11:56 AM

Έξυπνες συσκευές
έξυπνοι χρήστες

Password:

safer internet
cyberethics

Κυπριακό Κέντρο Ασφαλούς Διαδικτύου

Το Κυπριακό Κέντρο Ασφαλούς Διαδικτύου «CyberEthics» υλοποιείται με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης στα πλαίσια του Προγράμματος Safer Internet, και αποτελείται από κόμβο ενημέρωσης, γραμμή καταγγελιών και γραμμή βοήθειας.
Το CyberEthics είναι ο Εθνικός Εκπρόσωπος του Πανευρωπαϊκού Δικτύου Εθνικών Κέντρων Ενημέρωσης Insafe και του Παγκόσμιου Οργανισμού Καταγγελιών Παράνομου Περιεχομένου INHOPE. Συνεργάζεται με διάφορους φορείς του δημόσιου και ιδιωτικού τομέα στην Κύπρο, καθώς και με φορείς από το εξωτερικό με κύριο στόχο την εξασφάλιση ενός καλύτερου διαδικτύου για όλους.

Ο Κόμβος Ενημέρωσης στοχεύει:

- Στην εφαρμογή εκστρατειών ενημέρωσης του κοινού για την ασφάλεια στο διαδίκτυο και τους διαδικτυακούς κινδύνους.
- Στην εκπαίδευση εκπαιδευτικών και άλλων επαγγελματιών για την ασφαλή χρήση του διαδικτύου και γενικότερα των νέων τεχνολογιών.
- Στη δημιουργία ενημερωτικού υλικού και άλλων εργαλείων ενημέρωσης για την ασφάλεια στο διαδίκτυο, τα οποία μπορούν να χρησιμοποιηθούν από παιδιά, εφήβους, εκπαιδευτικούς και γονείς.

safer internet
hotline

Γραμμή Καταγγελιών
Στόχος της Γραμμής Καταγγελιών είναι να παρέχει στο κοινό, και ιδιαίτερα στους έφηβους και νεαρούς ενήλικες, την ευκαιρία να στηρίξουν τις προσπάθειες για ένα ασφαλές διαδικτυακό περιβάλλον μέσω της καταγγελίας παράνομου περιεχομένου, ιδιαίτερα σχετικά με τις περιπτώσεις υλικού σεξουαλικής κακοποίησης παιδιών, ρατσισμού και ξενοφοβίας. Καταγγελίες στη Γραμμή Καταγγελιών μπορούν να γίνουν μέσω:
1. Της ειδικής φόρμας στην ιστοσελίδα: www.cyberethics.info 2. Τηλεφώνου στο 22674747 3. Μηνύματος στο: reports@cyberethics.info 4. Της εφαρμογής για κινητά τηλέφωνα «CyberEthics HotHelp».

safer internet
helpline

Γραμμή Βοήθειας
Η Γραμμή Βοήθειας προσφέρει την ευκαιρία στο κοινό να απαντήσει ερωτήματα και να εκφράσει τις ανησυχίες του ή τις απορίες του σχετικά με επιβλαβείς διαδικτυακές συμπεριφορές, επιβλαβή επικοινωνία και επιβλαβές περιεχόμενο στο διαδίκτυο. Η επικοινωνία με τη Γραμμή Βοήθειας μπορεί να γίνει μέσω:
1. Chat στην ιστοσελίδα: www.cyberethics.info (Ώρες λειτουργίας: 3μμ - 7μμ Δευτέρα - Παρασκευή) 2. Τηλεφώνου: 70000116 (Ώρες λειτουργίας: 9πμ - 7μμ Δευτέρα - Παρασκευή) 3. Μηνύματος στο: helpline@cyberethics.info 4. Offline μήνυμα στο chat σε 24ώρη βάση 5. Της εφαρμογής για κινητά τηλέφωνα «CyberEthics HotHelp»

Το υλικό και τα εργαλεία του Κέντρου, καθώς και άλλες χρήσιμες πηγές, είναι διαθέσιμα στις ιστοσελίδες:
www.cyberethics.info I www.pi.ac.cy/InternetSafety I www.cytasafety.com.cy

"Το CyberEthics συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση στα πλαίσια του Προγράμματος Safer Internet.

