ΕΡΓΟ ΨΗΦΙΑΚΗΣ ΠΡΟΣΒΑΣΗΣ

ΕΝΟΤΗΤΑ

Βασικές γνώσεις ασφαλείας στο διαδίκτυο

Κωδικός: M6BC

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 μάθει στους αρχάριους χρήστες του διαδικτύου τις βασικές γνώσεις σχετικά με την ασφάλειά του στο διαδίκτυο. Οι κύριοι στόχοι της ενότητας είναι να μάθουν οι χρήστες πώς να διατηρούν τα προσωπικά τους δεδομένα ασφαλή, εξασφαλίζοντας ότι τα ηλεκτρονικά τους δεδομένα και στοιχεία δεν διακυβεύονται.

ΛΕΞΕΙΣ - ΚΛΕΙΔΙΑ

Ασφάλεια στο διαδίκτυο, Προσωπικά δεδομένα, Κωδικός πρόσβασης, Ηλεκτρονική καταδίωξη (Cyber-stalking), Διαχείριση κωδικών πρόσβασης

ΣΤΟΧΟΙ

Ενέργειες / Επιτεύγματα		
Κατανόηση των εγκληματικών δραστηριοτήτων που βασίζονται στο διαδίκτυο με στόχο τα άτομα και απόκτηση δεξιοτήτων για τον εντοπισμό και την αποφυγή αυτών των δραστηριοτήτων.		
Γνώσεις	**Δεξιότητες**	**Αρμοδιότητες**
Ασφάλεια στο διαδίκτυο	Η κατανόηση της ασφάλειας στο διαδίκτυο. Η κατανόηση των τύπων των διαδικτυακών κινδύνων Η κατανόηση των βασικών λέξεων – κλειδιών	Η κατανόηση της σημαντικότητας της ασφάλειας στο διαδίκτυο και ποιοι είναι οι κίνδυνοι
Προσωπικά δεδομένα	Τι είναι τα προσωπικά δεδομένα; Η αποκάλυψη των προσωπικών σας δεδομένων στο διαδίκτυο. Τι μπορεί να γίνει αν μοιραστείτε της προσωπικές σας πληροφορίες στο διαδίκτυο;	Να είστε σε θέση να καταλάβετε τι είναι τα προσωπικά δεδομένα, ποιοι είναι οι κίνδυνοι στο διαδικτυακό περιβάλλον και να είστε σε θέση για να προστατεύσετε τα προσωπικά σας

	Πως μπορείτε να προστατεύεστε της προσωπικές σας πληροφορίες;	δεδομένα
Κωδικός πρόσβασης	Η επιλογή του καλύτερου κωδικού πρόσβασης Προσέχετε τους κωδικούς πρόσβασης Ενέργειες που πρέπει να πραγματοποιήσετε για να προστατευθείτε	Η κατανόηση της σημασίας ενός ισχυρού κωδικού πρόσβασης. Δημιουργία και διαχείριση των κωδικών και των ονομάτων χρήστη
Ρυθμίσεις απορρήτου	Να αναγνωρίζετε τη διαδικτυακή παρακολούθηση (Cyberstalking) Στρατηγικές αντιμετώπισης Χρησιμοποιώντας διαχειριστή κωδικών πρόσβασης Διαχείριση των λογαριασμών χρήστη	Η κατανόηση της σημασίας ενός ισχυρού κωδικού πρόσβασης. Δημιουργία και διαχείριση των κωδικών και των ονομάτων χρήστη

Ενότητα 1: Ασφάλεια στο διαδίκτυο

Στόχοι για την ενότητα 1

Κατανόηση της σημασίας για την ασφάλεια στο διαδίκτυο και προσδιορισμός των κινδύνων.

10 Βασικοί κανόνες διαδικτυακής ασφάλειας

1. Διατηρείτε τα προσωπικά σας δεδομένα με επαγγελματικό τρόπο.

Κανείς δεν χρειάζεται να γνωρίζει την προσωπική σας κατάσταση ή τη διεύθυνση κατοικίας σας. Πρέπει να γνωρίζουν την εμπειρία σας, το επαγγελματικό υπόβαθρό σας και το πώς να έρθουν σε επαφή μαζί σας. Δεν θα δίνατε αμιγώς προσωπικές πληροφορίες σε ξένους, οπότε μην τις παραδώσετε σε εκατομμύρια ανθρώπους στο διαδίκτυο.

2. Διατηρείτε τις ρυθμίσεις απορρήτου σας ανοιχτές.

Οι διαφημιστές αγαπούν να μάθουν τα πάντα γύρω από εσάς, έτσι κάνουν και οι χάκερ. Και οι δύο μπορούν να μάθουν πολλά από την περιήγησή σας και τη χρήση των μέσων κοινωνικής δικτύωσης. Παρόλα αυτά μπορείτε να προστατεύετε τις πληροφορίες σας. Τόσο τα προγράμματα περιήγησης ιστού, όσο και τα λειτουργικά συστήματα κινητής τηλεφωνίας, έχουν διαθέσιμες ρυθμίσεις για την προστασία της ιδιωτικής ζωής σας στο διαδίκτυο. Σημαντικοί ιστότοποι, όπως το Facebook, έχουν επίσης διαθέσιμες ρυθμίσεις βελτίωσης της ιδιωτικότητας. Αυτές οι ρυθμίσεις είναι μερικές φορές (σκόπιμα) δύσκολο να βρεθούν, επειδή οι εταιρείες θέλουν τα προσωπικά σας στοιχεία για την αυξήσουν την αξία του μάρκετινγκ που κάνουν. Βεβαιωθείτε ότι έχετε ενεργοποιήσει αυτές τις διασφαλίσεις απορρήτου.

