ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Το ΚΥΔ του Πανεπιστημίου Μακεδονίας σας ενημερώνει σχετικά με θέματα που αφορούν σε ηλεκτρονικές απάτες. Η ενημέρωση μάς προστατεύει.

- Phishing
- Pharming
- Spam
- Scam
- Blog
- Διαδικτυακός τζόγος

- Phishing

Το "Ψάρεμα" είναι κάτι περισσότερο από ανεπιθύμητα και ενοχλητικά ηλεκτρονικά μηνύματα. Μπορούν να οδηγήσουν στην κλοπή των αριθμών πιστωτικών καρτών, των κωδικών πρόσβασης, των πληροφοριών λογαριασμών ή άλλων προσωπικών δεδομένων.

Πώς μπορείτε να εντοπίσετε ένα μήνυμα ψαρέματος;
Το "Phishing" είναι ένας τύπος εξαπάτησης που έχει σχεδιαστεί για την κλοπή της ταυτότητάς σας. Οι επιτήδειοι της ηλεκτρονικής απάτης σας πλησιάζουν με ψεύτικα προσχήματα και προσπαθούν να σας πείσουν να κοινοποιήσετε σημαντικές προσωπικές πληροφορίες όπως αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης ή δεδομένα του λογαριασμού σας. Οι απάτες ψαρέματος μπορεί να γίνουν αυτοπροσώπως ή μέσω τηλεφώνου ενώ διακινούνται μέσω ανεπιθύμητων ηλεκτρονικών μηνυμάτων, pop up windows ή άμεσων μηνυμάτων (Instant messaging).

Πώς να διακρίνετε μία απάτη ψαρέματος;
Δεν είναι ασφαλές να εισάγετε προσωπικές ή οικονομικές πληροφορίες σε pop up windows (αναδυόμενα παράθυρα). Μια κοινή τεχνική ψαρέματος είναι το άνοιγμα ενός ψεύτικου αναδυόμενου παραθύρου όταν κάποιος κάνει κλικ σε ένα ηλεκτρονικό μήνυμα ψαρέματος. Μπορεί να φαίνεται πολύ πειστικό ή μπορεί να εμφανίζεται πάνω από ένα παράθυρο που εμπιστεύεστε. Ακόμη και εάν το αναδυόμενο παράθυρο φαίνεται πολύ επίσημο ή διακηρύσσει πως είναι ασφαλές, θα πρέπει να αποφεύγετε να εισάγετε ευαίσθητα προσωπικά δεδομένα γιατί δεν υπάρχει τρόπος να ελέγξετε την πιστοποίηση ασφάλειας.

Ποιος τρόπος υπάρχει να διαπιστώσετε εάν μία τοποθεσία Web προσφέρει ασφάλεια για να προστατέψετε τα ευαίσθητα προσωπικά σας δεδομένα;
Το πιστοποιητικό ασφαλείας της τοποθεσίας αντιστοιχεί στο όνομα της τοποθεσίας. Η εμφάνιση του εικονιδίου με το κίτρινο λουκέτο είναι ένα σημάδι, επειδή το κλειστό λουκέτο υποδεικνύει πως η τοποθεσία Web χρησιμοποιεί κρυπτογράφηση για την προστασία των ευαίσθητων προσωπικών πληροφοριών που εισάγετε (όπως ο αριθμός της πιστωτικής σας κάρτας ή άλλη πληροφορία ταυτοποίησης). Όμως, το εικονίδιο με το κίτρινο λουκέτο μπορεί να είναι ψεύτικο. Για να διασφαλίσετε τη γνησιότητά του κάντε διπλό κλικ για να διαπιστώσετε το πιστοποιητικό ασφαλείας της τοποθεσίας. Το όνομα που ακολουθεί το "Issued to" (Εκδόθηκε για), θα πρέπει να αντιστοιχεί με το όνομα της τοποθεσίας. Εάν το όνομα διαφέρει, πιθανόν να βρίσκεστε σε μια ψεύτικη τοποθεσία, γνωστή και ως "spoofed" (πλαστή) τοποθεσία. Εάν δεν είστε σίγουροι εάν το πιστοποιητικό είναι νόμιμο, μην εισαγάγετε προσωπικά δεδομένα.

Η εκτέλεση λογισμικού προστασίας από ιούς μπορεί να βοηθήσει στην προστασία σας από απάτες ψαρέματος. Αληθεύει;
Αν και το λογισμικό προστασίας από ιούς δεν μπορεί να σας αποτρέψει να ανοίξετε ένα πλαστό ηλεκτρονικό μήνυμα ή να κάνετε κλικ σε επικίνδυνους συνδέσμους, μπορεί εντούτοις να σταματήσει ιούς ή λογισμικό υποκλοπής που θα προέλθει από τέτοιες ενέργειες. Κάποιο πλαστό ηλεκτρονικό μήνυμα μπορεί να σας οδηγήσει σε τοποθεσίες Web που εγκαθιστούν στον υπολογιστή σας λογισμικό το οποίο συνεχίζει να καταγράφει τις πληροφορίες που εισάγετε όπως τον κωδικό πρόσβασης, πληροφορίες σύνδεσης και δεδομένα του λογαριασμού. Αυτού του είδους το ανεπιθύμητο λογισμικό συχνά καλείται spyware (λογισμικό υποκλοπής) ενώ μπορεί να περιέχει ακόμη και ιό.

