

Κωδικοί πρόσβασης

Οι συμμετέχοντες θα μάθουν πώς να προστατεύουν καλύτερα τις ηλεκτρονικές τους πληροφορίες χρησιμοποιώντας και διατηρώντας ισχυρούς κωδικούς πρόσβασης. Οι συμμετέχοντες θα μάθουν σχετικά με τις αρχές δημιουργίας ενός ισχυρού κωδικού πρόσβασης και για τα πιθανά προβλήματα που προκαλούνται από την κοινή χρήση κωδικών πρόσβασης. Θα μάθουν επίσης πώς να διατηρούν τους κωδικούς τους ασφαλείς και πώς να λαμβάνουν μέτρα για την αποτροπή μη εξουσιοδοτημένης πρόσβασης στους λογαριασμούς τους.

Υλικά

Φυλλάδιο "Μαθαίνουμε για τους κωδικούς πρόσβασης"

Βασικές πληροφορίες για τους κωδικούς πρόσβασης

Μέρος πρώτο

Ενημερώστε τους μαθητές σας

Συνήθως δεν πολυσκεφτόμαστε τους κωδικούς πρόσβασης που χρησιμοποιούμε σε ιστότοπους, εφαρμογές και υπηρεσίες. Ωστόσο, η ισχύς των κωδικών πρόσβασης καθορίζει πόσο ασφαλείς θα είναι και οι πληροφορίες σας.

Αλληλεπίδραση στην τάξη

Ξεκινήστε μια συζήτηση με τους συμμετέχοντες κάνοντας τις ακόλουθες ερωτήσεις. Υπενθυμίστε στους συμμετέχοντες ότι είναι σημαντικό να μην μοιραστούν τους πραγματικούς τους κωδικούς πρόσβασης σε αυτή ή σε οποιαδήποτε άλλη άσκηση.

Ρωτήστε τους μαθητές σας

Πόσους κωδικούς πρόσβασης έχετε;

Έχετε διαφορετικούς κωδικούς πρόσβασης για κάθε λογαριασμό email και κάθε μέσο κοινωνικής δικτύωσης που χρησιμοποιείτε;

Διαφέρουν αρκετά μεταξύ τους ή είναι απλά παραλλαγή ενός μόνο κωδικού;

Αν έχετε περισσότερους από έναν κωδικούς πρόσβασης, πώς θυμάστε ποιος κωδικός ανήκει σε ποιον λογαριασμό;

Ρωτήστε τους μαθητές σας

Πόσο συχνά ξεχνάτε κάποιον σημαντικό κωδικό πρόσβασης;

Τι έχετε κάνει στις περιπτώσεις που έχετε ξεχάσει τον κωδικό σας;

Πώς δημιουργείτε ευκολομνημόνευτους κωδικούς πρόσβασης;

Υπάρχει κάποιος κωδικός που χρησιμοποιείτε καθημερινά;

Τι θα συμβεί αν, χωρίς να το γνωρίζετε, κάποιος βρει τον κωδικό πρόσβασής σας;

Θα εξαρτηθεί από το ποιος είναι;

Τι είδους πληροφορίες θα μπορούσε να μάθει κάποιος για εσάς αν χρησιμοποιούσε τον κωδικό πρόσβασής σας για να μπει στο λογαριασμό σας;

Μέρος δεύτερο

Αλληλεπίδραση στην τάξη

Χωρίστε τους συμμετέχοντες σε ζευγάρια.

Ενημερώστε τους μαθητές σας

Με το ζευγάρι σας, συζητήστε τι θα μπορούσε να συμβεί αν κάποιος με κακόβουλες προθέσεις μάθαινε τον κωδικό πρόσβασης του λογαριασμού σας στην αγαπημένη σας πλατφόρμα κοινωνικής δικτύωσης.

Αλληλεπίδραση στην τάξη

Δώστε στους συμμετέχοντες 5 λεπτά για να συζητήσουν. Ζητήστε από τις ομάδες να μοιραστούν ό,τι συζήτησαν.

Ενημερώστε τους μαθητές σας

Τώρα συζητήστε με το ζευγάρι σας τι θα μπορούσε να συμβεί αν κάποιος χάκερ μάθαινε τον κωδικό πρόσβασης του online τραπεζικού λογαριασμού των γονιών σας ή των ατόμων που σας φροντίζουν.

Αλληλεπίδραση στην τάξη

Δώστε στους συμμετέχοντες 5 λεπτά για να συζητήσουν. Έπειτα ζητήστε από τις ομάδες να μοιραστούν ό,τι συζήτησαν.

