

Κυβερνοασφάλεια, ηλεκτρονικό ψάρεμα και σπαμ

Οι συμμετέχοντες θα μάθουν για τους κακόβουλους διαδικτυακούς χρήστες που μπορεί να προσπαθήσουν να εκμεταλλευτούν αδύναμα σημεία στην ασφάλεια για να συλλέξουν προσωπικές πληροφορίες. Οι συμμετέχοντες θα μπορούν να περιγράψουν τους κινδύνους χρήσης του διαδικτύου, να αναπτύξουν στρατηγικές ώστε να υιοθετήσουν πιο ασφαλείς συμπεριφορές, να αναγνωρίζουν τα μηνύματα σπαμ και να εξηγούν ποιος είναι αποδεκτό να ζητά τους προσωπικούς τους κωδικούς πρόσβασης.

Υλικά

Φυλλάδιο για το σπαμ

Οι κίνδυνοι στο διαδίκτυο

Μέρος πρώτο

Ενημερώστε τους μαθητές σας

Όταν χρησιμοποιείτε το Internet, μπορεί να εκτεθείτε σε κινδύνους απλώς επισκεπτόμενοι μια ιστοσελίδα, επικοινωνώντας online ή κατεβάζοντας δεδομένα. Ορισμένες φορές, οι ιστότοποι που επισκέπτεστε, άλλα άτομα στο ίδιο δίκτυο ή ακόμα και τρίτοι μπορούν να βρουν την τοποθεσία σας ή άλλες πληροφορίες για το άτομό σας ενώ εσείς περιηγείστε.

Ρωτήστε τους μαθητές σας

Ποιος μπορεί να επωφεληθεί από τα τρωτά σημεία της διαδικτυακής ασφάλειας για να δει τις προσωπικές σας πληροφορίες;

1. Οι πιθανές απαντήσεις περιλαμβάνουν κακόβουλους χάκερς, κυβερνητική παρακολούθηση κ.λπ.

Ενημερώστε τους μαθητές σας

Όταν περιηγείστε στο διαδίκτυο, κακόβουλοι χάκερς μπορεί να προσπαθήσουν να συλλέξουν δεδομένα για το άτομό σας, όπως ακριβώς κάνουν οι πάροχοι υπηρεσιών Internet. Για να μειώσετε αυτόν τον κίνδυνο, πρέπει να χρησιμοποιείτε ασφαλή σύνδεση για να συνδέεστε στους ιστότοπους που προσπαθείτε να προσπελάσετε. Ανεξάρτητα από τη σύνδεσή σας, πολλοί ιστότοποι προσπαθούν να ανιχνεύσουν τα μοτίβα χρήσης σας σε πολλές διαφορετικές πλατφόρμες. Μπορούν να παρακολουθούν το πρόγραμμα περιήγησής σας, την τοποθεσία σας και άλλα μοτίβα χρήσης για να μάθουν πληροφορίες για το άτομό σας.

Ρωτήστε τους μαθητές σας

Γιατί μπορεί κακόβουλοι χάκερς να προσπαθήσουν να αποκτήσουν πρόσβαση στα δεδομένα σας μέσω διαδικτύου; Τι είδους πληροφορίες ψάχνουν; Γιατί ένας ιστότοπος στον οποίο δεν είστε συνδεδεμένοι μπορεί να θέλει να παρακολουθεί ποιος είστε;

1. Οποιαδήποτε πληροφορία ταυτοποίησης ή στοιχείο μπορεί να πωληθεί ή να χρησιμοποιηθεί για κέρδος.

