RestartVET

RESTART VET:

An innovative approach to support VET teachers/trainers through the digital transformation of VET education

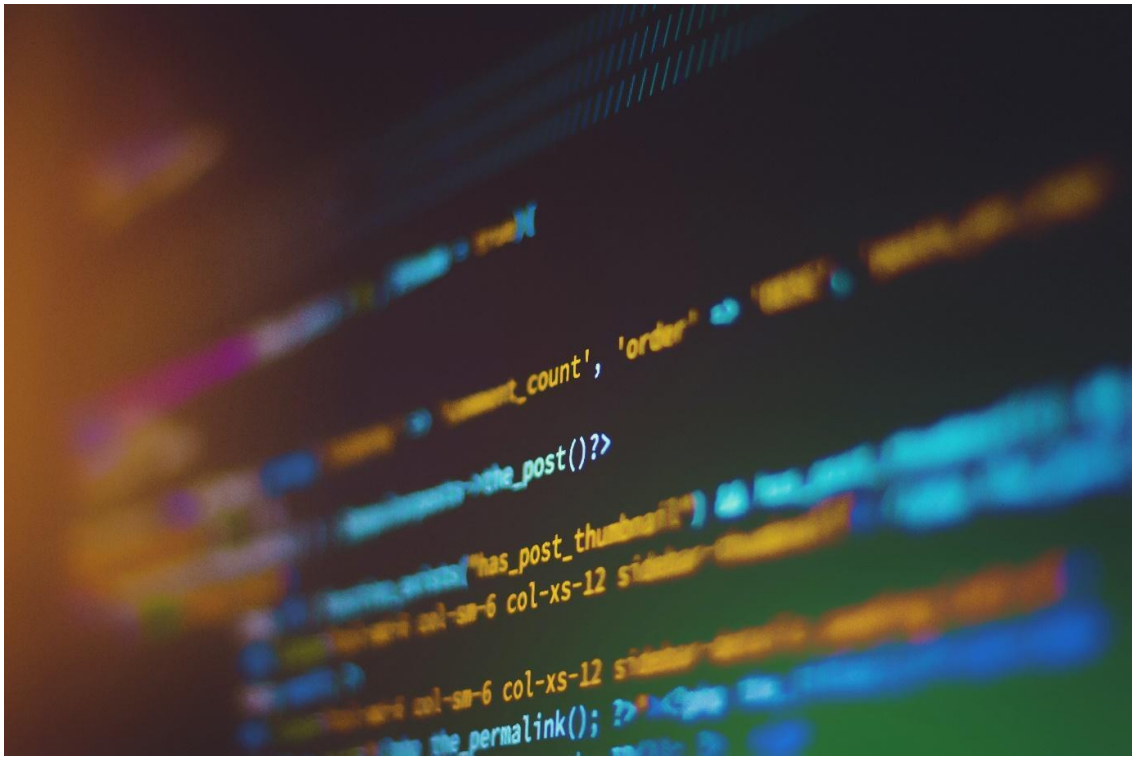
Digital Security Safety (Greek)

Εισαγωγή:

Ορισμένες από τις πιο συνηθισμένες πτυχές της καθημερινής μας ζωής σήμερα θα έμοιαζαν με επιστημονική φαντασία μόλις μερικές δεκαετίες πριν! Η χρήση κινητών συσκευών για όλες σχεδόν τις τεχνολογικές μας ανάγκες, η ταχύτητα και η εμβέλεια του διαδικτύου, ο πλούτος των εφαρμογών και των λύσεων πληροφορικής, έχουν αναδιαμορφώσει την καθημερινή μας εμπειρία, το εμπόριο, την εκπαίδευση, την ψυχαγωγία, την έρευνα, ακόμη και τη διαπροσωπική μας ζωή.

Υπολογίζεται ότι σήμερα υπάρχουν 4,66 δισεκατομμύρια ενεργοί χρήστες του διαδικτύου στον κόσμο σε σύνολο 7,83 δισεκατομμυρίων κατοίκων, πράγμα που σημαίνει ότι το 92,6% των ανθρώπων στον πλανήτη έχουν πρόσβαση στον Παγκόσμιο Ιστό μέσω διαφόρων συσκευών. Εκτός από τα παραπάνω, το 56,8% του παγκόσμιου πληθυσμού χρησιμοποιεί επίσης τακτικά εφαρμογές των μέσων κοινωνικής δικτύωσης στην προσωπική και επαγγελματική του ζωή.

