ΠΡΕΠΕΙ ΝΑ ΒΑΛΟΥΜΕ ΤΑ ΠΡΟΣΩΠΙΚΑ ΜΑΣ ΣΤΟΙΧΕΙΑ ΔΕΝ ΤΑ ΒΑΖΟΥΜΕ ΠΟΤΕ
- ΔΕΝ ΔΕΙΧΝΟΥΜΕ ΠΟΤΕ ΧΩΡΙΣ ΤΗΝ ΑΔΕΙΑ ΤΩΝ ΓΟΝΙΩΝ ΜΑΣ ΤΟ ΠΡΟΣΩΠΟ ΜΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ
- ΔΕ ΣΥΝΟΜΙΛΟΥΜΕ ΜΕ ΚΑΠΟΙΟΝ ΠΟΥ ΔΕΝ ΤΟΝ ΓΝΩΡΙΖΟΥΜΕ

ΠΑΜΕ ΤΩΡΑ ΝΑ ΔΟΥΜΕ ΚΑΙ ΤΑ ΠΡΟΣΩΠΙΚΑ ΜΑΣ ΣΤΟΙΧΕΙΑ

- ★ ΤΗΝ ΗΜΕΡΟΜΗΝΙΑ ΓΕΝΝΗΣΗΣ ΜΟΥ- ΤΗΝ ΗΛΙΚΙΑ ΜΟΥ
- ★ ΤΟ ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΜΑΣ
- ★ ΤΗ ΔΙΕΥΘΥΝΣΗ ΚΑΤΟΙΚΙΑΣ ΜΑΣ
- ★ ΤΑ ΟΝΟΜΑΤΑ ΤΗΣ ΟΙΚΟΓΕΝΕΙΑΣ ΜΑΣ
- ★ ΤΗ ΧΡΕΩΣΤΙΚΗ- ΠΙΣΤΩΤΙΚΗ ΚΑΡΤΑ ΤΩΝ ΓΟΝΙΩΝ ΜΑΣ





Κάθε γονέας στην ηλικία μας πρέπει να έχει τη συγκεκριμένη εφαρμογή.

Family Link: Το family link είναι μια εφαρμογή που βοηθάει τους γονείς μας αλλά και εμάς από διάφορους κινδύνους στο διαδίκτυο όπως links και site που θέλουν το κακό μας .



Το λεγόμενο “ΨΑΡΕΜΑ” στο διαδίκτυο είναι μια επικίνδυνη υπόθεση.



Με τον όρο ηλεκτρονικό ψάρεμα (phishing) περιγράφεται η προσπάθεια που καταβάλει κάποιος όταν με διάφορους τρόπους προσπαθεί να αποσπάσει από εσένα προσωπικά σου στοιχεία στο διαδίκτυο. Συνήθως γίνεται μέσω ηλεκτρονικού ταχυδρομείου (email) και ο πραγματικός αποστολέας δεν είναι αυτός που φαίνεται. Για παράδειγμα μπορεί να λάβετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από μια ιστοσελίδα που χρησιμοποιείς και μέσω του οποίου να σου ζητάνε να δώσεις κάποια προσωπικά σου στοιχεία για λόγους ασφαλείας ή να λάβεις ένα μήνυμα που να υποστηρίζει ότι κέρδισες ένα σημαντικό ποσό και να σε προτρέπει να δώσεις τα προσωπικά σου στοιχεία για να λάβετε τα χρήματα.

Ένας άλλος τρόπος να σου αποσπάσουν προσωπικά στοιχεία είναι να σου ζητήσουν να πατήσεις σε κάποιο σύνδεσμο ο οποίος όμως στην πραγματικότητα δεν είναι αθώος και με αυτό τον τρόπο γίνεται εγκατάσταση κακόβουλου ή κατασκοπευτικού λογισμικού στον υπολογιστή σου.

Η επιτυχία της μεθόδου είναι μεγάλη. Σε πρόσφατο πείραμα που πραγματοποιήθηκε στις Ηνωμένες Πολιτείες, το 70% όσων έλαβαν το εξατομικευμένο μήνυμα πάτησε στο σύνδεσμο που περιλαμβάνεται σε αυτό και συμπλήρωσε τα στοιχεία του στην ιστοσελίδα υποκλοπής δεδομένων.

Εκφοβισμός στο διαδίκτυο



1. ΠΟΛΛΑ ΠΑΙΔΙΑ ΣΤΙΣ ΜΕΡΕΣ ΜΑΣ ΔΕΧΟΝΤΑΙ BULLYING Ή ΑΛΛΙΩΣ ΕΚΦΟΒΙΣΜΟ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.
2. ΠΑΙΖΟΝΤΑΣ ΕΝΑ ΠΑΙΧΝΙΔΙ ΜΕ ΑΤΟΜΑ ΤΑ ΟΠΟΙΑ ΔΕΝ ΓΝΩΡΙΖΟΥΜΕ ΚΑΙ ΧΑΣΟΥΜΕ ΠΟΛΛΑ ΠΑΙΔΙΑ ΔΕΧΟΝΤΑΙ ΥΒΡΙΣΤΙΚΑ ΣΧΟΛΙΑ ΑΠΟ ΑΤΟΜΑ ΤΑ ΟΠΟΙΑ ΤΟ ΚΥΡΙΟΤΕΡΟ ΔΕΝ ΤΑ ΓΝΩΡΙΖΟΥΝ
3. ΙΣΩΣ ΝΑ ΜΑΣ ΑΝΑΓΚΑΖΟΥΝ ΝΑ ΤΟΥΣ ΔΩΣΟΥΜΕ ΧΡΗΜΑΤΑ ΜΕ ΑΠΕΙΛΗ ΝΑ ΔΗΜΟΣΙΕΎΣΟΥΝ ΚΑΤΙ ΠΡΟΣΩΠΙΚΟ ΜΑΣ .
4. ΑΝ ΓΝΩΡΙΖΟΥΜΕ ΚΑΠΟΙΟ ΠΑΙΔΙ ΠΟΥ ΔΕΧΕΤΑΙ ΚΑΤΙ ΤΕΤΟΙΟ ΠΡΕΠΕΙ ΚΑΤΕΥΘΕΪΑΝ ΝΑ ΤΟ ΠΟΥΜΕ ΣΕ ΕΝΑ ΜΕΓΑΛΥΤΕΡΟ.

ΟΙ ΨΕΥΤΙΚΟΙ ΔΙΑΓΩΝΙΣΜΟΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΠΟΛΛΕΣ ΦΟΡΕΣ ΠΑΙΖΟΝΤΑΣ ΕΝΑ ΠΑΙΧΝΙΔΙ ΜΑΣ ΠΕΤΑΓΕΤΑΙ ΟΤΙ ΚΕΡΔΙΣΑΜΕ ΜΕΓΑΛΑ ΔΩΡΑ ΟΠΩΣ... ΚΙΝΗΤΑ PLAYSTATION ΚΑΙ ΠΟΛΛΑ ΑΛΛΑ. ΣΤΗΝ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ ΟΜΩΣ ΖΗΤΩΝΤΑΣ ΜΑΣ ΤΑ ΠΡΟΣΩΠΙΚΑ ΜΑΣ ΣΤΟΙΧΕΙΑ ΤΟΤΕ ΓΙΝΟΝΤΑΙ ΟΙ ΛΕΓΟΜΕΝΕΣ “ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ”



ΣΑΣ ΕΥΧΑΡΙΣΤΟΥΜΕ ΓΙΑ ΤΟΝ ΧΡΟΝΟ ΣΑΣ.....



**Internet
Safety**