1

Κλειδώστε το κινητό σας ή/και το tablet σας
Δημιουργήστε ένα κλείδωμα οθόνης έτσι ώστε η συσκευή σας να μην μπορεί να χρησιμοποιηθεί χωρίς κωδικό και βεβαιωθείτε ότι η οθόνη κλειδώνει αυτόματα μετά από κάποια λεπτά αδράνειας.

2

Εγκαταστήστε antivirus
Με την εκτεταμένη χρήση των έξυπνων συσκευών αναπόφευκτα αυξήθηκε και ο αριθμός των ιών και των κακόβουλων εφαρμογών. Μέσα από τα «stores» των έξυπνων συσκευών υπάρχουν δωρεάν προγράμματα antivirus που προστατεύουν το κινητό σας από ιούς και κακόβουλες εφαρμογές και καλό είναι να έχετε πάντα εγκατεστημένο ένα τέτοιο πρόγραμμα στις συσκευές σας.

Χρησιμοποιήστε λογισμικό εύρεσης της συσκευής σας

Για τις έξυπνες συσκευές υπάρχει ένα πολύ χρήσιμο λογισμικό που σας επιτρέπει να βρείτε τις συσκευές σας σε περίπτωση που χαθούν ή κλαπούν. Το λογισμικό αυτό επιτρέπει επίσης το κλείδωμα της συσκευής και τη διαγραφή των προσωπικών σας δεδομένων σε περίπτωση που αυτή χαθεί. Τα λογισμικά αυτά είναι διαθέσιμα για όλους τους τύπους έξυπνων συσκευών (Android, BlackBerry, iOS, Windows).

Διατηρήστε τη συσκευή σας ενημερωμένη

Σχεδόν όλες οι αναβαθμίσεις των έξυπνων συσκευών περιλαμβάνουν βελτιώσεις στην ασφάλεια τους. Όταν υπάρχουν ενημερώσεις από τον κατασκευαστή, καλό είναι να εγκαθίστανται. Επίσης, είναι σημαντικό οι εφαρμογές της συσκευής σας να αναβαθμίζονται όταν αυτό σας ζητηθεί.

4

Ρυθμίσεις τοποθεσίας
Οι περισσότερες φορητές συσκευές διαθέτουν GPS για δική μας διευκόλυνση. Σήμερα όμως, υπάρχουν εφαρμογές που θέλουν να αποκτήσουν πρόσβαση στα δεδομένα της τοποθεσίας μας (Google +, Facebook, Twitter, Viber). Μπορείτε να ελέγξετε τις ρυθμίσεις της τοποθεσίας σε αυτές τις εφαρμογές χωριστά ή να κάνετε τη θέση σας απόρρητη από τις ρυθμίσεις της συσκευής, έτσι ώστε να απενεργοποιηθεί αυτόματα η προβολή τοποθεσίας σας σε όλες αυτές τις εφαρμογές.

