

Δημόσια δίκτυα Wi-Fi

Οι συμμετέχοντες θα μάθουν για τα δημόσια δίκτυα Wi-Fi, τα πλεονεκτήματά τους και τους κινδύνους. Πιο συγκεκριμένα, θα μάθουν να αναγνωρίζουν τα μη ασφαλή δίκτυα Wi-Fi όταν είναι διαθέσιμα, να κατανοούν τα εγγενή μειονεκτήματα που έχει η χρήση μη ασφαλών δικτύων Wi-Fi, και να λαμβάνουν συνειδητές αποφάσεις για το πότε να συνδέονται και να χρησιμοποιούν μη ασφαλή δίκτυα Wi-Fi.

Πηγές

Εικόνα ασύρματου μόντεμ
Φυλλάδιο "Ασφάλεια σύνδεσης"

Τι είναι το Wi-Fi;

Μέρος πρώτο

Ρωτήστε τους μαθητές σας

Ποιες συσκευές χρησιμοποιείτε για να συνδεθείτε στο Internet;

Πώς συνδέονται αυτές οι συσκευές στο Internet;

Image Class Interaction

Η σύνδεση μέσω Wi-Fi είναι ο πιο συνηθισμένος τρόπος σύνδεσης των συσκευών στο Internet. Το Wi-Fi χρησιμοποιεί ραδιοσήματα για τη σύνδεση των συσκευών χωρίς φυσική ή ενσύρματη σύνδεση.

Φανταστείτε ότι έχετε τρεις φορητούς υπολογιστές στο σπίτι, τους οποίους θέλετε να συνδέσετε στο Internet. Για να το κάνετε αυτό, χρειάζεστε τα εξής:

1. Σημείο πρόσβασης: Σημείο πρόσβασης είναι οτιδήποτε μεταδίδει (εκπέμπει;) σήμα Wi-Fi και παρέχει πρόσβαση στο Internet. Οι συσκευές σας πρέπει να λάβουν αυτά τα σήματα προκειμένου να συνδεθούν στο Internet. Ορισμένες φορές, ενδέχεται να χρειάζεστε ειδική άδεια (π.χ. όνομα χρήστη και κωδικό πρόσβασης) για να συνδεθείτε και να χρησιμοποιήσετε το ασύρματο σήμα που εκπέμπει ένα σημείο πρόσβασης.

2. Δρομολογητής: Ο δρομολογητής είναι μια συσκευή που δημιουργεί ένα δίκτυο μεταξύ όλων των συσκευών (π.χ. υπολογιστές, tablet, κινητά τηλέφωνα) σε μια συγκεκριμένη τοποθεσία (σχολείο, βιβλιοθήκη ή το σπίτι σας). Συνήθως, οι δρομολογητές διαθέτουν ενσωματωμένο σημείο πρόσβασης (δείτε το παραπάνω διάγραμμα).

Οι δρομολογητές έχουν περιορισμένη (συνήθως μικρή) εμβέλεια. Αυτός είναι ο λόγος που αν η συσκευή σας βρίσκεται μακριά από το δρομολογητή, έχετε αδύναμο ή και καθόλου σήμα Wi-Fi. Επίσης, αν παρεμβάλλεται κάτι μεταξύ εσάς και του δρομολογητή (π.χ. κάποιο κτίριο ή τοίχος), το σήμα μειώνεται.

Παρόλο που η σύνδεση σε ένα δρομολογητή παρέχει πρόσβαση σε ένα δίκτυο, αυτό δεν μεταφράζεται αυτόματα σε σύνδεση στο Internet. Για να μπορέσουν πολλές συσκευές που είναι συνδεδεμένες σε ένα δίκτυο να συνδεθούν στο Internet, ο δρομολογητής πρέπει να συνδεθεί σε μόντεμ.