3. Πρακτικές ασφαλούς περιήγησης στο διαδίκτυο

Δεν θα επιλέξετε να περπατήσετε σε μια επικίνδυνη γειτονιά - μην επισκέπτεστε επικίνδυνες γειτονιές στο διαδίκτυο. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν το θορυβώδες περιεχόμενο ως δόλωμα. Ξέρουν ότι ο κόσμος είναι μερικές φορές επηρεασμένος από αμφίβολο περιεχόμενο και μπορεί να μην προσέχουν όταν το ψάχνουν. Το διαδίκτυο είναι γεμάτο από παγίδες που δύσκολα φαίνονται, όπου ένα απρόβλεπτο κλικ μπορεί να εκθέσει προσωπικά δεδομένα ή να μολύνει τη συσκευή σας με κακόβουλο λογισμικό. Με το να μην προχωρήσετε στα προτεινόμενα κλικ, απομακρύνεται τους χάκερ.

4. Να σιγουρευτείτε ότι η σύνδεση σας στο διαδίκτυο είναι ασφαλής

Όταν μπαίνετε στο διαδίκτυο σε δημόσιο χώρο, για παράδειγμα χρησιμοποιώντας μια δημόσια Wi-Fi σύνδεση, δεν έχετε άμεσο έλεγχο της ασφάλειας. Οι εμπειρογνώμονες στον τομέα της ασφάλειας στον κυβερνοχώρο ανησυχούν για τα "τελικά σημεία" - τους χώρους όπου ένα ιδιωτικό δίκτυο συνδέεται με τον έξω κόσμο. Το ευπαθές τελικό σημείο είναι η τοπική σας σύνδεση στο Internet. Βεβαιωθείτε ότι η συσκευή σας είναι ασφαλής και, όταν υπάρχει αμφιβολία, περιμένετε για καλύτερο χρόνο (δηλ. μέχρι να μπορέσετε να

συνδεθείτε σε ένα ασφαλές δίκτυο Wi-Fi) προτού δώσετε πληροφορίες όπως ο αριθμός του τραπεζικού σας λογαριασμού. Θα μάθετε περισσότερα σε επόμενη ενότητα.

5. Να είστε προσεκτικοί στο τι κάνετε λήψη

Ένας κορυφαίος στόχος των εγκληματιών στον κυβερνοχώρο είναι να σας εξαπατήσουν να κατεβάσετε προγράμματα κακόβουλου λογισμικού ή εφαρμογές που μεταφέρουν κακόβουλο λογισμικό ή να προσπαθήσουν να κλέψουν πληροφορίες. Αυτό το κακόβουλο λογισμικό μπορεί να μεταμφιεστεί ως μια εφαρμογή: οτιδήποτε, από ένα δημοφιλές παιχνίδι, σε κάτι που ελέγχει την κίνηση ή τον καιρό. Μην κάνετε λήψη εφαρμογών που φαίνονται ύποπτες ή προέρχονται από έναν ιστότοπο που δεν εμπιστεύεστε.

6. Επιλέξτε ισχυρούς κωδικούς πρόσβασης

Οι κωδικοί πρόσβασης είναι ένα από τα μεγαλύτερα αδύνατα σημεία σε ολόκληρη τη δομή ασφάλειας του διαδικτύου, αλλά αυτή τη στιγμή δεν υπάρχει τρόπος να τους αποφύγετε. Το πρόβλημα με τους κωδικούς πρόσβασης είναι ότι οι άνθρωποι τείνουν να επιλέγουν εύκολους κωδικούς ώστε να τους θυμούνται (όπως "123456"), τα οποία είναι επίσης εύκολο να μαντέψουν οι κλέφτες του κυβερνοχώρου. Επιλέξτε ισχυρούς κωδικούς πρόσβασης που είναι πιο δύσκολο για τους κυβερνο-εγκληματίες να ανακαλύψουν. Το λογισμικό διαχείρισης κωδικών πρόσβασης μπορεί να σας βοηθήσει να διαχειριστείτε πολλαπλούς κωδικούς πρόσβασης ώστε να μην τους ξεχάσετε. Ένας ισχυρός κωδικός είναι αυτός που είναι μοναδικός και σύνθετος - μήκους τουλάχιστον 15 χαρακτήρων, με ανάμειξη γραμμάτων, αριθμών και ειδικών χαρακτήρων. Θα μιλήσουμε για αυτό αργότερα σε αυτό το μάθημα.

7. Κάντε διαδικτυακές αγορές από ασφαλής ιστοσελίδες

Κάθε φορά που κάνετε μια ηλεκτρονική αγορά, πρέπει να δώσετε πληροφορίες σχετικά με πιστωτικές κάρτες ή τραπεζικούς λογαριασμούς - ακριβώς ό, τι αναζητούν και οι εγκληματίες του κυβερνοχώρου. Παρέχετε αυτές τις πληροφορίες μόνο σε ιστότοπους που παρέχουν ασφαλείς, κρυπτογραφημένες συνδέσεις. Μπορείτε να ξεχωρίσετε τους ασφαλείς ιστότοπους, καθώς η διεύθυνσή τους ξεκινάει με https: (όπου το S σημαίνει ασφαλές) και όχι απλά http:. Επιπλεον, οι ασφαλείς ιστοσελίδες έχουν ένα εικονίδιο λουκέτου δίπλα στη γραμμή διευθύνσεων.

8. Να είστε προσεκτικοί σε ότι αναρτάται στο διαδίκτυο

Το διαδίκτυο δεν διαθέτει πλήκτρο διαγραφής. Οποιοδήποτε σχόλιο ή εικόνα που δημοσιεύετε στο διαδίκτυο μπορεί να παραμείνει στο διαδίκτυο για πάντα, επειδή η κατάργηση του πρωτοτύπου (για παράδειγμα, από το Twitter) δεν αφαιρεί τα αντίγραφα που έχουν κάνει άλλοι. Δεν υπάρχει κανένας τρόπος για να "πάρετε πίσω" μια παρατήρηση που επιθυμείτε να μην είχατε κάνει. Μην αναρτάται κάτι που δεν θέλετε να δουν οι συγγενείς σας ή άλλοι ανθρώπους.

9. Να είστε προσεκτικοί ως προς το ποιόν συναντάτε στο διαδίκτυο

Οι άνθρωποι που συναντάτε στο διαδίκτυο δεν είναι πάντα εκείνοι που ισχυρίζονται ότι είναι. Πράγματι, μπορεί να μην είναι καν πραγματικοί. Τα ψεύτικα προφίλ των κοινωνικών μέσων είναι ένας δημοφιλής τρόπος για τους χάκερ να ανακαλύψουν τους απρόσεκτους χρήστες του διαδικτύου και να κλέψουν. Να είστε τόσο προσεκτικοί και ευαίσθητοι στην ηλεκτρονική σας κοινωνική ζωή, όσο είστε και στην πραγματική σας κοινωνική ζωή.

10. Κρατήστε το πρόγραμμα προστασίας από τους ιούς ενημερωμένο

Το λογισμικό ασφάλειας στο διαδίκτυο δεν μπορεί να προστατεύσει από κάθε απειλή, αλλά θα εντοπίσει και θα αφαιρέσει τα περισσότερα κακόβουλα προγράμματα αν και θα πρέπει να βεβαιωθείτε ότι είναι ενημερωμένο μέχρι σήμερα. Βεβαιωθείτε ότι είστε ενημερωμένοι με τις ενημερώσεις του λειτουργικού σας συστήματος και τις ενημερώσεις στις εφαρμογές που χρησιμοποιείτε. Παρέχουν ένα ζωτικό επίπεδο ασφάλειας.

Κρατήστε αυτούς τους 10 βασικούς κανόνες ασφαλείας στο μυαλό σας και θα αποφύγετε πολλές από τις δυσάρεστες εκπλήξεις που κρύβονται στο διαδίκτυο για τους απρόσεκτους χρήστες του. Στις επόμενες ενότητες θα προχωρήσουμε σε περισσότερες λεπτομέρειες για να σας διδάξουμε πώς να εφαρμόσετε αυτούς τους κανόνες στην πράξη.

ΕΝΟΤΗΤΑ 2: Προσωπικά δεδομένα

Στόχοι για την ενότητα 2

Η κατανόηση των προσωπικών δεδομένων, των κινδύνων στο διαδικτυακό περιβάλλον και ικανότητα προστασίας των προσωπικών σας δεδομένων.

Τι είναι τα προσωπικά δεδομένα ;

Τα προσωπικά σας δεδομένα μπορεί να περιλαμβάνουν τα εξής:

- Πλήρες όνομα
- Διεύθυνση
- Αριθμός τηλεφώνου
- Σχολείο
- Ημερομηνία γέννησης
- Διεύθυνση ηλεκτρονικού ταχυδρομείου
- Όνομα χρήστη και κωδικός
- Στοιχεία τραπεζών και πιστωτικών καρτών

Αποκάλυψη προσωπικών δεδομένων στο διαδίκτυο

Πολλές ιστοσελίδες απαιτούν από τους χρήστες να παρέχουν ορισμένες προσωπικές πληροφορίες προκειμένου να χρησιμοποιήσουν την υπηρεσία τους. Πριν από την παροχή προσωπικών πληροφοριών, θα πρέπει να σκεφτείτε τι μπορεί να γίνει με τα προσωπικά σας στοιχεία και να αξιολογήσετε αν εξακολουθείτε να είστε ικανοποιημένοι με αυτά τα στοιχεία. Εκτός από την ακατάλληλη ή παράνομη χρήση των πληροφοριών, η αποκάλυψη ηλεκτρονικών προσωπικών δεδομένων μπορεί να επηρεάσει την ψηφιακή σας φήμη.

Υπάρχουν διάφορες δραστηριότητες που απαιτούν ένα επίπεδο αποκάλυψης των προσωπικών δεδομένων. Για παράδειγμα:

- Αγορές: για επαλήθευση της ταυτότητας του αγοραστή, επεξεργασία πληρωμών ή για παράδοση αγαθών.

- Η εγγραφή ή η δημιουργία λογαριασμού: ένα όνομα ή ένα παρατσούκλι και μια διεύθυνση ηλεκτρονικού ταχυδρομείου είναι συχνά οι ελάχιστες απαιτήσεις, αλλά άλλες πληροφορίες που απαιτούνται μπορεί να περιλαμβάνουν: ηλικία, φύλο, διεύθυνση, φωτογραφίες και προσωπικές απόψεις αν σου αρέσει ή αντιπαθείς κάτι (ένας κόκκινος αστερίσκος (*) προσδιορίζει γενικά υποχρεωτικά πεδία που απαιτούνται για να εγγραφείτε).

- Διαγωνισμοί, βραβεία και ανταμοιβές: απαιτούν συχνά από τους χρήστες να παρέχουν εκτεταμένα προσωπικά δεδομένα, συμπεριλαμβανομένων προσωπικών

ενδιαφερόντων και δημογραφικών λεπτομερειών - αυτά χρησιμοποιούνται συχνά από τους διαφημιστές για την προώθηση προϊόντων και υπηρεσιών.

- Διαδικτυακά παιχνίδια και εικονικοί κόσμοι: μπορεί να απαιτείται από τους χρήστες να εγγραφούν πριν αρχίσουν να παίζουν.

Τι θα μπορούσε να συμβεί αν μοιραζόσασταν τα προσωπικά σας δεδομένα στο διαδίκτυο;

Μηνύματα ανεπιθύμητης αλληλογραφίας, απάτες, κλοπή ταυτότητας είναι μόνο μερικά από τα σοβαρότερα ζητήματα που μπορεί να αντιμετωπίσετε εάν μοιράζεστε τα προσωπικά σας δεδομένα στο διαδίκτυο .

Πως μπορείτε να προστατεύσετε τα προσωπικά σας στοιχεία;

Είναι σημαντικό να κατανοήσετε πώς χρησιμοποιούνται τα προσωπικά σας δεδομένα στο διαδίκτυο και πώς να προστατεύετε τις πληροφορίες και την ψηφιακή σας φήμη.
Οι παρακάτω συμβουλές αποτελούν μια εξαιρετική βάση για την προστασία των προσωπικών σας δεδομένων στο διαδίκτυο:

- Δημοσιεύστε οικονομικές πληροφορίες μόνο σε ασφαλείς ιστότοπους. Αναζητήστε μια διεύθυνση που αρχίζει με το https: // και ένα σύμβολο λουκέτου κλειδωμένο στο κάτω μέρος της οθόνης, το οποίο υποδεικνύει ότι τα δεδομένα κρυπτογραφούνται.

- Σε περίπτωση αμφιβολίας σχετικά με τη νομιμότητα ενός δικτυακού τόπου, καλέστε τον οργανισμό που ισχυρίζεται ότι αντιπροσωπεύει. Ο δικτυακός τόπος SCAMwatch παρέχει περαιτέρω συμβουλές σχετικά με τον τρόπο εντοπισμού και αναφοράς πιθανών απάτών.

- Τα τραπεζικά ιδρύματα δεν θα αποστέλλουν μηνύματα ηλεκτρονικού ταχυδρομείου σε άτομα που ζητούν το όνομα χρήστη ή τον κωδικό πρόσβασης. Αν λάβετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από έναν οργανισμό που ισχυρίζεται ότι εκπροσωπεί ένα τραπεζικό ίδρυμα, αναφέρετε το μήνυμα ηλεκτρονικού ταχυδρομείου στην τράπεζα και στο SCAMwatch. Μην απαντάτε και μην κάνετε κλικ σε οποιονδήποτε σύνδεσμο παρέχεται.

- Διαβάστε τις συμφωνίες χρηστών και τις πολιτικές απορρήτου. Πολλοί οργανισμοί χρησιμοποιούν πληροφορίες για σκοπούς μάρκετινγκ και μπορούν να το πουλήσουν σε άλλες εμπορικές εταιρείες. Εάν δημοσιεύονται πληροφορίες σε ιστότοπους που πωλούν πληροφορίες σε διαφημιζόμενους, τα άτομα ενδέχεται να λαμβάνουν διαφημιστικά μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία είναι δύσκολο να σταματήσουν.

Μειώστε τα μηνύματα ανεπιθύμητης αλληλογραφίας προστατεύοντας τα στοιχεία σας. Τα μηνύματα ανεπιθύμητης αλληλογραφίας μπορούν να μειωθούν:

- περιορίζοντας την αποκάλυψη των διευθύνσεων ηλεκτρονικού ταχυδρομείου και αριθμών κινητής τηλεφωνίας
- εγκαθιστώντας και χρησιμοποιώντας λογισμικο φιλτραρίσματος ανεπιθύμητης αλληλογραφίας
- ελέγχοντας τους όρους και τις προυποθέσεις κατά την αγορά προϊόντων, την είσοδο σε διαγωνισμούς ή την εγγραφή σε υπηρεσίες ή ενημερωτικά δελτία ηλεκτρονικού ταχυδρομείου
- μη επιτρέπωντας τη χρήση των στοιχείων επικοινωνίας σας για σκοπούς μάρκετινγκ (βεβαιωθείτε ότι έχετε ελέγξει το πλαίσιο εξαίρεσης)
- ενισχύοντας την ασφάλεια στο διαδίκτυο για να περιορίσετε τα μηνύματα ανεπιθύμητης αλληλογραφίας (spam).
- κατανοώντας ότι οι πληροφορίες που μοιράζονται στο διαδίκτυο μπορούν να είναι μόνιμες - οι χρήστες ενδέχεται να μην έχουν τον έλεγχο του ποιος τις βλέπει ή ποιος έχει πρόσβαση στις προσωπικές σας πληροφορίες

Επιλέξτε προσεκτικά τους κωδικούς πρόσβασης. Κατά τη δημιουργία κωδικών πρόσβασης υπάρχουν κάποιες σαφείς δεσμεύσεις, όπως:

Να κάνετε:

- χρησιμοποιήστε οκτώ ή περισσότερους χαρακτήρες
- χρησιμοποιήστε ένα συνδυασμό λέξεων που δεν είναι προβλέψιμος
- χρησιμοποιήστε έλεγχο ταυτότητας δύο παραγόντων σε λογαριασμούς που περιέχουν προσωπικές πληροφορίες

Τι δεν πρέπει να κάνετε:

- Χρησιμοποιήστε ονόματα κατοικίδιων ζώων, ημερομηνίες γέννησης, ονόματα συγγενών ή φίλων
- Χρησιμοποιήστε έναν προβλέψιμο συνδυασμό λέξεων (π.χ. 'ilovehiking'), μια συγκεκριμένη λέξη-πλαίσιο (π.χ. 'google') ή επαναλαμβανόμενους διαδοχικούς χαρακτήρες (π.χ .: 'aaaaaa' ή '123456')
- Να μοιράζεστε τον κωδικό πρόσβαση σας με άλλους, ακόμα και με έναν φίλο σας
- Αποθηκεύστε τα στη συσκευή σας, εκτός αν είναι μέσω ενός διαχειριστή κωδικών πρόσβασης που τα αποθηκεύει σε μια κρυπτογραφημένη βάση δεδομένων. Οι άπατες απειλών και οι απάτες εκβιασμών περιλαμβάνουν απάτες "ransomware",

"malware" και "hit man". Οι απάτες εκβιασμού και κακόβουλου λογισμικού ενδέχεται να περιλαμβάνουν επιβλαβές λογισμικό που τοποθετείται στον υπολογιστή σας. Αυτό μπορεί να δώσει στους εγκληματίες πρόσβαση στις προσωπικές σας πληροφορίες, κάτι που μπορεί να οδηγήσει σε απώλεια δεδομένων ή να σας εμποδίσει να έχετε πρόσβαση στα προγράμματα και τα αρχεία σας. Οι απατεώνες στη συνέχεια απαιτούν πληρωμή πριν σας επιτρέψουν να αποκτήσετε πρόσβαση στον υπολογιστή σας ξανά.

ΕΝΟΤΗΤΑ 3: Κωδικοί προσβάσεις

Στόχοι για την ενότητα 3

Προσδιορισμός και αντιμετώπιση της ηλεκτρονικής καταδίωξης (cyberstalking) και των τρόπων αναφοράς της.

Εισαγωγή

Οι κωδικοί πρόσβασης είναι ο πιο συνηθισμένος τρόπος για να αποδείξετε την ταυτότητά σας όταν χρησιμοποιείτε ιστότοπους, λογαριασμούς ηλεκτρονικού ταχυδρομείου και τον ίδιο τον υπολογιστή σας (μέσω λογαριασμών χρηστών). Η χρήση ισχυρών κωδικών πρόσβασης είναι επομένως απαραίτητη για την προστασία της ασφάλειας και της ταυτότητάς σας. Η καλύτερη ασφάλεια στον κόσμο είναι άχρηστη όταν ένα κακόβουλο άτομο έχει το σωστό όνομα χρήστη και κωδικό πρόσβασης.

Οι κωδικοί πρόσβασης χρησιμοποιούνται συνήθως σε συνδυασμό με το όνομα χρήστη σας. Ωστόσο, σε ασφαλείς τοποθεσίες μπορούν επίσης να χρησιμοποιηθούν παράλληλα με άλλες μεθόδους ταυτοποίησης, όπως ξεχωριστό PIN ή / και αξέχαστες πληροφορίες. Σε ορισμένες περιπτώσεις θα σας ζητηθεί επίσης να εισαγάγετε μόνο ορισμένους χαρακτήρες του κωδικού σας, για πρόσθετη ασφάλεια.

Ο κίνδυνος χρήσης αδύναμων κωδικών πρόσβασης και το να μην έχετε ξεχωριστό κωδικό πρόσβασης για τον λογαριασμό ηλεκτρονικού ταχυδρομείου σας

Άτομα που παριστάνουν εσάς για να διαπράξουν άπατες και άλλα εγκλήματα, όπως:

- Να έχουν πρόσβαση στον τραπεζικό σας λογαριασμό
- Να αγοράσουν αντικείμενα στο διαδίκτυο με τα χρήματά σας
- Να προσποιούνται ότι είστε εσείς σε σελίδες κοινωνικής δικτύωσης και γνωριμιών
- Να αποστέλλουν μηνύματα ηλεκτρονικού ταχυδρομείου στο όνομά σας
- Να έχουν πρόσβαση στις προσωπικές πληροφορίες που διατηρούνται στον υπολογιστή σας

Επιλέγοντας τους καλύτερους κωδικούς πρόσβασης

Να κάνετε:

- Χρησιμοποιείτε πάντα κωδικό πρόσβασης
- Χρησιμοποιήστε έναν ισχυρό, ξεχωριστό κωδικό πρόσβασης για τον λογαριασμό ηλεκτρονικού ταχυδρομείου σας
- Για να δημιουργήσετε έναν ισχυρό κωδικό πρόσβασης, επιλέξτε τρεις τυχαίες λέξεις. Οι αριθμοί, τα σύμβολα και οι συνδυασμοί κεφαλαίων και κεφαλαίων μπορούν να χρησιμοποιηθούν αν νομίζετε ότι πρέπει να δημιουργήσετε έναν ισχυρότερο κωδικό

πρόσβασης ή αν ο λογαριασμός που δημιουργείτε κωδικό πρόσβασης, απαιτεί κάτι περισσότερο από απλά γράμματα.

Υπάρχουν εναλλακτικές λύσεις, χωρίς σκληρούς και γρήγορους κανόνες, αλλά θα μπορούσατε να λάβετε υπόψη σας τις ακόλουθες προτάσεις:

Επιλέξτε έναν κωδικό πρόσβασης με τουλάχιστον οκτώ χαρακτήρες (και περισσότερους αν μπορείτε, καθώς οι κωδικοί πρόσβασης είναι μεγαλύτεροι για τους εγκληματίες να μαντέψουν ή να σπάσουν), ένας συνδυασμός κεφαλαίων και πεζών γραμμάτων, αριθμών και συμβόλων πληκτρολογίου όπως @ # $% ^ & * ( ) _ +. (για παράδειγμα SP1D3Rm @ n - μια παραλλαγή του spiderman, με γράμματα, αριθμούς, κεφαλαία και πεζά). Ωστόσο, να γνωρίζετε ότι ορισμένα από αυτά τα σημάδια στίξης μπορεί να είναι δύσκολο να εισέλθουν στα ξένα πληκτρολόγια. Επίσης, να θυμάστε ότι η αλλαγή των γραμμάτων σε αριθμούς (για παράδειγμα το E έως το 3 και το I έως το 1) είναι τεχνικές γνωστές στους εγκληματίες.

Μια γραμμή ενός τραγουδιού που άλλοι άνθρωποι δεν θα το συσχέτιζαν μαζί σας.

Το πατρικό όνομα της μητέρας κάποιου άλλου (όχι το πατρικό όνομα της μητέρας σας).

Διαλέξτε μια φράση από ένα τραγούδι που είναι γνωστή σε σας, για παράδειγμα "Μου χρωστάει η ζωή, το εμείς και το μαζί, του κορμιού σου τη σκιά, καθετί δικό σου" και να πάρει τον πρώτο χαρακτήρα από κάθε λέξη για να πάρει 'Μχηζ,τεκτμ,τκστς,κδσ'

Να μην κάνετε:
Χρησιμοποιήστε τα εξής ως κωδικούς πρόσβασης:

- Το όνομα χρήστη, το πραγματικό όνομα ή το όνομα της επιχείρησής σας
- Το όνομα από κάποιο μέλος της οικογένειας ή κάποιο κατοικίδιο ζώο
- Τα γενέθλια σας ή κάποιου από την οικογένεια σας
- Αγαπημένη ομάδα ποδοσφαίρου ή ομάδας F1 ή άλλες λέξεις που είναι εύκολο να καταλάβουν με λίγες γνώσεις για εσάς
- Τη λέξη ¨κωδικός πρόσβασης¨
- Ακολουθία αριθμών
- Μια απλή λέξη λεξικού, η οποία θα μπορούσε να σπάσει με κοινά προγράμματα ενός χακερ.

Κατά την επιλογή αριθμητικών κωδικών πρόσβασης ή αριθμών PIN, μην χρησιμοποιείτε αύξοντα ή κατιούσα αριθμούς (π.χ. 4321 ή 12345), διπλούς αριθμούς (όπως 1111) ή εύκολα αναγνωρίσιμα μοτίβα πληκτρολογίου (όπως 14789 ή 2580).

Να προσέχετε τους κωδικούς σας

Ποτέ μην αποκαλύπτετε τους κωδικούς σας σε κανέναν άλλο. Αν νομίζετε ότι κάποιος άλλος γνωρίζει τον κωδικό πρόσβασής σας, αλλάξτε τον αμέσως. Μην εισάγετε τον κωδικό πρόσβασής σας όταν οι άλλοι μπορούν να δουν τι πληκτρολογείτε.
Η συνήθης αλλαγή των κωδικών πρόσβασης δεν συνιστάται, εκτός εάν οι λογαριασμοί στους οποίους εφαρμόζονται, έχουν παραβιαστεί, οπότε θα πρέπει να αλλαχθούν αμέσως. Αυτό ισχύει και για άλλους λογαριασμούς ή ιστότοπους για τους οποίους χρησιμοποιείτε τα ίδια στοιχεία σύνδεσης.
Χρησιμοποιήστε έναν διαφορετικό κωδικό πρόσβασης για κάθε ιστότοπο. Αν έχετε μόνο έναν κωδικό πρόσβασης, ένας εγκληματίας απλά πρέπει να το σπάσει για να αποκτήσει πρόσβαση σε όλα.
Μην ανακυκλώνετε τους κωδικούς πρόσβασης (για παράδειγμα κωδικός2, κωδικός3).
Εάν πρέπει να γράψετε τους κωδικούς πρόσβασης για να τους θυμάστε, κρυπτογραφήστε τους με τρόπο που να είστε εξοικειωμένοι, αλλά τους καθιστά ακατόρθωτο για τους άλλους τα τους λύσουν.
Μια εναλλακτική λύση για την εγγραφή κωδικών πρόσβασης είναι να χρησιμοποιήσετε μια ηλεκτρονική θήκη κωδικών ή ασφαλή. Ζητήστε συστάσεις και βεβαιωθείτε ότι αυτό που επιλέγετε είναι ασφαλές και αξιόπιστο.
Μην στέλνετε τον κωδικό σας σε μήνυμα μέσο του ηλεκτρονικού ταχυδρομείου.
Το γεγονός ότι πρέπει να χρησιμοποιείτε διαφορετικούς κωδικούς πρόσβασης για κάθε λογαριασμό σας μπορεί να είναι πολύ δύσκολο να τους θυμηθείτε. Εξετάστε το ενδεχόμενο να χρησιμοποιήσετε έναν από τα πολλά ηλεκτρονικά φιλάκια κωδικών πρόσβασης που είναι διαθέσιμα στο διαδίκτυο, αλλά διαβάστε τις κριτικές και λάβετε συστάσεις.

Θύρες κωδικού πρόσβασης / Χρηματοκιβώτια

Υπάρχει ένας αριθμός θυλάκων κωδικών πρόσβασης (που είναι γνωστοί και ως κωδικοί ασφαλείας ή ίσως άλλος όρος) που είναι διαθέσιμοι για τη χρήση σας - κάποιοι είναι με αμοιβή και κάποιοι δωρεάν. Αυτά σας επιτρέπουν να αποθηκεύετε όλους τους κωδικούς σας σε μία, εύκολη στην πρόσβαση περιοχή, ώστε να μην χρειάζεται να τα θυμάστε όλα ή να τα γράψετε. Απλά πρέπει να θυμάστε ένα σύνολο στοιχείων σύνδεσης.

Θα πρέπει να διαβάσετε κριτικές ή να λάβετε προσωπικές συστάσεις πριν εισαγάγετε τους κωδικούς πρόσβασής σας σε μια θήκη κωδικών πρόσβασης. Όποια και αν επιλέξετε, η σύστασή μας είναι ότι διαθέτει έλεγχο ταυτότητας δύο παραγόντων (2FA) - με άλλα λόγια, αποστέλλει έναν κώδικα στο κινητό σας τηλέφωνο ή σε άλλη συσκευή, την οποία πρέπει να εισάγετε στο θυλάκιο κωδικών πρόσβασης για να αποκτήσετε πρόσβαση, όπως όταν επιβεβαιώνετε μια διαδικτυακή τραπεζική πληρωμή.

Έλεγχος λογαριασμών χρηστών

Όλοι όσοι χρησιμοποιούν έναν υπολογιστή θα πρέπει να έχουν το δικό τους λογαριασμό χρήστη, έτσι ώστε μόνο αυτοί να έχουν πρόσβαση στα αρχεία και τα προγράμματα τους. Κάθε λογαριασμός χρήστη θα πρέπει να είναι προσβάσιμος μόνο με την καταχώριση ενός ονόματος χρήστη και κωδικού πρόσβασης για την προστασία του απορρήτου των χρηστών.

Μην χρησιμοποιείτε έναν λογαριασμό με δικαιώματα διαχειριστή για καθημερινή χρήση, καθώς το κακόβουλο λογισμικό μπορεί να αναλάβει δικαιώματα διαχειριστή. Ακόμη και αν είστε ο μόνος χρήστης, ορίστε έναν λογαριασμό διαχειριστή που θα χρησιμοποιηθεί όταν πρέπει να εκτελέσετε εργασίες όπως η εγκατάσταση προγραμμάτων ή η αλλαγή της ρύθμισης του συστήματος και ένας άλλος λογαριασμός χρήστη ως ο κανονικός σας λογαριασμός. Εάν δεν είστε συνδεδεμένοι ως διαχειριστής, θα σας ζητηθεί να εισαγάγετε κωδικό πρόσβασης διαχειριστή κατά την εγκατάσταση ενός νέου προγράμματος οδήγησης ή προγράμματος συσκευής.

ΕΝΟΤΗΤΑ 4: Ρυθμίσεις απορρήτου

Στόχοι για την ενότητα 4

Να βοηθήσει έναν χρήστη να εντοπίσει, να αναγνωρίσει και να αναφέρει τον ηλεκτρονικό αποκλεισμό.

Τα απόρρητα του υπολογιστή

Ρίξτε μια ματιά στις ρυθμίσεις απορρήτου που προσφέρονται στο πρόγραμμα περιήγησης (που συνήθως βρίσκονται στο μενού Εργαλεία) για να δείτε αν μπορείτε να τις προσαρμόσετε ώστε να διατηρήσετε το καλό και να αποκλείσετε το κακό. Όταν πηγαίνετε στο διαδίκτυο, οι ιστότοποι εγκαθιστούν cookies στον υπολογιστή σας που παρακολουθούν τις κινήσεις σας. Ορισμένα cookies μπορεί να είναι ωφέλιμα, όπως αυτά που θυμούνται τα ονόματα σύνδεσης ή τα στοιχεία στο ηλεκτρονικό σας καλάθι αγορών. Ωστόσο, ορισμένα cookies έχουν σχεδιαστεί για να θυμούνται όλα όσα κάνετε στο διαδίκτυο, να δημιουργείτε ένα προφίλ των προσωπικών σας πληροφοριών και συνηθειών και να πωλούν αυτές τις πληροφορίες σε διαφημιστικές και άλλες εταιρείες.

Παράδειγμα :
Ρύθμισης του Internet Explorer

Για να προστατεύσετε τον υπολογιστή σας από εισβολή ή από ιούς που θα μπορούσαν να καταστρέψουν το σύστημά σας, πρέπει να ξέρετε πώς να αλλάξετε τις ρυθμίσεις απορρήτου στον Internet Explorer. Με την αλλαγή των ρυθμίσεων απορρήτου, αποφασίζετε ποια είδη ιστότοπων μπορεί να έχει πρόσβαση στο Internet Explorer και ποια είδη ιστότοπων θέλετε να επιτρέπονται τον υπολογιστή σας.

1. Ανοίξτε τον Internet Explorer, επιλέξτε Εργαλεία → Επιλογές Internet και κάντε κλικ στην καρτέλα Απόρρητο.
2. Σύρετε τη μπάρα προς τα πάνω και προς τα κάτω για να δείτε τα διαφορετικά επίπεδα ρυθμίσεων ασφαλείας. Σε κάθε επίπεδο, ο Internet Explorer θα σας δώσει πληροφορίες σχετικά με τη συγκεκριμένη ρύθμιση ασφαλείας.
3. Διαβάστε τις επιλογές και επιλέξτε μια ρύθμιση που σας ταιριάζει. Αν δεν ξέρετε τι να επιλέξετε, το Medium είναι μια καλή επιλογή για να ξεκινήσετε. Αν αυτό δεν φαίνεται να εμποδίζει αρκετά, μπορείτε πάντα να αυξήσετε το επίπεδο ασφάλειας.
4. Κάντε κλικ στο κουμπί ιστοτοπος (Sites) για να καθορίσετε τους ιστότοπους στους οποίους πρέπει πάντα να επιτρέπεται η χρήση cookies.

Ανοίγει το παράθυρο διαλόγου "Ενέργειες απορρήτου ανά τοποθεσία", επιτρέποντάς σας να αντικαταστήσετε τις γενικές ρυθμίσεις.
Εισαγάγετε έναν ιστότοπο στο πλαίσιο διεύθυνση της ιστοσελίδας και κάντε κλικ στο στοιχείο Αποκλεισμός ή Αποδοχή.

Κάντε κλικ στην επιλογή Να επιτρέπεται για ιστότοπους που γνωρίζετε ότι μπορείτε πάντα να εμπιστεύεστε και κάντε κλικ στην επιλογή Αποκλεισμός για ιστότοπους που γνωρίζετε ότι δεν μπορείτε ποτέ να εμπιστευτείτε (όπως www.ComputerDemolishingDownloads.com).

5. Κάντε κλικ στο OK για να αποθηκεύσετε τις νέες ρυθμίσεις. Επιστρέφετε στο παράθυρο διαλόγου Επιλογές Internet.

6. Προσαρμόστε τον αποκλεισμό αναδυόμενων παραθύρων και κάντε κλικ στο κουμπί OK όταν τελειώσετε.

Μπορείτε να ενεργοποιήσετε και να απενεργοποιήσετε τον αποκλεισμό αναδυόμενων παραθύρων από εδώ και μπορείτε να επιτρέψετε την εμφάνιση αναδυόμενων παραθύρων ορισμένων ιστότοπων μέσω του μηχανισμού αποκλεισμού κάνοντας κλικ στο κουμπί Ρυθμίσεις. Μπορείτε να προσθέσετε ιστότοπους εδώ με τον ίδιο τρόπο που προσθέσατε ιστότοπους στο παράθυρο διαλόγου Ενέργειες απορρήτου ανά τοποθεσία.

Ρυθμίσεις απορρήτου στο κινητό τηλέφωνο (smartphones)

Οι ρυθμίσεις για τα κινητά τηλεφώνα (smartphones) ποικίλλουν, αλλά μπορείτε να ενισχύσετε το απόρρητο με αυτές τις ρυθμίσεις:

- **Απενεργοποιήστε τις υπηρεσίες τοποθεσίας.** Αυτό εμποδίζει τις εφαρμογές να παρακολουθούν την τοποθεσία σας.

- **Μην αφήνετε τις εφαρμογές (apps) να μοιράζονται δεδομένα.** Ορισμένες εφαρμογές θέλουν να χρησιμοποιούν πληροφορίες που είναι αποθηκευμένες στο τηλέφωνό σας (για παράδειγμα, η λίστα επαφών σας). Πείτε όχι.
- **Ενεργοποιήστε τις ρυθμίσεις απορρήτου σε εφαρμογές που κάνετε λήψη.** Βεβαιωθείτε ότι χρησιμοποιείτε αυστηρές ρυθμίσεις απορρήτου σε υπηρεσίες όπως το Instagram και το Facebook.
- **Προσέξτε με τις συνδέσεις στα μέσα κοινωνικής δικτυώσεις .** Όταν συνδέεστε σε έναν ιστότοπο με το όνομα χρήστη και τον κωδικό πρόσβασής σας στο Facebook ή το Google, ενδέχεται να επιτρέπετε σε αυτήν την εφαρμογή να αποκτά πρόσβαση σε ορισμένες πληροφορίες από το προφίλ σας. Διαβάστε τα λεπτά γράμματα για να μάθετε τι μοιράζεστε.

ΑΣΚΗΣΕΙΣ

Άσκηση 1: Ποιο είναι το IQ απορρήτου σας; Πάρτε το κουίζ μας και μάθετε!

https://blog.avast.com/2014/01/27/what-is-your-privacy-iq-take-our-quiz-and-find-out-2/

Άσκηση 2: Διαδικτυακό παιχνίδι για την ασφάλεια στον κυβερνοχώρο

Η NOVA έχει ενώσει τις δυνάμεις της με τους εμπειρογνώμονες στον τομέα της ασφάλειας στον κυβερνοχώρο για τη δημιουργία του εργαστηρίου Cybersecurity Lab. Αυτό είναι ένα παιχνίδι όπου οι παίκτες ανακαλύπτουν πώς μπορούν να διατηρήσουν την ψηφιακή ζωή τους ασφαλή. Το παιχνίδι βοηθά τους παίκτες να κατανοήσουν τις κοινές απειλές στον κυβερνοχώρο και τις άμυνες τους.

https://www.pbs.org/wgbh/nova/labs/lab/cyber/

Η λίστα με τούς χειρότερους κωδικούς πρόσβασης

Υλικό για περαιτέρω ανάγνωση και πόροι

Όροι που πρέπει να γνωρίζετε
https://www.lifewire.com/top-internet-terms-for-beginners-2483381

Σχεδιασμός ασφάλειας διαδικτύου για ηλικιωμένους (λήψηPDF)
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=18&cad=rja&uact=8&ved=2ahUKEwiz8LGAjNjdAhVSGsAKHbISB8QQFjAReggQIBxAC&url=https%3A%2F%2Fvictimserviceslanark.ca%2Fphotos%2Fcustom%2FVSLG%2FResources%2FSafetyPlanningForSeniors_English.pdf&usg=AOvVaw3WNu9papw-5PbHbhKSxVFi

Διαδικτυακή ασφάλεια για ηλικιωμένους
https://www.connectsafely.org/seniors/

Περισσότερες πληροφορίες σχετικά με την ασφάλεια στο διαδίκτυο
https://www.protectseniorsonline.com/resources/

Πώς να είστε ασφαλής στο διαδίκτυο για ηλικιωμένους –YouTube βίντεο
https://www.youtube.com/watch?v=HGHxRNT6PjU

Κανόνες για ασφάλεια στο διαδίκτυο
https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online