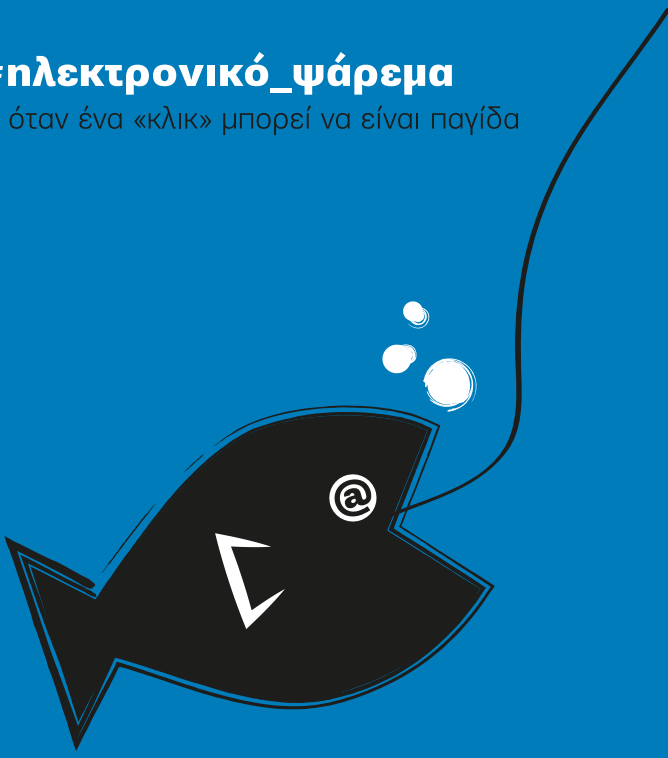
#ηλεκτρονικό_ψάρεμα

όταν ένα «κλικ» μπορεί να είναι παγίδα



Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#ηλεκτρονικό_ψάρεμα

όταν ένα «κλικ» μπορεί να είναι παγίδα

Σίγουρα, καθένας από εμάς έχει ακούσει να λέγονται πολλά για το διαδίκτυο και τους κινδύνους που μπορεί να κρύβει ανάμεσα στις χιλιάδες ιστοσελίδες και blogs, σε φαινομενικά αθώα μηνύματα στο ηλεκτρονικό μας ταχυδρομείο, αλλά και σε εφαρμογές που, εκεί που «σερφάρουμε» ανυποψίαστοι, εμφανίζονται ως διά μαγείας και ζητάνε τη συνεισφορά μας ή να πατήσουμε «ΟΚ» για να συνεχίσουμε... πού, όμως;

Πολλές και διαφορετικές είναι οι καιροσκοπικές ή κακόβουλες ενέργειες κατά των χρηστών του διαδικτύου, και το λιγότερο που μπορούμε να κάνουμε είναι να μη σταματήσουμε ποτέ να ρωτάμε και να ενημερωνόμαστε για το τι μπορεί ν' αποτελέσει κίνδυνο στο διαδίκτυο τόσο για εμάς όσο και για τα παιδιά μας, τους φίλους και τους συγγενείς μας. Ήρθε η στιγμή, λοιπόν, να ενημερωθούμε σε βάθος, επίσημα και υπεύθυνα, για τους κινδύνους του διαδικτύου. Στα χέρια σας κρατάτε ένα επίσημο πληροφοριακό έντυπο από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, το οποίο θα σας βοηθήσει να ενημερωθείτε σε βάθος και υπεύθυνα για τους κινδύνους που διατρέχετε κατά την παραμονή σας στο διαδίκτυο.

Για να μην «τσιμπάμε» τόσο εύκολα...

Ηλεκρονικές συσκευές και διαδίκτυο

Ασφαλής χρήση κινητών συσκευών

iPhone & iPad

1. Συμβουλές ασφαλούς χρήσης προσωπικών iPhone & iPad

Στην παρακάτω ενότητα θα βρείτε μερικές βασικές συμβουλές για την ασφαλή χρήση του iPhone και του iPad που χρησιμοποιούν το λειτουργικό σύστημα iOS 4. Οι οδηγίες δεν αφορούν συσκευές οι οποίες λειτουργούν σε εταιρικό περιβάλλον, αλλά μόνο συσκευές των οποίων τον έλεγχο έχει ο χρήστης. Πληροφορίες σχετικά με εταιρική σύνδεση και με θέματα όπως το VPN μπορείτε να αναζητήσετε στην ιστοσελίδα της Apple
http://www.apple.com/support/iphone/enterprise