3. Μόντεμ: Το μόντεμ είναι μια συσκευή που δημιουργεί και διατηρεί μια σύνδεση στον πάροχο υπηρεσιών Internet (ISP) σας ώστε να έχετε πρόσβαση στο Internet. Μετατρέπει τα σήματα εκτός της δεδομένης σας τοποθεσίας σε σήματα που μπορεί να διαβάσει ο υπολογιστής σας και άλλες ψηφιακές συσκευές.

Σε μια τυπική διαμόρφωση, το σημείο πρόσβασης και ο δρομολογητής είναι μία συσκευή η οποία είναι συνδεδεμένη στο μόντεμ μέσω ενός ειδικού καλωδίου που ονομάζεται "καλώδιο Ethernet". Αυτό εννοούμε όταν μιλάμε για "ενσύρματη" σύνδεση στο Internet.

Οι φορητές συσκευές μπορούν επίσης να χρησιμοποιήσουν μια σύνδεση κινητής τηλεφωνίας για να συνδεθούν στο Internet, ιδιαίτερα αν δεν βρίσκονται σε κάποιο δίκτυο σχολείου, βιβλιοθήκης ή σπιτιού. Οι συνδέσεις κινητής τηλεφωνίας είναι ένα είδος ασύρματων ραδιοσημάτων με πολύ μεγαλύτερη περιοχή κάλυψης σε σχέση με ένα δρομολογητή. Οι συνδέσεις κινητής τηλεφωνίας χρησιμοποιούν συγκεκριμένους πομποδέκτες, οι οποίοι ονομάζονται πύργοι κινητής τηλεφωνίας, για να συνδέσουν τη φορητή συσκευή σας στο Internet.

Μέρος δεύτερο

Ρωτήστε τους μαθητές σας

Ποια είναι τα πλεονεκτήματα ενός δικτύου Wi-Fi;

Ποια είναι μερικά από τα μειονεκτήματα του Wi-Fi;

Μπορείτε να σκεφτείτε μερικά προβλήματα ασφάλειας όταν χρησιμοποιείτε δίκτυο Wi-Fi αντί ενσύρματης σύνδεσης στο Internet;

Γιατί χάνετε την πρόσβαση στο δίκτυο Wi-Fi όταν φεύγετε από ένα κτίριο;

Επιλογή δικτύου Wi-Fi

Μέρος πρώτο

Ρωτήστε τους μαθητές σας

Είναι όλα τα δίκτυα Wi-Fi ασφαλή; Γιατί/Γιατί όχι;

Ενημερώστε τους μαθητές σας

Ορισμένες φορές, σας δίνεται η επιλογή ως προς ποιο δίκτυο Wi-Fi θα θέλατε να χρησιμοποιήσετε. Είναι σημαντικό να θυμάστε ότι υπάρχουν σοβαροί κίνδυνοι αν συνδεθείτε στο λάθος δίκτυο. Όπως αναφέρθηκε νωρίτερα, μη ασφαλή δίκτυα Wi-Fi είναι εκείνα για τα οποία δεν απαιτείται κωδικός πρόσβασης για να συνδεθείτε. Αν είστε συνδεδεμένοι σε μη ασφαλές δίκτυο, είναι πιθανό άλλα άτομα συνδεδεμένα στο ίδιο δίκτυο να δουν τις πληροφορίες σας. Μπορεί να κλέψουν τις πληροφορίες που στέλνετε μέσω του δικτύου ή να παρακολουθούν τι κάνετε.

Από την άλλη πλευρά, ασφαλή και αξιόπιστα δίκτυα Wi-Fi είναι εκείνα για τα οποία απαιτείται κωδικός πρόσβασης, διαθέτουν δυνατότητα κρυπτογράφησης, κι εκείνα για τα οποία είστε σίγουροι ότι το δίκτυο στο οποίο συνδέεστε είναι αυτό που αναγράφεται στο όνομα δικτύου. Για παράδειγμα, η σύνδεση σε ένα δίκτυο που μιμείται το όνομα του σχολικού σας δικτύου θα μπορούσε να οδηγήσει στη δημοσιοποίηση πληροφοριών του λογαριασμού σας. Συνεπώς, τα δίκτυα τα οποία είναι ασφαλή και αξιόπιστα είναι αυτά που προσφέρουν τη μεγαλύτερη προστασία.