Μέρος τρίτο

Ενημερώστε τους μαθητές σας

Ίσως αναρωτιέστε πώς ένας χάκερ θα μπορούσε να μάθει έναν ιδιωτικό κωδικό πρόσβασης. Υπάρχουν διάφοροι τρόποι, όπως μέσω της κοινωνικής μηχανικής, δηλ. εξαπατώντας κάποιον να μοιραστεί τον κωδικό πρόσβασής του. Ένας χάκερ μπορεί να στείλει ένα email που μοιάζει να προέρχεται νόμιμα από μια πλατφόρμα ή έναν ιστότοπο όπου κάποιος έχει λογαριασμό. Το email μπορεί να προτρέψει τον παραλήπτη να κάνει κλικ σε ένα σύνδεσμο και να συνδεθεί με το όνομα χρήστη και τον κωδικό πρόσβασής του. Μόλις συνδεθεί, οι πληροφορίες αυτές είναι πλέον διαθέσιμες στο χάκερ.

Οι χάκερ προσπαθούν μερικές φορές να μαντέψουν τους κωδικούς πρόσβασης χρησιμοποιώντας κοινότυπες φράσεις όπως "password123", "test" ή το όνομα ή το

επώνυμό σας.

Ένας άλλος τρόπος που χρησιμοποιούν οι χάκερ για να μάθουν ιδιωτικούς κωδικούς πρόσβασης είναι μέσω της λεγόμενης επίθεσης Brute Force. Μια επίθεση ωμής βίας προκύπτει όταν ένας χάκερ προσπαθεί να συνδεθεί στο λογαριασμό σας δοκιμάζοντας επανειλημμένα διάφορους κωδικούς πρόσβασης. Ο χάκερ μπορεί να εξαπολύσει μια επίθεση Brute Force χωρίς αυτοματισμούς, ωστόσο συνήθως το κάνει εκτελώντας ένα πρόγραμμα υπολογιστή που δοκιμάζει γρήγορα και αυτόματα κάθε πιθανό συνδυασμό κωδικών πρόσβασης. Για παράδειγμα, μια λίστα πιθανών κωδικών πρόσβασης ή ένα σύνολο κωδικών πρόσβασης που αποτελούνται από συνδυασμούς διαφορετικών γραμμάτων και αριθμών, μέχρι να βρεθεί ο σωστός κωδικός πρόσβασης.

Φυσικά, κάποιες επιθέσεις Brute Force είναι πιο εξελιγμένες. Αν ο κωδικός πρόσβασής σας περιλαμβάνεται σε μια λίστα πιθανών κωδικών πρόσβασης, π.χ. "fido123" ή "password", τότε κάποια προγράμματα μπορούν να τον μαντέψουν ταχύτερα δοκιμάζοντας πρώτα αυτές τις επιλογές πριν από άλλες λιγότερο πιθανές επιλογές ή τυχαίες πιθανότητες. Η επίθεση μπορεί να είναι πιο στοχευμένη αν ο χάκερ γνωρίζει πληροφορίες για εσάς. Για παράδειγμα, αν ο χάκερ γνωρίζει ότι το κατοικίδιό σας ονομάζεται Toby, μπορεί να δοκιμάσει το Toby με παραλλαγές αριθμών στο τέλος (π.χ. "Toby629" ή "Toby3020").

Αρχές δημιουργίας κωδικού πρόσβασης

Μέρος πρώτο

Ρωτήστε τους μαθητές σας

Ποιος ξέρει τι σημαίνει να έχεις "ισχυρό" ή "ισχυρότερο" κωδικό πρόσβασης; Γιατί είναι καλή ιδέα αυτό;

Ενημερώστε τους μαθητές σας

Ο ισχυρός κωδικός πρόσβασης προστατεύει τις πληροφορίες σας. Παρότι ένας ισχυρός κωδικός δεν εγγυάται ότι ο λογαριασμός σας δεν θα παραβιαστεί, το να έχετε έναν ασθενή κωδικό διευκολύνει την κακόβουλη πρόσβαση στις πληροφορίες σας.

Άσκηση για τους κωδικούς πρόσβασης

Ρωτήστε τους μαθητές σας

Ποια είναι ορισμένα παραδείγματα ασθενών κωδικών πρόσβασης;

1. Κάποια παραδείγματα: Password, 12345, Hello!, μια ημερομηνία γέννησης, ένα ψευδώνυμο.

Γιατί νομίζετε ότι είναι ασθενείς αυτοί οι κωδικοί;

1. Μπορούν να τους μαντέψουν εύκολα τρίτοι ή/και κάποιος υπολογιστής που εκτελεί επίθεση Brute Force.