Ενδείξεις πως ένα ηλεκτρονικό μήνυμα πιθανόν να είναι πλαστό
Στις απάτες ψαρέματος συνηθίζονται οι γενικές προσφωνήσεις όπως "Αγαπητέ πελάτη" αντί για το

όνομά σας. Σας ζητούν να κάνετε κλικ σε κάποιο σύνδεσμο, με φρασεολογία που δίνει την εντύπωση του επείγοντος ή σας ζητούν να επιβεβαιώσετε κάποιες προσωπικές σας πληροφορίες.

Τι να κάνετε εάν πέσετε θύμα απάτης με την πιστωτική σας κάρτα
Εάν πιστεύετε πως πέσατε θύμα απάτης με την πιστωτική σας κάρτα, μπορείτε να ακολουθήσετε αυτά τα βήματα ώστε να ελαχιστοποιήσετε τη ζημιά που μπορεί να προκαλέσει ένας απατεώνας στο λογαριασμό της ταυτότητας, της πιστωτικής κάρτας ή του τραπεζικού λογαριασμού σας. Όταν χρησιμοποιείτε πιστωτική κάρτα, μπορεί να γίνετε ευάλωτοι σε πιθανή απάτη πληρώνοντας μέσω Διαδικτύου, μέσω τηλεφώνου ή ακόμη και αυτοπροσώπως στο μανάβικο της γειτονιάς σας. Γι' αυτό κάθε φορά που πληρώνετε με πιστωτική κάρτα, οι επιχειρήσεις θα πρέπει να επιβεβαιώνουν τα στοιχεία του λογαριασμού σας πριν σας παρέχουν αγαθά και υπηρεσίες. Δυστυχώς, επειδή τα στοιχεία της πιστωτικής σας κάρτας αποθηκεύονται σε μεγάλους υπολογιστές, οι διακομιστές μπορούν να γίνουν στόχος χάκερ οι οποίοι αναζητούν τρόπους για να εισχωρήσουν στο σύστημα και να ανακτήσουν στοιχεία τα οποία κατόπιν, θα τα χρησιμοποιήσουν για να διαπράξουν κάποια απάτη.

Εάν πιστεύετε πως πέσατε θύμα απάτης ή δόλου, ακολουθήστε αμέσως τα παρακάτω βήματα.

- Όσο ταχύτερα επικοινωνήσετε με τις αρμόδιες αρχές, τόσο πιθανότερο είναι να μειώσετε τη ζημιά που μπορεί να κάνει ο απατεώνας με τα στοιχεία σας, την πιστωτική σας κάρτα και τον τραπεζικό σας λογαριασμό.
- Κλείστε όλους τους λογαριασμούς που επηρεάζονται.
- Επικοινωνήστε με την πραγματική εταιρεία ή τον οργανισμό εάν πιστεύετε πως δώσατε ευαίσθητες πληροφορίες σε άγνωστη πηγή, η οποία προσποιήθηκε πώς ήταν η πραγματική εταιρεία ή οργανισμός. Εάν επικοινωνήσετε αμέσως με την πραγματική εταιρεία, ίσως μπορέσουν να περιορίσουν τη ζημιά προς εσάς και προς τους υπολοίπους.
- Επικοινωνήστε με το τμήμα ασφάλειας ή απάτης κάθε τράπεζας ή πιστωτικού ιδρύματος με το οποίο συνεργάζεστε, συμπεριλαμβανομένων των εταιριών πιστωτικών καρτών, εργαλείων, παρόχων υπηρεσιών Διαδικτύου και άλλων τοποθεσιών όπου χρησιμοποιείτε την πιστωτική σας κάρτα, για κάθε ύποπτη πρόσβαση ή άνοιγμα λογαριασμού.
- Στη συνέχεια στείλτε μία επιστολή και κρατήστε και ένα αντίγραφο για εσάς.
- Όταν ανοίξετε νέους λογαριασμούς χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης, όχι δηλαδή το όνομα της μητέρας σας μαζί με αριθμό λογαριασμού.
- Αλλάξτε τους κωδικούς πρόσβασης σε όλους τους διαδικτυακούς λογαριασμούς και αρχίστε από αυτούς που έχουν σχέση με χρηματοπιστωτικά ιδρύματα ή πληροφορίες.
- Προσθέστε ειδοποίηση απάτης στους πιστωτικούς λογαριασμούς
- Ζητήστε ένα αντίγραφο της αναλυτικής κατάστασης του λογαριασμού σας (τα θύματα κλοπής στοιχείων ταυτότητας μπορούν να λάβουν αντίγραφα των αναλυτικών καταστάσεων των πιστωτικών τους λογαριασμών δωρεάν) και ζητήστε να μην γίνει καμία νέα πίστωση του λογαριασμού χωρίς την έγκριση σας.
- Βεβαιωθείτε πως ο λογαριασμός σας διαθέτει επισήμανση "ειδοποίησης απάτης" και "δήλωση θύματος" και επιμείνετε ώστε η προειδοποίηση να παραμείνει ενεργή το πολύ για εφτά χρόνια.
- Στείλτε τις αιτήσεις γραπτώς και φυλάξτε αντίγραφα για εσάς.
- Όταν λάβετε τις αναλυτικές καταστάσεις εξετάστε τις προσεκτικά.
- Ψάξτε για ερωτήσεις που δεν κάνατε, λογαριασμούς που δεν ανοίξατε και ανεξήγητες χρεώσεις.
- Καταθέστε μια καταγγελία.
- Κάντε αναφορά στο τοπικό αστυνομικό τμήμα.
- Ζητήστε αντίγραφο της αναφοράς της αστυνομίας για να ενημερώσετε την τράπεζα, την εταιρεία της πιστωτικής κάρτας και τους υπόλοιπους πιστωτές ότι είστε θύμα απάτης και όχι καταχραστής της πίστωσης.
- Να καταχωρίζετε και να αποθηκεύετε τα πάντα
- Μόλις ολοκληρώσετε όλα τα βήματα, καλό είναι αφού δημιουργήσετε εκτυπωμένα αντίγραφα των εγγράφων για σας, περιλαμβανομένων των ηλεκτρονικών μηνυμάτων και γραπτών απαντήσεων και αφού καταγράψετε τις τηλεφωνικές σας κλήσεις, να τα φυλάξετε σε κάποιο ασφαλές μέρος.
- Για τηλεφωνικές ή κατ' ιδίαν συνομιλίες, επανέλθετε με επιστολές επιβεβαίωσης προς τους οργανισμούς και φυλάξτε ένα αντίγραφο για τον εαυτό σας.
- Αναφέρετε στην επιστολή ό,τι ειπώθηκε κατά τη συνομιλία και καταγράψτε κάθε στοιχείο που ακολουθεί και για το οποίο δεσμευτήκατε εσείς ή ο αντιπρόσωπός σας κατά την συζήτηση.

