ΕΡΓΟ ΨΗΦΙΑΚΗΣ ΠΡΟΣΒΑΣΗΣ

ΕΝΟΤΗΤΑ

Ενδιάμεση γνώση σχετικά με την ασφάλεια στο διαδίκτυο

Κωδικός: M3IC

Προετοιμαστήκαν από: Δήμος Καρδίτσας

Οκτώβριος 2018

Το πρόγραμμα χρηματοδοτείτε με την υποστήριξη της Ευρωπαϊκής Επιτροπής.

Περιεχόμενα

ΩΡΕΣ ΜΑΘΗΣΗΣ: [ΟΛΕΣ ΤΙΣ ΩΡΕΣ ΕΚΠΑΙΔΕΥΣΗΣ]

ΦΟΡΤΟ ΕΡΓΑΣΙΑΣ: [ΟΛΕΣ ΤΙΣ ΩΡΕΣ ΕΚΠΑΙΔΕΥΣΗΣ + ΣΥΝΟΛΙΚΟ ΧΡΟΝΟ ΓΙΑ ΑΣΚΗΣΕΙΣ]

ΠΕΡΙΛΗΨΗ

Η ενότητα δημιουργήθηκε για να επεκτείνει τις βασικές γνώσεις του χρήστη σχετικά με την ασφάλεια στο διαδίκτυο, οι οποίες χρησιμοποιούνται για την εκμετάλλευση του αρχαρίου χρήστη του διαδικτύου. Οι πρωταρχικοί στόχοι είναι να ενδυναμώσει τον χρήστη, να τον προστατεύσει από τους εγκληματίες στον κυβερνοχώρο και να διατηρήσει την ασφάλεια των προσωπικών δεδομένων του χωρίς να θέσει σε κίνδυνο τα ηλεκτρονικά δεδομένα και τα περιουσιακά του στοιχεία.

ΛΕΞΕΙΣ - ΚΛΕΙΔΙΑ

Οικιακό ασύρματο δίκτυο, πρόγραμμα προστασίας από ιούς, ιός, κακόβουλο πρόγραμμα, πρόγραμμα προστασίας από προϊόντα υποκλοπής, λογισμικό υποκλοπής (spyware)

ΣΤΟΧΟΙ

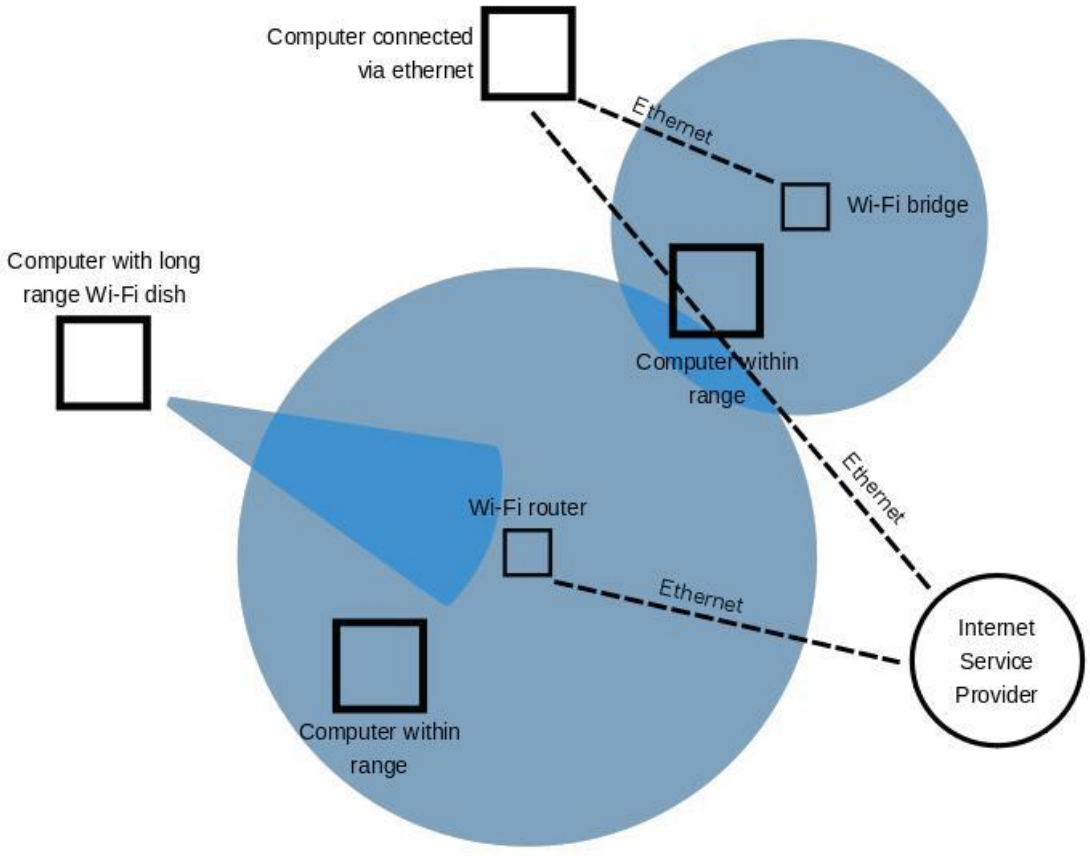
Ενέργειες / Επιτεύγματα		
Κατανόηση των εγκληματικών δραστηριοτήτων που βασίζονται στο διαδίκτυο με στόχο τα άτομα και την απόκτηση δεξιοτήτων για τον εντοπισμό και την αποφυγή αυτών των δραστηριοτήτων.		
Γνώσεις	**Δεξιότητες**	**Αρμοδιότητες**
Ασφάλεια στο διαδίκτυο	Κατανόηση του ασύρματου οικιακού δικτύου Γνώση για το πως να κάνετε τις σχετικές ρυθμίσεις Γνώση για την ασφάλειά σας	Να είστε σε θέση να ρυθμίσετε και να διαχειριστείτε την ασφάλεια του ασύρματου οικιακού σας δικτύου
Αντιικά προγράμματα	Κατανόηση των ιών και της αναγκαιότητας για την χρήση αντιικών προγραμμάτων Να είστε σε θέση να επιλέγετε το κατάλληλο αντιικό πρόγραμμα Γνώση για το πως να αποφεύγετε τους ιούς στον υπολογιστή σας	Γνώση για το πως να προστατεύεται τον υπολογιστή σας απέναντι στους ιούς

Κακόβουλο λογισμικό (Malware)	Κατανόηση των κακόβουλων λογισμικών και της αναγκαιότητας για την χρήση προγραμμάτων που προστατεύουν από κακόβουλα λογισμικά Να είστε σε θέση να επιλέγετε το κατάλληλο πρόγραμμα καταπολέμησης κακόβουλων λογισμικών Γνώση για το πως να αποφεύγεται τα κακόβουλα λογισμικά στον υπολογιστή σας	Γνώση για το πως να προστατεύεται τον υπολογιστή σας απέναντι στα κακόβουλα λογισμικά

Ενότητα 1: Διασφάλιση σύνδεσης στο Διαδίκτυο

Οικιακό ασύρματο δίκτυο

Με απλά λόγια, ένα βασικό οικιακό ασύρματο δίκτυο υπάρχει όταν συνδέσετε ένα σημείο πρόσβασης στο διαδίκτυο (Internet), όπως ένα καλώδιο από τον πάροχο υπηρεσιών διαδικτύου (Internet), σε έναν (ασύρματο) δρομολογητή, για να επιτρέψετε σε πολλές συσκευές να συνδεθούν πολύ γρήγορα στο δίκτυο. Σε πολλές περιπτώσεις, μόλις εγκατασταθεί ένας ασύρματος δρομολογητής, θα βρούμε ένα μέρος στο σπίτι μας για αυτό και θα το ξεχάσουμε. Από την στιγμή που όλες οι συσκευές μας έχουν εγκατασταθεί και συνδεθεί μέσω του δικτύου Wi-Fi, η διαδικασία έχει ολοκληρωθεί, έτσι; Λάθος!



Πιθανώς πολλοί από εσάς δεν το συνειδητοποιούν, αλλά ο δρομολογητής διαδικτύου είναι μία από τις πιο σημαντικές συσκευές στο σπίτι μας. Είναι η πύλη για την πρόσβαση στο διαδίκτυο και επίσης είναι επιρρεπής σε εκμεταλλεύσεις από κυβερνο-εγκληματίες που μπορούν να εισχωρήσουν στις συσκευές σας και να αποκτήσουν πρόσβαση στο σύστημά σας.