2. Ασφάλεια της συσκευής

Πρέπει συνεχώς να προστατεύουμε τη φορητή ηλεκτρονική συσκευή από τυχόν επιτήδειους που θα θελήσουν να προσθέσουν κάποιο ύποπτο λογισμικό ή απλώς να διαβάσουν προσωπικά στοιχεία μας. Υπάρχουν αρκετοί τρόποι με τους οποίους κάποιος μπορεί να παρακάμψει τους μηχανισμούς ασφαλείας μιας συσκευής, έχοντας αποκτήσει πρόσβαση σ' αυτήν. Ιδιαίτερα για τα κινητά τηλέφωνα είναι αυξημένος ο κίνδυνος να αποκτήσει κάποιος πρόσβαση σ' αυτά. Ο καλύτερος τρόπος προφύλαξης είναι να εξασφαλίσουμε ότι οι συσκευές μας με λειτουργικό iOS δεν θα βρεθούν σε χέρια ανθρώπων που θέλουν να μας βλάψουν. Αν αναλογιστούμε τον ιδιαίτερα υψηλό κίνδυνο να διαρρεύσουν ευαίσθητα δεδομένα που είναι αποθηκευμένα στη συσκευή μας, μπορούμε να αντιληφθούμε πόσο σημαντικό θέμα είναι η προστασία της. Τα δεδομένα που αποθηκεύονται μπορεί να είναι από συνθηματικές λέξεις που χρησιμοποιούνται σε κοινωνικά δίκτυα, μέχρι κωδικοί πιστωτικών καρτών. Αν το κινητό σας τηλέφωνο βρεθεί σε λάθος χέρια, σκεφτείτε σε πόσες πληροφορίες θα μπορεί κάποιος να έχει πρόσβαση!

3. Αναβάθμιση – Ενημέρωση Λογισμικού

Κάθε φορά η αναβάθμιση του κινητού τηλεφώνου θα πρέπει να γίνεται με το πιο πρόσφατο λογισμικό του iOS.
Οι αναβαθμίσεις αυτές θα πρέπει να γίνονται μέσω ενός συνδεδεμένου με το διαδίκτυο προσωπικού υπολογιστή, στον οποίο έχουμε εγκαταστήσει το πρόγραμμα iTunes. Τόσο η ενημέρωση του λογισμικού της κινητής συσκευής όσο και η εγκατάσταση του iTunes αποτελούν αποκλειστική ευθύνη του χρήστη. Προτείνεται να γίνεται ενημέρωση του λογισμικού από ηλεκτρονικό υπολογιστή τον οποίο γνωρίζουμε.

4. Μη χρησιμοποιείτε τεχνικές «Jailbreak»

Ο όρος «Jailbreak» αναφέρεται στη διαδικασία αλλαγής του λειτουργικού συστήματος μιας συσκευής iOS, κατά παράβαση της άδειας χρήσης του τελικού χρήστη. Με τη διαδικασία του «Jailbreak» μειώνεται σημαντικά η ικανότητα της συσκευής να αντιμετωπίσει επιθέσεις, γιατί αναστέλλεται η εφαρμογή των υπογραφών κώδικα, οι οποίες αποτελούν σημαντικό στοιχείο ασφαλείας. Με τη διαδικασία του «Jailbreak» είναι κατά πολύ ευκολότερο να έχει κανείς πρόσβαση σε ένα iPhone ή iPad. Οι περισσότερες δημόσιες επιθέσεις με στόχο συσκευές iOS απαιτούν να έχει γίνει πρώτα «Jailbreak». Μία ακόμα παρεμφερής ανησυχία που εκφράζεται, αφορά την ποιότητα των εργαλείων και των εφαρμογών που προσφέρει η κοινότητα του «Jailbreak». Αυτές οι δωρεάν εφαρμογές κατασκευάζονται με ελάχιστη επίβλεψη και περιορισμένες δοκιμές. Εν

δέχεται να περιλαμβάνουν ιούς ή άλλο κακόβουλο λογισμικό, και μπορεί να προκαλέσουν σοβαρές, ανεπανόρθωτες βλάβες στη συσκευή σας, καταστρέφοντας τα δεδομένα σας.

5. Ενεργοποίηση του Αυτόματου Κλειδώματος και του Κλειδώματος Συνθηματικού

Η ενεργοποίηση του Αυτόματου Κλειδώματος κλειδώνει αυτόματα την οθόνη του κινητού μετά από μια εκ των προτέρων ορισμένη περίοδο αδράνειας του κινητού τηλεφώνου. Θα πρέπει να βεβαιωθούμε ότι το Αυτόματο Κλείδωμα είναι ενεργοποιημένο. Προτεινόμενος χρόνος κλειδώματος του τηλεφώνου είναι τα 3 λεπτά περίπου.