- Pharming

Απάτη με pharming (παραπλάνηση): ανακατεύθυνση του browser σε ψεύτικες ιστοσελίδες. Έχετε ακούσει για το pharming, όπου η κίνηση του Διαδικτύου ανακατευθύνεται από μία τοποθεσία σε μία άλλη, πανομοιότυπη που είναι όμως απάτη; "Pharming" σημαίνει όταν εγκληματίες χάκερ ανακατευθύνουν την κίνηση του Διαδικτύου από μία ιστοσελίδα σε μια άλλη, πανομοιότυπη έτσι ώστε να σας ξεγελάσουν και να καταχωρήσετε το όνομα χρήστη και τον κωδικό χρήστη στη βάση δεδομένων της πλαστής ιστοσελίδας. Ιστοσελίδες τραπεζών ή αντίστοιχων οικονομικών οργανισμών είναι συχνά στόχοι τέτοιων επιθέσεων, κατά τις οποίες εγκληματίες προσπαθούν να αποσπάσουν προσωπικά δεδομένα, με σκοπό να βρουν πρόσβαση στον τραπεζικό σας λογαριασμό, να κλέψουν την ταυτότητά σας ή να διαπράξουν άλλου είδους απάτη στο όνομά σας.

Το Pharming (παραπλάνηση), η χρήση δηλαδή ψεύτικων ιστοσελίδων πιθανόν να θυμίζει τις απάτες ψαρέματος από ηλεκτρονικά μηνύματα, όμως η παραπλάνηση είναι πιο ύπουλη, αφού μπορεί να κατευθυνθείτε σε μία ψεύτικη ιστοσελίδα χωρίς να το γνωρίζετε. Εώς σήμερα έχουν γίνει αρκετές επιθέσεις, γεγονός που έχει αρχίσει να ανησυχεί αρκετά κυβερνήσεις και επιχειρήσεις. Είναι επίσης σημαντικό να θυμάστε πως το Διαδίκτυο είναι μια δωρεάν και ανεξάρτητη πηγή, όπως μία βιβλιοθήκη ή άλλες δημόσιες υπηρεσίες, στον τόπο όπου ζείτε. Εάν παρατηρήσετε κάτι ύποπτο σχετικά με μία ιστοσελίδα που εμπιστεύεστε, αναφέρετέ το —τηλεφωνικά εάν είναι δυνατόν—στην επιχείρηση ή στον ιδιοκτήτη της ιστοσελίδας.

Αναλυτικά

Πώς μπορεί κάποιος απατεώνας που θέλει να με παραπλανήσει, να κατευθύνει το browser μου σε κάποια άλλη ιστοσελίδα; Με τη χρήση μιας διαδικασίας που ονομάζεται "δηλητηρίαση DNS" κατά την οποία κάποιος εισβολέας αποκτά πρόσβαση στις τεράστιες βάσεις δεδομένων που χρησιμοποιούν οι πάροχοι υπηρεσιών Διαδικτύου για να δρομολογήσουν τη διαδικτυακή κίνηση και μπορεί να κάνει τροποποιήσεις σε κάποιο σημείο έτσι ώστε να εκτρέπεστε στην ψεύτικη ιστοσελίδα πριν αποκτήσετε πρόσβαση σε αυτή που τελικά επιθυμούσατε. Κάποιες εταιρίες υποστηρίζουν πως το λογισμικό firewall (τείχος προστασίας) που χρησιμοποιούν προστατεύει και από την παραπλάνηση (pharming).

Κάποιοι πάροχοι υπηρεσιών διαδικτυακής ασφάλειας πιστεύουν πως οι πελάτες τους που καθοδηγούν όλη τους την διαδικτυακή κίνηση μέσω των δικών τους, ασφαλών, διακομιστών είναι και προστατευμένοι από επιθέσεις παραπλανήσεις. Η φύση της παραπλάνησης υποδεικνύει το αντίθετο αλλά, ανεξάρτητα από το τι υποστηρίζει η κάθε εταιρεία, είναι καλή ιδέα να αναζητάτε προσεκτικά τα προϊόντα ασφαλείας πριν επενδύσετε και εμπιστευτείτε κάποιες λύσεις λογισμικού.