Το μόνο μέτρο που χρησιμοποιούν τα περισσότερα άτομα για να προστατεύσουν το οικιακό τους δίκτυο είναι να δημιουργήσουν έναν κωδικό πρόσβασης και να εμποδίσουν τους γείτονες και άλλα άτομα να αναλάβουν τον έλεγχο των δεδομένων σας. Αλλά πρέπει να είμαστε περισσότερο σοβαροί με την ασφάλεια και δεν επαρκεί απλώς ένας κωδικός πρόσβασης. Ένας σοβαρός κίνδυνος είναι ότι ένας εγκληματίας σε απευθείας σύνδεση μπορεί να εκμεταλλευτεί τα φτωχά μέτρα ασφάλειάς σας στο Wi-fi και να "ακούσει" την κυκλοφορία σας για να ανακτήσει ευαίσθητες πληροφορίες ή να εκμεταλλευτεί το δίκτυό σας για να ξεκινήσει κακόβουλες επιθέσεις όπως οι επιθέσεις Man-in-the-Middle, η θωράκιση δικτύου ή η κλοπή δεδομένων.

Παρόλο που είναι σχετικά εύκολα στη χρήση και στη πρόσβαση, τα δίκτυα Wi-Fi δεν είναι πάντα ασφαλείς δίκτυα. Το Wi-Fi έχει πολλά προβλήματα ασφάλειας και αξίζει να θυμίσουμε το Krack που εντοπίστηκε στο πρωτόκολλο Wireless Protected Access II (WPA2) που επηρέασε όλες τις συσκευές που συνδέονται μέσω Wi-fi.

Για το λόγο αυτό, η μάθηση για το πώς να ασφαλίσετε το ασύρματο οικιακό σας δίκτυο κατά των εγκληματιών στον κυβερνοχώρο είναι μια σοφή και έξυπνη κίνηση. Δεδομένου του αριθμού των συσκευών διαδικτύου που μπορείτε να διαθέτετε, βεβαιωθείτε ότι το δίκτυό σας είναι ασφαλές, παρά του ότι κάποιες φορές η φροντίδα του κυβερνοχώρου σας μπορεί να είναι μια κουραστική διαδικασία.

Σε αυτό το μάθημα, θα μάθετε πώς μπορείτε να εξασφαλίσετε καλύτερα το οικιακό σας δίκτυο και να μειώσετε τις πιθανότητες να υπονομεύουν τα πολύτιμα δεδομένα σας.

Βήμα 1. Αλλάξτε το όνομα του προεπιλεγμένου οικείου δικτύου σας

Αν θέλετε να ασφαλίσετε καλύτερα το οικιακό σας δίκτυο, το πρώτο πράγμα που πρέπει να κάνετε είναι να αλλάξετε το όνομα του δικτύου Wi-Fi, γνωστό και ως SSID (Service Set Identifier).

Αν και το να δίνετε στο Wi-Fi σας ένα προκλητικό όνομα όπως το "Δεν μπορείς να το χάκαρεις" μπορεί να σας γυρίσει μπούμερανγκ κατά καιρούς, άλλα ονόματα όπως "αυτό δεν είναι wifi" ή "πολύ γρήγορο για wifi" είναι απολύτως αποδεκτά.

Η αλλαγή του προεπιλεγμένου ονόματος του Wi-Fi καθιστά πιο δύσκολο για τους εγκληματίες του κυβερνοχώρου να μάθουν τι είδους δρομολογητή έχετε. Εάν ένας κυβερνο-εγκληματίας γνωρίζει το όνομα του κατασκευαστή του δρομολογητή σας, θα γνωρίζει τι τρωτά σημεία έχει το μοντέλο και στη συνέχεια θα προσπαθήσει να τα εκμεταλλευτεί.

Σας συνιστούμε να μην ονομάσετε το οικιακό σας δίκτυο κάτι σαν το "John's Wi-Fi". Δεν θέλετε να γνωρίζουν με την πρώτη ματιά ποιο ασύρματο δίκτυο είναι δικός σας όταν υπάρχουν πιθανώς τρία ή τέσσερα άλλα γειτονικά Wi-Fi.

Επίσης, να θυμάστε ότι η αποκάλυψη πάρα πολύ προσωπικών δεδομένων σχετικά με ένα όνομα ασύρματου δικτύου, μπορεί να σας κάνει περισσότερο ευάλωτους για κλοπές από τους εγκληματίες του κυβερνοχώρου.

Ακολουθεί ένας βήμα προς βήμα απλός οδηγός που εξηγεί πώς μπορείτε εύκολα να αλλάξετε το όνομα του ασύρματου δικτύου σας.

Βήμα 2. Βεβαιωθείτε ότι έχετε ορίσει έναν ισχυρό και μοναδικό κωδικό πρόσβασης για να ασφαλίσετε το ασύρματο δίκτυό σας

Πιθανότατα γνωρίζετε ότι κάθε ασύρματος δρομολογητής έρχεται προκαθορισμένος με προεπιλεγμένο όνομα χρήστη και κωδικό πρόσβασης, ο οποίος είναι απαραίτητος για την εγκατάσταση και τη σύνδεση του δρομολογητή σας. Το χειρότερο κομμάτι είναι ότι μπορούν εύκολα οι χακερς (hackers) να το μαντέψουν, ειδικά αν γνωρίζουν τον κατασκευαστή.

Για αυτό βεβαιωθείτε ότι έχετε αλλάξει και τα δύο.

Ένας καλός κωδικός πρόσβασης ασύρματου δικτύου πρέπει να έχει μήκος τουλάχιστον 20 χαρακτήρων και να περιλαμβάνει αριθμούς, γράμματα και διάφορα σύμβολα.

Χρησιμοποιήστε αυτόν τον οδηγό για να ρυθμίσετε έναν ισχυρό κωδικό πρόσβασης για το δίκτυό σας. Οι φίλοι που έρχονται για μια επίσκεψη μπορούν να διαμαρτυρηθούν για το ασυνήθιστο μήκος του κωδικού πρόσβασης, αλλά αυτό μπορεί να τους αποθαρρύνει από την άσκοπη κατανάλωση των δεδομένων σας με βαρετές δημοσιεύσεις στο Facebook ή στο Instagram.

Βήμα 3. Αυξήστε την ασφάλεια του ασύρματου διχτυού (Wi-Fi) ενεργοποιώντας την κρυπτογράφηση δικτύου

Τα ασύρματα δίκτυα διαθέτουν πολλές γλώσσες κρυπτογράφησης, όπως WEP, WPA ή WPA2.

Για την καλύτερη κατανόηση αυτής της ορολογίας, το WPA2 σημαίνει Wi-Fi Protected Access 2, αποτελεί πρωτόκολλο ασφαλείας, είναι το τρέχον πρότυπο στη βιομηχανία και κρυπτογραφούν την κυκλοφορία σε δίκτυα Wi-Fi. Αντικαθιστά επίσης το παλαιότερο και λιγότερο ασφαλές WEP (Wired Equivalent Privacy) ενώ αποτελεί αναβάθμιση της αρχικής τεχνολογίας WPA (Wi-Fi Protected Access). Από το 2006, όλα τα προϊόντα που έχουν πιστοποιηθεί με Wi-Fi πρέπει να χρησιμοποιούν ασφάλεια WPA2.

Το WPA2 AES είναι επίσης ένα τυποποιημένο σύστημα ασφαλείας, έτσι όλα τα ασύρματα δίκτυα είναι συμβατά με αυτό. Εάν θέλετε να ενεργοποιήσετε την κρυπτογράφηση WPA2

στον ασύρματο δρομολογητή σας, χρησιμοποιήστε αυτά τα έξι βήματα. Αν χρησιμοποιείτε ασύρματο δρομολογητή TP-Link, μπορείτε να ασφαλίσετε το ασύρματο δίκτυό σας.

Τα καλά νέα είναι ότι το WPA3 είναι ήδη εδώ και θα αντικαταστήσει το WPA2. Η Wi-Fi Alliance ανακοίνωσε πρόσφατα το πρότυπο ασφάλειας ασύρματου δικτύου της επόμενης γενιάς, το οποίο στοχεύει στην επίλυση ενός κοινού προβλήματος ασφάλειας: ανοιχτά δίκτυα Wi-Fi. Πέρα από αυτό, έρχεται με βελτιώσεις ασφαλείας και περιλαμβάνει μια σειρά χαρακτηριστικών για την απλοποίηση των ρυθμίσεων ασφαλείας Wi-Fi για χρήστες και παρόχους υπηρεσιών.

Βήμα 4. Απενεργοποιήστε το ασύρματο οικιακό δίκτυο όταν δεν είστε στο σπίτι

Για να ασφαλίσετε το δίκτυό σας, σας συνιστούμε να απενεργοποιήσετε το ασύρματο οικιακό δίκτυο σε περίπτωση εκτεταμένων περιόδων μη χρήσης. Θα πρέπει να κάνετε το ίδιο πράγμα με όλες τις συσκευές σας που χρησιμοποιούν καλώδια Ethernet ή όταν δεν θα είστε στο σπίτι. Με αυτόν τον τρόπο, κλείνετε οποιαδήποτε παράθυρα ευκαιριών μπορούν να χρησιμοποιήσουν οι κακόβουλοι χάκερς.

Εδώ είναι μερικά πλεονεκτήματα από την απενεργοποίηση του ασύρματου δικτύου σας:

Αιτίες ασφάλειας - Απενεργοποιώντας τις συσκευές δικτύου, ελαχιστοποιείτε τις πιθανότητες να γίνετε στόχος για τους χάκερς.

Προστασία από υπέρταση - Όταν απενεργοποιείτε τη συσκευή δικτύου, μειώνετε επίσης την πιθανότητα να υποστεί βλάβη από ηλεκτρικές τάσεις.

Μείωση θορύβου - Αν και τα σύγχρονα οικιακά δίκτυα είναι πολύ πιο αθόρυβα τα τελευταία χρόνια, η απενεργοποίηση του ασύρματου οικιακού σας δικτύου μπορεί να προσθέσει ηρεμία στο σπίτι σας.

Βήμα 5. Πού βρίσκεται ο δρομολογητής στο σπίτι σας;

Πιθανότατα δεν έχετε σκεφτεί αυτό, αλλά το που είναι η θέση του Wi-Fi στο σπίτι σας μπορεί επίσης να έχει αντίκτυπο στην ασφάλειά σας.

Τοποθετήστε τον ασύρματο δρομολογητή όσο το δυνατόν πιο κοντά στο μέσο του σπιτιού σας. Γιατί; Πρώτα απ 'όλα, θα παρέχει ισότιμη πρόσβαση στο διαδίκτυο σε όλα τα δωμάτια του σπιτιού σας. Δεύτερον, το ασύρματο δίκτυο δεν θα φτάνει πολύ μακριά από το σπίτι σας, όπου θα μπορούσε εύκολα να παρεμποδιστεί από κακόβουλα άτομα.

Για το λόγο αυτό, συνιστούμε να μην τοποθετήσετε τον ασύρματο δρομολογητή σας κοντά σε ένα παράθυρο. Δεν υπάρχει τίποτα που να εμποδίζει το σήμα που βρίσκεται εκτός του σπιτιού σας.

Βήμα 6. Χρησιμοποιήστε έναν ισχυρό κωδικό πρόσβασης διαχειριστή δικτύου για να αυξήσετε την ασφάλεια Wi-Fi.

Για να ρυθμίσετε τον ασύρματο δρομολογητή σας, πρέπει να έχετε πρόσβαση σε μια ηλεκτρονική πλατφόρμα ή ιστότοπο, όπου μπορείτε να κάνετε πολλές αλλαγές στις ρυθμίσεις δικτύου.

Οι περισσότεροι δρομολογητές Wi-Fi έρχονται με προεπιλεγμένα διαπιστευτήρια, όπως "admin" και "password", τα οποία είναι τόσο εύκολο για να εισέλθουν σε κακόβουλους χάκερ.

Γνωρίζατε ότι ο αριθμός των ασύρματων δικτύων έχει αυξηθεί δραματικά τα τελευταία 8 χρόνια; Το 2010 υπήρχαν 20 εκατομμύρια δίκτυα Wi-Fi ανά τον κόσμο και μέσα σε 8 χρόνια ο αριθμός αυτός αυξήθηκε σε 400 εκατομμύρια.

Βήμα 7. Αλλάξτε την προεπιλεγμένη διεύθυνση IP στον ασύρματο δρομολογητή

Η αλλαγή της προεπιλεγμένης διεύθυνσης IP σε μια λιγότερο συνηθισμένη είναι ένα άλλο πράγμα που πρέπει να σκεφτείτε για να διασφαλίσετε καλύτερα το οικιακό σας δίκτυο και να κάνετε πιο δύσκολη την παρακολούθηση από τους χάκερ.

Για να αλλάξετε τη διεύθυνση IP ενός δρομολογητή, ακολουθήστε τα εξής βήματα:

1. Συνδεθείτε στην κονσόλα του δρομολογητή σας ως διαχειριστής. Αυτά τα βασικά βήματα θα σας διδάξουν πώς μπορείτε εύκολα να συνδεθείτε στο οικιακό σας δίκτυο ως διαχειριστής. Συνήθως, ο τύπος γραμμής διευθύνσεων μοιάζει με http://192.168.1.1 ή http://192.168.0.1
2. Μόλις είστε εκεί, εισαγάγετε το όνομα χρήστη και τον κωδικό πρόσβασης στη σελίδα σύνδεσης.
3. Στη συνέχεια, επιλέξτε «Δίκτυο LAN» που βρίσκεται στο μενού της αριστερής πλευράς.
4. Αλλάξτε τη διεύθυνση IP σε προτίμηση και, στη συνέχεια, κάντε κλικ στην επιλογή «Αποθήκευση».

Σημείωση: Αφού αλλάξετε τη διεύθυνση IP, θα πρέπει να πληκτρολογήσετε τη νέα διεύθυνση IP στη γραμμή περιήγησης στο Web.

Μπορείτε επίσης να αλλάξετε το διακομιστή DNS που χρησιμοποιεί ο ασύρματος δρομολογητής σας για να φιλτράρει την κίνηση στο διαδίκτυο και αυτό το μάθημα θα σας δείξει πώς να το κάνετε.

Βήμα 8. Απενεργοποιήστε τη λειτουργία DHCP στο δρομολογητή

Για να ενισχύσετε την ασφάλεια του ασύρματου δικτύου, θα πρέπει να απενεργοποιήσετε το διακομιστή DHCP (Dynamic Host Configuration Protocol) στον δρομολογητή σας, πράγμα

που αντιστοιχεί στις διευθύνσεις IP σε κάθε συσκευή σε ένα δίκτυο. Αντ 'αυτού, θα πρέπει να χρησιμοποιήσετε μια στατική διεύθυνση και να εισαγάγετε τις ρυθμίσεις δικτύου.

Αυτό σημαίνει ότι πρέπει να μπείτε στη συσκευή σας και να την ορίσετε μια διεύθυνση IP κατάλληλη για το δρομολογητή σας.

Βήμα 9. Απενεργοποίηση απομακρυσμένης πρόσβασης

Οι περισσότεροι δρομολογητές επιτρέπουν να έχετε πρόσβαση στη διασύνδεσή τους μόνο από μια συνδεδεμένη συσκευή. Ωστόσο, ορισμένοι από αυτούς επιτρέπουν την πρόσβαση ακόμη και από απομακρυσμένα συστήματα.

Αφού απενεργοποιήσετε την απομακρυσμένη πρόσβαση, οι κακόβουλοι χάκερ δεν θα έχουν πρόσβαση στις ρυθμίσεις απορρήτου του δρομολογητή σας από συσκευή που δεν είναι συνδεδεμένη στο ασύρματο δίκτυό σας.

Για να πραγματοποιήσετε αυτήν την αλλαγή, μεταβείτε στη διαδικτυακή διασύνδεση και αναζητήστε "Απομακρυσμένη πρόσβαση" ή "Απομακρυσμένη διαχείριση".

Βήμα 10. Διατηρείτε πάντα το λογισμικό του δρομολογητή σας ενημερωμένο

Το λογισμικό αποτελεί ουσιαστικό μέρος της ασφάλειας του ασύρματου δικτύου σας. Το υλικό λογισμικό του ασύρματου δρομολογητή, όπως και κάθε άλλο λογισμικό, περιέχει ελαττώματα τα οποία μπορούν να γίνουν σημαντικά τρωτά σημεία και να τα εκμεταλλευτούν οι χάκερς.

Δυστυχώς, πολλοί ασύρματοι δρομολογητές δεν έρχονται με την επιλογή να ενημερώνουν αυτόματα το λογισμικό τους, οπότε πρέπει να περάσετε να το κάνετε εσείς.

Ακόμα και για τα δίκτυα Wi-Fi που μπορούν να ενημερώνονται αυτόματα, εξακολουθεί να απαιτείται να ενεργοποιήσετε αυτήν τη ρύθμιση. Όμως, σας υπενθυμίζουμε τη σημασία της εγκατάστασης του λογισμικού και πώς η παραμέληση μπορεί να αφήσει ανοιχτές πόρτες για τους κυβερνο-εγκληματίες να εκμεταλλευτούν διάφορες αδυναμίες. Διαβάστε τι έχουν να που οι εμπειρογνώμονες ασφαλείας σχετικά με την ενημέρωση του λογισμικού σας και γιατί είναι το κλειδί για την ασφάλεια στο διαδίκτυο.

Βήμα 11. Ένα τείχος προστασίας μπορεί να βοηθήσει στη διασφάλιση του δικτύου Wi-Fi

Τα τείχη προστασίας (firewalls) είναι προγράμματα λογισμικού που χρησιμοποιούνται στον υπολογιστή σας και υπάρχουν πολλές επιλογές.

Ένα τείχος προστασίας έχει σχεδόν το ίδιο αποτέλεσμα με ένα λογισμικό, αλλά το μεγαλύτερο πλεονέκτημά του είναι ότι προσθέτει ένα επιπλέον επίπεδο ασφάλειας.

Το καλύτερο μέρος για τα τείχη προστασίας είναι ότι οι περισσότεροι από τους καλύτερους ασύρματους δρομολογητές διαθέτουν ενσωματωμένο τείχος προστασίας που θα προστατεύει το δίκτυό σας από πιθανές επιθέσεις στον κυβερνοχώρο. Αυτό το μάθημα μπορεί να σας βοηθήσει να καταλάβετε εάν ο δρομολογητής έχει ενσωματωμένο τείχος προστασίας και πώς μπορείτε να τον ενεργοποιήσετε. Προτείνουμε να το ενεργοποιήσετε εάν δεν είναι από προεπιλογή ως πρόσθετο επίπεδο προστασίας.

Εάν ο δρομολογητής σας δεν το διαθέτει, μπορείτε να εγκαταστήσετε ένα καλό τοίχος προστασίας στο δρομολογητή σας, προκειμένου να προστατεύσετε το σύστημά σας από κακόβουλες προσπάθειες hacking εναντίον του οικείου δικτύου σας.

Βήμα 12. Βελτιώστε την προστασία των συσκευών που συνδέονται πιο συχνά με το οικιακό σας δίκτυο.

Σημαντικό: Μην αφήνετε εκτεθειμένα τρωτά σημεία για τους διαδικτυακούς εγκληματίες!

Αν και έχετε αυξημένη προστασία για το δρομολογητή και το οικιακό σας δίκτυο, πρέπει να βεβαιωθείτε ότι δεν έχετε κενά που μπορούν να εκμεταλλευτούν οι εγκληματίες στο διαδίκτυο.

Σας προτείνουμε να κάνετε τα παρακάτω:

1. Να θυμάστε πάντα να διατηρείτε τις συσκευές σας ενημερωμένες με το πιο πρόσφατο διαθέσιμο λογισμικό.
2. Να εφαρμόζετε πάντα τις πιο πρόσφατες ενημερωμένες εκδόσεις ασφαλείας για να διασφαλίσετε ότι δεν υπάρχει ανοιχτή οπή ασφαλείας σε κακόβουλους χάκερς.
3. Ελέγξτε ποιες συσκευές συνδέονται πιο συχνά με το οικιακό σας δίκτυο και βεβαιωθείτε ότι τους έχετε εγκαταστήσει λογισμικό προστασίας από ιούς και / ή λογισμικό προστασίας από κακόβουλο λογισμικό. Αν δεν γνωρίζετε ποια θα πρέπει να επιλέξετε, αυτός ο οδηγός θα είναι πολύ χρήσιμος.
4. Βεβαιωθείτε ότι προστατεύετε τις συσκευές σας χρησιμοποιώντας πολλαπλά επίπεδα ασφαλείας που αποτελούνται από εξειδικευμένο λογισμικό ασφαλείας, όπως ενημερωμένα προγράμματα προστασίας από ιούς και λογισμικό φιλτραρίσματος κυκλοφορίας. Μπορεί να εξετάσετε τη χρήση ενός προγράμματος λογισμικού κατά του λογισμικού αντιμετώπισης προβλημάτων.

Συμπέρασμα

Η διασφάλιση του οικιακού δικτύου θα πρέπει να αποτελεί κορυφαία προτεραιότητα για καθέναν από μας που ενδιαφέρεται να διατηρήσει τα δεδομένα του ασφαλή. Αυτά τα βήματα μπορούν να είναι πραγματικά χρήσιμα ακόμη και για άτομα που δεν γνωρίζουν από τεχνολογία να υποβάλουν αίτηση.

Επίσης, μην ξεχνάτε ότι η ασφάλεια ασύρματου δικτύου σας μπορεί να είναι μερικές φορές αδύναμη και επιρρεπής σε εκμεταλλεύσεις. Σχεδόν δεν έχει σημασία πόσο ισχυρός είναι ο κωδικός πρόσβασής σας ή αν το λογισμικό σας είναι ενημερωμένο αν οι κυβερνο-εγκληματίες μπορούν απλώς να καταλάβουν τα δεδομένα Wi-Fi.

Ενότητα 2: Προγράμματα προστασίας από ιούς.

Στόχοι για την ενότητα 2

Τα περισσότερα συστήματα χρειάζονται λογισμικό προστασίας από ιούς. Εδώ παρουσιάζεται το τι να επιλέξετε, πώς να το εγκαταστήσετε και το πώς να το χρησιμοποιήσετε για να είστε «ασφαλείς».

Ιοί

Είναι κάτι που όλοι ελπίζουμε να αποφύγουμε, αλλά η αλήθεια του θέματος είναι ότι δεν μπορούμε να τους αποφεύγουμε πάντα. Κάποιοι ενδεχομένως να έχετε πληγεί από ιούς. Οι ακόλουθοι κανόνες σας βοηθούν να ελαχιστοποιήσετε τους κινδύνους.

Εγκαταστήστε ένα πρόγραμμα προστασίας από ιούς

Είτε συνδέεστε στο διαδίκτυο είτε όχι, η αξιόπιστη προστασία είναι απαραίτητη. Τα προγράμματα προστασίας από ιούς είναι μια ελάχιστη επένδυση και αξίζουν τα χρήματα, καθώς με το που θα ανοίγεται τον υπολογιστή σας θα είστε βέβαιοι ότι είστε προστατευμένοι! Σε αυτό το μάθημα μπορείτε να βρείτε σύνδεσμο με σχόλια για λογισμικό προστασίας από ιούς. Μπορείτε να επιλέξετε από τις δωρεάν και πληρωμένες προσφορές, να επιλέξετε το κατάλληλο για εσάς και να το εγκαταστήσετε εύκολα από διαδίκτυο.

Αποφύγετε ύποπτες ιστοσελίδες

Πολλές φορές τα προγράμματα περιήγησις στο διαδίκτυο θα σας ειδοποιήσουν αν πρόκειται να εισέλθετε σε έναν ιστότοπο που επιχειρεί να εγκαταστήσει ή να εκτελέσει ένα πρόγραμμα στον υπολογιστή σας, αλλά όχι πάντα. Αποφύγετε ιστοσελίδες όπως αυτές.

Ποτέ μην ανοίγετε συνημμένα ηλεκτρονικού ταχυδρομείου χωρίς να τα σαρώσετε στο πρόγραμμα προστασίας από ιούς

Ο πιο συνηθισμένος τρόπος διάδοσης των ιών παραμένει να είναι μέσω ηλεκτρονικού ταχυδρομείου. Βεβαιωθείτε ότι χρησιμοποιείτε πάροχο ηλεκτρονικού ταχυδρομείου που απαιτεί τη σάρωση όλων των συνημμένων πριν το άνοιγμα, για να διασφαλίσετε ότι ο υπολογιστής σας δεν θα λάβει ιό.

Ρύθμιση αυτόματων σαρώσεων

Η δημιουργία σαρώσεων για την εκτέλεση στον υπολογιστή σας καθημερινά ή εβδομαδιαία είναι μια καλή ιδέα να απαλλαγείτε από οποιονδήποτε ιό. Αυτό διατηρεί τον υπολογιστή σας ενημερωμένο και χωρίς προβλήματα.

Παρακολουθήστε τις λήψεις σας

Αντιλαμβανόμαστε ότι η λήψη αρχείων από το διαδίκτυο, όπως η μουσική και οι ταινίες, είναι αυτό που κάνουν όλοι ή πολλοί, αλλά αυτό προκαλεί και προβλήματα. Μεγάλα αρχεία όπως αυτά είναι εύκολο να κρύβουν μέσα τους κάποιο κακόβουλο λογισμικό και να μην το γνωρίζετε όταν κάνετε λήψη.

Ενημέρωση, ενημέρωση, ενημέρωση!

Το “Critical Update” των Microsoft Windows είναι ένα παράδειγμα προστασίας από τους χάκερς εκεί έξω. Το “Critical Update” είναι μια υπηρεσία της Microsoft που προσπαθεί να διατηρήσεις του ηλεκτρονικούς υπολογιστές ασφαλείς και χωρίς ιούς. Πάντα να ενημερώνετε το σύστημά σας.

Πάντα να μαθαίνετε

Είτε είστε φανατικός χρήστης είτε χρησιμοποιείτε τον υπολογιστή σας για απλά πράγματα, πρέπει να ξέρετε πάντα ποιοι είναι οι πιο πρόσφατοι ιοί και πως μπορούν να επηρεάσουν τον υπολογιστή σας. Αυτό θα σας προετοιμάσει ώστε να αντιμετωπίσετε αποτελεσματικά ένα ενδεχόμενο πρόβλημα.

Αποφύγετε τα «σπασμένα» (cracked) λογισμικά

Όλοι γνωρίζουν ότι μπορείτε να κατεβάσετε παράνομο ή «σπασμένο» λογισμικό από το διαδίκτυο που φαίνεται να είναι ευκολότερο για το πορτοφόλι σας, αλλά στην πραγματικότητα η λήψη αυτών των προγραμμάτων σας βλάπτει. Υποβάλλουν τον υπολογιστή σας σε δύσκολα εντοπισμένα σφάλματα και θα σας οδηγήσουν σε περισσότερα προβλήματα.

Εγκαταστήστε ένα τείχος προστασίας

Ένα τείχος προστασίας είναι ένα πρόγραμμα που ελέγχει την εισερχόμενη διαδικτυακή κυκλοφορία. Μαζί με το πρόγραμμα ιών σας, μπορεί να αποτρέψει την μη εξουσιοδοτημένη πρόσβαση στον υπολογιστή σας.

Να είστε προετοιμασμένοι

Αν έχετε ακούσει για έναν ιό που εξαπλώνεται γρήγορα , τότε βεβαιωθείτε ότι βρίσκεστε σε υψηλό επίπεδο συναγερμού. Μην δέχεστε τυχόν λήψεις και να είστε ιδιαίτερα προσεκτικοί όταν ανοίγετε μηνύματα και αρχεία ηλεκτρονικού ταχυδρομείου.

Αυτή η ενότητα θα σας βοηθήσει να προετοιμαστείτε για τυχόν ιούς υπολογιστών που θα μπορούσαν να έρθουν στο δρόμο σας. Θυμηθείτε να είστε πάντοτε προσεκτικοί και έξυπνοι όταν χρησιμοποιείτε τον υπολογιστή σας!

Ενότητα 3: Κακόβουλο λογισμικό (Malware)

Στόχοι για την ενότητα 3

Προσδιορισμός και αντιμετώπιση της εμμονής διαδικτυακής παρενοχλητικής παρακολούθησης (cyberstalking) και των τρόπων αναφοράς της.

Κακόβουλο λογισμικό (Malware)

Το κακόβουλο λογισμικό, αναφέρεται σε ένα είδος προγράμματος υπολογιστή σχεδιασμένο να μολύνει τον υπολογιστή ενός νόμιμου χρήστη και να προκαλεί βλάβη με πολλούς τρόπους. Το κακόβουλο λογισμικό μπορεί να μολύνει υπολογιστές και συσκευές με διάφορους τρόπους και εμφανίζεται με διάφορες μορφές, μερικές από τις οποίες περιλαμβάνουν ιούς, σκουλήκια (worms), trojans, λογισμικό υποκλοπής (spyware) και πολλά άλλα. Είναι ζωτικής σημασίας όλοι οι χρήστες να γνωρίζουν πώς να αναγνωρίζουν και να προστατεύονται από κακόβουλο λογισμικό σε όλες τις μορφές του.

Τι είναι το κακόβουλο λογισμικό; Έρχεται σε μια μπερδεμένη ποικιλία μορφών. Οι ιοί υπολογιστών είναι ίσως ο πιο γνωστός τύπος κακόβουλου λογισμικού - ονομάζεται έτσι επειδή εξαπλώνονται κάνοντας αντίγραφα του εαυτού τους. Τα warms έχουν παρόμοια ιδιότητα. Άλλοι τύποι κακόβουλου λογισμικού, όπως το λογισμικό υποκλοπής, ονομάζονται για αυτό που κάνουν: Στην περίπτωση του λογισμικού υποκλοπής, μεταδίδει προσωπικές πληροφορίες, όπως αριθμούς πιστωτικών καρτών.

Η προστασία του υπολογιστή και των προσωπικών σας συσκευών από κακόβουλο λογισμικό απαιτεί συνεχή προσωπική επαγρύπνηση και βοήθεια από επαγγελματικές εταιρείες ασφαλείας υπολογιστών. Σήμερα, το κακόβουλο λογισμικό δεν απευθύνεται μόνο στους οικιακούς υπολογιστές, αλλά και στις κινητές συσκευές που χρησιμοποιείτε εσείς και η οικογένειά σας. Το πρόβλημα είναι μεγαλύτερο από αυτό που νομίζετε.

Μπορείτε να είστε θύμα μιας επίθεσης κακόβουλου λογισμικού (malware) μέσω των φυλλομετρητών ιστού (web browsers), του ηλεκτρονικού σας ταχυδρομείου, των κοινωνικών δικτύων που χρησιμοποιείτε, των άμεσων μηνυμάτων και των αρχείων που έχετε λάβει.

Η συσκευή σας μπορεί να μολυνθεί σχεδόν από οποιαδήποτε διαδικτυακή διαδικασία ή ακόμα και από ένα USB stick ενός φίλου, οπότε είναι σημαντικό να χρησιμοποιήσετε ένα πρόγραμμα ασφαλείας που μπορεί να προσφέρει πλήρη προληπτική προστασία, βοηθώντας σας προτού να μολυνθείτε.

Έτσι, αφού απαντήθηκε το "Τι είναι το κακόβουλο πρόγραμμα;" το επόμενο λογικό ερωτήμα είναι "ποιος το δημιουργεί και γιατί;" Οι ημέρες κατά τις οποίες δημιουργοντουσαν τα περισσότερα κακόβουλα προγράμματα από έφηβους φαρσερ έχουν περάσει πολύ. Το κακόβουλο πρόγραμμα σήμερα σχεδιάζεται σε μεγάλο βαθμό από και για επαγγελματίες εγκληματίες.

Αυτοί οι εγκληματίες μπορούν να χρησιμοποιήσουν μια ποικιλία εξελιγμένων τακτικών. Σε ορισμένες περιπτώσεις, όπως σημειώνει ο δημόσιος ιστότοπος CIO για την τεχνολογία, οι κυβερνο-εγκληματίες «κλειδώνουν» τα δεδομένα υπολογιστών, καθιστώντας τις πληροφορίες απρόσιτες και στη συνέχεια ζητούν λύτρα από τους χρήστες προκειμένουν να τους επιτραπεί και πάλι η πρόσβαση σε αυτά τα δεδομένα.

Αλλά ο κύριος κίνδυνος που προέρχεται από τους εγκληματίες του κυβερνοχώρου είναι η κλοπή τραπεζικών πληροφοριών, τραπεζικών λογαριασμών, λογαριασμών πιστωτικών καρτών και κωδικών πρόσβασης. Οι χάκερς που κλέβουν αυτές τις πληροφορίες μπορούν στη συνέχεια να τις χρησιμοποιήσουν για να αδειάσουν τον λογαριασμό σας ή να χρεώσουν δόλιους λογαριασμούς πιστωτικών καρτών στο όνομά σας. Μπορούν επίσης να πουλήσουν τις πληροφορίες του λογαριασμού σας στη μαύρη αγορά, σε μια πάρα πολύ καλή τιμή.

Προστασία από κακόβουλα λογισμικά (Malware)

Τώρα λοιπόν, είμαστε στο μεγαλύτερο ζήτημα όλων: "Πώς μπορώ να βεβαιωθώ ότι ο υπολογιστής μου ή το δίκτυό μου δεν έχει πληγεί από κακόβουλα λογισμικά;"

Η απάντηση έχει δύο μέρη: Προσωπική επαγρύπνηση και εργαλεία προστασίας. Ένας από τους πιο δημοφιλείς τρόπους για την εξάπλωση κακόβουλου λογισμικού είναι μέσω ηλεκτρονικού ταχυδρομείου, το οποίο μπορεί να είναι «μεταμφιεσμένο» για να φαίνεται ότι προέρχεται από μια γνωστή εταιρεία όπως μια τράπεζα ή ένα προσωπικό ηλεκτρονικό μήνυμα από έναν φίλο.

Να είστε επιφυλακτικοί με τα μηνύματα ηλεκτρονικού ταχυδρομείου που σας ζητούν να δώσετε κωδικούς πρόσβασης. Ή τα μηνύματα ηλεκτρονικού ταχυδρομείου που φαίνεται να είναι από φίλους, αλλά έχουν μόνο ένα μήνυμα όπως "δείτε αυτή την ενδιαφέρουσα ιστοσελίδα (cool website!)" ακολουθούμενη από μια σύνδεση. Η προσωπική επαγρύπνηση είναι το πρώτο επίπεδο προστασίας από κακόβουλο λογισμικό, αλλά η προσοχή απλά δεν αρκεί. Επειδή η ασφάλεια των επιχειρήσεων δεν είναι τέλεια, ακόμη και οι λήψεις από νόμιμους ιστότοπους μπορεί μερικές φορές να έχουν συνημμένο κακόβουλο λογισμικό. Αυτό σημαίνει ότι ακόμη και ο πιο συνετός χρήστης κινδυνεύει, εκτός εάν λάβει πρόσθετα μέτρα.

Εγκατάσταση λογισμικού προστασίας από λογισμικό κατασκοπείας:

Το λογισμικό κατασκοπείας είναι ένα πρόγραμμα λογισμικού που συλλέγει προσωπικά δεδομένα ή πληροφορίες για έναν οργανισμό χωρίς την έγκρισή του. Αυτές οι πληροφορίες ανακατευθύνονται σε ιστότοπο τρίτων. Τα προγράμματα κατασκοπίας είναι σχεδιασμένα με τέτοιο τρόπο ώστε να μην είναι εύκολο να αφαιρεθούν. Το λογισμικό ‘Anti-Spyware’ είναι αποκλειστικά αφιερωμένο στην καταπολέμηση του spyware. Παρόμοια με το λογισμικό προστασίας από ιούς, το λογισμικό anti-spyware προσφέρει προστασία σε πραγματικό χρόνο. Σαρώνει όλες τις εισερχόμενες πληροφορίες και βοηθά στην αποτροπή της απειλής όταν εντοπιστεί.

Προτείνονται λογισμικά anti spyware στο τέλος της ενότητας. Μπορείτε να τα δείτε και να επιλέξετε το καταλληλότερο για εσάς.

Δεν υπάρχει απόλυτη προστασία. Αλλά ένας συνδυασμός προσωπικής ευαισθητοποίησης και καλά σχεδιασμένων εργαλείων προστασίας, θα κάνει τον υπολογιστή σας όσο τον δυνατόν ασφαλέστερο.

ΑΣΚΗΣΕΙΣ

Άσκηση 1 : Πάρτε τον έλεγχο του δρομολογητή σας μέσω μοναδικού κωδικού πρόσβασης:

Βήμα 1: Συνδεθείτε στον ασύρματο δρομολογητή σας.

Ανοίξτε τον Internet Explorer και πληκτρολογήστε τη διεύθυνση http://192.168.0.1 ή http://192.168.1.1 (Από προεπιλογή, οι περισσότεροι δρομολογητές έχουν 192.168.0.1 ή 192.168.1.1 ως προεπιλεγμένη διεύθυνση IP δρομολογητή. Αυτή είναι η διεύθυνση που θα πληκτρολογήσετε στο πρόγραμμα περιήγησης για να αποκτήσετε πρόσβαση στη σελίδα διαμόρφωσης του δρομολογητή)

Τώρα συνδεθείτε στο δρομολογητή σας. Τι; Δεν έχετε αναγνωριστικό χρήστη και κωδικό πρόσβασης; Μην ανησυχείτε. Έχετε διαπιστευτήρια (υπό τον όρο ότι δεν το έχετε αλλάξει νωρίτερα)

Το αναγνωριστικό χρήστη (user ID) και ο κωδικός πρόσβασής σας πρέπει να είναι:

Πέντε χαρακτήρες. Όλοι μικροί και στα αγγλικά . 1ο γράμμα τις αλφάβητου , έπειτα 4ο γράμμα τις αλφάβητου, στη συνέχεια 13ο γράμμα τις αλφάβητου, στη συνέχεια 12ο γράμμα τις αλφάβητου, κατόπιν 14ο γράμμα τις αλφάβητου.

Κάνοντάς το απλό:

Αναγνωριστικό χρήστη (User ID): admin

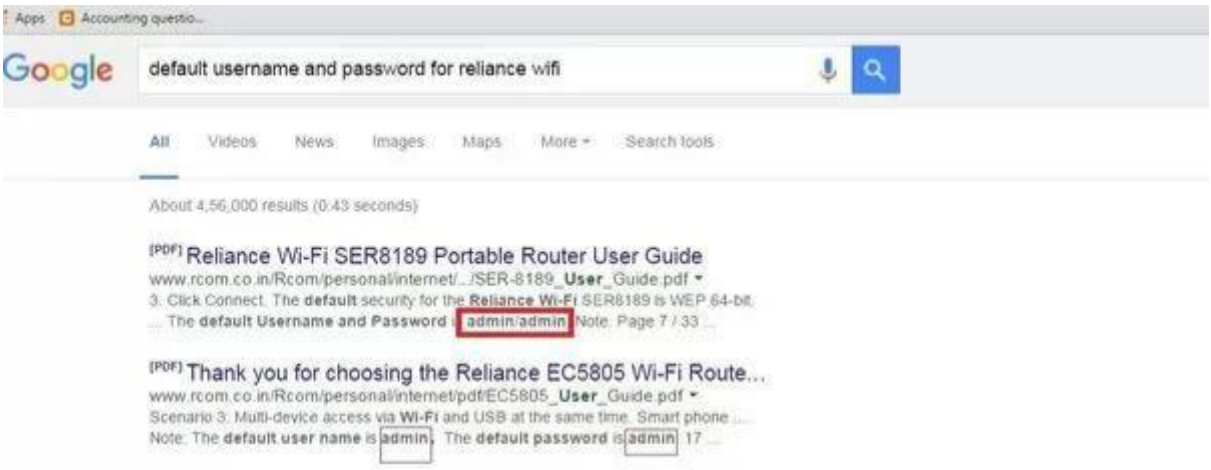
Κωδικός πρόσβασης (Password): admin

ή

Αναγνωριστικό χρήστη (User ID): admin

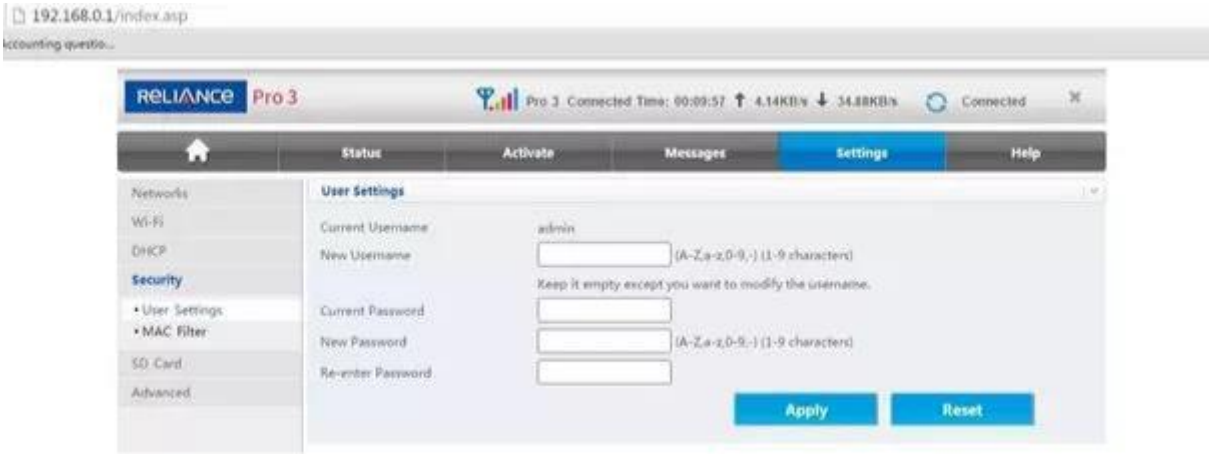
Κωδικός πρόσβασης (Password): κενό

Εάν δεν λειτουργεί για εσάς, παρακαλώ αναζητήστε στο διαδίκτυο για προεπιλεγμένο όνομα χρήστη / κωδικό πρόσβασης για τον δρομολογητή σας / φορέα παροχής υπηρεσιών.



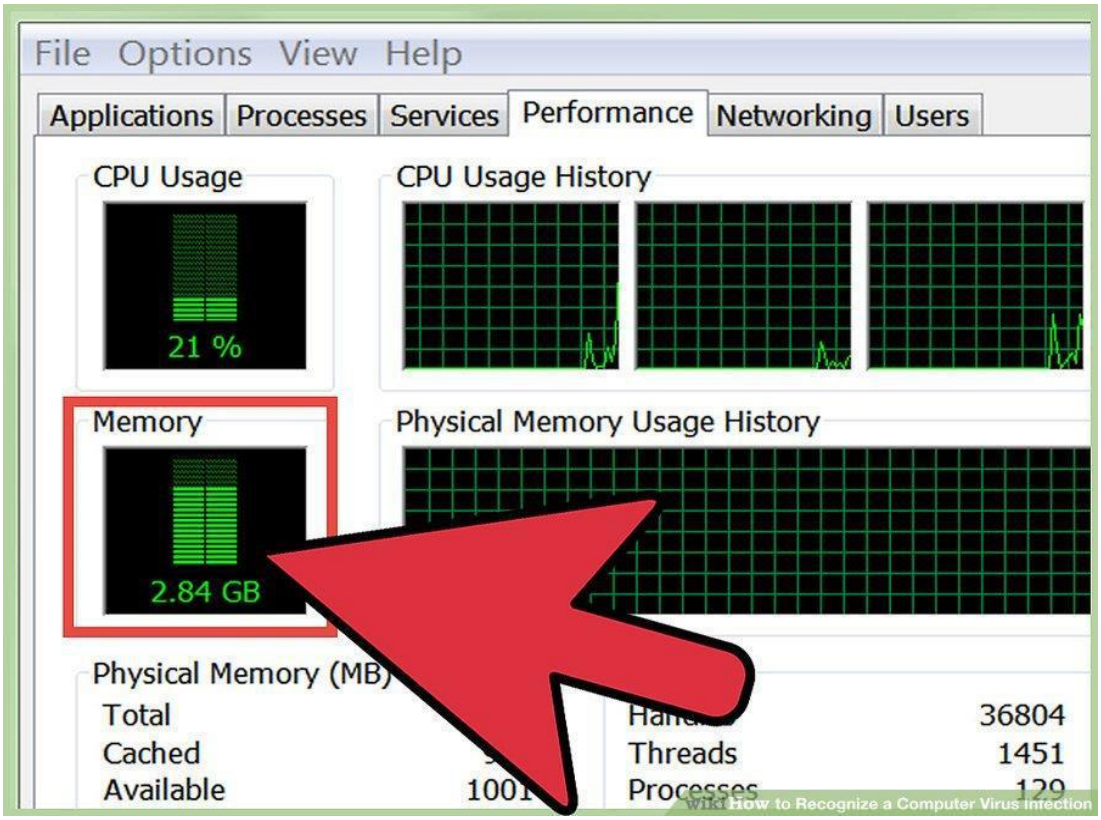
Βήμα 2: Αλλαγή του ονόματος χρήστη και του κωδικού σας.

- Πατήστε στις ρυθμίσεις
- Ρυθμίσεις χρήστη
- Ενημερώστε τα νέα σας διαπιστευτήρια



Άσκηση 2: Αναγνωρίστε τον ιό στον υπολογιστή σας

1. Ελέγξτε τη δραστηριότητα του σκληρού σας δίσκου. Εάν δεν εκτελείτε κάποιο προγράμματα και η φωτεινή ένδειξη του σκληρού δίσκου σας ανάβει ή σβήνει συνεχώς ή όταν ακούτε την εργασία του σκληρού δίσκου, τότε ενδέχεται να έχετε έναν ιό που λειτουργεί στο παρασκήνιο.



2. Πόσος χρόνος χρειάζεται ο υπολογιστής σας για εκκίνηση. Εάν αρχίσετε να παρατηρείτε ότι ο υπολογιστής σας χρειάζεται πολύ περισσότερο χρόνο από ό, τι συνήθως για να ξεκινήσει, ένας ιός μπορεί να επιβραδύνει τη διαδικασία εκκίνησης. Εάν δεν μπορείτε να συνδεθείτε στα Windows, ακόμη και με τις σωστές πληροφορίες σύνδεσης, ένας ιός πιθανότατα ανέλαβε τη διαδικασία σύνδεσης.
3. Δείτε τα φώτα του μόντεμ σας. Αν δεν έχετε τρέξει κανένα πρόγραμμα και τα φώτα μεταφοράς του μόντεμ σας αναβοσβήνουν συνεχώς, μπορεί να έχετε έναν ιό που μεταδίδει δεδομένα μέσω του δικτύου.

Άσκηση 3: Αναγνώριση κακόβουλων λογισμικών στο ηλεκτρονικό ταχυδρομείο σας

1. **Ηλεκτρονική διεύθυνση αποστολέα**. Εάν η διεύθυνση του αποστολέα δεν είναι οικεία ή δεν ταιριάζει με μια αναμενόμενη για μια εταιρεία διεύθυνση, τότε πιθανότατα πρόκειται για μήνυμα ηλεκτρονικού ταχυδρομείου κακόβουλου λογισμικού. Τα περισσότερα μηνύματα ηλεκτρονικού ταχυδρομείου με κακόβουλα προγράμματα εμφανίζονται ως ειδοποιήσεις παραλαβής πακέτων, τιμολόγια, φαξ / σαρώσεις ή ειδοποιήσεις δικαστηρίου. Αυτά τα μηνύματα σπάνια φαίνεται να προέρχονται από μια κατάλληλη διεύθυνση, όπως για παράδειγμα τα μηνύματα ηλεκτρονικού ταχυδρομείου που ισχυρίζονται ότι προέρχονται από την DHL ή την UPS είναι πιθανό να είναι κακόβουλα προγράμματα αν είναι η διεύθυνση δεν θα ταιριάζει με τα ups.com ή dhl.com.

2. **Το θέμα του μηνύματος στο ηλεκτρονικό ταχυδρομείο ή αν το συνημμένο περιέχει μέσα όνομα χρήστη.** Ένα ηλεκτρονικό μήνυμα με κακόβουλου λογισμικού μπορεί να περιέχει το όνομα χρήστη σας στο θέμα ή το όνομα αρχείου συνημμένου ή στο πεδίο Θέμα μπορεί να είναι κενό. Αντίθετα, τα κανονικά μηνύματα ηλεκτρονικού ταχυδρομείου σχεδόν πάντα έχουν θέμα και σπάνια αναφέρουν το όνομα χρήστη του ηλεκτρονικού ταχυδρομείου.

3. **Ενθάρρυνση για να ανοίξετε ένα συνημμένο αρχείο.** Πολλά μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν κακόβουλο λογισμικό θα σας ενθαρρύνουν να ανοίξετε ένα συνημμένο. Πολλά συνημμένα μπορούν ακόμη να είναι επιβλαβή ακόμη και αν εκτελείτε πρόγραμμα προστασίας από ιούς (antivirus). Τα μηνύματα ηλεκτρονικού ταχυδρομείου σχετικά με τα προβλήματα παράδοσης πακέτων δεν έχουν κανέναν καλό λόγο να σας ζητήσουν να ανοίξετε ένα συνημμένο. εάν σάς έστελναν μέσω ηλεκτρονικού ταχυδρομείου σχετικά με ένα νόμιμο πρόβλημα παράδοσης, θα μπορούσαν απλώς να σας ενημερώσουν στο σώμα του μηνύματος ηλεκτρονικού ταχυδρομείου.

4. **Ενθάρρυνση για να ακολουθήσετε ένα σύνδεσμο.** Ορισμένα μηνύματα ηλεκτρονικού ταχυδρομείου με κακόβουλα προγράμματα είναι παρόμοια με τα ηλεκτρονικά μηνύματα ηλεκτρονικού "ψαρέματος" (phishing), όπου σας ενθαρρύνουν να ακολουθήσετε μια σύνδεση ιστού. Αυτός ο σύνδεσμος ιστού θα μπορούσε να σας οδηγήσει σε κακόβουλο λογισμικό.

5. **Επαλήθευση πληροφοριών.** Αν ένα μήνυμα ηλεκτρονικού ταχυδρομείου σας ζητά να επιβεβαιώσετε, να ελέγξετε ή να δώσετε πληροφορίες χρησιμοποιώντας ένα συνημμένο, μπορεί να είναι ένα συνημμένο κακόβουλο λογισμικό. Ελέγξτε εάν αυτό φαίνεται ασφαλές και επικοινωνήστε με την εταιρεία σε περίπτωση αμφιβολίας. Ενδέχεται να μην είναι ασφαλές να ανοίξετε το συνημμένο.

6. **Προειδοποίηση προβλήματος, απειλή ή επείγουσα ανάγκη**. Τα μηνύματα ηλεκτρονικού ταχυδρομείου με κακόβουλα προγράμματα μέσα προσπαθούν συχνά να υποκινήσουν τον φόβο, την ανησυχία σας ή την αίσθηση του επείγοντος. Εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου σας ενθαρρύνει να λύσετε ένα πρόβλημα ανοίγοντας ένα συνημμένο τότε θα πρέπει να είστε πολύ επιφυλακτικοί. Ορισμένα μηνύματα ηλεκτρονικού ταχυδρομείου φαίνεται να είναι μια δεύτερη απάντηση που σας ζητάει τη συνέχεια. Παραδείγματα περιλαμβάνουν την αντιμετώπιση προβλημάτων παράδοσης πακέτων, πληροφοριών σχετικά με ψεύτικες εμφανίσεις δικαστηρίων ή πλαστών τιμολογίων από οντότητες με τις οποίες ενδέχεται να μην ασχολείστε.

7. **Άγνωστη παραλήπτες / μη καταχωρισμένοι παραλήπτες.** Εάν η λίστα παραληπτών ηλεκτρονικού ταχυδρομείου εμφανίζει άγνωστους παραλήπτες / μη καταχωρισμένους παραλήπτες ή διεύθυνση ηλεκτρονικού ταχυδρομείου διαφορετική από τη δική σας, τότε μπορεί να είναι κακόβουλο λογισμικό.

8. **Ύποπτη προσκόλληση.** Εάν το μήνυμα στο ηλεκτρονικό ταχυδρομείο έχει ένα μη αναμενόμενο συνημμένο, όπως ένα αρχείο με τις επεκτάσεις .doc, .zip, .xls, .js, .pdf, .ace, .arj, .wsh, .scr, .exe, .com, .bat, ή άλλους τύπους αρχείων του Microsoft Office τότε μπορεί να είναι κακόβουλο λογισμικό. Εκτιμήστε ότι μερικές φορές η επέκταση αρχείου είναι κρυμμένη ή το περιεχόμενο είναι διαφορετικό από αυτό που υποδεικνύεται.

9. **Απλό κείμενο / απουσία λογοτύπων.** Τα περισσότερα νόμιμα μηνύματα ηλεκτρονικού ταχυδρομείου τείνουν να γράφονται με HTML και μπορεί να έχουν ένα συνδυασμό κειμένου και εικόνων. Τα μηνύματα ηλεκτρονικού ταχυδρομείου κακόβουλων προγραμμάτων σπάνια έχουν εικόνες και τείνουν να έχουν απλή μορφοποίηση.

10. **Γενικός χαιρετισμός**. Εάν το μήνυμα στο ηλεκτρονικό ταχυδρομείο απευθύνεται με μια γενική φράση όπως "Αγαπητέ πελάτη", τότε μπορεί να είναι κακόβουλο λογισμικό ή απόπειρα ηλεκτρονικού "ψαρέματος".

11. **Μη αναγνωρίσιμο περιεχόμενο συνημμένου**. Εάν τελικά ανοίξετε ένα συνημμένο και το περιεχόμενο είναι άδειο ή είναι πολύ διαφορετικό από αυτό που περιμένατε, μπορεί να είναι κακόβουλο λογισμικό. Επικοινωνήστε άμεσα με την εταιρεία για βοήθεια! Μπορεί να είναι σε θέση να περιορίσει τη ζημιά ή να σας βοηθήσει να ανακτήσετε τα αρχεία σας.

Πως μοιάζουν τα μηνύματα στο ηλεκτρονικό ταχυδρομείο όταν έχουν κακόβουλα λογισμικά μέσα?

Εδώ είναι ένα πραγματικό στιγμιότυπο οθόνης ενός γραμματοκιβωτίου που περιέχει 19 ηλεκτρονικού ταχυδρομείου με κακόβουλο λογισμικό μέσα (malware):

Subject	Correspondents	Date
URGENT RFQ	AL WALEED EQUIPMENTS	03/13/2017 06:55
	starsescorts@gmail.com	03/15/2017 01:27
New Order Attached **KINDLY SEND INVOICE	Amr Hassan	03/15/2017 19:30
We're sad to let you know that our delivery was unusuccessful....	FedEx Expedited Express	03/16/2017 02:53
47929 username2	pkeith@gejlaw.com	03/16/2017 05:29
Delivery Status Notification	webmaster@stroy-exp...	03/16/2017 05:47
	vowsbyjudy@shaw.ca	03/16/2017 14:38
Formal Inquiry	"Anaïs VANACKER"<Va...	03/16/2017 21:16
We have delivery problems with your parcel #7104543	webmaster@whfarm2....	03/17/2017 00:57
INQUIRY	Saigon Offshore	03/17/2017 03:47
	dava@ac-lyon.fr	03/17/2017 14:25
54343 username	juanro5554@hotmail.c...	03/17/2017 14:48
Item Delivery Notification	alifeof8@server.alifeofj...	00:34
UPS courier can not deliver parcel #004287245 to you	webmaster@stroy-exp...	06:23
Parcel Delivery Notification	abidjanbateau@vps286...	06:52
Visa Card Award	info@visa.com	07:21
Problems with item delivery, n.4930349	Apache	09:54
Package Delivery Notification	Apache	10:06
Delivery Status Notification	contrav8@box980.blue...	17:05

Άσκηση 4: Διαδικτυακό κουίζ ασφάλειας

Κάντε αυτό το διαδικτυακό κουίζ και δείτε ποσό καλά θα πάτε.

https://www.proprofs.com/quiz-school/story.php?title=esafety-quiz

Υλικό για περαιτέρω ανάγνωση και πόροι

Οροί που πρέπει να ξέρετε

https://www.lifewire.com/top-internet-terms-for-beginners-2483381

Σχεδιασμός ασφάλειας διαδικτύου για ηλικιωμένους (Λήψη PDF)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=18&cad=rja&uact=8&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjARegQIBxAC&url=https%3A%2F%2Fvict imserviceslanark.ca%2Fphotos%2Fcustom%2FVSLG%2FResources%2FSafetyPlanningForSe niors_English.pdf&usg=AOvVaw3WNu9papw-5PbHbhKSxVFi

Κορυφαίες συμβολές ασφάλειας στο διαδίκτυο (Λήψη PDF)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjALegQIBRAC&url=https%3A%2F%2Fquery.prod.cms.rt.microsoft.com%2Fcms%2Fapi%2Fam%2Fbinary%2FRE1ImTu&usg=AOvVaw0QyXRMv5RLg-kAS0tIaUvz

Πώς να προστατευτείτε από κακόβουλα λογισμικά (malware) – YouTube video

https://www.youtube.com/watch?v=uJRqZTNMCMo

Οι καλύτερες υπηρεσίες προστασίας από ιούς για 2018

https://www.itproportal.com/guides/best-antivirus-services-for-2018/

***Οι καλύτερες υπηρεσίες προστασίας από* κακόβουλα λογισμικά για 2018**

https://www.techradar.com/best/best-free-anti-malware-software

Προστατεύεστε τα δεδομένα σας

https://youtu.be/BL7WJM342Uc

Ηλεκτρονική ασφάλεια για ηλικιωμένους

https://www.connectsafely.org/seniors/

Περισσότερες πληροφορίες σχετικά με την ασφάλεια στο διαδίκτυο

https://www.protectseniorsonline.com/resources/

Πώς να ελέγξετε αν ο υπολογιστής σας έχει ιό

https://www.youtube.com/watch?v=4i_cCPhewu4