- Πηγαίνουμε στα Settings → General → Auto Lock.
- Ορίζουμε το χρόνο Αυτόματου Κλειδώματος στα 3 λεπτά.

Για να είναι αποτελεσματικό το Αυτόματο Κλείδωμα, θα πρέπει να συνδυάζεται με το Κλείδωμα Συνθηματικού. Με τη χρήση του Αυτόματου Κλειδώματος και του Κλειδώματος Συνθηματικού μπορούμε να έχουμε καλύτερη προστασία. Το συνθηματικό θα πρέπει να έχει 4 ψηφία και θα πρέπει να δίνεται κάθε φορά που κλειδώνει η οθόνη. Για να γίνει αυτό, πρέπει να γίνουν οι παρακάτω ρυθμίσεις:

- Πηγαίνουμε στα Settings → General → Passcode Lock.
- Θέτουμε σε λειτουργία (ON) το «Passcode Lock».
- Ορίζουμε το «Require Passcode» σε Immediately.

Σημείωση: Στην ίδια οθόνη θα πρέπει να τεθεί εκτός λειτουργίας το Simple Passcode, ούτως ώστε να μπορούν να οριστούν συνθηματικά που συνδυάζουν γράμματα και αριθμούς.

Για να έχετε περισσότερη ασφάλεια, ενεργοποιήστε την Αυτόματη Διαγραφή Δεδομένων για να διαγράψετε όλα τα δεδομένα που έχουν δημιουργηθεί από τον χρήστη, μετά από δέκα αποτυχημένες προσπάθειες πρόσβασης με συνθηματικό στη συσκευή.

- Πηγαίνουμε στα Settings → General → Passcode Lock.
- Θέτουμε σε λειτουργία (ON) το «Erase Data».

6. Μη συνδέεστε με ασύρματα δίκτυα που δεν εμπιστεύεστε

Όσο είναι δυνατόν, να αποφεύγετε ή να περιορίζετε τη χρήση ασύρματων δικτύων. Όταν δεν τα χρησιμοποιείτε, θα πρέπει να απενεργοποιείτε τη συσκευή για να μην είναι εκτεθειμένη.

- Πηγαίνουμε στα Settings → Wi-Fi.
- Θέτουμε εκτός λειτουργίας (OFF) τα Wi-Fi.

Αντισταθείτε στον πειρασμό να χρησιμοποιήσετε σημεία δωρεάν ασύρματης πρόσβασης στο διαδίκτυο. Τα περισσότερα από αυτά δεν προσφέρουν καμιά προστασία σε δεδομένα που μεταδίδονται ασύρματα, κάτι που σημαίνει ότι οποιοσδήποτε βρίσκεται κοντά μπορεί να τα υποκλέψει. Αν, παρ' όλα αυτά, είναι απολύτως απαραίτητο να χρησιμοποιήσετε ασύρματο δίκτυο, διαλέξτε κάποιο που να το ξέρετε, και φροντίστε τα δεδομένα που ανταλλάσσετε με άλλους να είναι κρυπτογραφημένα. Στη λίστα των διαθέσιμων δικτύων, όσα είναι προστατευμένα συνοδεύονται από το εικονίδιο κλειδαριάς δίπλα στο όνομά τους.

Για να απενεργοποιηθεί η αυτόματη σύνδεση σε ασύρματα δίκτυα, κάνουμε τις παρακάτω ενέργειες:

- Πηγαίνουμε στα Settings → Wi-Fi.
- Θέτουμε την εντολή «Ask to join Networks» στο OFF.

Σημαντική Σημείωση. Ακόμα και αν τεθεί εκτός λειτουργίας η αυτόματη σύνδεση σε ασύρματο δίκτυο, η συσκευή θα συνδεθεί αυτομάτως με δίκτυα τα οποία έχει επισκεφθεί προηγουμένως και τα οποία εξακολουθούν να υπάρχουν στη μνήμη της.