Δεν μπορώ να αναγνωρίσω εάν μία ιστοσελίδα είναι ψεύτικη απλά μετακινώντας το δείκτη πάνω από τα link και παρατηρώντας εάν ο κώδικας με οδηγεί σε κάποιο εμφανώς άσχετο σημείο εκτός ιστοσελίδας; Όχι απαραίτητα. Οι ψεύτικες ιστοσελίδες που χρησιμοποιούνται στις απάτες παραπλάνησης συνήθως "πλαστογραφούν" τα link τους έτσι ώστε να μοιάζουν ακριβώς με αυτά που αναμένετε να δείτε, ακόμη και στον κώδικα που εμφανίζεται όταν το ποντίκι περάσει πάνω από αυτά. Επίσης, οι ιστοσελίδες πιθανόν να αλλάζουν τον κώδικα των δικών τους links αρκετά συχνά και για διάφορους λόγους, όπως όταν αναβαθμίζουν το λογισμικό τους, την πλατφόρμα του διακομιστή τους ή τις μεθόδους ανάλυσης των στατιστικών κίνησης της ιστοσελίδας τους.

- Spam

Τι είναι ένα ανεπιθύμητο ηλεκτρονικό μήνυμα;
Το e-mail spam είναι ανεπιθύμητο διαφημιστικό ηλεκτρονικό μήνυμα.

Τι θα πρέπει να κάνετε εάν λάβετε ένα μήνυμα που πιθανόν να είναι ανεπιθύμητο;
Εάν λάβετε ένα ηλεκτρονικό μήνυμα που πιθανόν να είναι ανεπιθύμητο, δεν θα πρέπει να απαντήσετε σε αυτό, να κάνετε κλικ ή να το προωθήσετε. Εάν είναι δυνατόν θα πρέπει να το αναφέρετε και να το διαγράψετε χωρίς να το ανοίξετε ή να κάνετε κλικ σε κάποιο σύνδεσμο μέσα σε αυτό.

Γιατί είναι ενοχλητικό ένα ηλεκτρονικό ανεπιθύμητο μήνυμα;
Το spam είναι ενοχλητικό, γιατί πιθανόν να εμπεριέχει απάτη ή να μολύνει τον υπολογιστή σας με ιό ή άλλο κακόβουλο λογισμικό.

Μερικά βήματα που μπορείτε να ακολουθήσετε ώστε να προστατευτείτε από τα ανεπιθύμητα μηνύματα:

- Μην δίνετε σε οποιονδήποτε την ηλεκτρονική σας διεύθυνση.
- Χρησιμοποιήστε ενημερωμένα φίλτρα κατά των ανεπιθύμητων μηνυμάτων.
- Ποτέ μην ανοίγετε τα συνημμένα των μηνυμάτων εκτός και αν γνωρίζετε περί τίνος πρόκειται.
- Αναφέρετε στις αρμόδιες αρχές τους αποστολείς των ανεπιθύμητων μηνυμάτων.

Downloading. Κάντε λήψη με προσοχή:
Πρώτα να σκέφτεστε και μετά να κάνετε κλικ. Αναρωτηθήκατε ποτέ εάν είναι ασφαλές να ανοίξετε ένα λογιστικό φύλλο που λάβατε ως συνημμένο από κάποιον συνάδελφο ή να «κατεβάσετε» ένα όμορφο μικρό screensaver από το Διαδίκτυο ή να κάνετε λήψη μουσικών αρχείων ή αρχείων βίντεο από τον υπολογιστή ενός αγνώστου; Πριν το επιχειρήσετε, σκεφτείτε σοβαρά την πιθανότητα κινδύνου για τον υπολογιστή σας ή το δίκτυο της εταιρείας. Για να προστατέψετε το υπολογιστή σας από πιθανούς κινδύνους απαιτείται λίγη προνοητικότητα και προσοχή.

Τι είναι το downloading;
Στη διαδικασία λήψης αρχείων "downloading" συμπεριλαμβάνεται η εγκατάσταση προγραμμάτων από CD, το άνοιγμα εικόνων ή η σύνδεση σε τοποθεσίες Web από ηλεκτρονικά μηνύματα, αντιγραφή εγγράφων Word ή λογιστικών φύλλων Excel από το δίκτυο της εταιρείας, η ενημέρωση λογισμικού που απαιτείται από το Διαδίκτυο ή η μεταφορά μουσικών αρχείων από έναν υπολογιστή στην άλλη άκρη του κόσμου. Αυτά τα αρχεία μπορεί να είναι αυτό που αναμένατε αλλά μπορεί να είναι και εντελώς επικίνδυνα. Κακόβουλο λογισμικό (malware) είναι το λογισμικό το οποίο μπορεί να βλάψει τον υπολογιστή σας. Μπορεί να περιέχει ιούς, worm, προγράμματα υποκλοπής ή άλλα ενοχλητικά προγράμματα. Η απελευθέρωση ενός ιού μπορεί να προκαλέσει την καταστροφή δεδομένων στον υπολογιστή σας ή να επιτρέψει την πρόσβαση τρίτων σε αυτόν, στο δίκτυο και σε όλους τους υπολογιστές που είναι συνδεδεμένοι σε αυτό. Αυτό μπορεί να έχει καταστροφικό αντίκτυπο στην παραγωγική διαδικασία της εταιρείας σας, ειδικά εάν ο ιός καταστρέψει σημαντικές πληροφορίες, όπως καταλόγους διευθύνσεων ή άλλες εμπιστευτικές πληροφορίες. Οι πιο γνωστές μορφές προγραμμάτων υποκλοπής μπορούν να αλλάξουν τη συμπεριφορά του υπολογιστή σας —να τον καθυστερούν υπερβολικά, ακόμη και να του προκαλέσουν βλάβη. Περισσότερο επικίνδυνο είναι το γεγονός ότι τα προγράμματα υποκλοπής μπορούν να παρακολουθήσουν της συνήθειες περιήγησης, να αποσπάσουν κωδικούς πρόσβασης καθώς επίσης και να επιτρέψουν σε κάποιον εισβολέα να πάρει τον έλεγχο του υπολογιστή σας. Κακόβουλο λογισμικό μπορεί να εγκατασταθεί στον υπολογιστή χωρίς να το γνωρίζετε ή χωρίς να συναινείτε ή μπορεί να είναι ενσωματωμένο σε κάποιο πρόγραμμα που σκοπεύετε να κατεβάσετε από το Διαδίκτυο. Για παράδειγμα, ενώ εσείς πιστεύετε πως κάνατε λήψη ενός παιχνιδιού, ανακαλύπτετε πως το "παιχνίδι" βρήκε στον υπολογιστή τον αριθμό της πιστωτικής σας κάρτας και το έστειλε σε κάποιον εισβολέα. Κάποια είδη κακόβουλου λογισμικού εξαπλώνονται όταν αποστέλλουν ηλεκτρονικά μηνύματα από έναν "μολυσμένο" υπολογιστή σε κάθε ηλεκτρονική διεύθυνση που βρίσκουν.