Με ποιους ενδεικτικούς τρόπους μπορείτε να κάνετε έναν κωδικό πρόσβασης πιο ισχυρό;

1. Με την προσθήκη αριθμών, πεζών και κεφαλαίων γραμμάτων, συμβόλων, κάνοντας τον κωδικό πρόσβασης πιο μεγάλο και αποφεύγοντας τη χρήση κοινότοπων φράσεων και λέξεων από μόνες τους.

Αλληλεπίδραση στην τάξη

Αφού οι συμμετέχοντες εκφράσουν τη γνώμη τους, γράψτε αυτές τις οδηγίες στον πίνακα:

Συμπεριλάβετε τουλάχιστον έναν αριθμό.

Συμπεριλάβετε τουλάχιστον ένα σύμβολο.

Συμπεριλάβετε τουλάχιστον ένα κεφαλαίο και ένα πεζό γράμμα.

Οι κωδικοί πρόσβασης θα πρέπει να περιέχουν τουλάχιστον 7 χαρακτήρες.

Οι κωδικοί πρόσβασης πρέπει να είναι ευκολομνημόνευτοι (εκτός αν χρησιμοποιείται κάποιος ιστότοπος ή κάποια εφαρμογή διαχείρισης κωδικών πρόσβασης).

Οι ιστότοποι και οι εφαρμογές διαχείρισης κωδικών πρόσβασης είναι ιστότοποι/εφαρμογές που βοηθούν τους χρήστες να αποθηκεύουν και να οργανώνουν τους κωδικούς πρόσβασής τους.

Οι κωδικοί πρόσβασης δεν πρέπει να είναι μια μεμονωμένη λέξη ή προσωπικές πληροφορίες (ημερομηνία γέννησης, όνομα γονέα κλπ.).

Οι κωδικοί πρόσβασης δεν πρέπει να είναι κοινοί μεταξύ ιστότοπων.

Ενημερώστε τους μαθητές σας

Υπάρχουν δύο προσεγγίσεις για τη δημιουργία ισχυρών κωδικών πρόσβασης. Η πρώτη είναι να ακολουθήσετε μια "συνταγή κωδικού πρόσβασης", όπως αυτή που δίνεται στον πίνακα. Η χρήση μιας τέτοιας συνταγής σας ενθαρρύνει να συμπεριλάβετε στοιχεία που είναι πιο δύσκολο να μαντέψει κανείς σε έναν κειμενικό/αριθμητικό κωδικό πρόσβασης, δυσχεραίνοντας έτσι το μάντεμα του κωδικού. Το μειονέκτημα αυτής της προσέγγισης είναι ότι οι κωδικοί πρόσβασης απομνημονεύονται δύσκολα.

Ισχυροί κωδικοί πρόσβασης

Ενημερώστε τους μαθητές σας

Μια άλλη προσέγγιση για τη δημιουργία ισχυρών κωδικών πρόσβασης συνδέεται με το μήκος τους. Επειδή η ισχύς του κωδικού πρόσβασης αποτελεί συνάρτηση του μήκους του, η χρήση μιας σειράς τεσσάρων ή περισσότερων ασύνδετων λέξεων κάνει τους κωδικούς πολύ πιο δύσκολο να τους μαντέψουν τρίτοι ή να υποστούν επιθέσεις Brute Force. Αυτή η μέθοδος έχει το πρόσθετο πλεονέκτημα ότι οι κωδικοί πρόσβασης που προκύπτουν απομνημονεύονται πιο εύκολα σε σύγκριση με τη μέθοδο συνταγής.

Τέλος, μπορεί κανείς να χρησιμοποιήσει ένα συνδυασμό αυτών των δύο μεθόδων, δημιουργώντας μια σειρά τεσσάρων ή περισσότερων ασύνδετων λέξεων, συμπεριλαμβανομένων επίσης συμβόλων και αριθμών.

Ο στόχος αυτών των διαφορετικών μεθόδων είναι ο ίδιος: η δημιουργία κωδικών

πρόσβασης που είναι μοναδικοί και δύσκολοι να τους μαντέψουν τρίτοι.

Ενημερώστε τους μαθητές σας

Χωρίστε τους συμμετέχοντες σε ζευγάρια.

Σε ζευγάρια, προσπαθήστε να δημιουργήσετε έναν ισχυρό κωδικό πρόσβασης χρησιμοποιώντας τις οδηγίες που γράψαμε νωρίτερα στον πίνακα. Να θυμάστε ότι ένας κωδικός που δύσκολα μπορεί να τον μαντέψει τυχαία ένας υπολογιστής μπορεί να είναι εύκολος για κάποιον άνθρωπο ή υπολογιστή που έχει μια λίστα με κοινούς κωδικούς πρόσβασης μεγάλου μήκους. Το χαρτί με τον κωδικό πρόσβασής σας δεν θα παραδοθεί στο τέλος της δραστηριότητας. Μην χρησιμοποιήσετε αυτόν τον κωδικό για τους λογαριασμούς σας, καθώς θα τον γνωρίζουν τα άλλα μέλη της ομάδας.