Με μια τέτοια τεράστια εμβέλεια της τεχνολογίας, δεν είναι περίεργο ότι υπάρχουν αρκετοί κίνδυνοι που μπορούν να επηρεάσουν αρνητικά την εμπειρία και απειλές που μπορούν να θέσουν σε κίνδυνο την ασφάλεια και την προστασία των χρηστών στον ψηφιακό κόσμο. Σε αυτή την ενότητα, θα εξετάσουμε και θα παρουσιάσουμε τις κύριες πτυχές της ψηφιακής ασφάλειας και προστασίας τόσο για τη γενική χρήση των διαδικτυακών εργαλείων όσο και για την πτυχή της μάθησης/διδασκαλίας στον τομέα της ΕΕΚ.



Μαθησιακοί στόχοι:

Στο τέλος αυτής της ενότητας θα έχετε:

- κατανοήσει τους κινδύνους που συνδέονται με τη χρήση ψηφιακών και ηλεκτρονικων εργαλείων
- αυξημένη ευαισθητοποίηση όσον αφορά την ψηφιακή ασφάλεια και προστασία
- αποκτήσει βασικές δεξιότητες για να αντιμετωπίσετε τις ανάγκες σας για ψηφιακή ασφάλεια και προστασία
- αποκτήσει δεξιότητες που θα σας επιτρέψουν να διατηρήσετε μια ασφαλή και προστατευμένη εμπειρία ηλεκτρονικής μάθησης για τους μαθητές σας.
- να ενδυναμωθούν και να κινητοποιηθούν ώστε να διαφυλάξουν την ψηφιακή ασφάλεια και προστασία και να υιοθετήσουν τις πιο πρόσφατες πρακτικές και λύσεις.

Γενικές συμβουλές προς τον εκπαιδευτή:

Βεβαιωθείτε ότι υπάρχει κοινή κατανόηση των όρων που χρησιμοποιούνται σε αυτή την ενότητα, ώστε να διασφαλιστεί η ομαλή παράδοση του περιεχομένου- ίσως είναι χρήσιμο να αφιερώσετε λίγο χρόνο για να διακρίνετε τις διαφορετικές λέξεις και τα διαφορετικά εργαλεία.

Ζητήστε από τους μαθητές να σκεφτούν τη δική τους χρήση ψηφιακών και διαδικτυακών εργαλείων και πόσο εκτεταμένη είναι- ίσως ρωτήστε τους πώς θα ήταν διαφορετική, πιο

δύσκολη ή ακόμα και καλύτερη η ζωή τους αν για τις επόμενες 24 ώρες δεν υπήρχε διαθέσιμο διαδίκτυο.

Ζητήστε από τους εκπαιδευόμενους να μοιραστούν τις εμπειρίες ή τις ανησυχίες τους σχετικά με την ψηφιακή ασφάλεια και προστασία, σημειώστε τα θέματα αυτά και συνδέστε τα με το περιεχόμενο της ενότητας, όπου είναι δυνατόν. Εάν υπάρχουν θέματα που δεν καλύπτονται, προσπαθήστε να προσφέρετε περαιτέρω εξωτερικές πηγές.

1. Ποιες είναι οι σημαντικότερες απειλές/ κίνδυνοι που υπάρχουν στο διαδίκτυο;

Adware/Διαφημιστικό λογισμικό

Το adware είναι ανεπιθύμητο λογισμικό που έχει σχεδιαστεί για να προβάλλει διαφημίσεις στην οθόνη σας, που ονομάζονται επίσης αναδυόμενα παράθυρα.

Ακολουθούν μερικά τυπικά σημάδια που μαρτυρούν ότι έχετε adware στο σύστημά σας:

- Οι διαφημίσεις εμφανίζονται σε μέρη που δεν θα έπρεπε να υπάρχουν.
- Η αρχική σελίδα του προγράμματος περιήγησής σας έχει αλλάξει μυστηριωδώς χωρίς την άδειά σας.
- Οι ιστοσελίδες που συνήθως επισκέπτεστε δεν εμφανίζονται σωστά.
- Οι σύνδεσμοι ιστοτόπων ανακατευθύνουν σε ιστότοπους διαφορετικούς από αυτούς που περιμένατε.
- Το πρόγραμμα περιήγησής σας επιβραδύνει.
- Νέες γραμμές εργαλείων, επεκτάσεις ή πρόσθετα εμφανίζονται ξαφνικά στο πρόγραμμα περιήγησής σας.
- Ο υπολογιστής σας αρχίζει να εγκαθιστά αυτόματα ανεπιθύμητες εφαρμογές λογισμικού.