Για αρχή κάντε τον υπολογιστή σας λιγότερο τρωτό σε εξωτερικούς κινδύνους.
Σημειώστε πως όλες αυτές οι διαδικασίες προστασίας πιθανόν να υπάρχουν ήδη στην εταιρεία σας, γι' αυτό συμβουλευτείτε πρώτα το διαχειριστή του συστήματος πριν ακολουθήσετε κάποιες από τις οδηγίες που ακολουθούν.

- Ακολουθήστε τις οδηγίες που ταιριάζουν στη έκδοση του δικού σας λειτουργικού συστήματος για να χρησιμοποιήσετε ένα τείχος προστασίας ή να εγκαταστήσετε λογισμικό προστασίας από ιούς.
- Ρυθμίστε το πρόγραμμα προστασίας από ιούς ώστε να ανιχνεύει όλα τα εισερχόμενα αρχεία και τα συνημμένα των ηλεκτρονικών μηνυμάτων πριν τα ανοίξετε. Αυτό είναι διαφορετικό για κάθε πρόγραμμα προστασίας από ιούς, γι' αυτό συμβουλευτείτε το εγχειρίδιο χρήσης του.
- Χρησιμοποιήστε ένα φίλτρο ανεπιθύμητων μηνυμάτων (spam). Πολλά προγράμματα ηλεκτρονικών μηνυμάτων προσφέρουν φίλτρα που εμποδίζουν τα ανεπιθύμητα μηνύματα. Το Microsoft Outlook διαθέτει ισχυρές άμυνες απέναντι στα άχρηστα μηνύματα, αλλά μπορείτε επίσης να ενισχύσετε την άμυνα σας απέναντι στα ανεπιθύμητα μηνύματα.
- Εγκαταστήστε και εκτελέστε ένα πρόγραμμα για τον εντοπισμό και την αφαίρεση λογισμικού υποκλοπής. Τα πακέτα υπηρεσίας που προσφέρουν ορισμένοι πάροχοι υπηρεσιών Διαδικτύου (ISP) περιλαμβάνουν λογισμικό προστασίας από υποκλοπή. Εάν ο πάροχος δεν σας το παρέχει, εξετάστε την περίπτωση του Microsoft Windows AntiSpyware (Beta) ή δωρεάν λογισμικού προστασίας από υποκλοπή άλλων εταιρειών.

Σήμερα τι ποσοστό της κίνησης των ηλεκτρονικών μηνυμάτων είναι ανεπιθύμητα;
Με βάση έγκυρα sites στην Αμερική τα οποία μετρούν την κίνηση στο Διαδίκτυο και κάποιους υπολογισμούς, το 80% ολόκληρης της κίνησης των ηλεκτρονικών μηνυμάτων είναι ανεπιθύμητα.

Δεν υπάρχουν ανεπιθύμητα άμεσα μηνύματα. ***Λάθος***
Όπως μπορείτε να λάβετε ανεπιθύμητα μηνύματα στο ηλεκτρονικό σας ταχυδρομείο έτσι μπορείτε να λάβετε και ανεπιθύμητα άμεσα μηνύματα (Instant messaging, Messenger, IRC κ.ά) (συχνά αναφέρονται ως "**spim**"). Αυτά τα άμεσα μηνύματα μπορεί να προέρχονται από κάποιον τελείως άγνωστο σας ή και από ανθρώπους που γνωρίζετε. Μπορεί επίσης να περιέχουν και επικίνδυνους ιούς. Εάν λάβετε μια ηλεκτρονική κάρτα από κάποιον που δεν γνωρίζετε, θα πρέπει να την διαγράψετε.

- Scam

Μέχρι πρόσφατα, οι επαγγελματίες απατεώνες περιορίστηκαν στη χρήση αργών και αναποτελεσματικών τηλεφωνημάτων και έντυπων αγγελιών για να προωθήσουν τις απάτες τους. Σήμερα, τα ίδια χαρακτηριστικά που κάνουν το Διαδίκτυο τόσο βολικό για όσους αναζητούν εργασία, δηλαδή η παγκοσμιότητα, η ευχρηστία και η ταχύτητα, διευκολύνουν τους εγκληματίες να επιδίδονται σε απάτες με θέμα την απασχόληση, διατρέχοντας μικρότερο κίνδυνο.