Γνωρίζει κανείς τι είναι το κακόβουλο λογισμικό; Τι μπορεί να κάνει;

Ενημερώστε τους μαθητές σας

Το κακόβουλο λογισμικό είναι ένας επιβλαβής κώδικας που εκτελείται κρυφά στον υπολογιστή σας. Ορισμένα κακόβουλα προγράμματα μπορούν να συλλέξουν δεδομένα από οποιοδήποτε τμήμα του τοπικού υπολογιστή σας, από τον σκληρό δίσκο έως το πρόγραμμα περιήγησής σας. Μπορούν επίσης να επιτρέψουν σε χάκερς να πάρουν τον έλεγχο του υπολογιστή σας και να τον χρησιμοποιήσουν με οποιονδήποτε τρόπο θέλουν. Όμως, οι περισσότερες εφαρμογές κακόβουλου λογισμικού είναι πιο απλές, όπως ιστότοποι που μιμούνται ασφαλείς πύλες, για παράδειγμα τράπεζες, ή επεκτάσεις που βάζουν διαφημίσεις στο πρόγραμμα περιήγησής σας με σκοπό το κέρδος.

Ρωτήστε τους μαθητές σας

Τι μπορείτε να κάνετε για να προστατευθείτε από το κακόβουλο λογισμικό, την κατασκοπία και την παρακολούθηση;

Ενημερώστε τους μαθητές σας

Να είστε προσεκτικοί όταν κάνετε κλικ σε συνδέσμους, διαφημίσεις ή δημοσιεύσεις μέσω κοινωνικής δικτύωσης. Η διεύθυνση URL σάς οδηγεί στη σελίδα που περιμένατε; Οδηγείστε στην ίδια σελίδα όταν πληκτρολογείτε μόνοι σας τη διεύθυνση ή όταν κάνετε αναζήτηση του ιστότοπου; Κατά κανόνα, το SSL/TLS προστατεύει οποιαδήποτε σελίδα σύνδεσης σε έναν σημαντικό λογαριασμό (όπως λογαριασμούς στο Google, το Facebook, το Twitter ή τραπεζικούς λογαριασμούς). Με το SSL/TLS είναι πολύ δύσκολο για ένα χάκερ στο ίδιο δίκτυο να σας στείλει σε έναν ψεύτικο ιστότοπο όταν εσείς πληκτρολογείτε τη σωστή διεύθυνση URL, κάτι που διαφορετικά θα ήταν πολύ εύκολο.

Κάποιοι ιστότοποι εκτελούν κώδικα για να αποκτήσουν πρόσβαση στις προσωπικές πληροφορίες σας ή στους διαδικτυακούς λογαριασμούς σας, αν υπάρχει σφάλμα κωδικοποίησης σε αυτές τις πλατφόρμες. Μετά, μέσω του λογαριασμού σας μπορούν να σπαμάρουν άλλους.

Φροντίστε να κατεβάζετε και να εγκαθιστάτε λογισμικό μόνο από αξιόπιστες πηγές και να είστε προσεκτικοί όταν κατεβάζετε εκτελέσιμα αρχεία (επεκτάσεις .exe, .pkg, .sh, .dll ή .dmg). Τα εκτελέσιμα είναι οτιδήποτε μπορεί να εκτελέσει μια ενέργεια. Ορισμένες φορές, μπορεί να είναι κακόβουλες ενέργειες. Για παράδειγμα, κάποιος μπορεί να γράψει ένα εκτελέσιμο κείμενο για να διαγράψει τον σκληρό δίσκο ενός χρήστη ή να εγκαταστήσει ένα ψεύτικο πρόγραμμα περιήγησης. Γι' αυτόν το λόγο, πρέπει να εγκαθιστάτε περιεχόμενο μόνο από αξιόπιστες πηγές.

Μπορείτε να χρησιμοποιήσετε λογισμικό προστασίας από ιούς για να προστατευτείτε από την εκτέλεση κακόβουλου λογισμικού. Ορισμένα προγράμματα προστασίας από ιούς παρέχονται εγκατεστημένα στον υπολογιστή σας (π.χ. το Microsoft Security Essentials για Windows), ενώ κάποια λειτουργικά συστήματα, όπως αυτά στους υπολογιστές Apple, έχουν ρυθμίσεις ασφάλειας που εμποδίζουν την εγκατάσταση λογισμικού από αναξιόπιστες πηγές. Σκεφτείτε προσεκτικά πριν αποφασίσετε να παρακάμψετε αυτές τις ρυθμίσεις.