Δώστε στους συμμετέχοντες 5 λεπτά για την άσκηση αυτή. Στη συνέχεια, ρωτήστε τους συμμετέχοντες ποια νομίζουν ότι είναι παραδείγματα ισχυρών κωδικών. Ρωτήστε τους συμμετέχοντες αν μπορούν να θυμηθούν τους κωδικούς πρόσβασης που δημιούργησαν χωρίς να τους κοιτάξουν.

Αν και σε κάποιους ιστότοπους ο κωδικός σας θα πρέπει να ικανοποιεί μερικές (ή και όλες) από αυτές τις συνθήκες, σε άλλους ιστότοπους δεν υπάρχουν τέτοιοι περιορισμοί. Μπορείτε επίσης να δημιουργήσετε κωδικούς πρόσβασης χρησιμοποιώντας μια σειρά τυχαίων κοινών λέξεων.

Αλληλεπίδραση στην τάξη

Κρατώντας τα ίδια ζευγάρια, ζητήστε από τους συμμετέχοντες να δημιουργήσουν νέους κωδικούς πρόσβασης χρησιμοποιώντας μια σειρά λέξεων. Εξηγήστε ότι κάθε κωδικός πρόσβασης θα πρέπει να έχει τουλάχιστον τέσσερις λέξεις, προκειμένου να είναι ισχυρός αλλά και να μπορεί να τον θυμάται εύκολα ο χρήστης. Δώστε στους συμμετέχοντες 5 λεπτά για την άσκηση αυτή. Στη συνέχεια, ζητήστε από τους συμμετέχοντες να δείξουν τους κωδικούς πρόσβασης που δημιούργησαν. Και πάλι, υπενθυμίστε στους συμμετέχοντες ότι δεν θα κρατήσετε τα χαρτιά με τους κωδικούς πρόσβασης στο τέλος της δραστηριότητας και ότι δεν θα πρέπει να χρησιμοποιήσουν αυτούς τους κωδικούς πρόσβασης σε κανέναν λογαριασμό τους.

Ενημερώστε τους μαθητές σας

Ορισμένοι ιστότοποι χρησιμοποιούν ένα σύστημα που ονομάζεται έλεγχος ταυτότητας πολλαπλών παραγόντων (ή δύο παραγόντων) για την επαλήθευση της ταυτότητάς σας. Αυτοί οι ιστότοποι χρησιμοποιούν συχνά μηνύματα κειμένου, μια εφαρμογή ή ένα email για να στείλουν έναν κωδικό μίας χρήσης που πρέπει να εισαχθεί μαζί με τον κωδικό πρόσβασης.

Με αυτή τη μέθοδο, οι λογαριασμοί σας είναι πολύ πιο ασφαλείς, καθώς προστίθεται ένα επιπλέον επίπεδο ασφάλειας που είναι πολύ πιο δύσκολο να παραβιαστεί. Για

παράδειγμα, για να συνδεθεί κάποιος στο λογαριασμό σας, πρέπει να έχει τον κωδικό πρόσβασής σας και να ανοίξει την εφαρμογή, τη συσκευή ή τη διεύθυνση email που σχετίζεται με το λογαριασμό.

Προστασία των κωδικών πρόσβασης

Μέρος πρώτο

Ενημερώστε τους μαθητές σας

Ακόμα κι αν δημιουργήσετε έναν κωδικό που δύσκολα θα τον παραβιάσει κάποιος υπολογιστής ή άνθρωπος, ο κωδικός πρόσβασης μπορεί να είναι ασθενής για άλλους λόγους.

Ρωτήστε τους μαθητές σας

Πώς αλλιώς μπορεί να είναι ασθενής ένας κωδικός πρόσβασης;

1. Μερικά ενδεικτικά παραδείγματα είναι τα εξής: επαναχρησιμοποίηση κωδικού πρόσβασης για πολλούς λογαριασμούς, χρήση κωδικού πρόσβασης που περιέχει προσωπικές πληροφορίες, χρήση του ίδιου κωδικού πρόσβασης για πολλά χρόνια, απώλεια του κωδικού πρόσβασης.

Πόσο συχνά νομίζετε ότι πρέπει να αλλάζετε τους κωδικούς σας;

Ενημερώστε τους μαθητές σας

Ακόμη και οι ισχυροί κωδικοί πρόσβασης μπορούν να παραβιαστούν ή να υποκλαπούν, μπορείτε όμως να προστατευτείτε. Αν έχει γίνει παραβίαση δεδομένων σε έναν ιστότοπο όπου έχετε λογαριασμό, αλλάξτε τον κωδικό σας εκεί και σε κάθε άλλον ιστότοπο όπου χρησιμοποιείτε παρόμοιους κωδικούς πρόσβασης.