Ψεύτικες ευκαιρίες απασχόλησης.
Δημιουργώντας ψεύτικες αγγελίες θέσεων εργασίας που μοιάζουν με τις αληθινές και, συχνά, δημοσιεύοντάς τις σε νόμιμες ιστοσελίδες εύρεσης εργασίας, οι απατεώνες ελπίζουν να παραπλανήσουν τους πρόθυμους και ανυποψίαστους που αναζητούν εργασία και να τους πείσουν να στείλουν τα προσωπικά τους στοιχεία (το γνωστό ψάρεμα). Αυτές οι ψεύτικες αγγελίες εύρεσης εργασίας γίνονται όλο και πιο κομψές και, συχνά, χρησιμοποιούν συνηθισμένη εικόνα ή πειστικά εταιρικά λογότυπα και φρασεολογία. Πολλές φορές, διαθέτουν και συνδέσμους προς πλαστές ιστοσελίδες που εμφανίζονται ως τοποθεσίες πραγματικών εταιρειών. Κάποιες φορές ακόμα χρεώνουν για υπηρεσίες που δεν θα παράσχουν ποτέ. Τυπικά, μετά από μερικές μέρες, οι κλέφτες κλείνουν το scam και εξαφανίζονται.

Παράνομα γραφεία ευρέσεως εργασίας.
Ακόμα, εκτός από τη σάρωση προσωπικών ιστοσελίδων και τη δημοσίευση ανακοινώσεων σε δημόσιες ιστοσελίδες, οι επαγγελματίες απατεώνες συχνά εμφανίζονται ως γραφεία ευρέσεως εργασίας που διαθέτουν ευκαιρίες απασχόλησης και στέλνουν ανεπιθύμητη αλληλογραφία (ή spam) σε πιθανούς υποψηφίους ή νόμιμα γραφεία ευρέσεως εργασίας. Ένας επαγγελματίας απατεώνας τέτοιου είδους θα προσπαθήσει να κερδίσει την εμπιστοσύνη του θύματος, χρησιμοποιώντας ψεύτικο προσωπικό για να αποσπάσει προσωπικά στοιχεία, ακόμη και από το τηλέφωνο. Είναι σημαντικό να θυμάστε ότι τέτοια στοιχεία θα σας ζητηθούν μόνον σε προσωπική συνέντευξη.

Οι καλύτερες πρακτικές για όσους αναζητούν εργασία μέσω Διαδικτύου

- Ποτέ μην δίνετε κανένα προσωπικό στοιχείο που να μην σχετίζεται με τη δουλειά, όπως στοιχεία ταυτότητας, τον αριθμό φορολογικού μητρώου, τον αριθμό της πιστωτικής σας κάρτας, την ημερομηνία γέννησης και την οικογενειακή σας κατάσταση στο Διαδίκτυο, μέσω e-mail, από το τηλέφωνο, σε φαξ ή στο βιογραφικό σας.
- Να δημοσιεύσετε το βιογραφικό σας μόνον σε ιστοσελίδα εύρεσης εργασίας που εφαρμόζει πολιτική προστασίας προσωπικών δεδομένων και επιτρέπει την πρόσβαση στα βιογραφικά μόνον σε πιστοποιημένα γραφεία εύρεσης εργασίας.
- Να διασταυρώνετε τα στοιχεία κάθε ενδεχόμενου εργοδότη, επαγγελματία ή γραφείου εύρεσης εργασίας και μέσω δεύτερης πηγής ή του τηλεφωνικού καταλόγου και, στη συνέχεια, απευθυνθείτε στον εργοδότη απευθείας. Ο καλύτερος τρόπος να διασταυρώσετε τα στοιχεία ενός ενδεχόμενου εργοδότη είναι να επισκεφθείτε τα γραφεία της εταιρείας του, σε ώρες εργασίας.
- Εάν κάποιος ενδεχόμενος εργοδότης ή γραφείο εύρεσης εργασίας θελήσει να κάνει έλεγχο των στοιχείων σας, να το δεχθείτε μόνον αφού συναντηθείτε με τον εργοδότη στα γραφεία της εταιρείας, σε ώρες εργασίας.
- Να μην εμπιστεύεστε όσους σας ζητούν χρήματα εκ των προτέρων για να σας βρουν δουλειά.
- Ποτέ να μην δεχθείτε να πληρώσετε για "αποκλειστικές" πληροφορίες για θέσεις εργασίας ή για να πάρετε κάποια συγκεκριμένη θέση. Εάν πληρώσετε για υπηρεσίες εύρεσης εργασίας, μην δώσετε τα στοιχεία της πιστωτικής σας κάρτας ή του τραπεζικού σας λογαριασμού και μην κάνετε καμία συναλλαγή σε μετρητά με οποιονδήποτε επαγγελματία ή γραφείο ευρέσεως εργασίας, εκτός εάν το κάνετε αυτοπροσώπως, επιτόπου.
- Να αξιολογείτε προσεκτικά τα στοιχεία επαφής που δίνονται σε αγγελίες εργασίας ή σε σχετικά e-mail και να προσέχετε εάν υπάρχουν ανορθογραφίες, κάποια διεύθυνση e-mail που δεν αναφέρει το όνομα της εταιρείας ή εάν η περιοχή ή ο ταχ. κώδικας δεν είναι παντού τα ίδια.