Μπορείτε επίσης να εξετάσετε το ενδεχόμενο να χρησιμοποιήσετε επεκτάσεις προγραμμάτων περιήγησης που μπορούν, για παράδειγμα, να μπλοκάρουν τα πρόσθετα, με αποτέλεσμα να είναι δύσκολο οι ιστότοποι να μάθουν ποιος είστε ή να σας παρακολουθούν. Το ίδιο πρόσθετο, ωστόσο, μπορεί να μπλοκάρει κάποιες λειτουργίες ιστότοπων, όπως τη δυνατότητα αναπαραγωγής βίντεο. Το αν θα αποφασίσετε ή όχι να εγκαταστήσετε επεκτάσεις προγραμμάτων περιήγησης εξαρτάται από τις προτιμήσεις σας και το τι συμβιβασμούς είστε πρόθυμοι να κάνετε όσον αφορά την ασφάλεια στο διαδίκτυο. Μπορείτε να αναρωτηθείτε τα εξής: Πόσο πρόβλημα θα δημιουργήσει τυχόν παρακολούθηση του λογαριασμού μου; Πόσο αξίζει η διαφύλαξη του απορρήτου μου; Πόσο σημαντικό είναι να δω αυτό το περιεχόμενο (αν, για παράδειγμα, η επέκταση του προγράμματος περιήγησης μπλοκάρει κάποιο πρόσθετο που παίζει βίντεο);

Εργαλεία ασφάλειας

Μέρος πρώτο

Αλληλεπίδραση στην τάξη

Σημείωση: Μέρος του περιεχομένου αυτής της δραστηριότητας έχει καλυφθεί στην ενότητα "Δραστηριότητα 1: Οι κίνδυνοι στο διαδίκτυο". Σε περίπτωση που έχετε ήδη ολοκληρώσει τη Δραστηριότητα 1, εναπόκειται στην κρίση σας αν θα επαναλάβετε αυτό το υλικό ή όχι.

Ρωτήστε τους μαθητές σας

Γνωρίζετε κατά πόσο είστε ασφαλείς όταν χρησιμοποιείτε το διαδίκτυο;

Ενημερώστε τους μαθητές σας

Χωρίς τις κατάλληλες προφυλάξεις, είναι δύσκολο, αν όχι αδύνατο, να προστατευτείτε επιτυχώς από τους κινδύνους του διαδικτύου (αυτούς που περιγράφηκαν στην προηγούμενη ενότητα).

Μάλιστα, διαρκώς παρουσιάζονται νέες διαδικτυακές απειλές, και γι' αυτό είναι σημαντικό να είστε πάντα σε επιφυλακή.

Ρωτήστε τους μαθητές σας

Τι θα μπορούσε να κάνει κάποιος αν σας έπειθε ότι ο ιστότοπός του είναι αξιόπιστος και σοβαρός;

Υπάρχουν εργαλεία που μπορείτε να χρησιμοποιήσετε ώστε να αποφύγετε ή να μειώσετε αυτούς τους κινδύνους. Γνωρίζει κανείς κάποιος;

Ενημερώστε τους μαθητές σας

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. Υπάρχουν εργαλεία λογισμικού που διασφαλίζουν τη χρήση του πρωτοκόλλου HTTPS όποτε είναι δυνατό.
3. Τα περισσότερα δημοφιλή προγράμματα περιήγησης έχουν, κοντά στη γραμμή διευθύνσεων, δείκτες ασφάλειας που μοιάζουν με λουκέτα οι οποίοι υποδεικνύουν τη χρήση σύνδεσης HTTPS.
4. 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.