Ένα άλλο μέτρο προστασίας που μπορούμε να πάρουμε, είναι να επιλέξουμε την εντολή «Forget this Network» μετά από κάθε ασύρματη σύνδεση. Αυτό θα μειώσει τις πιθανότητες να συνδεθεί η συσκευή μας με λειτουργικό σύστημα iOS με κάποιο άλλο ασύρματο δίκτυο που έχει το ίδιο όνομα. Είναι σημαντικό να επιλέξουμε αυτή την εκδοχή πριν βγούμε από το βελνεκές του συγκεκριμένου δικτύου. Σε διαφορετική περίπτωση, το δίκτυο δεν θα εμφανίζεται στη λίστα των διαθέσιμων δικτύων και δεν θα είναι δυνατόν να το αφαιρέσουμε.

- Πηγαίνουμε στα Settings → Wi-Fi.
- Επιλέγουμε δίκτυο από τη λίστα.
- Επιλέγουμε την εντολή «Forget this Network».

7. Απενεργοποιήστε το Bluetooth, εκτός αν το χρειάζεστε

Το Bluetooth θα πρέπει να είναι ενεργοποιημένο μόνο όταν μας είναι απολύτως απαραίτητο. Όταν δεν το χρησιμοποιούμε, θα πρέπει να το έχουμε κλειστό, ώστε να μην μπορούν άλλες συσκευές να ανακαλύψουν την iOS συσκευή μας και να προσπαθήσουν να συνδεθούν μαζί της.

- Πηγαίνουμε στα Settings → General → Bluetooth.
- Θέτουμε το «Bluetooth» στο OFF.

8. Απενεργοποιήστε τις Υπηρεσίες Εντοπισμού, εκτός αν τις χρειάζεστε

Οι Υπηρεσίες Εντοπισμού μπορεί να χρησιμοποιηθούν από εφαρμογές στη συσκευή σας με σκοπό να ανακαλύψουν το σημείο στο οποίο είστε. Οι Υπηρεσίες Εντοπισμού θα πρέπει να είναι σε λειτουργία μόνο αν υπάρχει κάποια επείγουσα ανάγκη και οι Εφαρμογές πρέπει να γνωρίζουν πού βρίσκεστε. Διαφορετικά, απενεργοποιήστε τες ή κάντε περιορισμένη χρήση τους. Για να απενεργοποιήσουμε τις Υπηρεσίες Εντοπισμού, κάνουμε τα ακόλουθα:

- Πηγαίνουμε στα Settings (Settings → General σε iPads).
- Θέτουμε το «Location Services» στο OFF.

Οι εφαρμογές που χρησιμοποιούν την υπηρεσία «Location Services» θα ζητήσουν να κάνουν χρήση της την πρώτη φορά που θα τις θέσετε σε λειτουργία. **Σκεφθείτε προσεκτικά αυτά τα αιτήματα και επιτρέψτε τη λειτουργία των Υπηρεσιών Εντοπισμού μόνο όταν αυτό είναι απολύτως απαραίτητο.**

9. Ασφαλής Χρήση του Safari

Η δυνατότητα «Autofill» θα πρέπει να απενεργοποιηθεί στο Safari. Με αυτόν τον τρόπο το Safari δεν θα μπορεί να αποθηκεύει κρίσιμες ενδεχομένως πληροφορίες που υπάρχουν στη συσκευή σας, όπως username και password.

- Πηγαίνουμε στα Settings → Safari.
- Θέτουμε το «Autofill» στο OFF.

Επιπλέον, η τεχνολογία JavaScript μπορεί να απενεργοποιηθεί, προκειμένου να εμποδίσουμε τυχόν κακόβουλο λογισμικό να βλάψει τη συσκευή μας. Ωστόσο, η απενεργοποίηση αυτή ενδέχεται να καταστήσει άχρηστες ορισμένες ιστοσελίδες, επομένως είναι αναγκαίο να εξακαλουθήσει το JavaScript να βρίσκεται σε λειτουργία. Αν θελήσουμε να το απενεργοποιήσουμε:

- Πηγαίνουμε στα Settings → Safari.
- Θέτουμε τα «JavaScripts» στο OFF.

Επιπλέον, τα «cookies» μπορεί να θέσουν σε κίνδυνο προσωπικά δεδομένα και συνήθειες πλοήγησης στο διαδίκτυο. Για να αποτρέψουμε κάτι τέτοιο, τα θέτουμε εκτός λειτουργίας, όταν αυτό είναι δυνατόν, ή ρυθμίζουμε την iOS συσκευή μας ώστε να δέχεται «cookies» μόνο από ιστοσελίδες τις οποίες έχουμε επισκεφθεί.

