Tech Savvy Seniors

Εισαγωγή στην κυβερνοασφάλεια: Πώς να μείνετε ασφαλής στο διαδίκτυο

Το διαδίκτυο έχει γίνει αναπόσπαστο μέρος της καθημερινής μας ζωής και μπορούμε με αυτό να κάνουμε πολλές διαδικτυακές εργασίες.
θέλουμε να σας ενημερώσουμε για το πώς μπορείτε να χρησιμοποιείται το διαδίκτυο με περισσότερη ασφάλεια και μέτρα προφύλαξης ώστε να προστατεύσουμε τα προσωπικά μας δεδομένα.

1. Είναι απαραίτητο να προστατεύσω τον εαυτό μου στο internet;

Στο διαδίκτυο, οποιοσδήποτε μπορεί να παραποιήσει την ταυτότητά του, οπότε πρέπει να γνωρίζετε από ποιόν πρέπει να δέχεστε μηνύματα ηλεκτρονικού ταχυδρομείου, από πού είναι ασφαλές να ψωνίζετε και σε ποιόν πρέπει να δώσετε τα στοιχεία σας. Το λογισμικό ασφάλειας στο διαδίκτυο διαδραματίζει σημαντικό ρόλο για να σας κρατήσει ασφαλές από το έγκλημα στον κυβερνοχώρο.

Υπάρχουν μερικά απλά βήματα που μπορούμε να ακολουθήσουμε ώστε να αποφύγουμε αυτή την διαδικτυακή απάτη:

- Έχουν οι υπολογιστές σας και τα ασύρματα δίκτυα σας κωδικό προστασίας;
- Ποτέ να μην δίνετε τα προσωπικά σας στοιχεία και λεπτομέρειες σε αγνώστους στο διαδίκτυο.
- Εγκαταστήστε ένα λογισμικό ασφαλείας.

2. Οι απειλές που ενδέχεται να αντιμετωπίσετε:

1. Κακόβουλο λογισμικό

Malware (κακόβουλο λογισμικό): δημιουργείται με σκοπό την πρόσβαση στον υπολογιστή σας και τη συλλογή πληροφοριών, συνήθως με σκοπό την πώληση σε άλλα ενδιαφερόμενα μέλη. Ο πιο κοινός τύπος κακόβουλου λογισμικού είναι ένας ιός.

Πρέπει να είστε προσεκτικοί σχετικά με τα προγράμματα που κάνετε λήψη και εκτελείται στον υπολογιστή σας. Εάν κάνετε λήψη ενός προγράμματος από μια άγνωστη και μη έγκαιρη πηγή, μπορεί να υπάρχει ο κίνδυνος ο υπολογιστής σας να έχει μολυνθεί.

Ακόμα κι αν είστε πολύ προσεκτικοί στην διαδικτυακή σας περιήγηση, δεν μπορείτε να αποφύγετε 100% τα κακόβουλα λογισμικά, διότι αυτό μπορεί να προέλθει από δική μας απροσεξία ή του ότι τα κακόβουλα αυτά λογισμικά ενημερώνονται και εξελίσσονται συνέχεια. Συνεπώς, θα πρέπει να εγκαταστήσετε λογισμικό προστασίας από ιούς στον υπολογιστή σας και να ενεργοποιήσετε την προστασία του, ώστε να έχετε προστασία αμέσως, δηλαδή να γίνεται ο έλεγχος σε πραγματικό χρόνο. Το λογισμικό προστασίας μπορεί να είναι σημαντικό για την ασφάλεια του υπολογιστή επειδή εκτελεί ελέγχους, όχι μόνο στο διαδίκτυο, αλλά εντοπίζει ιούς και στις εξωτερικές συσκευές του υπολογιστή σας, όπως το USB και το CD.

2. Χάκερ (Ηλεκτρονικοί πειρατές)

Hacker (ή bot): είναι άτομα ή άτομο που επιχειρεί να εκμεταλλευτεί την αδυναμία στην ασφάλεια του υπολογιστή σας για να αποκτήσει πρόσβαση στα προσωπικά σας αρχεία.

Για παράδειγμα, γνωρίζετε για την κοινή χρήση αρχείων των Windows; Αυτό που επιτρέπει σε έναν υπολογιστή να στείλει τα έγγραφα σε έναν άλλο υπολογιστή μέσω δικτύου. Εάν ο υπολογιστής σας, δεν προστατεύεται με κωδικό πρόσβασης, ένας χάκερ μπορεί να ανιχνεύσει και στη συνέχεια να το χρησιμοποιήσει, προκειμένου να έχει πρόσβαση στα αρχεία σας ή ακόμα και να σας στείλει έναν ιό ή άλλο είδους κακόβουλου λογισμικού στον υπολογιστή σας.