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 στέλνате 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. 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 (δείτε το παράδειγμα στην παρακάτω εικόνα). 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". [Ίσως 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".

Το λογισμικό προστασίας από ιούς, εκτός από το να σας αποτρέψει να εκτελέσετε λογισμικό από αναξιόπιστες πηγές, μπορεί να σας αποτρέψει να επισκεφτείτε αναξιόπιστες σελίδες και να κατεβάσετε κακόβουλο λογισμικό.

Το λεγόμενο "ηλεκτρονικό ψάρεμα" γίνεται κυρίως μέσω email από κάποιον σπάμερ που προσποιείται ότι είναι αξιόπιστος χρήστης. Στη συνέχεια, το άτομο αυτό σας ζητάει τον κωδικό πρόσβασής σας, με την ελπίδα ότι θα τον στείλετε μέσω email ή θα τον καταχωρήσετε σε έναν ψεύτικο ιστότοπο. Τα φίλτρα σπαμ μπορούν να αποτρέψουν να εμφανίζονται τέτοια email στα εισερχόμενά σας. Για να κάνετε τα φίλτρα σπαμ πιο ισχυρά, φροντίστε να επισημαίνετε τυχόν ύποπτα email που καταλήγουν στα εισερχόμενά σας ως σπαμ.

Ρωτήστε τους μαθητές σας

Σε τι ενέργειες μπορείτε να προβείτε ώστε να προστατευτείτε από την ακούσια λήψη αρχείων που είναι επιβλαβή για τον υπολογιστή σας;

Ενημερώστε τους μαθητές σας

Φροντίστε να ελέγχετε πάντα ότι κατεβάζετε περιεχόμενο από αξιόπιστους ιστότοπους. Να είστε εξαιρετικά προσεκτικοί και να μην ανοίγετε συνημμένα email που δεν αναγνωρίζετε ούτε να κάνετε κλικ σε αναδυόμενα παράθυρα και μηνύματα σφάλματος. Εξετάστε επίσης το ενδεχόμενο να εγκαταστήσετε στον υπολογιστή σας γνωστά προγράμματα προστασίας από κακόβουλο λογισμικό.

Κοινοποίηση κωδικών πρόσβασης

Μέρος πρώτο

Ρωτήστε τους μαθητές σας

Πότε πιστεύετε ότι είναι εντάξει να κοινοποιήσετε τον κωδικό πρόσβασής σας;

1. Οι πιθανές απαντήσεις περιλαμβάνουν κοινόχρηστους λογαριασμούς (π.χ. στο Netflix).

Ποιοι είναι οι πιθανοί κίνδυνοι που σχετίζονται με την κοινοποίηση του κωδικού πρόσβασής σας;

1. Αν κάποιο κακόβολο άτομο αποκτήσει τον κωδικό πρόσβασής σας, τότε μπορεί να παραβιάσει το λογαριασμό σας. Όταν κοινοποιείτε τον κωδικό σας, αυξάνονται οι πιθανότητες να αποκτήσει κάποιος πρόσβαση στο λογαριασμό σας. Αν χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης και σε άλλους ιστότοπους, τότε το άτομο αυτό μπορεί να αποκτήσει πρόσβαση στους λογαριασμούς σας και σε αυτούς τους ιστότοπους.

Ενημερώστε τους μαθητές σας

Ως πάγια πρακτική, δεν πρέπει να κοινοποιείτε τους κωδικούς σας σε κανέναν, παρά μόνο στην εκάστοτε εφαρμογή στην οποία θέλετε να συνδεθείτε. Όπως περιγράφηκε παραπάνω, το ηλεκτρονικό ψάρεμα είναι μια μέθοδος με την οποία ορισμένοι προσπαθούν να σας ξεγελάσουν ώστε να κοινοποιήσετε τον κωδικό πρόσβασής σας.