Η απομνημόνευση πολλών και πολύπλοκων κωδικών πρόσβασης μπορεί να είναι δύσκολη.

Ρωτήστε τους μαθητές σας

Θεωρείτε καλή ιδέα να σημειώνετε τους κωδικούς σας σε κάποιο χαρτί ή σε ένα αρχείο στον υπολογιστή σας; Γιατί ή γιατί όχι;

Αλληλεπίδραση στην τάξη

Αναφέρετε πιθανά σενάρια, π.χ. κάποιος μπορεί να βρει το χαρτί όπου σημειώσατε τους κωδικούς ή να δει το αρχείο στον υπολογιστή σας. Εξηγήστε ότι μια προσέγγιση είναι η χρήση μιας εφαρμογής διαχείρισης κωδικών πρόσβασης, δηλ. μιας εφαρμογής για την αποθήκευση και οργάνωση των κωδικών πρόσβασης.

Μέρος δεύτερο

Ενημερώστε τους μαθητές σας

Καθημερινά χρησιμοποιούμε διάφορους λογαριασμούς σε διάφορους ιστότοπους. Η σύνδεση και αποσύνδεση σε κάθε ιστότοπο κάθε φορά μπορεί να είναι περίπλοκη.

Ρωτήστε τους μαθητές σας

Έχετε χρησιμοποιήσει ποτέ τη λειτουργία αποθήκευσης κωδικού πρόσβασης στο πρόγραμμα περιήγησής σας για να αποθηκεύσετε έναν κωδικό πρόσβασης σε κάποιον ιστότοπο; Γιατί ή γιατί όχι;

Καταλαβαίνετε με ποιον τρόπο θυμάται ο ιστότοπος ποιοι είστε;

1. Ζητήστε εξηγήσεις. Στη συνέχεια, εξηγήστε ότι οι ιστότοποι μπορούν να θυμούνται ότι έχετε συνδεθεί αποθηκεύοντας ένα cookie. Τα cookies είναι μικρά αρχεία που αποθηκεύονται στον υπολογιστή σας ώστε ο ιστότοπος να αναγνωρίζει εσάς και τον υπολογιστή σας σε μελλοντικές επισκέψεις, χωρίς να συνδεθείτε ξανά. Ωστόσο, τα cookies μπορούν επίσης να χρησιμοποιηθούν για να παρακολουθούν την περιήγησή σας στους διάφορους ιστότοπους. Αυτός είναι και ένας από τους τρόπους που μπορούν να σας στοχεύουν οι διαφημίσεις.

Είναι σωστό να αποθηκεύετε τους κωδικούς πρόσβασης στον δικό σας υπολογιστή;

Ρωτήστε τους μαθητές σας

Ο υπολογιστής σας έχει κωδικό πρόσβασης;

Τι γίνεται αν μοιράζεστε τον υπολογιστή με άλλους;

1. Σε αυτή την περίπτωση, ακόμα και αν ο κωδικός πρόσβασης στο αντίστοιχο πεδίο κρύβεται με κουκκίδες ή αστερίσκους, όσοι χρησιμοποιούν τον υπολογιστή σας ενδέχεται να καταλάβουν ποιος είναι ο κωδικός. Ακόμα και αν δεν φαίνεται ο κωδικός πρόσβασης στην οθόνη, δεν σημαίνει ότι δεν αποθηκεύεται κάπου.

Ρωτήστε τους μαθητές σας

Υπάρχουν περιπτώσεις που είναι εντάξει να μοιραστείτε έναν κωδικό πρόσβασης; Πότε; Γιατί;

1. Ένα παράδειγμα είναι να ζητήσουν τους κωδικούς τους οι γονείς τους ή να υπάρχει κοινός/οικογενειακός λογαριασμός σε υπηρεσίες όπως το Netflix.

Μοιράζεστε τους κωδικούς σας με άλλους; Αν ναι, με ποιον/γιατί;

Αν κάποιος στενός φίλος σας έπαιζε το χαρτί της εμπιστοσύνης, θα δίνετε τον κωδικό σας; Γιατί ή γιατί όχι;

Ενημερώστε τους μαθητές σας

Είστε ελεύθεροι να επιλέξετε αν θα μοιραστείτε τον κωδικό σας με κάποιον που εμπιστεύεστε, αυτό όμως δεν σημαίνει απαραίτητα ότι αξίζει να έχει πλήρη πρόσβαση στους λογαριασμούς σας.