10. Ασφαλής Χρήση e-mail

Βεβαιωθείτε ότι όλες οι συνδέσεις e-mail που χρησιμοποιείτε είναι κρυπτογραφημένες. Προϋπόθεση για κάτι τέτοιο είναι να μπορεί ο server που χρησιμοποιείτε να κάνει διακίνηση κρυπτογραφημένων δεδομένων: αυτό γίνεται στις περισσότερες περιπτώσεις. Αν δεν κρυπτογραφηθούν, τα μηνύματά σας θα μεταδίδονται ελεύθερα και θα είναι δυνατόν κάποιος να τα υποκλέψει και να τα διαβάσει.

- Πηγαίνουμε στα Settings → Mail, Contacts, Calendars.
- Πηγαίνουμε στο SMTP και επιλέγουμε το όνομα ενός server.
- Θέτουμε την εντολή «Use SSL» στο ON για κάθε λογαριασμό στη λίστα.
- Πηγαίνουμε στο Advanced.
- Θέτουμε την εντολή «Use SSL» στο ON για κάθε λογαριασμό στη λίστα.

Όταν ανοίγουμε το e-mail μέσω του Safari, θα πρέπει να είμαστε βέβαιοι ότι η σελίδα πιστοποίησης (login page) είναι **κρυπτογραφημένη** πριν δώσουμε τα στοιχεία μας. Αν είναι κρυπτογραφημένη, η διεύθυνση της σελίδας ξεκινάει με «https» αντί του «http» και το εικονίδιο μιας κλειδαριάς εμφανίζεται αριστερά από το URL.
Επιπλέον, η επιλογή «Remote Image Loading» θα πρέπει να είναι απενεργοποιημένη από τα e-mail. Με τον τρόπο αυτόν, μπορούμε να προστατεύουμε το σύστημά μας από παραποιημένες κακόβουλες εικόνες. Επίσης, δεν θα επιτρέψει σε όσους θέλουν να βλάψουν το σύστημά μας να συνδέσουν τη διεύθυνσή μας στο δίκτυο με το λογαριασμό e-mail που έχουμε.

- Πηγαίνουμε στα Settings → Mail, Contacts, Calendars.
- Ρυθμίζουμε το «Load Remote Image» σε OFF.

11. Ρύθμιση του iPhone Configuration Utility

Με την έκδοση του iOS 4, κάποιες ρυθμίσεις ασφαλείας, οι οποίες μπορούσαν να τεθούν σε λειτουργία μόνο μέσω του iPhone Configuration Utility, υπάρχουν τώρα στο Settings → General → Restrictions. Στις ρυθμίσεις αυτές περιλαμβάνονται η απενεργοποίηση της κάμερας και ενσωματωμένες iOS εφαρμογές όπως το Safari και το YouTube.

12. Σημαντικές ρυθμίσεις ασφαλείας iPhone & iPad

Άλλες σημαντικές ρυθμίσεις ασφαλείας, όπως κρυπτογραφημένα αντίγραφα ασφαλείας, περισσότερο πολύπλοκα PIN και καθαρισμός δίσκου εξ αποστάσεως, θα βρείτε στο iPhone Configuration Utility, ένα δωρεάν εργαλείο το οποίο σας προσφέρει η Apple απευθείας από την ιστοσελίδα της (http://www.apple.com/support/iphone/enterprise), όπου και θα βρείτε όλες τις σχετικές οδηγίες χρήσεως.

Ασφαλής χρήση του BlackBerry

1. 10 Συμβουλές

1. Μην αποθηκεύετε ή επεξεργάζεστε απόρρητες πληροφορίες σε μια συσκευή BlackBerry.
2. Κλείστε τη συσκευή σας και αφαιρέστε την μπαταρία πριν εισέλθετε σε χώρο υψίστης ασφαλείας.
3. Διατηρήστε το BlackBerry σε απόσταση 3 μέτρων από άλλη συσκευή επεξεργασίας απόρρητων πληροφοριών.
4. Έχετε πάντα εσείς τον έλεγχο της συσκευής σας.
5. Χρησιμοποιήστε συνθηματικό που να συνδυάζει γράμματα και αριθμούς, και να έχει τουλάχιστον 8 χαρακτήρες.
6. Αν πιστεύετε ότι η συσκευή σας έχει αλλοιωθεί από τρίτους, σταματήστε να τη χρησιμοποιείτε.
7. Όταν δεν τη χρησιμοποιείτε, κλειδώστε τη συσκευή σας με το εικονίδιο «Lock Keyboard» που βρίσκεται στην οθόνη της.
8. Μη κατεβάζετε αρχεία ή επισυναπτόμενα αρχεία από το διαδίκτυο, εκτός κι αν είστε βέβαιοι για το περιεχόμενό τους.
9. Μη δίνετε προσωπικά στοιχεία και κωδικούς.
10. Μη συνδέετε το BlackBerry με απόρρητα δίκτυα υπολογιστών.