Κάτι το οποίο πρέπει να αναλογιστούμε είναι το πλαίσιο ή η τοποθεσία του δικτύου Wi-Fi. Για παράδειγμα, αν βρίσκεστε στον κινηματογράφο και δείτε το όνομα του σχολικού σας δικτύου στο κινητό σας όταν ψάχνετε για σύνδεση Wi-Fi, είναι πιθανό να θεωρήσετε ότι αυτό το δίκτυο προσπαθεί να μιμηθεί το σχολικό σας δίκτυο προκειμένου να συλλέξει κωδικούς πρόσβασης από ανυποψίαστους μαθητές.

Κατά τη δημιουργία ενός δικτύου Wi-Fi που προστατεύεται με κωδικό πρόσβασης, ο κάτοχος του δικτύου θα πρέπει να επιλέξει να ενεργοποιήσει το πρωτόκολλο κρυπτογράφησης του δρομολογητή. Συνηθισμένα πρωτόκολλα κρυπτογράφησης είναι τα Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) και WPA2. Αυτά τα πρωτόκολλα εξασφαλίζουν ότι οι πληροφορίες που στέλνονται ασύρματα μέσω του δικτύου είναι κρυπτογραφημένες (ή "κωδικοποιημένες").

Η κρυπτογράφηση δημιουργήθηκε ώστε να είναι δυσκολότερο για τους χάκερς να βλέπουν τι στέλνετε. Όλα αυτά τα πρωτόκολλα (WEP, WPA και WPA2), ωστόσο, έχουν αποδειχθεί ευάλωτα στην πειρατεία. Συνεπώς, είναι επίσης σημαντικό να βασιζόμαστε σε ασφαλείς διαδικτυακές συνδέσεις όταν μεταδίδουμε πληροφορίες μέσω διαδικτύου.

Το HTTPS είναι ένα πρότυπο που χρησιμοποιούν οι ιστότοποι για να

κρυπτογραφήσουν δεδομένα που μεταδίδονται μέσω Internet. Η κρυπτογράφηση μπορεί να αποτρέψει κάποιον τρίτο από το να δει εύκολα δεδομένα μέσω της σύνδεσής σας. Παρέχει ένα πρόσθετο επίπεδο ασφάλειας και μπορεί να χρησιμοποιηθεί σε οποιοδήποτε πρόγραμμα περιήγησης, με την προσθήκη του "https://" μπροστά από τη διεύθυνση URL που χρησιμοποιείτε (π.χ. <https://www.mysite.com>). Ωστόσο, δεν υποστηρίζουν όλοι οι ιστότοποι το πρωτόκολλο HTTPS.

1. Θα πρέπει να καταχωρείτε ευαίσθητες πληροφορίες (π.χ. κωδικούς πρόσβασης, στοιχεία πιστωτικών καρτών) μόνο σε ιστοσελίδες με το πρόθεμα HTTPS://.
2. Τα περισσότερα δημοφιλή προγράμματα περιήγησης έχουν, κοντά στη γραμμή διευθύνσεων, δείκτες ασφάλειας που μοιάζουν με λουκέτα οι οποίοι υποδεικνύουν τη χρήση σύνδεσης HTTPS.
3. Δυστυχώς, το HTTPS δεν μπορεί να εγγυηθεί την ασφάλειά σας, καθώς ορισμένοι κακόβουλοι ιστότοποι μπορεί να υποστηρίζουν και HTTPS. Το HTTPS ασφαλίζει τη σύνδεση, αλλά δεν μπορεί να διασφαλίσει ότι ο ιστότοπος είναι αξιόπιστος.