Σκεφτείτε προσεκτικά τη σχέση σας με το εν λόγω άτομο πριν δώσετε τον κωδικό σας, καθώς και πώς αυτή η σχέση μπορεί να αλλάξει με το χρόνο. Για παράδειγμα, άλλο είναι να δώσετε τον κωδικό σας στους γονείς σας ή στα άτομα που σας φροντίζουν και άλλο στον καλύτερο σας φίλο.

Ρωτήστε τους μαθητές σας

Τι μπορεί να σας συμβεί αν μοιραστείτε έναν κωδικό πρόσβασης;

1. Κάποιος μπορεί να χακάρει τους τραπεζικούς λογαριασμούς σας, να σας παραστήσει στο διαδίκτυο ή να μάθει κάποια από τα μυστικά σας.

Αν κοινοποιούσατε τον κωδικό πρόσβασης ενός λογαριασμού, θα χρησιμοποιούσατε διαφορετικά το λογαριασμό;

Ρωτήστε τους μαθητές σας

Αν κάποιος μπορούσε να δει τι κάνετε, θα βλέπατε κάποια πράγματα στο Netflix ή θα τα γράφατε σε email;

Αλληλεπίδραση στην τάξη

Οι συμμετέχοντες πρέπει να σκεφτούν τη συμπεριφορά τους όταν χρησιμοποιούν έναν κοινόχρηστο λογαριασμό. Θα πρέπει να σκεφτούν ότι η διαδικτυακή τους δραστηριότητα θα είναι σε κοινή θέα από τους άλλους χρήστες του λογαριασμού.

Ρωτήστε τους μαθητές σας

Αν ο λογαριασμός σας αποτελεί μια εικονική αναπαράστασή σας, π.χ. είναι προφίλ σε κάποιο μέσο κοινωνικής δικτύωσης, είναι εντάξει να επιτρέπετε σε τρίτους να χρησιμοποιούν το λογαριασμό σας;

Αλληλεπίδραση στην τάξη

Συζητήστε την πιθανότητα κάποιος να προσποιηθεί ότι είστε εσείς για να στείλει μηνύματα στους φίλους σας.

Ρωτήστε τους μαθητές σας

Επιτρέψτε στις συσκευές που χρησιμοποιείτε να αποθηκεύουν τους κωδικούς σας; Γιατί ή γιατί όχι; Αυτό σημαίνει ότι είναι ασφαλές να αποθηκεύετε τους κωδικούς σας στο κινητό ή στον υπολογιστή σας; Τι θα συμβεί αν επιτρέψετε σε κάποιον φίλο να δανειστεί το κινητό ή τον υπολογιστή σας;

Μοιράζετε συσκευές με άλλους, όπως συγγενείς ή φίλους; Μοιράζετε τον ίδιο λογαριασμό σε αυτές τις συσκευές ή έχει ο καθένας τον δικό του λογαριασμό;

Χρησιμοποιείτε ποτέ "δημόσιες" συσκευές, όπως συσκευές στη βιβλιοθήκη, στο σχολείο ή κάπου αλλού; Κάνετε τα ίδια στις συσκευές αυτές όπως και αλλού;

Μέρος τρίτο

Αλληλεπίδραση στην τάξη

Χωρίστε τους συμμετέχοντες σε ζευγάρια.

Ενημερώστε τους μαθητές σας

Σε ζευγάρια, συζητήστε αν έχετε ποτέ συνδεθεί σε κάποιον υπολογιστή στο σχολείο, στη βιβλιοθήκη ή σε άλλο δημόσιο χώρο και έτυχε να δείτε ότι κάποιος άλλος ήταν ακόμα συνδεδεμένος στο λογαριασμό του κοινωνικής δικτύωσης ή στο email του. Ζητήστε τους να σκεφτούν αν θα περιεργάζονταν το λογαριασμό ή αν θα έκαναν κάτι άλλο.

Αλληλεπίδραση στην τάξη

Δώστε στους συμμετέχοντες 5 λεπτά για να συζητήσουν, έπειτα ζητήστε τους να μοιραστούν τις απόψεις τους. Συζητήστε με την ομάδα για το ενδεχόμενο χρήσης χωρίς εξουσιοδότηση.

Πρόσβαση σε λογαριασμό χωρίς εξουσιοδότηση

Μέρος πρώτο

Αλληλεπίδραση στην τάξη

Σημείωση: Μέρος του περιεχομένου αυτής της δραστηριότητας έχει καλυφθεί στην ενότητα "Δραστηριότητα 1: Βασικές πληροφορίες για τους κωδικούς πρόσβασης". Το αν επιθυμείτε ή όχι να αναλύσετε ξανά αυτό το υλικό ή να το προσπεράσετε, το αφήνουμε στην κρίση σας.