2. Απόρρητα Δεδομένα

Σε περίπτωση κατά την οποία απόρρητα δεδομένα αποθηκευτούν στη συσκευή ή μεταδοθούν μέσω αυτής, θα πρέπει η συσκευή να καταστραφεί, καθώς η εντολή «Wipe» δεν εξασφαλίζει απόλυτη ασφάλεια.

3. Ταξίδια

Κατά τη διάρκεια τελωνειακών ελέγχων, θα πρέπει να αφαιρούνται η μπαταρία και η κάρτα SIM από τη συσκευή BlackBerry, η οποία καλό θα ήταν να τοποθετηθεί αλλού, λ.χ. σε μια τσάντα.

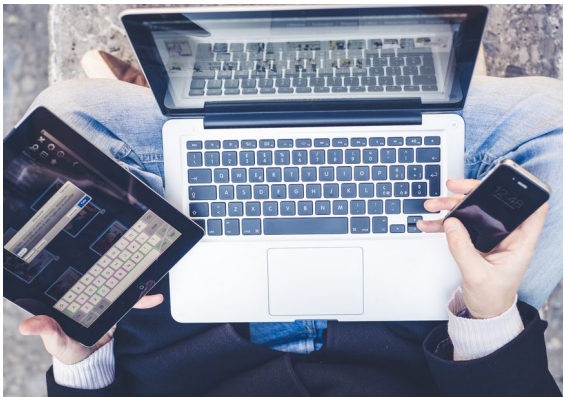
4. Ενεργοποίηση χαρακτηριστικών ασφαλείας

Υπάρχουν διάφοροι τρόποι με τους οποίους εξασφαλίζεται η ασφαλής χρήση του BlackBerry. Μεταξύ άλλων:

- Από την αρχική οθόνη επιλέγουμε «Option» και μετά «Security».
- Το πεδίο «Password» θα πρέπει να είναι ενεργοποιημένο.
- Το πεδίο «Lock Handheld Upon Holstering» θα πρέπει να είναι ρυθμισμένο στο «Yes».
- Από την αρχική οθόνη επιλέγουμε «Option» και μετά «Firewall».
- Το πεδίο «Status» θα πρέπει να είναι ενεργοποιημένο.
- Από την αρχική οθόνη επιλέγουμε το εικονίδιο «Icon», και στη συνέχεια, σκρολάροντας, επιλέγουμε «Options» και, τέλος, «General Options».
- Η επιλογή «Auto Answer» θα πρέπει να ρυθμιστεί σε «Never».

5. Φίλος ή εχθρός;

Η τεχνολογία BlackBerry είναι ένα πολυσύνθετο σύστημα λογισμικού και υλικού που προσφέρει στον χρήστη άπειρες δυνατότητες επικοινωνίας. Σε κάθε συσκευή θα πρέπει να γίνεται προσεκτική χρήση



προκειμένου να προστατεύουμε τα προσωπικά μας δεδομένα. Επιπλέον πληροφορίες μπορείτε να βρείτε στην επίσημη ιστοσελίδα της BlackBerry (us.blackberry.com).

Πηγές

Το παραπάνω κείμενο προέρχεται από φυλλάδιο του Κέντρου Ανάλυσης Συστημάτων και Δικτύων (Systems and Networks Analysis Center) της Υπηρεσίας Εθνικής Ασφαλείας (National Security Agency) των Ηνωμένων Πολιτειών της Αμερικής. Επιπλέον πληροφορίες μπορούμε να βρούμε στην ιστοσελίδα www.nsa.gov/snac

Το συγκεκριμένο φυλλάδιο δεν μπορεί να αντικαταστήσει την πολιτική ασφαλείας που χρησιμοποιείται, αλλά συνεισφέρει στην προστασία των χρηστών.

Κλοπή ταυτότητας

Η κλοπή ταυτότητας είναι σπουδαία υπόθεση. Προσωπικά και οικονομικά δεδομένα που υφαρπάζονται διαδικτυακώς, πωλούνται στην υπόγεια οικονομία και χρησιμοποιούνται για παράνομους σκοπούς από εγκληματικές οργανώσεις σε όλο τον κόσμο. Η προστασία των δεδομένων σας δεν σας γλιτώνει μόνο από τη δυσάρεστη διαδικασία τού να αλλάζετε τους κωδικούς και τις πιστωτικές κάρτες σας, αλλά και βοηθάει στη μάχη ενάντια στο οργανωμένο έγκλημα και την τρομοκρατία.