- Να πληκτρολογείτε τις διευθύνσεις των ιστοσελίδων (URL) στο browser αντί να χρησιμοποιείτε links όταν ελέγχετε τις πηγές των θέσεων εργασίας και να προσέχετε ακόμη μια νέα μορφή απάτης που μοιάζει με το phishing και λέγεται "pharming" (παραπλάνηση) και η οποία κάνει ανακατεύθυνση των χρηστών από τις νόμιμες τοποθεσίες Web σε απομιμήσεις, με σκοπό την κλοπή προσωπικών στοιχείων.
- Να δημιουργήσετε διεύθυνση ηλεκτρονικού ταχυδρομείου και έναν λογαριασμό για όλες τις μη προσωπικές επικοινωνίες.
- Αν και δεν υπάρχει καμία μέθοδος να εντοπίσετε τις ψεύτικες αγγελίες εργασίας που να προστατεύει απολύτως από τις απάτες, να προσέχετε εάν υπάρχουν πολλά ορθογραφικά λάθη και άλλες ανακρίβειες, καθώς αυτό αποτελεί συνηθισμένη ένδειξη.
- Να εμπιστεύεστε το ένστικτό σας και να δίνετε ιδιαίτερη προσοχή όταν απευθύνεστε σε εταιρείες που βρίσκονται έξω από τη χώρα σας.
- Εάν κάποια ευκαιρία υπόσχεται υπερβολικά πολλά ή κάτι άλλο δεν φαίνεται σωστό, μάλλον πρόκειται για παραπλανητικό μήνυμα.

- Blog

Η πρακτική του blogging, η τήρηση προσωπικού ημερολογίου στο Διαδίκτυο, μεγαλώνει δραματικά—ειδικά ανάμεσα στους έφηβους, οι οποίοι ορισμένες φορές διατηρούν ημερολόγια blog χωρίς να το γνωρίζουν οι γονείς ή οι κηδεμόνες τους.

Σύμφωνα με κάποιες πρόσφατες μελέτες έδειξαν πως **τα μισά από τα ημερολόγια blog σήμερα δημιουργούνται από εφήβους** με δύο στους τρεις να δημοσιοποιούν την ηλικία τους, τρεις στους πέντε να αποκαλύπτουν την τοποθεσία τους και έναν στους πέντε να αποκαλύπτει το πλήρες όνομα του. Αυτό συμβαίνει χωρίς να λέγεται ότι υπάρχουν πιθανοί κίνδυνοι από τη δημοσιοποίηση αυτού του τύπου προσωπικών λεπτομερειών. Και καθώς πολλά νεαρά παιδιά δημιουργούν όλο και περισσότερα ημερολόγια blog, οδηγούνται σε έναν αυξανόμενο ανταγωνισμό μεταξύ τους για να τραβήξουν την προσοχή. Μερικές φορές αυτό μπορεί να οδηγήσει τα παιδιά να δημοσιεύσουν ακατάλληλο υλικό όπως **προκλητικές εικόνες των εαυτών τους ή των φίλων τους**.

Αν και η διατήρηση ενός ημερολογίου blog προσφέρει πιθανά οφέλη, όπως την βελτίωση των ικανοτήτων στη γραφή και στην επικοινωνία, είναι σημαντικό να εκπαιδεύσετε τα παιδιά σας σχετικά με το Διαδίκτυο και τη δημιουργία ημερολογίων πριν ακόμη ξεκινήσουν.

Να μερικές προτάσεις για να ξεκινήσετε:

- Καθιερώστε κανόνες για τη χρήση του Διαδικτύου με τα παιδιά σας και να είστε επιμελής.
- Δείτε τι πρόκειται να δημοσιεύσουν τα παιδιά σας πριν το δημοσιεύσουν. Πληροφορίες που πιθανόν φαίνονται ακίνδυνες όπως το σήμα ή το όνομα του σχολείου ή φωτογραφίες της πόλης μπορούν, αν τοποθετηθούν μαζί να αποκαλύψουν που πηγαίνουν σχολείο τα παιδιά.
- Αναρωτηθείτε (και καθοδηγήστε τα παιδιά σας ώστε να πράξουν το ίδιο) εάν είστε άνετοι δείχνοντας το σε κάποιο ξένο. Εάν αμφιβάλλετε, υποχρεώστε τα να το διαγράψουν.
- Δοκιμάστε την υπηρεσία δημιουργίας ημερολόγιων blog και βρείτε εάν προσφέρει ιδιωτικά ημερολόγια με προστασία κωδικού πρόσβασης.
- Επισκεφθείτε το ημερολόγιο του παιδιού σας συχνά και επιθεωρήστε το. Επισκεφθείτε άλλα ημερολόγια για να βρείτε καλά παραδείγματα ώστε να τα υιοθετήσουν τα παιδιά σας.

Βασικές οδηγίες για δημιουργούς ημερολογίων blog
Οι ακόλουθες συμβουλές είναι ένα καλό σημείο εκκίνησης για παιδιά που ενδιαφέρονται να δημιουργήσουν ημερολόγια blog.

- Μην παρέχετε ποτέ προσωπικές πληροφορίες όπως επώνυμο, πληροφορίες επικοινωνίας, διεύθυνση κατοικίας, αριθμούς τηλεφώνων, όνομα σχολείου, ηλεκτρονική διεύθυνση, επώνυμο φίλων ή συγγενών, όνομα άμεσης επικοινωνίας, ηλικία ή ημερομηνία γέννησης.
- Μην δημοσιεύετε ποτέ προκλητικές φωτογραφίες του εαυτού σας ή κάποιον άλλο και βεβαιωθείτε πως όποια φωτογραφία δημοσιεύεται δεν αποκαλύπτει κάποιες προσωπικές πληροφορίες.
- Επίσης να θυμάστε να κοιτάτε πάντα στο background της φωτογραφίας.
- Θεωρείστε πως ό,τι δημοσιεύεται στο Διαδίκτυο είναι μόνιμο. Οποιοσδήποτε μπορεί στο Διαδίκτυο να εκτυπώσει ένα ημερολόγιο ή να το αποθηκεύσει στον υπολογιστή του.