Ενημερώστε τους μαθητές σας

Η πρόσβαση στο λογαριασμό σας από τρίτους μπορεί να γίνει ακόμη και χωρίς να γνωρίζουν ήδη τον κωδικό σας ή να τον μαντέψουν τυχαία. Αν κάποιος γνωρίζει αρκετές προσωπικές πληροφορίες για εσάς, μπορεί να μαντέψει τον κωδικό σας ή να πείσει κάποιον από μια εταιρεία να του δώσει πληροφορίες σας. Επειδή δεν γίνεται χρήση της τεχνολογίας για την παραβίαση των λογαριασμών σας, αυτό το είδος επίθεσης ονομάζεται κοινωνικό χάκινγκ ή κοινωνική μηχανική.

Ρωτήστε τους μαθητές σας

Σηκώστε το χέρι σας αν έχετε ξεχάσει ποτέ τον κωδικό σας σε κάποιον ιστότοπο.

Τι συμβαίνει όταν κάνετε κλικ στην επιλογή "Ξέχασα τον κωδικό μου";

1. Ο ιστότοπος συνήθως σας ζητά να απαντήσετε σε ερωτήσεις ασφαλείας ή επιχειρεί να επικοινωνήσει μαζί σας χρησιμοποιώντας έναν αριθμό τηλεφώνου ή μια διεύθυνση email.

Ποιες είναι οι ερωτήσεις ασφαλείας που ζητάει ο ιστότοπος;

1. Εξηγήστε πώς ορισμένες από αυτές τις ερωτήσεις είναι ερωτήσεις που θα μπορούσαν να απαντήσουν ή να μαντέψουν φίλοι ή γνωστοί. Στοιχεία όπως το όνομα του κατοικίδιού τους, ο τόπος γέννησης, το πατρικό όνομα της μητέρας τους, το όνομα του αγαπημένου τους δάσκαλου, το όνομα του καλύτερου φίλου τους, το όνομα της αγαπημένης τους ομάδας.

Ποιος άλλος μπορεί να γνωρίζει αυτές τις πληροφορίες για το άτομό σας;

Πώς μπορεί να επικοινωνήσει μαζί σας κάποιος ιστότοπος αν ξεχάσετε κάποιον κωδικό πρόσβασης;

Ποιος άλλος μπορεί να έχει πρόσβαση στα σημεία επαφής σας;

Ρωτήστε τους μαθητές σας

Πώς μπορεί να μάθει ένας άγνωστος τις προσωπικές πληροφορίες που σχετίζονται με τις απαντήσεις σας σε ερωτήσεις ασφαλείας;

1. Δημοσιεύσεις σε μέσα κοινωνικής δικτύωσης, αναζητήσεις στο διαδίκτυο για δημόσιες πληροφορίες, πολλαπλές απόπειρες μαντέματος, επικοινωνία με τους φίλους σας κ.λπ.

Ποια είναι μερικά παραδείγματα δημοσιεύσεων σε μέσα κοινωνικής δικτύωσης με προσωπικές πληροφορίες;

1. Για παράδειγμα, μια φωτογραφία της γάτας σας στο Instagram με το όνομά της στη λεζάντα, μια φωτογραφία όπου έχει προστεθεί με ετικέτα η τοποθεσία σας ή δημόσιες αναρτήσεις για τα γενέθλιά σας.

Πώς μπορείτε να χρησιμοποιήσετε το Google για να βρείτε περισσότερες πληροφορίες για κάποιον και να χακάρετε τον κωδικό πρόσβασής του;

1. Αν μια μηχανή αναζήτησης δείχνει στα αποτελέσματα τη φωτογραφία τρίτης λυκείου κάποιου που είχε δημοσιευθεί σε μια διαδικτυακή σχολική εφημερίδα, μπορείτε να μάθετε το όνομα του καθηγητή του.

Μέρος δεύτερο

Ενημερώστε τους μαθητές σας

Η δημοσίευση πληροφοριών που περιέχουν τις απαντήσεις στις ερωτήσεις ασφαλείας σας μπορεί να είναι πολύ επικίνδυνη. Βεβαιωθείτε ότι έχετε επιλέξει ερωτήσεις ασφαλείας με απαντήσεις που γνωρίζετε μόνο εσείς. Μπορείτε επίσης να βρείτε φανταστικές απαντήσεις σε ερωτήσεις ασφαλείας, αρκεί να τις αποθηκεύσετε σε μια εφαρμογή διαχείρισης κωδικών πρόσβασης ή να είναι εύκολες για να τις θυμάστε.