Τι να αποφεύγετε:

1. Να ανοίγετε συνημμένα αρχεία και συνδέσμους χωρίς να γνωρίζετε την αληθινή τους προέλευση.

Αυτό που μπορεί εκ πρώτης όψεως να μοιάζει με αθώο βίντεο ή εικόνα, ενδέχεται στην πραγματικότητα να είναι κακόβουλο λογισμικό, σχεδιασμένο να υποκλέπτει τα δεδομένα σας. Ακόμα και το να ανοίξετε μόνο ένα spam mail μπορεί να βάλει τη διεύθυνσή σας στη λίστα των spammers για μελλοντικές επιθέσεις.

2. Να δίνετε περισσότερες πληροφορίες από όσες είναι απολύτως απαραίτητες.

Η τράπεζα και ο πάροχος της πιστωτικής σας κάρτας ήδη γνωρίζουν τον κωδικό σας και τη διεύθυνσή σας. Δεν χρειάζεται να τους δώσετε αυτά τα στοιχεία μέσω e-mail, τηλεφώνου ή ιστοσελίδας.

3. Να έχετε πρόσβαση σε διαδικτυακές τραπεζικές υπηρεσίες (online banking) από υπολογιστές με πολλαπλούς χρήστες ή από δημόσια προσβάσιμους υπολογιστές.

Ποτέ δεν ξέρετε τι μπορεί να κρύβεται στον σκληρό τους δίσκο.

4. Να μοιράζεστε κωδικούς, λογαριασμούς ηλεκτρονικού ταχυδρομείου ή άλλα διαδικτυακά προσωπικά δεδομένα με άλλους ανθρώπους.

Είναι πολύ δυσκολότερο να προστατευτείτε όταν περισσότερα από ένα άτομα έχουν πρόσβαση.

5. Να αποθηκεύετε πιστοποιητικά σε φυλλομετρητές (browsers).

Θα αποθηκεύατε ποτέ τον κωδικό σας σ' ένα χαρτάκι Post-it; Το να τον αποθηκεύσετε σ' ένα φυλλομετρητή είναι εξίσου επικίνδυνο.

6. Να παίρνετε οτιδήποτε ως δεδομένο.

Αν μια προσφορά σε ένα e-mail ή σε κάποιο κοινωνικό δίκτυο σας φαίνεται πολύ καλή για να είναι αληθινή, τότε μάλλον δεν είναι. Επίσης, είναι πολύ εύκολο για εγκληματίες να αντιγράψουν τα λογότυπα εταιρειών και την ταυτότητα των αποστολέων.

Τι να κάνετε:

1. Να είστε σε επιφυλακή.

Ν' αντιμετωπίζετε τα αυτόκλητα e-mails ή σελίδες που ζητούν προσωπικές πληροφορίες, με επιφυλακτικότητα, ιδίως εκείνα που ισχυρίζονται ότι είναι από τράπεζες και εταιρείες πιστωτικών καρτών. Μια γρήγορη έρευνα στο διαδίκτυο μπορεί να σας πει αν το e-mail που λάβατε είναι μία από τις γνωστές απάτες. Να θυμάστε ότι πάντα μπορείτε να διασταυρώνετε με την τράπεζά σας ή την εταιρεία πιστωτικών καρτών κατά πόσο το e-mail που λάβατε είναι πράγματι από αυτούς.

2. Να ενημερώνετε (update) συστηματικά το λογισμικό σας.

Πολλές κακόβουλες μολύνσεις προκύπτουν επειδή οι εγκληματίες εκμεταλλεύονται κενά ασφαλείας στο λογισμικό (σε διαδικτυακούς φυλλομετρητές, σε

λειτουργικά συστήματα, σε διάφορα προγράμματα κ.λπ.). Η διαρκής ενημέρωσή τους θα σας βοηθήσει να είστε ασφαλείς.

3. Να χρησιμοποιείτε αντιικό λογισμικό (anti-virus).