3. Κλοπή προσωπικών δεδομένων, «ψάρεμα» και απατεώνες

Δεν υπάρχουν κανόνες για την παρουσία σας στο διαδίκτυο, έτσι μερικοί χρήστες προσπαθούν να προσποιηθούν και να σας αποσπάσουν πληροφορίες, με την προυπόθεση ότι δεν ενδιαφέρονται να τους δώσετε χρήματα αλλά τελικά ο σκοπός τους είναι να τους αποκαλύψετε προσωπικές πληροφορίες, όπως αριθμούς πιστωτικών καρτών και ηλεκτρονικών τραπεζικών υπηρεσιών και συνδέσεων. Ουσιαστικά, οι απατεώνες έχουν αναλάβει την επιχειρισιακή τους απάτη μέσω διαδικτύου, και προσπαθούν να επωφεληθούν από εσάς. Μια κοινή απάτη είναι η προσπάθεια ψαρέματος, όπου ο «πειρατής» προσποιείται ότι είναι ένα άτομο ή μια οργάνωση που έχετε κάποια σχέση, και θέλει να πείσει να δώσετε προσωπικά δεδομένα σας όπως πληροφορίες, ή τα στοιχεία του τραπεζικού σας λογαριασμού.

Υπάρχουν κάποιοι απλοί τρόποι για να σας βοηθήσουν να αναγνωρίσετε τα ανεπιθύμητα μηνύματα και τις απάτες ηλεκτρονικού "ψαρέματος" και να αποφύγετε προβλήματα στο διαδίκτυο. Παρακάτω είναι μερικά πράγματα που πρέπει να προσέξετε.

- Ελέγξτε το ηλεκτρονικό σας ταχυδρομείο αλλά και τον αποστολέα. Είναι τα μηνύματα από κάποιον που γνωρίζετε, ή είναι κάτι το οποίο περιγράφει κάτι που σας θυμίζει; Αν όχι, πιθανότατα πρόκειται για ανεπιθύμητη αλληλογραφία (spam).
- Υπάρχει συνήθως και η απάτη, ότι κερδίσατε ένα μεγάλο ποσό χρημάτων με αντάλλαγμα όμως τα προσωπικά σας δεδομένα; Σας πληροφορούν ότι θα έχετε αρνητικές συνέπειες αν δεν απαντήσετε με προσωπικές πληροφορίες ή αν δεν κάνετε κλικ ή αν δεν συνδεθείτε; Επίσης αν δείτε το όνομα σας έτοιμο σε κάποια φόρμα. Όλα αυτά είναι σημάδια μιας απάτης ηλεκτρονικού "ψαρέματος".
- Το ηλεκτρονικό μήνυμα (email) που έχετε λάβει, περιέχει ορθογραφικά και γραμματικά λάθη, ή είναι τελείως λάθος; Είναι το ηλεκτρονικό μήνυμα από ένα "δωρεάν" πάροχο όπως (outlook.com, ή gmail.com); Αν ναι, και αν ο αποστολέας δεν είναι γνωστός σε εσάς, πρέπει να το αντιμετωπίσετε με καχυποψία.

Υπάρχει και η ηλεκτρονική απάτη, που να μας κάνει να ξεγελαστούμε ακόμα και από από την ελκυστικότητα του μηνύματος π.χ μια ωραία εικόνα ή μια παράξενη είδηση, η οποία μπορεί να μοιάζει αληθινή. Εάν μπείτε στον πειρασμό, φροντίστε πολύ απλά να θέσετε στον εαυτό σας την ερώτηση, γιατί θέλετε να λαμβάνετε ένα τέτοιο μήνυμα email, τα οποία είναι συνήθως ιστότοποι που θα σας οδηγήσουν στα χέρια των «πειρατών».

3. Τι λογισμικό ασφαλείας πρέπει να χρησιμοποιήσω;

ΤΥΠΟΙ ΛΟΓΙΣΜΙΚΟΥ ΑΣΦΑΛΕΙΑΣ

Τα καλά νέα είναι ότι μπορείτε να προστατευτείτε από τις περισσότερες επιθέσεις χρησιμοποιώντας ένα λογισμικό ασφαλείας. Ο υπολογιστής σας διαθέτει κάποια ασφάλεια με ενσωματωμένο λογισμικό στο λειτουργικό του σύστημα, αλλά θα πρέπει να προσθέσετε επιπλέον λογισμικό. Υπάρχουν διάφοροι τύποι λογισμικού ασφαλείας που μπορείτε να βάλετε:

1. Το λογισμικό προστασίας από ιούς: Λογισμικό που προστατεύει τον υπολογιστή σας από τους περισσότερους τύπους κακόβουλου λογισμικού (και βασίζεται στην ενσωματωμένη άμυνα του υπολογιστή σας). Μπορείτε να λάβετε λογισμικό προστασίας από ιούς δωρεάν ή με μικρή χρέωση.
2. Διαδικτυακές σουίτες ασφαλείας: Ένα πακέτο λογισμικού που προστατεύει τον υπολογιστή σας από μια σειρά απειλών, όπως κακόβουλο λογισμικό, απατεώνες, ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου, δικτυακούς τόπους, χάκερς και πολλά άλλα. Οι σουίτες ασφαλείας στο διαδίκτυο έχουν ετήσια χρέωση (συνήθως μεταξύ $ 60 και $ 130).

ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΥΠΟΛΟΓΙΣΤΗ ΣΑΣ

1. Ένα τείχος προστασίας λειτουργεί ως σημείο ελέγχου ασφαλείας για την κίνηση στο διαδίκτυο - επιτρέπει μόνο εξουσιοδοτημένες και απλές επιλογές.
2. Το λογισμικό εντοπισμού ιών εντοπίζει και καταργεί κάθε κακόβουλο λογισμικό - συμπεριλαμβανομένων των ιών, του spyware και του adware - που έρχονται στον υπολογιστή σας. Ο υπολογιστής σας πιθανότατα δεν συνοδεύεται από λογισμικό προστασίας από ιούς και θα πρέπει να το εγκαταστήσετε.

4. Επιλογή λογισμικού ασφαλείας

Συνιστάται να προστατεύεται οποιαδήποτε συσκευή που συνδέεστε στο διαδίκτυο - τον υπολογιστή σας, το tablet ή το smartphone με λογισμικό προστασίας από ιούς ή καλύτερα, μια σουίτα ασφαλείας στο διαδίκτυο. Εάν δεν μπορείτε να αντέξετε οικονομικά την ετήσια χρέωση, μπορείτε να βάλετε δωρεάν μια εφαρμογή προστασίας από ιούς. Δεν θα προστατεύσει το σύστημά σας όπως ένα λογισμικό ασφαλείας, αλλά θα σας προσφέρει μια βασική προστασίας. Δωρεάν προγράμματα αντιιών έχουν ως εξής:

Microsoft: Www.microsoft.com/securityessentials

AVG: www.avgfree.com.au

Το Avast!: www.avast.com

Comodo: www.antivirus.comodo.com

5. Διατηρώντας τον εαυτό σας ασφαλές (όταν το λογισμικό ασφαλείας δεν είναι αρκετό)

Η εγκατάσταση του λογισμικού ασφαλείας στον υπολογιστή σας είναι ένα μεγάλο και σημαντικό βήμα για την προστασία σας στο διαδίκτυο. Αλλά αυτή η λύση δεν είναι ολοκληρωμένη διότι το λογισμικό ασφαλείας δεν μπορεί να σας προστατεύσει από τους απατεώνες και τους εγκληματίες του κυβερνοχώρου. Πολλά πράγματα που πρέπει να κάνουμε στο διαδίκτυο περιλαμβάνουν έλεγχο των πληροφοριών που είναι σημαντικές, προσωπικές ή ιδιωτικές. Τα προσωπικά σας στοιχεία είναι πληροφορίες που σας ανήκουν και σας χαρακτηρίζουν. Προκειμένου να προστατεύσετε τα προσωπικά σας στοιχεία, θα πρέπει να είστε προσεκτικοί σχετικά με αυτά που μοιράζεστε δημοσίως στο διαδίκτυο.

Η κοινή λογική και η καχυποψία θα μας θωρακίσουν ώστε να κάνουμε την διαδικτυακή απάτη ακόμα πιο δύσκολη!

Υπάρχουν ορισμένα απλά πράγματα που μπορείτε να κάνετε για να είστε ασφαλείς:

1. Χρησιμοποιήστε έναν ισχυρό και μοναδικό κωδικό πρόσβασης/φράση, και να τον αλλάζετε τακτικά
2. Μην δημοσιεύετε προσωπικές πληροφορίες σε δημόσιους ιστότοπους
3. Μην ανοίγετε συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου εκτός αν είστε πραγματικά σίγουροι
4. Να είστε προσεκτικοί σχετικά με τα μηνύματα ηλεκτρονικού ταχυδρομείου στα οποία ανταποκρίνεστε
5. Να είστε προσεκτικοί με αυτούς που ζητούν και δίνετε τα στοιχεία της πιστωτικής η χρεωστική σας κάρτας
6. Μην εγκαταστήσετε προγράμματα από αναξιόπιστες πηγές