Ένας ιστότοπος μπορεί να επικοινωνήσει με ένα χρήστη χρησιμοποιώντας τον αριθμό τηλεφώνου ή τη διεύθυνση email που σχετίζεται με το λογαριασμό του. Σε περίπτωση που κάποιος ξεχάσει τον κωδικό του, οι ιστότοποι συχνά δίνουν έναν προσωρινό κωδικό πρόσβασης ή ένα σύνδεσμο για επαναφορά του κωδικού πρόσβασης.

Ρωτήστε τους μαθητές σας

Αρκεί αυτή η μέθοδος για να διασφαλιστεί ότι αυτός που ζητάει τον νέο κωδικό πρόσβασης είναι ο χρήστης;

Τι γίνεται αν μοιράζεστε τη διεύθυνση email που σχετίζεται με το λογαριασμό;

1. Η μέθοδος επαναφοράς του κωδικού πρόσβασης μέσω συνδέσμου είναι ασφαλής τις περισσότερες φορές, αν όμως μοιράζεστε το λογαριασμό ή τον κωδικό πρόσβασης, είστε εκτεθειμένοι σε κίνδυνο.

Ενημερώστε τους μαθητές σας

Το κοινωνικό χάκινγκ είναι μια μέθοδος όπου κάποιος επικοινωνεί απευθείας μαζί σας και προσπαθεί να σας εξαπατήσει για να του δώσετε τις πληροφορίες σας. Μπορεί να λάβετε email από ένα άτομο που προσποιείται ότι είναι κάποιος άλλος (π.χ. φίλος, συγγενής ή υπάλληλος τράπεζας) και σας ζητάει να του δώσετε σημαντικές πληροφορίες (π.χ. την ημερομηνία γέννησής σας) προκειμένου να επαληθεύσετε την ταυτότητά σας. Αυτό μπορεί να μην είναι τόσο άμεσο, π.χ. κάποιος μπορεί να χακάρει το λογαριασμό ενός φίλου σας σε ένα μέσο κοινωνικής δικτύωσης και να σας στείλει μηνύματα (και πιθανώς σε πολλούς άλλους) ρωτώντας σας για τα γενέθλιά σας ή πού μεγαλώσατε. Αν λάβετε μηνύματα που θεωρείται περίεργα από κάποιον φίλο σας, ρωτήστε τον πρώτα (εκτός της πλατφόρμας κοινωνικής δικτύωσης) για να επιβεβαιώσετε αν όντως σας έχει στείλει τα μηνύματα.

Οι επιθέσεις που χρησιμοποιούν ένα νομιμοφανές email ή ιστότοπο ονομάζονται "ηλεκτρονικό ψάρεμα" και μπορούν να οδηγήσουν σε κλοπή ταυτότητας. Για παράδειγμα, ένας κλέφτης ταυτότητας μπορεί να εκδώσει πιστωτικές κάρτες στο όνομά σας και να τις χρησιμοποιήσει, με αποτέλεσμα να αντιμετωπίσετε ενδεχομένως δυσκολίες όταν αργότερα θελήσετε να αποκτήσετε πιστωτική κάρτα.

Μέσω του ηλεκτρονικού ψαρέματος, ο κλέφτης μπορεί να σας υποδυθεί για να αποκτήσει πρόσβαση σε περισσότερες πληροφορίες και να εισβάλει στα email σας, να στείλει μηνύματα στους φίλους σας υποκρινόμενος ότι είστε εσείς ή να κλέψει τα χρήματά σας. Με αυτή τη διαδικασία, ο κλέφτης θα μπορούσε επίσης να σας αποκλείσει από το λογαριασμό σας δημιουργώντας έναν νέο κωδικό πρόσβασης που δεν θα γνωρίζετε.

Άσκηση

Έντυπο υλικό

Άσκηση

Ζητήστε από τους συμμετέχοντες να απαντήσουν στις ακόλουθες ερωτήσεις και να προσθέσουν τις απαντήσεις τους με τη μορφή κειμένου ή γραφικών στο φυλλάδιο "Μαθαίνουμε για τους κωδικούς πρόσβασης".

1. Ποιες τρεις πληροφορίες που αποκομίσατε από αυτό το μάθημα θα εφαρμόσετε την επόμενη φορά που θα χρειαστεί να δημιουργήσετε κωδικό πρόσβασης;
2. Σε ποια περίπτωση πιστεύετε ότι είναι εντάξει να μοιραστείτε τον κωδικό πρόσβασής σας με κάποιον άλλο;
3. Ποιες τρεις στρατηγικές μπορείτε να χρησιμοποιήσετε για να μοιραστείτε με ασφάλεια τον κωδικό πρόσβασής σας με κάποιον άλλο;
4. Μπορείτε να σκεφτείτε τρία παραδείγματα για το τι μπορεί να πάει στραβά αν ένας κωδικός πρόσβασης πέσει σε λάθος χέρια;