Malvertising/ Κακόβουλη διαφήμιση

Η κακόβουλη διαφήμιση - ή κακόβουλη διαφήμιση - είναι μια τεχνική κυβερνοεπιθέσεων που εισάγει κακόβουλο κώδικα σε ψηφιακές διαφημίσεις. Είναι δύσκολο να εντοπιστούν τόσο από τους χρήστες του διαδικτύου όσο και από τους εκδότες, και αυτές οι μολυσμένες διαφημίσεις συνήθως προβάλλονται στους καταναλωτές μέσω νόμιμων διαφημιστικών δικτύων. Επειδή οι διαφημίσεις προβάλλονται σε όλους τους επισκέπτες του ιστότοπου, ουσιαστικά κάθε θεατής της σελίδας διατρέχει κίνδυνο μόλυνσης.

Phishing/ 'Ψάρεμα'

Phishing είναι η επίθεση που αποστέλλεται συνήθως μέσω ηλεκτρονικού ταχυδρομείου και παρασύρει τους τελικούς χρήστες να κάνουν κλικ σε έναν κακόβουλο σύνδεσμο ή συνημμένο

αρχείο. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν το phishing για να αποκτήσουν ερείσματα σε έναν οργανισμό, συχνά διανέμοντας κακόβουλο λογισμικό[1] .

Spear phishing

Το spear phishing είναι μια μέθοδος phishing που στοχεύει συγκεκριμένα άτομα ή ομάδες μέσα σε έναν οργανισμό. Πρόκειται για μια ισχυρή παραλλαγή του phishing, μιας κακόβουλης τακτικής που χρησιμοποιεί μηνύματα ηλεκτρονικού ταχυδρομείου, μέσα κοινωνικής δικτύωσης, άμεσα μηνύματα και άλλες πλατφόρμες για να πείσει τους χρήστες να αποκαλύψουν προσωπικές πληροφορίες ή να εκτελέσουν ενέργειες που προκαλούν παραβίαση του δικτύου, απώλεια δεδομένων ή οικονομική απώλεια. Μια τυπική επίθεση spear phishing περιλαμβάνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου και ένα συνημμένο αρχείο. Το μήνυμα ηλεκτρονικού ταχυδρομείου περιλαμβάνει πληροφορίες που αφορούν συγκεκριμένα τον στόχο, συμπεριλαμβανομένου του ονόματος και της θέσης του στόχου στην εταιρεία. Αυτή η τακτική κοινωνικής μηχανικής αυξάνει τις πιθανότητες το θύμα να εκτελέσει όλες τις απαραίτητες ενέργειες για τη μόλυνση, συμπεριλαμβανομένου του ανοίγματος του email και του συνημμένου αρχείου που περιλαμβάνεται.

Cybersquatting (κατάληψη τομέων)

Cybersquatting είναι η μη εξουσιοδοτημένη καταχώριση και χρήση ονομάτων τομέα στο Διαδίκτυο που είναι πανομοιότυπα ή παρόμοια με εμπορικά σήματα, σήματα υπηρεσιών, ονόματα εταιρειών ή προσωπικά ονόματα με σκοπό τη δημιουργία σύγχυσης ή την κακόβουλη προσέλκυση χρηστών ή τη διεξαγωγή απάτης.

Spyware

Το κατασκοπευτικό λογισμικό είναι λογισμικό με κακόβουλη συμπεριφορά που αποσκοπεί στη συλλογή πληροφοριών σχετικά με ένα άτομο ή έναν οργανισμό και την αποστολή τους σε άλλη οντότητα με τρόπο που βλάπτει τον χρήστη.

Smishing

Οι επιθέσεις Smishing χρησιμοποιούν την υπηρεσία σύντομων μηνυμάτων ή SMS, πιο γνωστή ως μηνύματα κειμένου.

Το Smishing περιλαμβάνει την κλοπή προσωπικών σας στοιχείων, προσποιούμενοι τον εκπρόσωπο της τράπεζάς σας, κάνοντάς σας να κάνετε κλικ σε έναν σύνδεσμο στο μήνυμα κειμένου για να συνδεθείτε στην ιστοσελίδα της τράπεζάς σας και να επαληθεύσετε μια πρόσφατη ύποπτη χρέωση, ζητώντας σας να καλέσετε τον αριθμό εξυπηρέτησης πελατών, που περιλαμβάνεται βολικά στο μήνυμα κειμένου, για να μιλήσετε μαζί τους σχετικά με μια πρόσφατη ύποπτη χρέωση ή έναν εκτεθειμένο λογαριασμό.

1

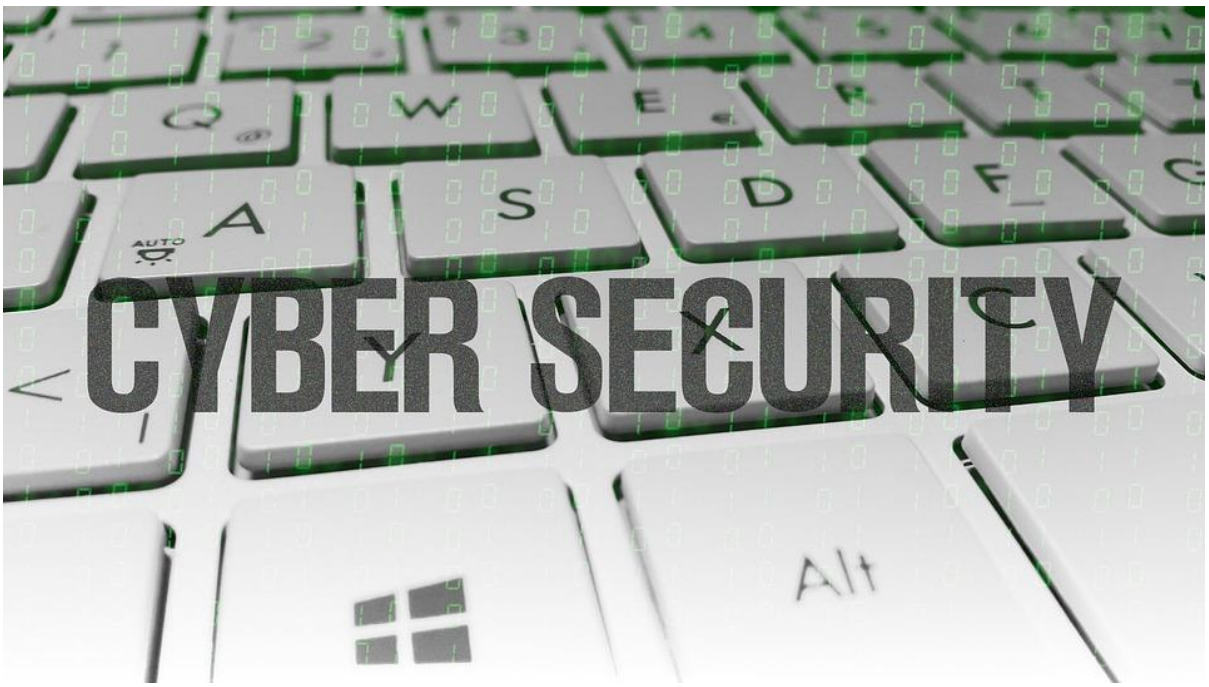
Τα παραπάνω αντιπροσωπεύουν μόνο μια περιορισμένη επιλογή των διαδικτυακών απειλών που είναι σήμερα διαδεδομένες και στοχεύουν εκατομμύρια χρήστες καθημερινά αυτή τη στιγμή. Συνιστάται στους χρήστες να παραμένουν ενήμεροι για τις εξελίξεις και τις νέες απειλές παρακολουθώντας τακτικά ιστότοπους όπως αυτοί που περιλαμβάνονται παρακάτω στην ενότητα "Περαιτέρω πόροι":

Περαιτέρω πόροι

ENISA (europa.eu)

Κίνδυνοι κυβερνοασφάλειας | NIST

Συνιστάται στους εκπαιδευτές να εμπλουτίσουν τον κατάλογο των περαιτέρω πόρων με υλικό στη δική τους γλώσσα ή/και υλικό σχετικό με τη χώρα/περιοχή. Μια καλή πηγή πληροφοριών μπορεί επίσης να βρεθεί σε διαδικτυακά άρθρα και δημοσιεύσεις εμπειρογνωμόνων και ερευνητών στον τομέα της ασφάλειας στον κυβερνοχώρο.



2. Μέτρα ψηφιακής ασφάλειας και προστασίας

Δημιουργήστε κωδικούς πρόσβασης και κάντε τους ισχυρούς.

Ένας μεγάλος αριθμός χρηστών δεν χρησιμοποιεί τη λειτουργία κωδικού πρόσβασης σε τουλάχιστον μία από τις συσκευές τους με δυνατότητα σύνδεσης στο διαδίκτυο, αφήνοντάς την ανοιχτή σε οποιονδήποτε μπορεί να την πάρει. Κλειδώστε όλες τις συσκευές σας, συμπεριλαμβανομένων των υπολογιστών, των tablet και των smartphones, με ασφαλείς κωδικούς πρόσβασης. Αυτό θα κρατήσει μακριά τα αδιάκριτα βλέμματα και θα προσθέσει μια γραμμή άμυνας σε περίπτωση που οι συσκευές σας χαθούν, τοποθετηθούν λάθος ή κλαπούν. Ένας ισχυρός κωδικός πρόσβασης έχει μήκος τουλάχιστον 12 χαρακτήρων. Οι συμβουλές για ισχυρούς κωδικούς πρόσβασης περιλαμβάνουν τη χρήση ενός συνδυασμού μικρών και κεφαλαίων γραμμάτων, αριθμών και συμβόλων και την αποφυγή χρήσης προσωπικών πληροφοριών που μπορούν εύκολα να αναγνωριστούν (όνομα συζύγου, όνομα κατοικίδιου ζώου, γενέθλια κ.λπ.). Ένας αδύναμος κωδικός πρόσβασης θα ήταν κάτι που ο καθένας θα μπορούσε εύκολα να ανακαλύψει, όπως το όνομα ενός αγαπημένου κατοικίδιου "KittkyCat"- ένας ισχυρός κωδικός πρόσβασης θα μπορούσε να μοιάζει με το "1Kitty234Cat!!!".

Πόσο συχνά πρέπει να αλλάζετε τους κωδικούς πρόσβασης;

Αν δεν αντιληφθείτε παραβίαση κωδικού πρόσβασης, δεν χρειάζεται να αλλάζετε τακτικά τους κωδικούς σας, αν ο κάθε κωδικός πρόσβασης είναι ισχυρός και μοναδικός. Αυτό ισχύει ακόμη περισσότερο αν χρησιμοποιείτε έλεγχο ταυτότητας δύο παραγόντων. Όποτε είναι δυνατόν, χρησιμοποιήστε κάποια μορφή ελέγχου ταυτότητας δύο παραγόντων, ώστε ένας παραβιασμένος κωδικός πρόσβασης να μην θέσει σε κίνδυνο τον λογαριασμό σας. Ο συνδυασμός του ελέγχου ταυτότητας δύο παραγόντων με κωδικούς πρόσβασης που δημιουργούνται από μηχανήματα καθιστά τους περισσότερους λογαριασμούς χρηστών πρακτικά απαραβίαστους.

Τι είναι ο μοναδικός κωδικός πρόσβασης;

Ένας μοναδικός κωδικός πρόσβασης είναι:

1. Δεν επαναχρησιμοποιήθηκε ποτέ. Μόλις χρησιμοποιήσετε έναν κωδικό πρόσβασης, δεν μπορείτε ποτέ να τον χρησιμοποιήσετε για άλλον λογαριασμό.
2. Αρκετά. Ένας ισχυρός κωδικός πρόσβασης έχει μήκος τουλάχιστον 12 χαρακτήρων. Οι συμβουλές για ισχυρούς κωδικούς πρόσβασης περιλαμβάνουν τη χρήση ενός συνδυασμού γραμμάτων, αριθμών και συμβόλων.
3. Τίποτα που να σχετίζεται με εσάς. Αυτό σημαίνει ότι δεν χρησιμοποιείτε το όνομα του παιδιού ή του κατοικίδιου ζώου σας στον κωδικό πρόσβασής σας ή άλλες πληροφορίες που μπορούν εύκολα να εντοπιστούν σε εσάς.

Λόγω του γεγονότος ότι οι χρήστες σήμερα χρησιμοποιούν πολλές εφαρμογές και συσκευές, μπορεί να είναι πολύ δελεαστικό να χρησιμοποιείτε έναν κωδικό πρόσβασης για την πλειονότητα των συσκευών και των εφαρμογών σας. Όσο βολική και αν είναι αυτή η πρακτική, μπορεί να προκαλέσει μεγάλη ευπάθεια, καθώς μια κακόβουλη επίθεση μπορεί να επηρεάσει την πλειονότητα των λογαριασμών σας και να θέσει σε κίνδυνο ακόμη και λύσεις ηλεκτρονικής τραπεζικής ή αποθήκευσης στο cloud. Επομένως, συνιστάται έντονα να χρησιμοποιούνται διαφορετικοί μοναδικοί κωδικοί πρόσβασης για τις διάφορες συσκευές και εφαρμογές και να είστε προσεκτικοί όταν μοιράζεστε ή πληκτρολογείτε αυτούς τους κωδικούς πρόσβασης μέσω δημόσιων δικτύων.

Πώς λειτουργεί ο έλεγχος ταυτότητας δύο παραγόντων;

Μπορείτε να ενεργοποιήσετε τον έλεγχο ταυτότητας δύο παραγόντων στις ρυθμίσεις του λογαριασμού σας στα μέσα κοινωνικής δικτύωσης, στο ηλεκτρονικό ταχυδρομείο ή σε άλλα προφίλ. Ο έλεγχος ταυτότητας δύο παραγόντων θα γίνεται με τη βοήθεια του αριθμού τηλεφώνου σας ή μέσω μιας εφαρμογής ελέγχου ταυτότητας στο smartphone σας. Αφού ενεργοποιήσετε τον έλεγχο ταυτότητας δύο παραγόντων, κάθε φορά που θα συνδέεστε στο λογαριασμό σας από μια νέα συσκευή ή πρόγραμμα περιήγησης, ο κωδικός ασφαλείας θα αποστέλλεται στο τηλέφωνό σας ή στην εφαρμογή ελέγχου ταυτότητας. Πρέπει να πληκτρολογήσετε αυτόν τον κωδικό και θα σας επιτραπεί η είσοδος. Εάν ένας εγκληματίας του κυβερνοχώρου προσπαθήσει να συνδεθεί στο λογαριασμό σας, δεν θα μπορέσει να το κάνει αυτό εάν δεν έχει πρόσβαση στο κινητό σας τηλέφωνο. Θα μπορείτε επίσης να αντιληφθείτε μια απόπειρα σύνδεσης στο λογαριασμό σας, καθώς θα λάβετε μια ειδοποίηση με έναν κωδικό. Ποτέ μην μοιράζεστε αυτόν τον κωδικό με άλλα άτομα! Ένας επιτιθέμενος θα προσπαθήσει να τον αποκτήσει. Αν λάβατε τον κωδικό αλλά δεν επιχειρήσατε να συνδεθείτε, διαγράψτε το μήνυμα με τον κωδικό και αλλάξτε τον κωδικό πρόσβασής σας το συντομότερο δυνατό.

Ρυθμίσεις απορρήτου στα μέσα κοινωνικής δικτύωσης

Όταν δημιουργείτε αναρτήσεις στα μέσα κοινωνικής δικτύωσης, μπορείτε να επιλέξετε ρυθμίσεις απορρήτου. Για παράδειγμα, μπορείτε να επιλέξετε ποιο κοινό θα βλέπει την ανάρτησή σας. Θα μπορούσε να είναι μόνο οι φίλοι σας που προσθέσατε στο κοινωνικό δίκτυο, θα μπορούσε να είναι μια δημόσια ανάρτηση για οποιονδήποτε ή θα μπορούσε να είναι μια ιδιωτική ανάρτηση μόνο για εσάς. Μπορείτε επίσης να καθορίσετε ή να μην καθορίσετε την τοποθεσία σας. Βεβαιωθείτε ότι οι προσωπικές σας πληροφορίες δεν κοινοποιούνται. Για παράδειγμα, οι κωδικοί πρόσβασης, ο αριθμός τηλεφώνου σας, το ηλεκτρονικό σας ταχυδρομείο κ.λπ.

Κανόνες ασφαλείας στα μέσα κοινωνικής δικτύωσης, τους αγγελιοφόρους και τα μηνύματα ηλεκτρονικού ταχυδρομείου

Κατά την επικοινωνία μέσω κοινωνικών δικτύων, μηνυμάτων και ηλεκτρονικού ταχυδρομείου πρέπει να είστε προσεκτικοί για να μην υποστείτε ζημιά από προσχηματικές ενέργειες, κακόβουλη διαφήμιση ή διάφορους τύπους phishing. Μην κάνετε κλικ στους συνδέσμους που σας στέλνει ένα άγνωστο άτομο. Να είστε προσεκτικοί - οι εγκληματίες του κυβερνοχώρου μπορούν να προσποιηθούν ότι είναι, για παράδειγμα, υπάλληλοι του Facebook ή της υπηρεσίας ασφαλείας του Instagram. Μην εμπιστεύεστε αυτά τα μηνύματα, αν τα λαμβάνετε μέσω μιας κανονικής συνομιλίας, μιας ανάρτησης ή από μια κανονική σελίδα του Facebook. Τα μηνύματα ασφαλείας θα σας παραδίδονται μέσω ειδοποιήσεων ή θα είναι διαθέσιμα στις ρυθμίσεις. Οι υπάλληλοι των μέσων κοινωνικής δικτύωσης δεν θα σας ζητήσουν ποτέ τον κωδικό πρόσβασής σας ή τις προσωπικές σας πληροφορίες.

Κάποιος σας ζητάει χρήματα;

Εάν φίλοι ή συγγενείς σας ζητήσουν να τους βοηθήσετε σε περίπτωση έκτακτης ανάγκης, τηλεφωνήστε πάντα για να μιλήσετε μαζί τους προσωπικά για να επιβεβαιώσετε ότι το μήνυμα προέρχεται από αυτούς. Διαφορετικά, τα μηνύματα αυτά μπορεί να προέρχονται από εγκληματίες του κυβερνοχώρου. Μπορούν να δημιουργήσουν ένα προφίλ που θα είναι πανομοιότυπο με το προφίλ του μέλους της οικογένειάς σας ή ενός φίλου σας και να προσπαθήσουν να πάρουν χρήματα από εσάς.