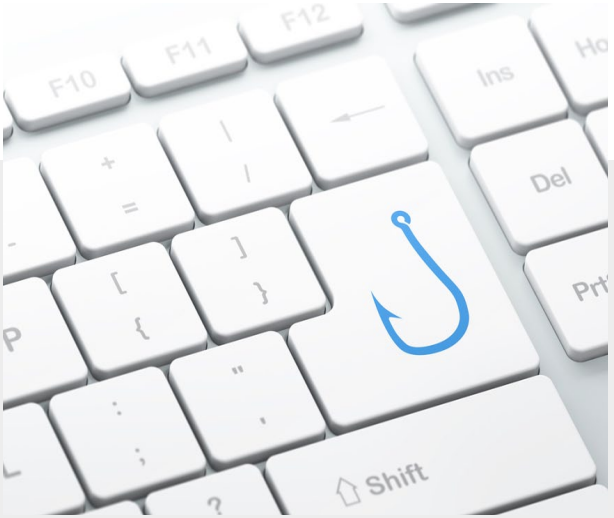
Το αντιικό λογισμικό βοηθάει στο να κρατήσετε τον υπολογιστή σας καθαρό από τα πιο συνήθη κακόβουλα λογισμικά –υπάρχουν, μάλιστα, αρκετές δωρεάν επιλογές. Πάντα να ελέγχετε τα αρχεία που κατεβάζετε, με το αντιικό πρόγραμμά σας. Να μην εγκαθιστάτε προγράμματα ή εφαρμογές στον υπολογιστή σας, αν δεν ξέρετε από πού προέρχονται.

4. Να απαγορεύετε την πρόσβαση στα προσωπικά σας στοιχεία από ιστοσελίδες κοινωνικής δικτύωσης.

Όσο περισσότερες πληροφορίες έχουν οι εγκληματίες, τόσο πιο εύκολα μπορούν να σας στοχοποιήσουν. Περιορίζοντας την ποσότητα πληροφοριών που μοιράζεστε, και τα άτομα με τα οποία τις μοιράζεστε, δυσκολεύετε τη δράση τους.

5. Να χρησιμοποιείτε πάντα ισχυρούς κωδικούς.

Οι υπολογιστές μπορούν να σπάσουν τους πιο συνηθισμένους κωδικούς πολύ γρήγορα. Είναι σημαντικό να σιγουρεύετε ότι οι κωδικοί σας είναι ισχυροί (πάνω από 8 χαρακτήρες, χρησιμοποιώντας ταυτόχρονα αριθμούς, γράμματα και σύμβολα).



6. Να προβαίνετε σε καταγγελίες.

Αν πέσετε θύμα κλοπής ταυτότητας, αναφέρετέ το αμέσως στο αστυνομικό τμήμα της περιοχής σας και στην εταιρεία την οποία αφορά (τράπεζα, διαδικτυακή υπηρεσία κ.λπ.). Οι υπηρεσίες επιβολής του Νόμου συνεργάζονται, τόσο σε ευρωπαϊκό όσο και σε παγκόσμιο επίπεδο, για να εμποδίζουν τις δραστηριότητες όσων ασχολούνται με απάτες ταυτότητας, και να τους φέρνουν ενώπιον της Δικαιοσύνης. Όσο περισσότερες πληροφορίες δίνετε στις Αρχές, τόσο πιο αποτελεσματικά θα στοχοποιούν τις πιο επικίνδυνες εγκληματικές οργανώσεις.

Χρήσιμα Links

Χρήσιμες συμβουλές από τη Δίωξη Ηλεκτρονικού Εγκλήματος:
http://www.astynomia.gr/

Ανοικτή γραμμή για το παράνομο περιεχόμενο στο διαδίκτυο:
http://www.safeline.gr

Ελληνικός κόμβος ασφαλούς διαδικτύου:
www.saferinternet.gr

Οργανισμός προστασίας των δικαιωμάτων των παιδιών:
http://www.hamogelo.gr

Συμβουλές ασφαλείας για online chatting:
http://www.chatdanger.com

Ιστότοπος από την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος:
www.cyberkid.gr

Πανελλήνιο σχολικό δίκτυο:
www.sch.gr

Μονάδα Εφηβικής Υγείας, Β' Παιδιατρική κλινική Πανεπιστημίου Αθηνών, Νοσοκομείο Παίδων:
www.youth-health.gr

Ελληνική Εταιρεία Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο:
www.hasiad.gr

Bold Ogilvy & Mather

ΕΠΙΚΟΙΝΩΝΙΑ

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος - Cyber Crime Division
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11521
e-mail: ccu@cybercrimeunit.gov.gr, Τηλ.: 11188, Fax: 2106476462

Βρείτε μας στα:

www.cyberkid.gr

www.facebook.com/cyberkid.gov.gr

www.cyberalert.gr

www.facebook.com/CyberAlertGR

twitter.com/cyberalertgr