ΑΣΤΥΝΟΜΙΑ ΚΥΠΡΟΥ

Για μια πιο ασφαλή κοινωνία

ΑΣΦΑΛΩΣ χρησιμοποιώ το διαδίκτυο!

ΥΠΟΔΙΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Το διαδίκτυο συνδέει όλον τον κόσμο, ανεξαρτήτως χώρου και χρόνου, παρέχοντάς μας τη δυνατότητα για πρόσβαση σε πληροφορίες για διάφορα θέματα, για ψυχαγωγία και για επικοινωνία με φίλους.

Το περιεχόμενο των ιστοσελίδων δεν ελέγχεται προτού δημοσιευθεί, με αποτέλεσμα να μπορεί οποιοσδήποτε να ανεβάζει ό,τι θέλει στο διαδίκτυο χωρίς κανέναν περιορισμό.

Στις **έγκυρες ιστοσελίδες** αναγράφεται στο τέλος τους η **σχεδιάστρια εταιρεία**, αλλά και ο **ιδιοκτήτης** της. Ακόμα, οι έγκυρες ιστοσελίδες παρέχουν **πληροφορίες για τον ιδιοκτήτη**, αλλά και τον **σκοπό ύπαρξής τους**. Επιπλέον παρέχουν τη **δυνατότητα επικοινωνίας**.

Με τον τρόπο αυτό υπάρχει η δυνατότητα να ελέγξεις και να αξιολογήσεις εάν η ιστοσελίδα είναι έγκυρη και ασφαλής για περιήγηση.

***ΠΟΤΕ** μην αποκαλύπτεις τα προσωπικά σου στοιχεία (διεύθυνση, τηλέφωνο, ηλικία ή φωτογραφία σου).*

ΤΙ ΠΡΕΠΕΙ ΝΑ ΠΡΟΣΕΧΕΙΣ ΓΕΝΙΚΑ

- Να είσαι προσεχτικός στα email και τα μηνύματα που λαμβάνεις. Να αποφεύγεις να ανοίγεις αυτά που προέρχονται από άγνωστο αποστολέα.
- Να αποφεύγεις να στέλνεις σε οποιονδήποτε προσωπικά σου δεδομένα, ιδιαίτερα βίντεο ή φωτογραφίες σου.
- Να αλλάζεις συχνά τους κωδικούς πρόσβασης και να μην τους αποκαλύπτεις σε κανέναν, εκτός από τους γονείς ή κηδεμόνες σου.
- Να αποφεύγεις να επισκέπτεσαι ιστοσελίδες με ακατάλληλο περιεχόμενο.
- Να προτιμάς ηλεκτρονικές διευθύνσεις με το ακρωνύμιο «https», καθώς **«s»** σημαίνει ασφάλεια (security).
- Η υπερβολική ενασχόληση με το διαδίκτυο και τα διαδικτυακά παιγνίδια είναι πιθανόν να προκαλέσει εξάρτηση με σοβαρές συνέπειες στη σωματική και ψυχική σου υγεία.

SOCIAL MEDIA

Τα μέσα κοινωνικής δικτύωσης (social media), αποτελούν έναν δημόσιο χώρο σύγχρονης επικοινωνίας, όπου, μέσα από τις διάφορες πλατφόρμες, οι χρήστες έχουν την ευκαιρία να έχουν άμεση επικοινωνία και να συνομιλούν μεταξύ τους σε πραγματικό χρόνο και να ανταλλάζουν αρχεία. Οι πιο δημοφιλείς πλατφόρμες είναι: ***Instagram, TikTok, Twitter, Facebook, YouTube, WhatsApp, Viber,*** κτλ. Τα διαδικτυακά παιχνίδια γίνονται επίσης χώροι «συνάντησης» των χρηστών που συνδέονται, συνομιλούν και παίζουν μεταξύ τους.

Η ευρεία χρήση των μέσων αυτών από άτομα από όλον τον κόσμο αυξάνει τους κινδύνους, καθώς αρκετοί επιτήδειοι προσπαθούν να προσεγγίσουν τα παιδιά και τους νέους για διάφορους σκοπούς.

Να αλλάζεις τακτικά το nickname και το password σου και να μην χρησιμοποιείς ποτέ τον ίδιο κωδικό πρόσβασης στα διάφορα μέσα κοινωνικής δικτύωσης.

ΠΩΣ ΜΠΟΡΕΙΣ ΝΑ ΠΡΟΣΤΑΤΕΥΤΕΙΣ

- Περιόρισε τον αριθμό των διαδικτυακών σου φίλων και επέλεξε οι διαδικτυακοί φίλοι σου να είναι άτομα που γνωρίζεις προσωπικά.
- Απόφυγε να δημοσιοποιείς προσωπικές σου φωτογραφίες.
- Το username που επιλέγεις να μην παραπέμπει στο όνομα, την ηλικία, το τηλέφωνο, την τοποθεσία και άλλα προσωπικά σου δεδομένα.
- Αφιέρωσε χρόνο για να εξερευνήσεις τις ρυθμίσεις ασφαλείας και απορρήτου των διαδικτυακών σου λογαριασμών.
- Μέσω των ρυθμίσεων απορρήτου του λογαριασμού σου επέλεξε ποιος μπορεί να σε επισημάνει (να σε κάνει tag) για να αποφύγεις τη χρήση του ονόματός σου χωρίς τη θέλησή σου.

Περιόρισε τον αριθμό των διαδικτυακών σου φίλων και επέλεξε ως διαδικτυακούς φίλους άτομα που γνωρίζεις προσωπικά.

Προβληματίσου πριν αναρτήσεις οτιδήποτε στο διαδίκτυο. Οτιδήποτε στέλνεις ή αναρτάς δεν θα διαγραφεί ποτέ, έστω κι αν αλλάξεις γνώμη. Σε ανύποπτο χρόνο, τα βίντεο και οι φωτογραφίες σου πιθανόν να βρεθούν στα χέρια άσχετων χρηστών.

ΠΩΣ ΜΠΟΡΕΙΣ ΝΑ ΠΡΟΣΤΑΤΕΥΤΕΙΣ

- Έχεις την επιλογή να διακόπτεις κάθε επικοινωνία όταν κάποιος σου κάνει ερωτήσεις πολύ προσωπικές, σεξουαλικού περιεχομένου ή που σε κάνουν να νιώθεις άβολα.
- Να κάνεις block οποιαδήποτε ανεπιθύμητη επικοινωνία. Επιπλέον, αν χρειάζεται, μπορείς να κάνεις αναφορά (report), οποιονδήποτε λογαριασμό για περαιτέρω έλεγχο από τους διαχειριστές της πλατφόρμας.
- Σε περίπτωση παραβίασης του λογαριασμού σου, ενημέρωσε γνωστούς και φίλους ότι δεν έχεις πρόσβαση στον λογαριασμό σου.
- Προβληματίσου πριν αναρτήσεις οτιδήποτε στο διαδίκτυο. Οτιδήποτε στέλνεις ή αναρτάς δεν θα διαγραφεί ποτέ, έστω κι αν αλλάξεις γνώμη. Πιθανόν μια ανάρτηση ή φωτογραφία σου να σου δημιουργήσει στο μέλλον προβλήματα, προσωπικά, επαγγελματικά ή άλλα.

Μπορώ να συναντήσω κάποιον ή κάποια που γνώρισα μέσω social media;

Γενικά δεν πρέπει να συναντάς άτομα τα οποία γνώρισες στο διαδίκτυο, αφού δεν μπορείς ποτέ να είσαι σίγουρος ότι τα άτομα αυτά χρησιμοποιούν τα πραγματικά τους στοιχεία. Μπορεί επίσης να προσποιούνται ότι είναι κάποιος ή κάποια που γνωρίζεις. Ωστόσο, εάν αποφασίσεις να συναντηθείτε:

- Διευθέτησε η συνάντηση αυτή να γίνει σε δημόσιο χώρο, όπου συχνάζεις και σε γνωρίζουν εκεί.
- Σίγουρα θα ήταν καλύτερα να μεταβείς με κάποιον άλλο σε αυτόν τον χώρο. Ζήτησε από κάποιον/α φίλο/η ή συγγενή σου να σε συνοδεύσει.
- Προτού πας, οπωσδήποτε ενημέρωσε τους γονείς ή κηδεμόνες σου για τη συνάντηση.

Τα άτομα που γνωρίζεις στο διαδίκτυο μπορεί να μην είναι αυτά που λένε ότι είναι ή να μην χρησιμοποιούν την πραγματική τους φωτογραφία. Θέλεις πραγματικά να συναντηθείς μαζί τους;

Η συμπεριφορά μας στο διαδίκτυο έχει νομικές συνέπειες. Είναι σημαντικό να αναφέρουμε οποιαδήποτε παράνομη συμπεριφορά στην Αστυνομία, ώστε να εντοπίζονται οι παραβάτες και να τιμωρούνται.

ΕΠΑΦΕΣ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

Μη διστάσεις να μιλήσεις στους γονείς σου και στην Αστυνομία.

Οι παιδεραστές/παιδόφιλοι συνομιλούν με τα υποψήφια θύματά τους για να δημιουργήσουν ένα προφίλ και να συλλέξουν όσο περισσότερες πληροφορίες μπορούν. Δημιουργούν μια φιλική σχέση και μαθαίνουν τα ενδιαφέροντά σου. Στη συνέχεια, οδηγούν τη συζήτηση σε θέματα σεξουαλικού περιεχομένου και πολλές φορές αποστέλλουν φωτογραφίες παιδικής πορνογραφίας για να δημιουργήσουν την αίσθηση ότι δεν είναι κάτι κακό. Έτσι προσπαθούν να σε φέρουν σε δύσκολη θέση για να ντραπείς και μην το αναφέρεις στους γονείς/κηδεμόνες σου.

Τέτοιες ενέργειες στοχεύουν στο να σε αποδυναμώσουν και να σε πείσουν να συμμετέχεις αργότερα σε σεξουαλικές πράξεις.

Μην επιτρέψεις σε κανέναν να σε εκμεταλλευτεί!

Μετέφερε στον φάκελο ανεπιθύμητης αλληλογραφίας (spam/junk mail) τα μηνύματα ηλεκτρονικού ταχυδρομείου που θεωρείς ύποπτα ή είναι από άγνωστο αποστολέα για να εξουδετερώσεις την ύποπτη και ενοχλητική αλληλογραφία.

Μπορώ να προστατεύσω τον υπολογιστή μου από «ΕΙΣΒΟΛΕΙΣ»;

Φυσικά! Υπάρχουν διάφοροι τρόποι να το πετύχεις:

- Εγκατέστησε στις συσκευές σου μόνο αυθεντικά λογισμικά προστασίας (antivirus) και να αποφεύγεις τα πειρατικά, αλλά και την εγκατάσταση λογισμικού ή εφαρμογών από άγνωστες πηγές.
- Ενεργοποίησε το αυτόματο κλείδωμα της οθόνης. Τους κωδικούς ξεκλειδώματος της συσκευής σου μην τους μοιράζεσαι.
- Μετέφερε στον φάκελο ανεπιθύμητης αλληλογραφίας τα μηνύματα που θεωρείς ύποπτα, ώστε να εντοπίζεται η ενοχλητική αλληλογραφία (spam/junk mails).
- Μην ανοίγεις ύποπτους συνδέσμους (links) ή συνδέσμους που προέρχονται από άγνωστα πρόσωπα ή διευθύνσεις.
- Να διατηρείς πάντα αντίγραφα ασφαλείας (back up) των δεδομένων σου σε διαφορετική τοποθεσία από τα πρωτότυπα αρχεία.
- Να κάνεις έξοδο (log out) από τους online λογαριασμούς σου μετά από κάθε χρήση.
- Μην χρησιμοποιείς ποτέ τους ίδιους κωδικούς πρόσβασης στους online λογαριασμούς σου και φρόντιζε να τους αλλάζεις συχνά.
- Απόφευγε να χρησιμοποιείς δημόσια ασύρματα δίκτυα (wi-fi).

Μην επιτρέψεις σε κανένα να σε προσβάλει, να σε κοροϊδέψει ή να σε απειλήσει μέσω διαδικτύου. Μπλόκαρε κάθε επικοινωνία, κάνε αναφορά (report), και ανάφερε άμεσα το γεγονός σε ενήλικα της εμπιστοσύνης σου ή την Αστυνομία.

Η ΠΡΟΣΤΑΣΙΑ ΣΟΥ ΕΙΝΑΙ ΔΕΔΟΜΕΝΗ

ΑΝΩΝΥΜΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Το διαδίκτυο είναι μια τεράστια πηγή γνώσης και δίνει τη δυνατότητα στους ανθρώπους να έχουν πρόσβαση σε πληροφορίες που δεν είχαν ποτέ στο παρελθόν. Χρειάζεται όμως προσοχή. Κάθε χρήστης μπορεί να δημιουργήσει διαδικτυακούς λογαριασμούς, να γράψει απόψεις που δεν ισχύουν ή να δημιουργήσει ψεύτικους διαδικτυακούς λογαριασμούς.

Το ψεύτικο αυτό περιεχόμενο μπορεί σε παραπληροφορήσει, να δημιουργήσει κακό στην ψυχική και σωματική σου υγεία ή απλά να σε ξεγελάσει. Χρησιμοποίησε την κριτική σκέψη σου και να διασταυρώνεις οποιαδήποτε πληροφορία διαβάζεις στο διαδίκτυο.

Δεν είναι όλα αληθινά όσα ανεβαίνουν στο διαδίκτυο (fake news).

Κάθε χρήστης μπορεί να δημιουργήσει διαδικτυακούς λογαριασμούς και να διαδώσει πληροφορίες που δεν ισχύουν ή να δημιουργήσει ψεύτικες διαδικτυακές ταυτότητες.

ΕΠΙΚΟΙΝΩΝΙΑ

Αρχηγείο Αστυνομίας
Ευάγγελου Φλοράκη 1478, Λευκωσία

Γραμμή του Πολίτη 1460
Τηλ.: 22808080
Τηλεομ.: 22808598

Υποδιεύθυνση Ηλεκτρονικού Εγκλήματος
Τηλ.: 22808200
Τηλεομ.: 22808465
Email: cybercrime@police.gov.cy
https://cyberalert.cy

Άλλες χρήσιμες ιστοσελίδες
https://www.police.gov.cy
https://cybersafety.cy (Γραμμή 1480)
https://pegi.info

Πλατφόρμα καταγγελιών στο διαδίκτυο
για υποθέσεις που αφορούν:

- απάτες μέσω διαδικτύου
- παιδική πορνογραφία
- παράνομη επέμβαση
- ξενοφοβία
- πνευματική ιδιοκτησία

μέσω της ιστοσελίδας **www.cyberalert.cy**
και επιλογή συνδέσμου *«Καταχώρηση καταγγελιών/πληροφοριών cybercrime για πλεκτρονικό έγκλημα»*

ή μέσω της εφαρμογής για έξυπνα κινητά *«Αστυνομία Κύπρου»*.

www.cyberalert.cy

GET IN ON Google Play

Download on the App Store

Βρείτε μας:

ΓΤΠ 228/2022-5.000
ISBN 978-9963-50-577-7

Εκδόθηκε από το Γραφείο Τύπου και Πληροφοριών
Εκτύπωση: Kailas Printers & Lithographers