Ασφάλεια συσκευής

Χρησιμοποιήστε λογισμικό ασφαλείας. Εγκαταστήστε λογισμικό ασφαλείας στις συσκευές σας από αξιόπιστη πηγή και διατηρήστε το ενημερωμένο. Είναι καλύτερο να εκτελείτε τακτικά το λογισμικό προστασίας από ιούς και λογισμικό κατά της κατασκοπείας. Να είστε επιφυλακτικοί σε ενημερώσεις ασφαλείας από αναδυόμενες διαφημίσεις ή μηνύματα ηλεκτρονικού ταχυδρομείου. Μπορεί στην πραγματικότητα να είναι κακόβουλο λογισμικό που θα μπορούσε να μολύνει τον υπολογιστή σας.

Χρησιμοποιήστε την προεπιλεγμένη προστασία ασφαλείας του τείχους προστασίας του υπολογιστή σας. Το λειτουργικό σας σύστημα (ΛΣ) πιθανόν να διαθέτει προεπιλεγμένες ρυθμίσεις τείχους προστασίας που θα προστατεύουν τον υπολογιστή σας χωρίς να χρειάζεται προσαρμογή. Εάν το λογισμικό προστασίας από ιούς περιλαμβάνει πρόσθετη προστασία τείχους προστασίας που μπορείτε να προσαρμόσετε ξεχωριστά, σκεφτείτε να απευθυνθείτε σε έναν επαγγελματία πληροφορικής για βοήθεια, ώστε να διασφαλίσετε ότι είστε ασφαλώς προστατευμένοι χωρίς να μπλοκάρετε υπερβολικά ιστότοπους και προγράμματα που χρησιμοποιείτε τακτικά.

Αποσύνδεση. Θυμηθείτε να αποσυνδεθείτε από εφαρμογές και ιστότοπους όταν τελειώσετε τη χρήση τους. Το να τις αφήνετε ανοιχτές στην οθόνη του υπολογιστή σας μπορεί να σας καταστήσει ευάλωτους σε κινδύνους για την ασφάλεια και το απόρρητο.

10 συμβουλές για να είστε ασφαλείς στο διαδίκτυο

1. Δημιουργήστε κωδικούς πρόσβασης και κάντε τους ισχυρούς.

2. Ασφαλής πρόσβαση στους λογαριασμούς σας. Δεδομένου ότι οι κωδικοί πρόσβασης μπορούν να κλαπούν, η προσθήκη ελέγχου ταυτότητας δύο βημάτων στους λογαριασμούς παρέχει ένα δεύτερο επίπεδο προστασίας. Πολλές διαδικτυακές υπηρεσίες, συμπεριλαμβανομένων εφαρμογών και ιστότοπων, προσφέρουν δωρεάν επιλογές που θα μπορούσαν να σας βοηθήσουν να προστατεύσετε τις πληροφορίες σας και να διασφαλίσετε ότι είστε πραγματικά εσείς που προσπαθείτε να αποκτήσετε πρόσβαση στο λογαριασμό σας - και όχι απλώς κάποιος με τον κωδικό πρόσβασής σας.

3. Σκεφτείτε πριν ενεργήσετε. Τα μηνύματα ηλεκτρονικού ταχυδρομείου και οι επικοινωνίες που δημιουργούν την αίσθηση του επείγοντος, όπως ένα πρόβλημα με τον τραπεζικό σας λογαριασμό ή τους φόρους σας, είναι πιθανότατα απάτη. Εξετάστε το ενδεχόμενο να επικοινωνήσετε απευθείας με την εταιρεία τηλεφωνικά για να διαπιστώσετε αν το email είναι νόμιμο ή όχι.

4. Όταν έχετε αμφιβολίες, πετάξτε το. Το κλικ σε συνδέσμους σε μηνύματα ηλεκτρονικού ταχυδρομείου είναι συχνά ο τρόπος με τον οποίο οι απατεώνες αποκτούν πρόσβαση σε προσωπικές πληροφορίες. Εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου φαίνεται ασυνήθιστο, ακόμη και αν γνωρίζετε το άτομο που το έστειλε, είναι καλύτερο να το διαγράψετε. Να θυμάστε ότι οι απατεώνες μπορούν να καταλαμβάνουν τις διευθύνσεις ηλεκτρονικού ταχυδρομείου φίλων και να σας στέλνουν μηνύματα υποδυόμενοι αυτούς. Ενεργοποιήστε τα φίλτρα ανεπιθύμητης αλληλογραφίας για το λογαριασμό ηλεκτρονικού ταχυδρομείου σας για να φιλτράρετε τα ύποπτα μηνύματα.

5. Μοιραστείτε με προσοχή. Προσέξτε τι μοιράζεστε δημοσίως σε ιστότοπους κοινωνικής δικτύωσης όπως το Facebook. Προσαρμόστε τις ρυθμίσεις απορρήτου για να περιορίσετε ποιος μπορεί να δει τις πληροφορίες σας. Αποφύγετε να μοιράζεστε την τοποθεσία σας.

6. Χρησιμοποιήστε λογισμικό ασφαλείας. Εγκαταστήστε λογισμικό ασφαλείας στις συσκευές σας από αξιόπιστη πηγή και διατηρήστε το ενημερωμένο. Είναι καλύτερο να εκτελείτε τακτικά το λογισμικό προστασίας από ιούς και λογισμικό κατά της κατασκοπείας. Να είστε επιφυλακτικοί σε ενημερώσεις ασφαλείας από αναδυόμενες διαφημίσεις ή μηνύματα ηλεκτρονικού ταχυδρομείου. Μπορεί στην πραγματικότητα να είναι κακόβουλο λογισμικό που θα μπορούσε να μολύνει τον υπολογιστή σας.

7. Προσαρμόστε τις ρυθμίσεις ασφαλείας του προγράμματος περιήγησής σας. Πιθανότατα αναζητάτε ειδήσεις, πληροφορίες και προϊόντα χρησιμοποιώντας ένα πρόγραμμα περιήγησης στο διαδίκτυο, όπως ο Firefox, το Google Chrome, ο Internet Explorer και ο Safari. Προσαρμόστε τις ρυθμίσεις σας σε καθένα από αυτά τα προγράμματα περιήγησης για να ορίσετε τις επιλογές σας για βέλτιστη ασφάλεια. Αυτά τα μενού βρίσκονται συχνά στην επάνω δεξιά γωνία του προγράμματος περιήγησής σας. Εξετάστε το ενδεχόμενο να διαγράψετε το ιστορικό περιήγησής σας στο τέλος της συνεδρίας σας, ώστε να μην αφήσετε ίχνη ευαίσθητων δεδομένων.

8. Χρησιμοποιήστε την προεπιλεγμένη προστασία ασφαλείας του τείχους προστασίας του υπολογιστή σας. Το λειτουργικό σας σύστημα (ΛΣ) πιθανόν να διαθέτει

προεπιλεγμένες ρυθμίσεις τείχους προστασίας που θα προστατεύουν τον υπολογιστή σας χωρίς να χρειάζεται προσαρμογή. Εάν το λογισμικό προστασίας από ιούς περιλαμβάνει πρόσθετη προστασία τείχους προστασίας που μπορείτε να προσαρμόσετε ξεχωριστά, σκεφτείτε να απευθυνθείτε σε έναν επαγγελματία πληροφορικής για βοήθεια, ώστε να διασφαλίσετε ότι είστε ασφαλώς προστατευμένοι χωρίς να μπλοκάρετε υπερβολικά ιστότοπους και προγράμματα που χρησιμοποιείτε τακτικά.

9. Αποσύνδεση. Θυμηθείτε να αποσυνδεθείτε από εφαρμογές και ιστότοπους όταν τελειώσετε τη χρήση τους. Το να τις αφήνετε ανοιχτές στην οθόνη του υπολογιστή σας μπορεί να σας καταστήσει ευάλωτους σε κινδύνους για την ασφάλεια και την ιδιωτικότητα.

Εξετάστε την υποστήριξη. Εάν έχετε ανησυχίες σχετικά με την ψηφιακή ασφάλεια και προστασία, απευθυνθείτε σε έναν έμπιστο επαγγελματία ή ζητήστε υποστήριξη και πληροφορίες μέσω του τμήματος πληροφορικής του οργανισμού σας.

ΑΥΤΟΑΞΙΟΛΌΓΗΣΗ:

- Αναλογιστείτε τις καθημερινές σας συνήθειες και πρακτικές, πιστεύετε ότι θα μπορούσατε να είστε ευάλωτοι όσον αφορά την ψηφιακή ασφάλεια/ασφάλεια;
- Πόσες από τις 10 συμβουλές που προσφέρονται εφαρμόζετε σήμερα;
- Ποιες είναι οι συμβουλές ή οι ιδέες που σκοπεύετε να χρησιμοποιήσετε;
- Ποιες είναι 3 συμβουλές που θα προσφέρατε στους εκπαιδευόμενους σχετικά με την ψηφιακή ασφάλεια/προστασία;