Ενημερώστε τους μαθητές σας

Το Secure Sockets Layer (SSL)/Transport Layer Security (TLS) είναι η τεχνολογία που διατηρεί το HTTPS ασφαλές. Το SSL/TLS χρησιμοποιεί ψηφιακά κλειδιά κρυπτογράφησης που λειτουργούν σε μεγάλο βαθμό ως αληθινά κλειδιά. Αν γράφατε ένα μυστικό μήνυμα για κάποιον φίλο σας σε ένα φύλλο χαρτί, όποιος έβρισκε το χαρτί θα μπορούσε να το διαβάσει. Αντί γι' αυτό, φανταστείτε να δίνετε στο φίλο σας ένα αντικλειδί και να στέλνατε το μυστικό μήνυμα μέσα σε ένα κλειδωμένο κουτί. Αν κάποιος έκλεβε το κουτί, δεν θα μπορούσε να διαβάσει το μυστικό μήνυμα χωρίς το κλειδί. Αν κάποιος δοκίμαζε να αντικαταστήσει το κουτί με ένα παρόμοιο, θα διαπιστώνατε ότι το κλειδί σας δεν λειτουργεί. Το SSL/TLS λειτουργεί με τον ίδιο τρόπο, αλλά με ιστότοπους.

Οι δείκτες ασφάλειας των προγραμμάτων περιήγησης μεταδίδουν επίσης πληροφορίες πιστοποιητικού εκτεταμένης επικύρωσης (Extended Validation - EV). Τα πιστοποιητικά EV παρέχονται σε ιστότοπους που επαληθεύουν την ταυτότητά τους σε μια αρχή έκδοσης πιστοποιητικών. Στα προγράμματα περιήγησης, ορισμένες φορές ο δείκτης EV παίρνει τη μορφή του ονόματος του ιστότοπου ή της αρχής καταχώρησης δίπλα στη γραμμή διευθύνσεων. Σε περίπτωση που υποπτεύεστε ότι το περιεχόμενο ενός συγκεκριμένου ιστότοπου είναι κακόβουλο, μπορείτε να ελέγξετε αν η διεύθυνση URL στο πιστοποιητικό ταιριάζει με τη διεύθυνση URL στο πρόγραμμα περιήγησης, κάνοντας κλικ στην επιλογή "Προβολή πιστοποιητικού". [Ισως είναι χρήσιμο να δείξετε στην οθόνη προβολής που βρίσκεται η επιλογή "Προβολή πιστοποιητικού".] Τα βήματα πλοήγησης σε αυτή την επιλογή διαφέρουν ανάλογα με το πρόγραμμα περιήγησης. Για παράδειγμα, στο Chrome, στην επιλογή "Προβολή", επιλέξτε "Προγραμματιστής" και έπειτα "Εργαλεία προγραμματισμού".

Στο μενού "Εργαλεία προγραμματισμού", επιλέξτε την καρτέλα "Ασφάλεια" και έπειτα "Προβολή πιστοποιητικού".

Ρωτήστε τους μαθητές σας

Τι πρέπει να έχετε υπόψη σας όταν συνδέεστε σε ένα καινούριο δίκτυο;

1. Πιθανές απαντήσεις περιλαμβάνουν: την τοποθεσία (ή το σε ποιον ανήκει το δίκτυο), την πρόσβαση (ή το ποιος άλλος συνδέεται στο δίκτυο) και τη δραστηριότητα (ή τι κάνετε μέσω του δικτύου).

Σε ποιον ανήκει το δίκτυο Wi-Fi του σπιτιού σας; Του σχολείου; Μιας καφετέριας;

1. Οι γονείς/τα άτομα που σας φροντίζουν κατέχουν το δίκτυο Wi-Fi του σπιτιού σας, οι διαχειριστές ή/και ο δήμος κατέχουν το δίκτυο του σχολείου σας και ο ιδιοκτήτης της καφετέριας κατέχει το δίκτυο της καφετέριας.

Γνωρίζετε τα άτομα αυτά προσωπικά; Εμπιστεύεστε αυτά τα άτομα;

1. Εμπλέξετε τους συμμετέχοντες σε μια συζήτηση σχετικά με το πώς μπορεί να εμπιστεύονται αυτά τα άτομα σε διαφορετικό βαθμό.