- Χρησιμοποιήστε τοποθεσίες παροχής ημερολογίων blog με ξεκάθαρους όρους χρήσης, και βεβαιωθείτε πως μπορείτε να προστατέψετε με κωδικό πρόσβασης και τα ενεργά ημερολόγια blog και όχι μόνο τους λογαριασμούς. (Εάν όχι, είναι καλύτερο να θεωρήσετε πως οποιοσδήποτε μπορεί να το δει).
- Αποφεύγετε να υπερβάλετε ή να ανταγωνίζεστε με άλλους δημιουργούς ημερολογίων (bloggers).
- Διατηρήστε τα ημερολόγια blog θετικά και μην τα χρησιμοποιείτε για να δυσφημήσετε ή να επιτεθείτε σε άλλους.

- Διαδικτυακός τζόγος

Ο διαδικτυακός τζόγος και τα παιδιά σας. Πώς να βοηθήσετε τα παιδιά σας να αποφύγουν τα τυχερά παιχνίδια στο Διαδίκτυο

Πολλά παιδιά απολαμβάνουν να χρησιμοποιούν το Internet για να ανακαλύπτουν δραστηριότητες ψυχαγωγίας, όπως τα διαδικτυακά παιχνίδια. Πολλές φορές, ενώ αναζητούν μια νέα ιστοσελίδα με παιχνίδια μπορεί να βρουν ιστοσελίδες με στοιχήματα και τυχερά παιχνίδια. Ενώ η χρήση των περισσότερων παιχνιδιών και δραστηριοτήτων από ανηλίκους είναι νόμιμη, η χρήση των τυχερών παιχνιδιών δεν είναι.

Ποιά είναι η διαφορά ανάμεσα στις τοποθεσίες παιχνιδιών και τις τοποθεσίες τυχερών παιχνιδιών;
Οι κυριότερες διαφορές μεταξύ των τύπων των ιστοσελίδων είναι οι εξής:

- Οι τοποθεσίες παιχνιδιών συνήθως περιέχουν παιχνίδια με κάρτες, πίνακες, λέξεις, arcade ή παζλ, με αυτόματη παρακολούθηση και προβολή του σκορ.
- Δεν γίνεται ανταλλαγή χρημάτων, αληθινών ή ψεύτικων. Οι τοποθεσίες τυχερών παιχνιδιών μπορούν να περιέχουν σενάρια, στα οποία οι άνθρωποι κερδίζουν ή χάνουν κάποιο τεχνητό νόμισμα. Οι τοποθεσίες Τζόγου συνήθως αφορούν το κέρδος ή την απώλεια αληθινών χρημάτων.

Βοηθήστε τα παιδιά σας να αποφύγουν το διαδικτυακό τζόγο
Οι γονείς θα πρέπει να αποφασίσουν ποιοί τύποι παιχνιδιών ή τοποθεσιών παιχνιδιών είναι κατάλληλοι για τα παιδιά τους. Για παράδειγμα, μπορείτε να βασίσετε τα κριτήριά σας στον τύπο του παιχνιδιού (μόνον παιχνίδια με κάρτες και πίνακα ή μόνον παιχνίδια στρατηγικής και φαντασίας), καθώς και στο εάν το παιχνίδι παίζεται διαδραστικά με άλλους στο Διαδίκτυο, εάν η τοποθεσία προσφέρει το παιχνίδι δωρεάν ή και κατά περίπτωση.

Μπορείτε επίσης να κάνετε και τα εξής:

- Μάθετε ποιές τοποθεσίες επισκέπτονται τα παιδιά σας στο Διαδίκτυο και τι κάνουν.
- Καθιερώστε σαφείς κανόνες σχετικά με τα διαδικτυακά παιχνίδια που μπορούν να παίξουν τα παιδιά σας και τοποθετήστε τους υπολογιστές που έχουν πρόσβαση στο Διαδίκτυο σε ανοικτό χώρο, όχι στο παιδικό δωμάτιο.
- Υπενθυμίστε στα παιδιά σας πώς είναι παράνομο να συμμετέχουν σε τυχερά παιχνίδια στο Διαδίκτυο. (Σε πολλές χώρες η συμμετοχή ανηλίκων σε τυχερά παιχνίδια απαγορεύεται, γι' αυτό ενημερωθείτε για την τοπική νομοθεσία).
- Βοηθήστε τα παιδιά σας να κατανοήσουν πώς λειτουργούν τα τυχερά παιχνίδια. Οι επιχειρήσεις τυχερών παιχνιδιών στο Διαδίκτυο σκοπό έχουν το κέρδος. Κερδίζουν περισσότερα χρήματα από όσα πληρώνουν.
- Βεβαιωθείτε ότι τα παιδιά σας πάντα ζητούν την άδειά σας προτού χρησιμοποιήσουν τον αριθμό της πιστωτικής σας κάρτας στο Διαδίκτυο. Η συμμετοχή σε τυχερά παιχνίδια στο Διαδίκτυο απαιτεί συνήθως τη χρήση πιστωτικής κάρτας. Εάν τα παιδιά συσσωρεύσουν χρέη στο Διαδίκτυο, μπορεί να καταστρέψουν την πιστοληπτική ικανότητά τους ή την πιστοληπτική ικανότητα των γονέων τους.
- Εξηγήστε ότι ο διαδικτυακός τζόγος είναι εθιστικός. Μπορεί κάποιος να παίζει αδιάκοπα και χωρίς να τον καταλάβει κανείς επί ώρες. Ο μοναχικός τζόγος επί πιστώσει μπορεί να δημιουργήσει κακές συνήθειες.

πηγή Microsoft