Οδηγίες και συμβουλές

Τηρήστε αυτές τις οδηγίες και συμβουλές προκειμένου να αποκτήσετε καλές συνήθειες όσον αφορά την επιγραμμική ασφάλεια. Η ενότητα αυτή αποτελεί προϊόν συνεργασίας της Get Safe Online (Ηνωμένο Βασίλειο) και του Υπουργείου Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών (ΗΠΑ)

- Προστατέψτε τον προσωπικό σας υπολογιστή και τις φορητές συσκευές σας
- Προστατέψτε τις πληροφορίες προσωπικού χαρακτήρα και την ταυτότητά σας
- Προστατέψτε πληροφορίες επιχειρηματικού χαρακτήρα εκτός της επιχείρησής σας
- Συνδεθείτε με προσοχή
- Χρησιμοποιείτε το διαδίκτυο με σύνεση

Προστατέψτε τον προσωπικό σας υπολογιστή (PC) και τις φορητές συσκευές σας

Προσωπικοί υπολογιστές

- Χρησιμοποιήστε τείχος προστασίας (firewall): Τα τείχη προστασίας προστατεύουν το δίκτυό σας από ιούς και πληροφορικούς πειρατές (hackers)
- Εγκαταστήστε λογισμικό κατά των ιών: Το λογισμικό κατά των ιών αποτρέπει τη μόλυνση από ιούς και την εξάπλωση της μόλυνσης στον υπολογιστή σας
- Λαμβάνετε τις πλέον πρόσφατες επικαιροποιήσεις ασφαλείας: Διατηρείτε τις εφαρμογές σας και το λειτουργικό σας σύστημα ακμαία, υγιή και επικαιροποιημένα
- Σταματήστε το κατασκοπευτικό λογισμικό: Μην επιτρέπετε σε αγνώστους την είσοδο στον υπολογιστή σας αποφεύγοντας ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου και επισυναπτόμενα αρχεία
- Δημιουργείτε ανά τακτά χρονικά διαστήματα αντίγραφα ασφαλείας (backups): Προστατέψτε τα δεδομένα σας από ενδεχόμενη καταστροφή

Φορητοί υπολογιστές

- Απενεργοποιείτε τις ασύρματες συνδέσεις όταν δεν τις χρησιμοποιείτε ή δεν τις χρειάζεστε
- Συνδέστε τον φορητό σας υπολογιστή σε αξιόπιστο δίκτυο που θα επικαιροποιεί σε τακτά χρονικά διαστήματα τους μηχανισμούς ασφαλείας σας
- Δημιουργείτε αντίγραφα ασφαλείας των πληροφοριών που βρίσκονται αποθηκευμένες στον φορητό υπολογιστή σας
- Μην αφήνετε αφύλακτο τον φορητό σας υπολογιστή

Οδηγοί USB

- Χρησιμοποιείτε κρυπτογραφημένο οδηγό USB

- Ρυθμίστε τον οδηγό USB της μνήμης τύπου flash σε λειτουργία «μόνο για ανάγνωση» χρησιμοποιώντας τον διακόπτη, για λόγους προστασίας από τη μετάδοση ιών. Ορισμένοι οδηγοί USB έχουν έναν διακόπτη για τη ρύθμιση της λειτουργίας «μόνο για ανάγνωση» προκειμένου να αποτρέπεται το ενδεχόμενο αντιγραφής ή τροποποίησης των δεδομένων του οδηγού από τον φιλοξενούντα υπολογιστή
- Μετά την αντιγραφή φακέλων από μη αξιόπιστο ή/και μη εξουσιοδοτημένο σύστημα Η/Υ, σαρώστε τον οδηγό μνήμης USB τύπου flash προκειμένου να αποφύγετε τη μετάδοση ιών
- Πριν τοποθετήσετε τον οδηγό USB στον υπολογιστή τρίτου προσώπου, διαγράψτε όλους τους φακέλους/αρχεία που δεν είναι συναφή προς τη χρήση που πρόκειται να κάνετε
- Δημιουργείτε στον οδηγό USB αντίγραφα ασφαλείας των πληροφοριών που χρειάζεστε ώστε να τις ανακτήσετε σε περίπτωση καταστροφής
- Προσαρτήστε στους οδηγούς USB κλειδοθήκη ή λουράκι για την προστασία τους από ενδεχόμενη απώλεια: το μικρό μέγεθος του οδηγού μνήμης USB τύπου flash τον καθιστά εύκολη λεία για κλοπή ή απώλεια. Εξάλλου, η μεγάλη χωρητικότητα αποθήκευσης δεδομένων αυτών των συσκευών αυξάνει και τον πιθανό όγκο των δεδομένων που διατρέχουν κίνδυνο μη εξουσιοδοτημένης πρόσβασης. Οι οδηγοί μνήμης USB τύπου flash τοποθετούνται συνήθως σε τσάντες, σακίδια πλάτης, θήκες φορητών υπολογιστών, πανωφόρια, τσέπες παντελονιών ή αφήνονται πάνω σε γραφεία χωρίς επιτήρηση. Ο αριθμός των συμβάντων απώλειας, ατυχούς τοποθέτησης, δανεισμού χωρίς άδεια ή κλοπής τέτοιων συσκευών βαίνει αυξανόμενος.

Κινητά τηλέφωνα και υπολογιστές χειρός

Οι υπολογιστές χειρός, όπως οι συσκευές Windows Mobile, Palm, iPhone, Android και Blackberry, διατίθενται με συνδέσμους στο διαδίκτυο και ικανότητα αποθήκευσης τεράστιων ποσοτήτων δεδομένων. Η ίδια η φορητότητά τους υπαγορεύει την ανάγκη να τυγχάνουν ιδιαίτερης φροντίδας.

- Απενεργοποιείτε τις ασύρματες συνδέσεις (π.χ., Bluetooth και WLAN) όταν οι συσκευές δεν βρίσκονται σε χρήση. Η τεχνολογία Bluetooth επιτρέπει στις ηλεκτρονικές συσκευές να επικοινωνούν μεταξύ τους ασύρματα μέσω ραδιοζεύξεων από μικρές αποστάσεις
- Μην αφήνετε αφύλακτο το κινητό σας τηλέφωνο ή τον υπολογιστή χειρός σας διότι διατρέχετε τον κίνδυνο απώλειας δεδομένων
- Χρησιμοποιείτε κωδικό πρόσβασης ώστε να εμποδίζετε τους πληροφορικούς πειρατές να εισέλθουν στο έξυπνο τηλέφωνό σας.

Προστατέψτε τις πληροφορίες προσωπικού χαρακτήρα και την ταυτότητά σας

- **Χρησιμοποιείτε ισχυρό κωδικό πρόσβασης**: Ο κωδικός πρόσβασης που χρησιμοποιείτε για την πρόσβασή σας στο διαδίκτυο είναι το αντίστοιχο της κλειδαριάς και του κλειδιού του σπιτιού σας. Οι κωδικοί πρόσβασης αποτελούν σημαντικό μέσο άμυνας, η δε τήρηση καλών πρακτικών όσον αφορά τη δημιουργία κωδικών πρόσβασης θα βελτιώσει το επίπεδο ασφάλειας των ευαίσθητων πληροφοριών προσωπικού χαρακτήρα και της

ταυτότητάς σας. Ο κωδικός πρόσβασης του υπολογιστή σας αποτελεί το κλειδί που επιτρέπει την πρόσβαση σε όλες τις πληροφορίες —τόσο τις επαγγελματικές όσο και τις προσωπικές— που έχετε αποθηκεύσει στον υπολογιστή σας, καθώς και στους επιγραμμικούς λογαριασμούς σας. Χρησιμοποιείτε έναν ισχυρό κωδικό πρόσβασης για να προστατεύσετε τα δεδομένα σας: χρησιμοποιείτε δηλαδή ένα σύνθετο σύνολο χαρακτήρων ή συνδυάστε γράμματα (κεφαλαία και πεζά), αριθμούς και σύμβολα. Όσο μεγαλύτερη ποικιλία χαρακτήρων περιέχει ο κωδικός πρόσβασής σας, τόσο δυσκολότερη γίνεται η πιθανολόγησή του. Μην χρησιμοποιείτε πληροφορίες προσωπικού χαρακτήρα —όνομα, ονόματα τέκνων, ημερομηνίες γεννήσεως, κ.λπ.— που ενδέχεται να είναι ήδη γνωστές σε κάποιους ή που μπορούν να αποκτηθούν εύκολα και προσπαθήστε να αποφύγετε κοινές λέξεις: ορισμένοι πληροφορικοί πειρατές χρησιμοποιούν προγράμματα τα οποία δοκιμάζουν όλες τις λέξεις του λεξικού

- **Αλλάζετε τακτικά τον κωδικό πρόσβασης**: Εάν πιστεύετε ότι το σύστημά σας έχει εκτεθεί σε κίνδυνο, αλλάξτε αμέσως τους κωδικούς πρόσβασης
- **Κρατήστε τον κωδικό πρόσβασης μυστικό**: Ο κωδικός πρόσβασης είναι μοναδικός και δεν πρέπει να τον μοιράζεστε με κανέναν. Προσπαθήστε να απομνημονεύσετε τους προσωπικούς σας κωδικούς πρόσβασης. Αναπτύξτε μια στρατηγική για την απομνημόνευση. Αν γράφετε κάπου τους προσωπικούς σας κωδικούς πρόσβασης, προσέξτε πού τους αποθηκεύετε. Μην τους αφήνετε σε σημεία όπου δεν θα αφήνατε τις πληροφορίες τις οποίες προστατεύουν
- **Τηρείτε για κάθε λογαριασμό ξεχωριστό κωδικό πρόσβασης**: Χρησιμοποιείτε διαφορετικούς κωδικούς πρόσβασης για κάθε επιγραμμικό λογαριασμό στον οποίο έχετε πρόσβαση (ή, τουλάχιστον, ποικιλία κωδικών πρόσβασης). Αν χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για πολλαπλούς λογαριασμούς, ο επιτιθέμενος που αποκτά πρόσβαση σε έναν λογαριασμό αποκτά αυτομάτως πρόσβαση και σε όλους τους υπόλοιπους λογαριασμούς σας
- **Ασφαλίζετε τους λογαριασμούς σας**: Πολλοί πάροχοι λογαριασμών παρέχουν πρόσθετους τρόπους επαλήθευσης της ταυτότητάς σας πριν από την πραγματοποίηση συναλλαγών στον συγκεκριμένο δικτυακό τόπο
- **Κατοχυρώστε την επιγραμμική σας παρουσία**: Όποτε παρέχεται η σχετική δυνατότητα, ρυθμίστε τις παραμέτρους προστασίας του απορρήτου της ιδιωτικής ζωής και ασφαλείας του εκάστοτε δικτυακού τόπου με βάση τις προσωπικές σας προτιμήσεις όσον αφορά το επίπεδο της ανταλλαγής πληροφοριών. Είναι προτιμότερο να επιτρέπετε την ανταλλαγή πληροφοριών μόνο με συγκεκριμένα πρόσωπα
- **Χρησιμοποιείτε προσεκτικά τους δικτυακούς τόπους κοινωνικής δικτύωσης**: Έχετε υπόψη ότι οι δικτυακοί τόποι κοινωνικής δικτύωσης εγκυμονούν πολλούς από τους κινδύνους που διατρέχετε όταν είστε συνδεδεμένος με το διαδίκτυο: εκφοβισμό μέσω διαδικτύου, δημοσιοποίηση πληροφοριών που αφορούν την ιδιωτική ζωή, παρενοχλητική παρακολούθηση μέσω διαδικτύου, πρόσβαση σε ηλικιακά ακατάλληλο περιεχόμενο και, η πλέον ακραία περίπτωση, προσέγγιση παιδιών για αθέμιτους σκοπούς μέσω διαδικτύου και κακοποίηση παιδιών.

Προστατέψτε πληροφορίες επιχειρηματικού χαρακτήρα εκτός της επιχείρησής σας

- **Βεβαιωθείτε ότι διατηρείτε τις ευαίσθητες πληροφορίες ασφαλείς**: Όταν βρίσκεστε εκτός της επιχείρησής σας, διασφαλίστε ότι οι ευαίσθητες πληροφορίες και ο σχετικός εξοπλισμός παραμένουν ασφαλείς και δεν διατρέχουν κίνδυνο κλοπής ή απώλειας. Ειδικότερα, όταν βρίσκεστε σε δημόσιους χώρους να χειρίζεσθε τις πληροφορίες με προσοχή
- **Διατηρήστε τις πληροφορίες που αφορούν την επιχείρησή σας εμπιστευτικές:** Έχετε υπόψη ότι κάποιος μπορεί να ακούει τις συζητήσεις σας. Μην γνωστοποιείτε εμπιστευτικές πληροφορίες που αφορούν την επιχείρησή σας στον κάθε τυχόντα.
- **Έχετε υπόψη ότι κάποιος μπορεί να σας παρακολουθεί**: Όταν ταξιδεύετε ή εργάζεσθε εξ αποστάσεως, προστατέψτε τον εαυτό σας από τεχνικές κακόβουλης παρακολούθησής σας μέσω διαδικτύου
- **Χρησιμοποιείτε το ηλεκτρονικό ταχυδρομείο με σύνεση**: Η χρήση κάποιου προγράμματος περιήγησης στο διαδίκτυο (internet browser) για την ανάγνωση των μηνυμάτων του ηλεκτρονικού σας ταχυδρομείου απαιτεί την ίδια προσοχή που απαιτείται και κατά τον χειρισμό ενός επιτραπέζιου συστήματος ταχυδρομείου, ενέχει δε αφ' εαυτή ορισμένους ειδικούς κινδύνους που αφορούν την ασφάλεια.

Συνδεθείτε με προσοχή

- **Απενεργοποιείτε τις ασύρματες συνδέσεις όταν δεν τις χρησιμοποιείτε ή δεν τις χρειάζεστε**
- **Να είστε προσεκτικοί με τα σημεία αναμετάδοσης ασύρματου σήματος (Wi-Fi hotspots)**: Όταν χρησιμοποιείτε σημεία αναμετάδοσης ασύρματου σήματος να περιορίζετε τον τύπο των δραστηριοτήτων που εκτελείτε και να προσαρμόζετε τις ρυθμίσεις ασφαλείας της συσκευής σας ώστε να περιορίζεται ο κύκλος των προσώπων που μπορούν να έχουν πρόσβαση στη συσκευή σας
- **Προστατεύστε τα χρήματά σας**: Όταν εκτελείτε τραπεζικές συναλλαγές ή πραγματοποιείτε αγορές μέσω διαδικτύου, να ελέγχετε αν οι αντίστοιχοι δικτυακοί τόποι είναι ασφαλείς. Αναζητείτε διευθύνσεις στο διαδίκτυο που αρχίζουν με τους χαρακτήρες https:// ή "shttp://", οι οποίοι σημαίνουν ότι ο αντίστοιχος δικτυακός τόπος λαμβάνει επιπλέον μέτρα ασφαλείας για να διασφαλίζει το απόρρητο των πληροφοριών που παρέχετε. Οι χαρακτήρες Http:// σημαίνουν ότι ο δικτυακός τόπος δεν είναι ασφαλής
- **Σταματήστε τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου**: Τα ανεπίκλητα μηνύματα ηλεκτρονικού ταχυδρομείου συνιστούν απειλή για την ασφάλειά σας. Μην ανοίγετε μηνύματα ηλεκτρονικού ταχυδρομείου και επισυναπτόμενα αρχεία που προέρχονται από άγνωστους αποστολείς
- **Σε περίπτωση αμφιβολίας διαγράψτε το μήνυμα**: Όταν σύνδεσμοι που περιέχονται σε μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα μέσω tweeter, σχόλια και επιγραμμικές διαφημίσεις σάς φαίνονται ύποπτα, είναι προτιμότερο, ακόμη και αν γνωρίζετε την πηγή,

να τα διαγράφετε ή, κατά περίπτωση, να επισημάνετε τη σχετική διεύθυνση ηλεκτρονικού ταχυδρομείου ως ανεπιθύμητη

- **Προωθείτε μηνύματα ηλεκτρονικού ταχυδρομείου μόνο αν το περιεχόμενό τους είναι κατάλληλο:** Εξετάστε το ενδεχόμενο να διαγράψετε το ιστορικό του μηνύματος προτού το προωθήσετε
- **Να είστε προσεκτικοί όταν περιηγείσθε στο Διαδίκτυο**
- **Μην μεταφορτώνετε έγγραφα και υλικό από μη αξιόπιστες τοποθεσίες**
- **Να επιδεικνύετε ιδιαίτερη προσοχή όταν χρησιμοποιείτε υπολογιστές δημόσιας χρήσης:** Να συνδέεστε με υπολογιστή δημόσιας χρήσης μόνο αν η σύνδεσή σας είναι κρυπτογραφημένη (κάτι που αποδεικνύεται από μια κλειδαριά που εμφανίζεται στην κάτω δεξιά πλευρά του παραθύρου του προγράμματος περιήγησης που χρησιμοποιείτε και από τους χαρακτήρες 'https://' στην αρχή της διεύθυνσης του δικτυακού τόπου)
- **Χρησιμοποιείτε υπηρεσίες ηλεκτρονικού ταχυδρομείου μόνο έγκυρων και αξιόπιστων επιχειρήσεων.**

Χρησιμοποιείτε το διαδίκτυο με σύνεση

- **Να ενημερώνεστε για τις τελευταίες εξελίξεις:** Να υιοθετείτε τις νέες μεθόδους ασφαλούς παραμονής στο διαδίκτυο. Αναζητήστε τις πλέον πρόσφατες πληροφορίες σε αξιόπιστους δικτυακούς τόπους και μοιραστείτε τες με την οικογένεια, τους φίλους και τους συναδέλφους σας. Ενθαρρύνετε όλους τους ανωτέρω να χρησιμοποιούν το διαδίκτυο με σύνεση. Καταστήστε το πρόγραμμα περιήγησής σας ασφαλές.
- **Να σκέφτεστε προτού δράσετε**: Να είστε ιδιαίτερα προσεκτικοί με τον χειρισμό ανακοινώσεων που σας προτρέπουν να δράσετε άμεσα, σας κάνουν απίστευτες προσφορές ή σας ζητούν να δώσετε πληροφορίες προσωπικού χαρακτήρα
- **Να δημιουργείτε αντίγραφα ασφαλείας**: Προστατεύστε τις εργασίες σας, τη μουσική σας, τις φωτογραφίες σας και άλλες ψηφιακές πληροφορίες δημιουργώντας ηλεκτρονικά αντίγραφα και αποθηκεύοντάς τα με ασφάλεια.