Ενημερώστε τους μαθητές σας

Πρέπει να γνωρίζετε και να εμπιστεύεστε το άτομο που παρέχει το δίκτυο Wi-Fi. Ορισμένες φορές, μπορείτε να καθορίσετε σε ποιον ανήκει ένα δίκτυο χρησιμοποιώντας το SSID του δικτύου.

Το Service Set Identifier (SSID) είναι το όνομα που έχει ένα δίκτυο Wi-Fi, το οποίο μπορείτε να δείτε όταν προσπαθείτε να συνδεθείτε. Το SSID χρησιμοποιείται συχνά για να γνωστοποιήσει τον κάτοχο του δικτύου και άλλες λεπτομέρειες που αφορούν το δίκτυο. Να είστε προσεκτικοί, ωστόσο, καθώς σχεδόν οποιοσδήποτε (που ξέρει με ποιον τρόπο) μπορεί να δημιουργήσει SSID. Για παράδειγμα, κάποιος μπορεί να δημιουργήσει ένα SSID το οποίο είναι όμοιο με αυτό που χρησιμοποιείτε στο σχολείο. Αυτό είναι ένα παράδειγμα μίμησης ενός γνωστού και αξιόπιστου δικτύου, ενδεχομένως με στόχο τη συλλογή ονομάτων χρηστών και κωδικών πρόσβασης.

Το να γνωρίζετε ποιος παρέχει το δίκτυο μπορεί να σας βοηθήσει να προσδιορίσετε αν το δίκτυο είναι ασφαλές. Αν ανήκει σε ένα άτομο ή σε έναν οργανισμό που εμπιστεύεστε, τότε πιθανώς να νιώσετε άνετα προκειμένου να συνδεθείτε. Ωστόσο, αν το δίκτυο είναι άγνωστο, δεν θα πρέπει να συνδεθείτε, καθώς δεν γνωρίζετε σε ποιον ανήκει ο δρομολογητής στον οποίο συνδέεστε. Επειδή όλη η κίνηση του δικτύου περνάει μέσα από το δρομολογητή, ο κάτοχος μπορεί να παρακολουθεί ή να καταγράφει τις διαδικτυακές σας κινήσεις.

Όταν συνδέεστε σε Wi-Fi, η συσκευή σας συνδέεται σε ένα τοπικό δίκτυο συσκευών και αυτό το δίκτυο συνδέεται στο ευρύτερο διαδίκτυο. Καθώς η συσκευή σας ανταλλάσσει πληροφορίες με αυτό το δίκτυο, είναι σημαντικό να εμπιστεύεστε τις άλλες συσκευές με τις οποίες είστε συνδεδεμένοι – και αυτό σημαίνει οποιαδήποτε συσκευή συνδεδεμένη στο δίκτυο. Ισχύει ό,τι και για μια ομαδική εργασία στο σχολείο – θέλετε να μπορείτε να εμπιστευτείτε τα άλλα άτομα με τα οποία δουλεύετε!

Η χρήση κωδικού πρόσβασης στο δίκτυο μπορεί να περιορίσει το ποιος μπορεί να συνδεθεί σε αυτό. Αυτό σημαίνει ότι θα έχετε μια καλύτερη ιδέα για το ποιος είναι συνδεδεμένος στο δίκτυο –είτε πρόκειται για την οικογένειά σας, τους φίλους σας ή άλλους πελάτες σε μια καφετέρια– απ' ό,τι αν το δίκτυο ήταν εντελώς ανοιχτό.

Το αν αποφασίσετε ή όχι να συνδεθείτε σε ένα δίκτυο το οποίο μπορεί να φαίνεται ύποπτο εξαρτάται από το συμβιβασμό που είστε πρόθυμοι να κάνετε όσον αφορά την ασφάλεια στο διαδίκτυο. Ίσως σκεφτείτε: Πώς θα σταθμίσω την πιθανότητα να παραβιαστεί ο λογαριασμός μου έναντι της άνεσης του να συνδεθώ σε ένα διαθέσιμο δίκτυο;

Ρωτήστε τους μαθητές σας

Θα πρέπει να διαβάσετε ειδήσεις/ιστολόγια στο διαδίκτυο χρησιμοποιώντας το δίκτυο Wi-Fi του σπιτιού σας; Του σχολείου; Μιας καφετέριας;

1. Εξηγήστε ότι το περιεχόμενο μιας ιστοσελίδας σε γενικές γραμμές δεν είναι ευαίσθητο περιεχόμενο. Πιθανότατα να μπορείτε να το κάνετε αυτό σε κάθε δίκτυο.

Θα πρέπει να στέλνετε τον αριθμό της πιστωτικής σας κάρτας χρησιμοποιώντας το δίκτυο Wi-Fi του σπιτιού σας; Του σχολείου; Μιας καφετέριας; Γιατί;

1. Ξεκινήστε μια συζήτηση σχετικά με το γιατί είναι ασφαλέστερο να χρησιμοποιεί κανείς το Wi-Fi του σπιτιού του για αυτόν το σκοπό και όχι το Wi-Fi κάποιας καφετέριας. Συζητήστε επίσης πώς, ενώ το δίκτυο του σχολείου είναι πιθανότατα αξιόπιστο, μπορεί να μην αξίζει το ρίσκο, καθώς αυτές οι πληροφορίες είναι ιδιαίτερα ευαίσθητες.

Θα πρέπει να τσεκάρετε το προσωπικό σας email χρησιμοποιώντας το δίκτυο Wi-Fi του σπιτιού σας; Του σχολείου; Μιας καφετέριας;

1. Συζητήστε πώς πιθανότατα είναι πιο ασφαλές να το κάνουν από το δίκτυο του σπιτιού τους, ανάλογα με το περιεχόμενο του λογαριασμού τους email. Για παράδειγμα, κάποιοι έχουν πολλούς λογαριασμούς email τους οποίους χρησιμοποιούν για διαφορετικούς σκοπούς (π.χ. ένα λογαριασμό για διαφημιστικά/προωθητικά email, έναν άλλο λογαριασμό για τα email σε φίλους και συγγενείς).

Ενημερώστε τους μαθητές σας

Για την αποστολή/προβολή ευαίσθητων πληροφοριών, όπως είναι οι κωδικοί πρόσβασης και τραπεζικά στοιχεία, είναι προτιμότερη η χρήση ιδιωτικών και ασφαλών δικτύων, σε ιστότοπους που χρησιμοποιούν SSL/TLS, και όχι η χρήση κοινόχρηστων δημόσιων δικτύων. Αυτές οι απόρρητες πληροφορίες βρίσκονται σε κίνδυνο αν τις υποβάλετε ή αποκτήσετε πρόσβαση σε αυτές ενώ είστε συνδεδεμένοι σε ένα κοινόχρηστο δίκτυο που χρησιμοποιείται από ανθρώπους που δεν γνωρίζετε ή δεν εμπιστεύεστε.

Μπορεί να μην είναι ξεκάθαρο ποιες πληροφορίες είναι ευαίσθητες και ποιες όχι, καθώς η ιδιωτικότητα είναι μια προσωπική απόφαση που παίρνει ο καθένας για τον εαυτό του. Είναι σημαντικό να εξετάζετε κάθε περίπτωση μεμονωμένα προκειμένου να αποφασίσετε αν θα πρέπει να συνδεθείτε σε κάποιο δίκτυο. Πριν αποφασίσετε αν θα συνδεθείτε ή όχι, αναρωτηθείτε αν εμπιστεύεστε τον κάτοχο του δικτύου, τους άλλους που είναι συνδεδεμένοι σε αυτό, τι κάνετε διαδικτυακά και ποιες πληροφορίες πρόκειται να μοιραστείτε.

Ασφαλή και μη ασφαλή δίκτυα

Μέρος πρώτο

Αλληλεπίδραση στην τάξη

Σημείωση: Μέρος του περιεχομένου αυτής της δραστηριότητας έχει καλυφθεί στην ενότητα "Δραστηριότητα 2: Επιλογή δικτύου Wi-Fi". Το αν επιθυμείτε ή όχι να αναλύσετε ξανά αυτό το υλικό ή να το προσπεράσετε, το αφήνουμε στην κρίση σας.

Ενημερώστε τους μαθητές σας

Όπως αναφέρθηκε νωρίτερα, τα μη ασφαλή δίκτυα Wi-Fi είναι εκείνα για τα οποία δεν απαιτείται κωδικός πρόσβασης για να συνδεθείτε. Η χρήση μη ασφαλών δικτύων θέτει σε κίνδυνο τα δεδομένα που στέλνετε και λαμβάνετε μέσω του δικτύου.

Ασφαλή δίκτυα Wi-Fi είναι εκείνα για τα οποία απαιτείται κωδικός πρόσβασης και διαθέτουν δυνατότητα κρυπτογράφησης. Το άτομο το οποίο διαμορφώνει το δίκτυο είναι εκείνο το οποίο επιλέγει αν θα ενεργοποιήσει την κρυπτογράφηση. Η κρυπτογράφηση κωδικοποιεί τις πληροφορίες που στέλνετε ή λαμβάνετε, καθιστώντας το δυσκολότερο για ένα χάκερ συνδεδεμένο στο ίδιο δίκτυο Wi-Fi να δει τι στέλνετε ή λαμβάνετε.

Το γεγονός ότι ένα δίκτυο είναι ασφαλές δεν σημαίνει ότι και τα δεδομένα σας είναι ασφαλή. Είναι σίγουρα ασφαλέστερο από τη χρήση ενός μη ασφαλούς δικτύου. Ωστόσο, ένας αποφασισμένος χάκερ μπορεί και πάλι να βρει κάποιον τρόπο για να αποκτήσει πρόσβαση στις πληροφορίες σας.

Υπάρχουν τρία συνηθισμένα πρωτόκολλα κρυπτογράφησης των δικτύων Wi-Fi: τα Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) και WPA2. Τα WEP και WPA είναι ξεπερασμένα και τα δίκτυα που βασίζονται σε αυτά θα πρέπει να θεωρούνται μη ασφαλή. Επιπλέον, το WPA2 έχει επίσης αποδειχθεί ευάλωτο στην πειρατεία.

Για να εξασφαλίσετε ότι οι πληροφορίες σας είναι προστατευμένες στον μέγιστο δυνατό βαθμό, ελέγξτε ότι οι ιστότοποι που χρησιμοποιείτε είναι κρυπτογραφημένοι μέσω SSL/TLS.

Ρωτήστε τους μαθητές σας

Μπορείτε να σκεφτείτε ένα παράδειγμα δικτύου προστατευμένου με κωδικό πρόσβασης που έχετε χρησιμοποιήσει;

1. Μερικά παραδείγματα περιλαμβάνουν το Wi-Fi του σπιτιού τους, το Wi-Fi ενός σχολείου και τα δίκτυα Wi-Fi σε ορισμένες δημόσιες τοποθεσίες όπως καφετέριες.

Μπορείτε να σκεφτείτε ένα παράδειγμα μη ασφαλούς δικτύου που έχετε χρησιμοποιήσει;

Και παραδείγματα ασφαλούς δικτύου;

Ενημερώστε τους μαθητές σας

Μπορείτε να ελέγξετε αν ένα δίκτυο Wi-Fi είναι κρυπτογραφημένο εξετάζοντας τις ρυθμίσεις δικτύου ή ασύρματης σύνδεσης στη συσκευή σας.

Μέρος δεύτερο

Αλληλεπίδραση στην τάξη

Πριν από αυτή την εκπαιδευτική εμπειρία, κάντε μια διαδικτυακή αναζήτηση για να δείτε πώς να ελέγχετε τους τύπους κρυπτογράφησης των δικτύων Wi-Fi για διαφορετικά λειτουργικά συστήματα. Έπειτα, δείξτε πώς μπορεί να βρει κανείς το είδος της κρυπτογράφησης που χρησιμοποιεί ένα δίκτυο. Για παράδειγμα, σε υπολογιστή MacOS, επιλέξτε System Preferences -> Network -> Select Wi-Fi -> Select the appropriate Network Name (Προτιμήσεις συστήματος -> Δίκτυο -> Επιλέξτε Wi-Fi -> Επιλέξτε το κατάλληλο όνομα δικτύου). Στην καρτέλα Wi-Fi, θα υπάρχει μια λίστα με γνωστά δίκτυα και μια στήλη που θα υποδεικνύει ποιος τύπος κρυπτογράφησης χρησιμοποιείται.

Ενημερώστε τους μαθητές σας

Δεν είναι όλες οι συνδέσεις ίδιες. Όταν ένα δίκτυο δεν είναι ασφαλές, οποιοσδήποτε μπορεί να συνδεθεί σε αυτό, ενώ δεν είναι ξεκάθαρο ποιος ελέγχει το δίκτυο. Η σύνδεση σε ένα μη ασφαλές δίκτυο σας αφήνει ευάλωτους, καθώς οποιοσδήποτε συνδεδεμένος στο δίκτυο μπορεί ενδεχομένως να δει τις πληροφορίες που στέλνετε και λαμβάνετε, όπως τις κινήσεις σας στο διαδίκτυο (σελίδες, κωδικούς πρόσβασης κ.λπ.), αν δεν χρησιμοποιείτε σύνδεση SSL/TLS.

Αλληλεπίδραση στην τάξη

Ανάλογα με τις τεχνικές γνώσεις των συμμετεχόντων, ίσως θέλετε να συζητήσετε τη χρήση εικονικών ιδιωτικών δικτύων (VPN) ως ένα επιπρόσθετο επίπεδο προστασίας κατά τη χρήση Wi-Fi. Ανατρέξτε στους συνδέσμους VPN στην ενότητα "Πόροι" για περισσότερες πληροφορίες.

Αναγνωρίζοντας την ασφάλεια σύνδεσης

Τίτλος μέρους

Αλληλεπίδραση στην τάξη

Χωρίστε τους συμμετέχοντες σε ομάδες των 2-3 ατόμων. Μοιράστε το φυλλάδιο "Ασφάλεια σύνδεσης" για τους συμμετέχοντες και αναθέστε ένα σενάριο σε κάθε ομάδα. Δώστε στους συμμετέχοντες 5 λεπτά για να συζητήσουν τα σενάρια. Στη συνέχεια, ζητήστε από τις ομάδες να μοιραστούν τις απαντήσεις τους. Οι απαντήσεις είναι με πράσινο χρώμα στο φυλλάδιο.

Άσκηση

Μέρος πρώτο

Άσκηση

Ζητήστε από τους συμμετέχοντες να κάνουν τα εξής:

1. Να φτιάξουν το ημερολόγιο μιας κλασικής ημέρας, σημειώνοντας σε ποια δίκτυα Wi-Fi συνδέονται.
2. Από τα επιλεγμένα δίκτυα που αναγράφονται στο ημερολόγιο, ζητήστε από τους συμμετέχοντες να επιλέξουν δύο και να γράψουν μια σύντομη παράγραφο για το καθένα, περιγράφοντάς το. Ποιοι άλλοι συνδέονται σε αυτό; Πόσο ασφαλές είναι;
3. Επιπλέον, όσον αφορά τα δύο επιλεγμένα δίκτυα, ζητήστε από τους συμμετέχοντες να περιγράψουν ποιες ευκαιρίες και ποιους κινδύνους μπορεί να συνεπάγεται η σύνδεση σε αυτά τα δίκτυα.