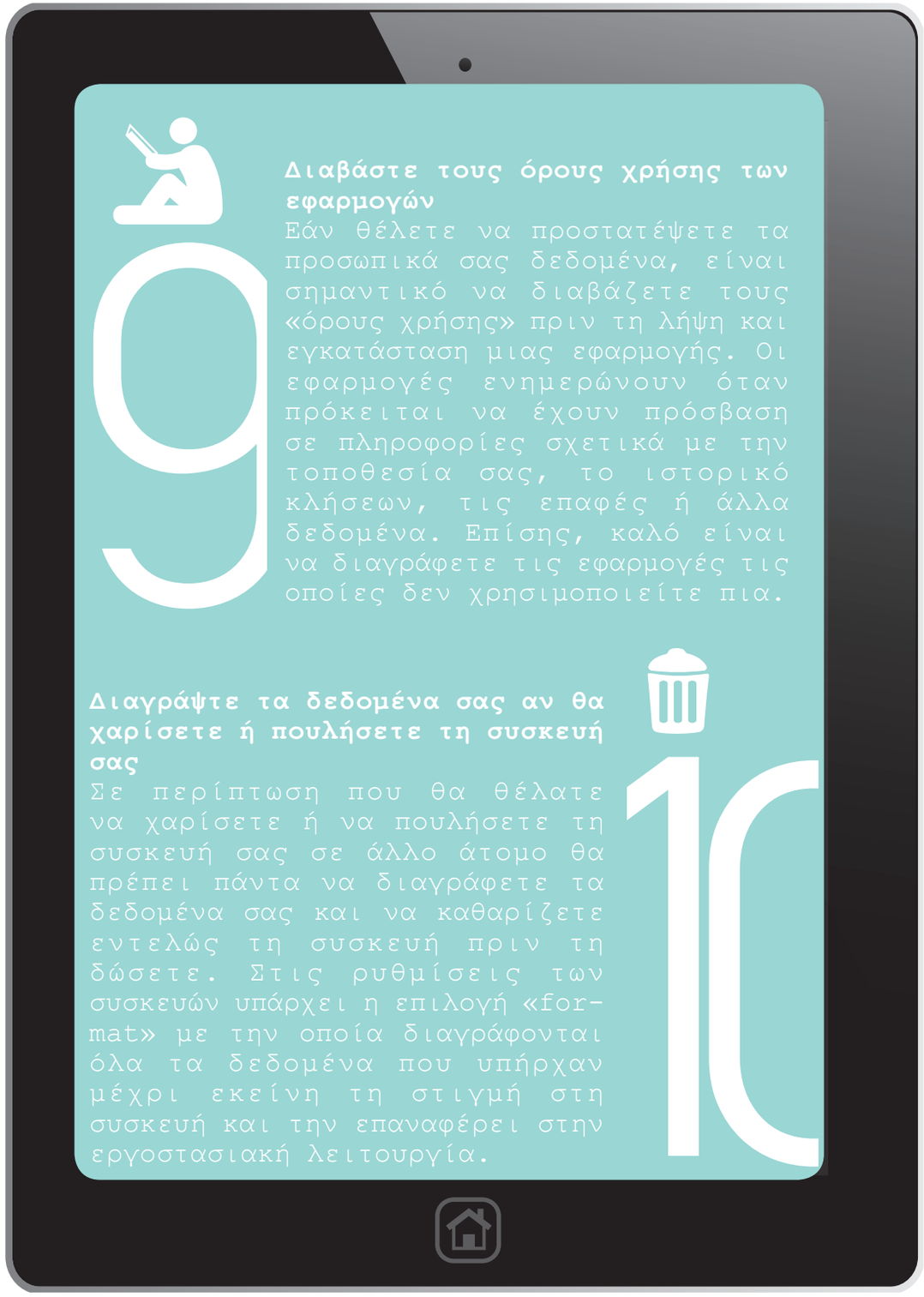
Μην κατεβάζετε εφαρμογές από άγνωστες πηγές
Εφαρμογές που δεν έχουν εγκριθεί από τον επίσημο κατασκευαστή μπορεί να δημιουργήσουν προβλήματα. Είναι προτιμότερο να κατεβάζετε εφαρμογές μόνο από τα «stores» των συσκευών σας.

Μην αφήνετε το Bluetooth της συσκευής σας ανοικτό εάν δεν το χρειάζεστε

Το Bluetooth χρησιμοποιείται για να ζευγαρώσει τη συσκευή σας με μια άλλη ή κάτι άλλο (ραδιόφωνο αυτοκινήτου, ακουστικό κλπ). Με το Bluetooth ανοικτό, υπάρχει ο κίνδυνος άλλα άτομα να αποκτήσουν πρόσβαση στη συσκευή σας και να κλέψουν τα αρχεία και τις επαφές σας, να σας στείλουν ανεπιθύμητα μηνύματα ή ακόμα να σας μπερδέψουν τις εντολές της συσκευής σας. Γι' αυτό, είναι σημαντικό να κλείνετε το Bluetooth σας όταν δεν το χρειάζεστε και όταν είναι ανοικτό να μην έχετε ορατή τη συσκευή σας.