Κάποιοι, ωστόσο, μπορεί να ζητήσουν ευθέως τον κωδικό σας, ισχυριζόμενοι ότι ίσως απειλείται η ασφάλεια του λογαριασμού σας. Αν και ορισμένα από αυτά τα άτομα μπορεί να έχουν καλές προθέσεις, όπως ένας φίλος που θέλει να σας βοηθήσει να ελέγξετε κάτι στο λογαριασμό σας το οποίο σας μπερδεύει, δεν είναι φρόνιμο να κοινοποιήσετε τον κωδικό πρόσβασής σας, ιδίως αν τον χρησιμοποιείτε για πολλούς λογαριασμούς. Αν σκοπεύετε να κοινοποιήσετε έναν κωδικό πρόσβασης, βεβαιωθείτε ότι δεν χρησιμοποιείται πουθενά αλλού και κοινοποιήστε τον μέσω ενός προγράμματος διαχείρισης κωδικών πρόσβασης.

Ορισμένες φορές, τα άτομα που ζητούν τον κωδικό πρόσβασής σας μπορεί να είναι ενήλικοι που γνωρίζετε και εμπιστεύεστε, όπως οι γονείς σας, ο δάσκαλός σας ή ο εργοδότης σας. Παρόλο που γνωρίζετε και εμπιστεύεστε αυτούς τους ενήλικους, το σωστό για όλους (τόσο για εσάς όσο και για εκείνους) είναι να συζητηθεί ο λόγος που σας ζητούν τον κωδικό σας και πώς θα τον χρησιμοποιήσουν. Όταν μάλιστα πρόκειται για έναν ενήλικο εκτός της οικογένειάς σας, καλό είναι να ρωτήσετε ευθέως

αν υπάρχει κάποιος νόμος ή άλλου είδους κανονισμός που πιστεύει ότι σας υποχρεώνει να κοινοποιήσετε τον κωδικό σας.

Το να κάνετε ευγενικές και σαφείς ερωτήσεις όσον αφορά τους σχετικούς νόμους και κανονισμούς είναι ιδιαίτερα σημαντικό όταν ζητά τον κωδικό πρόσβασής σας κάποιος εκτός της οικογένειάς σας τον οποίο δεν γνωρίζετε προσωπικά, όπως ένα όργανο της τάξης. Αν ένας αστυνομικός ή άλλος κρατικός λειτουργός σας ζητήσει τους κωδικούς πρόσβασής σας στα μέσα κοινωνικής δικτύωσης, παραμείνετε ψύχραιμοι και ευγενικοί. Ρωτήστε για ποιον λόγο σας ζητούν τους κωδικούς σας και βάσει ποιου νόμου ή κανονισμού έχουν, κατά τη γνώμη τους, το δικαίωμα να λάβουν μια τέτοια πληροφορία.

Ανάλογα με την περίπτωση υπό την οποία ένας γονιός/κηδεμόνας, δάσκαλος, εργοδότης, όργανο της τάξης, κυβερνητικός λειτουργός ή άλλος ενήλικος σας το ζητήσει, μπορεί να πρέπει να του δώσετε τους κωδικούς πρόσβασής σας. Για παράδειγμα, θα πρέπει να δώσετε τους κωδικούς σας αν υπάρχει νόμος ή κανονισμός που το υπαγορεύει ή αν κρίνετε ότι το όφελος από τη βοήθεια που θα λάβετε υπερτερεί των κινδύνων κοινοποίησης.

Αν ένας ενήλικος σας ζητήσει τους κωδικούς πρόσβασής σας και το αίτημα αυτό σας κάνει να μην αισθάνεστε άνετα, απευθυνθείτε αμέσως στο γονέα/κηδεμόνα σας ή σε άλλον έμπιστο ενήλικο, ιδανικά πριν απαντήσετε στο αίτημα.

Ρωτήστε τους μαθητές σας

Σε ποιες περιπτώσεις πρέπει να κοινοποιείτε τους κωδικούς πρόσβασής σας στο διαδίκτυο;

1. Μόνο όταν σας ζητηθεί να καταχωρήσετε τον κωδικό πρόσβασής σας από τον ιστότοπο στον οποίο προσπαθείτε να αποκτήσετε πρόσβαση. Ποτέ μην κοινοποιείτε τον κωδικό σας πουθενά αλλού, συμπεριλαμβανομένου μέσω email, που συνήθως δεν είναι κρυπτογραφημένο ή ασφαλές.

Άσκηση

Έντυπο υλικό

Άσκηση

Χωρίστε τους συμμετέχοντες σε ομάδες των 2-3 ατόμων. Μοιράστε το φυλλάδιο για τους συμμετέχοντες με θέμα το σπαμ. Στη συνέχεια, ζητήστε από κάθε συμμετέχοντα να δημιουργήσει ένα διάγραμμα ροής που θα δείχνει πώς μπορεί κανείς να αναγνωρίζει τα μηνύματα σπαμ και αν πρέπει συγκεκριμένες πληροφορίες να κοινοποιούνται σε συγκεκριμένα άτομα ή ομάδες.

Ενημερώστε τους μαθητές σας

Διαβάστε καθένα από τα σενάρια και συζητήστε κατά πόσο τα αντίστοιχα μηνύματα είναι σπαμ και αν θα πρέπει να κοινοποιήσετε πληροφορίες στο άτομο ή στην ομάδα του σεναρίου.

Αλληλεπίδραση στην τάξη

Δώστε στους συμμετέχοντες 10 λεπτά για την άσκηση αυτή. Στη συνέχεια, ζητήστε από τις ομάδες να μοιραστούν τις απαντήσεις τους.

Ρωτήστε τους μαθητές σας

Πότε πρέπει να κοινοποιείτε τον κωδικό πρόσβασής σας μέσω email;

Ενημερώστε τους μαθητές σας

Οι ιστότοποι και οι εταιρείες έχουν ως πάγια πρακτική να μην ζητούν ποτέ τον κωδικό πρόσβασής σας μέσω email. Ποτέ μην γνωστοποιείτε τον κωδικό σας κατ'αυτόν τον τρόπο, ακόμα κι αν η πηγή μοιάζει αξιόπιστη. Το email δεν είναι σχεδόν ποτέ ασφαλές μέσο.

Μέρος δεύτερο

Άσκηση

Ζητήστε από τους συμμετέχοντες να επιστρέψουν από τις ομάδες τους, καθώς η επόμενη άσκηση είναι ατομική.

Δώστε στους συμμετέχοντες 15 λεπτά για να δημιουργήσουν τα διαγράμματα ροής τους.

Ενημερώστε τους μαθητές σας

Σε ένα φύλλο χαρτί, δημιουργήστε ένα διάγραμμα ροής για να δείξετε πώς μπορεί κανείς να αναγνωρίζει τα μηνύματα σπαμ και αν πρέπει κανείς να κοινοποιεί συγκεκριμένες πληροφορίες online σε άλλους. Ίσως βοηθήσει να βασίσετε το διάγραμμά σας σε ένα συγκεκριμένο σενάριο, είτε σε κάποιο από τα σενάρια που παρουσιάζονται στο φυλλάδιο (αν χρησιμοποιήσετε κάποιο από εκεί, σημειώστε τον αριθμό του σεναρίου πάνω από το διάγραμμά σας) είτε σε ένα εντελώς νέο σενάριο! Αν επιλέξετε να φτιάξετε το δικό σας σενάριο, δώστε μια σύντομη περιγραφή μίας παραγράφου πάνω από το διάγραμμά σας.

Δώστε στους συμμετέχοντες 15 λεπτά για να δημιουργήσουν τα διαγράμματα ροής τους.