Κρυπτογράφηση δεδομένων

Οι έξυπνες συσκευές σήμερα κάνουν πολύ εύκολη την κρυπτογράφηση των περιεχομένων τους μέσα από τις ρυθμίσεις της συσκευής. Αυτό εξασφαλίζει ότι ακόμα και αν η συσκευή πέσει σε λάθος χέρια και παρακαμφθεί το όποιο κλείδωμα, θα συνεχίσει να υπάρχει κάποιο επίπεδο προστασίας σε αυτή. Αυτό είναι ιδιαίτερα σημαντικό προκειμένου να μην χάσετε τα δεδομένα στην κάρτα μνήμης, ή να σας κλέψουν τα έγγραφα, τις φωτογραφίες, τραγούδια και ότι άλλο έχετε μέσα σε αυτές.


9
Διαβάστε τους όρους χρήσης των εφαρμογών
Εάν θέλετε να προστατέψετε τα προσωπικά σας δεδομένα, είναι σημαντικό να διαβάζετε τους «όρους χρήσης» πριν τη λήψη και εγκατάσταση μιας εφαρμογής. Οι εφαρμογές ενημερώνουν όταν πρόκειται να έχουν πρόσβαση σε πληροφορίες σχετικά με την τοποθεσία σας, το ιστορικό κλήσεων, τις επαφές ή άλλα δεδομένα. Επίσης, καλό είναι να διαγράφετε τις εφαρμογές τις οποίες δεν χρησιμοποιείτε πια.
10
Διαγράψτε τα δεδομένα σας αν θα χαρίσετε ή πουλήσετε τη συσκευή σας
Σε περίπτωση που θα θέλατε να χαρίσετε ή να πουλήσετε τη συσκευή σας σε άλλο άτομο θα πρέπει πάντα να διαγράφετε τα δεδομένα σας και να καθαρίζετε εντελώς τη συσκευή πριν τη δώσετε. Στις ρυθμίσεις των συσκευών υπάρχει η επιλογή «format» με την οποία διαγράφονται όλα τα δεδομένα που υπήρχαν μέχρι εκείνη τη στιγμή στη συσκευή και την επαναφέρει στην εργοστασιακή λειτουργία.

safer internet
cyberethics

Ευχαριστίες:
Ευχαριστούμε το Τμήμα Ηλεκτρονικού Εγκλήματος της Αστυνομίας Κύπρου για τη συνεισφορά τους στη συγγραφή του βιβλιαρίου αυτού.

Το Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων (ΓΕΡΗΕΤ) και τα υπόλοιπα εμπλεκόμενα μέρη, στο πλαίσιο της υλοποίησης της Δράσης 14 της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας (http://www.ocecpr.org.cy/nqcontent.cfm?a_id=4141), συνεργάζονται με το Κυπριακό Κέντρο Ασφαλούς Διαδικτύου CyberEthics για την ενίσχυση του έργου και του ρόλου του. Η Δράση 14 της Στρατηγικής αφορά την ανάπτυξη ενός ολοκληρωμένου Προγράμματος Ενημέρωσης (Awareness) για θέματα ηλεκτρονικής ασφάλειας, που θα καλύπτει όλους τους χρήστες ηλεκτρονικών συστημάτων τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Το Πρόγραμμα Ενημέρωσης περιλαμβάνει σειρά δράσεων που προωθούν την ανάπτυξη κουλτούρας ασφάλειας στο διαδίκτυο στις οποίες περιλαμβάνεται η εκτύπωση και διανομή του βιβλιαρίου αυτού.

ΓΕΡΗΕΤ
Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων