INHOPE

Οδηγός Ψηφιακής Συμπεριφοράς

Authors: A. Sotiri, Marketing Communications Officer and A. Dyka, Marketing Content Specialist, September 2024

Funded by the European Union

Περιεχόμενα

Γιατί χρειάζεται ο ψηφιακός γραμματισμός;

Η Τεχνολογία εξελίσσεται συνεχώς και θα πρέπει να χρησιμοποιούμε με προσοχή και ασφάλεια τον διαδικτυακό κόσμο. Δεν αρκεί να γνωρίζουμε τις εφαρμογές που υπάρχουν, θα πρέπει επίσης να είμαστε σίγουροι ότι οι διαδικτυακοί τόποι στους οποίους κινούμαστε μας παρέχουν ασφάλεια, συνδεσιμότητα και σεβασμό.

Εκτός από το να αντιληφθούμε τη σημασία ενός ισχυρού κωδικού πρόσβασης, θα πρέπει να κατανοήσουμε τον τρόπο με τον οποίο θα παραμείνουμε ασφαλείς αλλά και το πως θα αλληλοεπιδρούμε διαδικτυακά με άλλους.

Για τους παραπάνω λόγους, συγκεντρώσαμε εδώ αυτές τις απλές αλλά σημαντικές συμβουλές. Σε λίγα μόλις λεπτά, μπορείς να μάθεις πως θα αποφεύγεις τις απάτες και την παραπληροφόρηση, να εντοπίζεις τους κινδύνους και να δημιουργείς ασφαλείς χώρους, στους οποίους εσύ και οι φίλοι σου θα μπορείτε να πλοηγείστε χωρίς ανησυχία. Όσο καλύτερα είσαι ενημερωμένος/η, τόσο καλύτερες θα είναι οι επιλογές σου και όλοι θα νιώθουν ήρεμοι.

Να θυμάσαι πάντα: Ακόμη και αν είσαι εξαιρετικά προσεκτικός/η, υπάρχουν πιθανότητες κάποιος να σκέφτεται κακόβουλα και να θέλει να σε εκμεταλλευτεί, γνωστός ή άγνωστος. Σε καμία περίπτωση πάντως δεν ευθύνεσαι εσύ.

Section 01

Μάθε τις συσκευές σου

Όπως το δωμάτιο σου ή το σπίτι σου, το κινητό είναι ο προσωπικός σου χώρος και πρέπει να το προστατεύεις. Οι κίνδυνοι ίσως έρθουν από αγνώστους, αλλά το πιο σημαντικό είναι ότι μερικές φορές οι γνωστοί, φίλοι ή συγγενείς, ίσως ξεπεράσουν τα όρια και αποκτήσουν πρόσβαση σε προσωπικές σου πληροφορίες χωρίς την άδεια σου. Με ποιο τρόπο λοιπόν μπορείς να κρατήσεις τα προσωπικά δεδομένα και τις κινήσεις σου απόρρητες;

Αναβαθμίζεις συχνά το τηλέφωνο σου;

Οι αναβαθμίσεις του λογισμικού είναι σημαντικές στην ασφάλεια εντός και εκτός διαδικτύου. Διορθώνουν τα λάθη της προηγούμενης έκδοσης και εξοπλίζουν τη συσκευή σου με τις τελευταίες ρυθμίσεις ασφαλείας. Η συχνή αναβάθμιση του λογισμικού προστατεύει τις πληροφορίες σου από μη εξουσιοδοτημένη πρόσβαση και πιθανές απειλές από εγκληματίες του διαδικτύου, οι οποίοι ανακαλύπτουν και εκμεταλλεύονται γρήγορα τις αδυναμίες του συστήματος.

Πως θα πρέπει να είναι ένας ισχυρός κωδικός;

Ο κωδικός είναι στην πρώτη γραμμή άμυνας, για αυτό και θα πρέπει να είναι ισχυρός. Να αποφεύγεις τη χρήση ημερομηνιών, όπως τα γενέθλια ή άλλες γνωστές πληροφορίες για το άτομό σου ή συνδυασμούς που είναι εύκολοι να τους θυμάσαι, όπως το «κωδικός123». Ανακάτεψε αριθμούς, γράμματα και σύμβολα, ακόμη και 12 χαρακτήρες. Χρησιμοποίησε διαφορετικό κωδικό σε κάθε λογαριασμό και προσπάθησε να είναι δύσκολος να ανακαλυφθεί. Για να το κάνεις ακόμη πιο δύσκολο, χρησιμοποίησε τον έλεγχο ταυτότητας πολλαπλών παραγόντων σε όλους τους διαδικτυακούς σου λογαριασμούς, το ηλεκτρονικό ταχυδρομείο και τα μέσα κοινωνικής δικτύωσης.

Είναι η τοποθεσία σου απόρρητη;

Η ενεργοποίηση της τοποθεσίας σου είναι χρήσιμη για να γνωρίζει η οικογένεια σου που βρίσκεσαι αλλά αν δεν επιλέγεις σωστά με ποιους θα τη μοιραστείς μπορεί να σε βάλει σε κίνδυνο από φίλους/συντρόφους με κτητική ή και κακοποιητική συμπεριφορά που παρατηρούν συνεχώς τις κινήσεις σου.

Για να προστατευθείς, πήγαινε στις ρυθμίσεις, εντόπισε την «Τοποθεσία» και επέλεξε ποιες εφαρμογές θα έχουν πρόσβαση σε αυτή. Σου προτείνουμε να επιτρέψεις τον εντοπισμό μόνο στις εφαρμογές που χρησιμοποιείς και είναι απόλυτα απαραίτητο, περιορίζοντας τη γενικευμένη ενεργοποίηση της τοποθεσίας σου.

«Ακούει» το τηλέφωνο σου;

Η συσκευή σου «ακούει» το τι συμβαίνει γύρω σου. Για να ελέγξεις ποιος σε ακούει, πήγαινε στις ρυθμίσεις της συσκευής σου, εντόπισε το «Ηχείο» ή το «Μικρόφωνο» και επέλεξε ποιες εφαρμογές θα έχουν πρόσβαση στο μικρόφωνο της συσκευής σου αλλά και το πότε. Βεβαιώσου ότι θα επιλέξεις να χρησιμοποιείται το μικρόφωνο της συσκευής σου μόνο όταν οι συγκεκριμένες εφαρμογές είναι ενεργοποιημένες.

Είναι ασφαλής η κάμερα του τηλεφώνου σου;

Πολλές εφαρμογές απαιτούν άδεια για να έχουν πρόσβαση στην κάμερα ή τη συλλογή φωτογραφιών σου όταν χρησιμοποιούνται, αλλά όχι όλες. Η πρόσβαση στην κάμερα μπορεί να επιφέρει υποκλοπή των προσωπικών πληροφοριών ή να χρησιμοποιηθεί για να μας κατασκοπεύσουν. Για να το εμποδίσεις, έλεγξε και περιόρισε μέσα από τις ρυθμίσεις τις εφαρμογές που έχουν πρόσβαση στην κάμερα. Να προσέχεις όταν κάνεις εγκατάσταση άγνωστων εφαρμογών στις αποδοχές άδειας που τους παρέχεις. Η ιδιωτικότητα και η ασφάλεια μας πρέπει να έχουν προτεραιότητα πάντα.

Πώς θα αναγνωρίσεις τις ασφαλείς εφαρμογές;

Δεν είναι όλες οι εφαρμογές ασφαλείς. Πριν τις εγκαταστήσεις κοίταξε τις κριτικές στο App Store (iOS) ή το Google Play (Android). Αναφέρεται κάτι επικίνδυνο ή ύποπτο; Αν όλες οι κριτικές είναι θετικές μπορείς να προχωρήσεις.

Ποιος μπορεί να δει τα Κοινωνικά σου Δίκτυα;

Όπως και στην πραγματική ζωή, εμείς ελέγχουμε ποιος είναι μέσα στον κύκλο των φίλων μας και ποιος γνωρίζει τις προσωπικές μας πληροφορίες. Οι περισσότερες πλατφόρμες επιτρέπουν τη δημιουργία λίστας με ποιοι φίλοι μπορούν να δουν τις δημοσιεύσεις σου, για αυτό προσπάθησε τα νέα σου να είναι διαθέσιμα μόνο σε αυτούς που εμπιστεύεσαι. Σε περίπτωση που επιθυμείς να διατηρήσεις δημόσιο το προφίλ σου θα πρέπει να είσαι πολύ προσεκτικός/ή στο τι δημοσιεύεις και να αποφεύγεις να διαμοιράζονται πληροφορίες όπως η διεύθυνση σου, οικονομικά στοιχεία ή η τοποθεσία σου.

Πώς να πλοηγηθείς με ασφάλεια;

Για να παραμένεις πάντα στην ασφαλή πλευρά του διαδικτύου, να ελέγχεις τις ρυθμίσεις και τις δικλείδες ασφαλείας σου. Τα δημοφιλή προγράμματα περιήγησης προσφέρουν ενισχυμένη προστασία που σε προειδοποιούν για επικίνδυνους ιστότοπους. Εάν όμως θέλεις να αυξήσεις ακόμη περισσότερο την ασφάλεια της περιήγησής σου, σου προτείνουμε να χρησιμοποιήσεις προγράμματα περιήγησης που εστιάζουν στην προστασία της ιδιωτικής ζωής, όπως το DuckDuckGo ή το Qwant, καθώς έχουν σχεδιαστεί για αυτούς ακριβώς τους σκοπούς.

Βεβαιώσου ότι η σύνδεση σου είναι κωδικοποιημένη και ασφαλής, ελέγχοντας το “HTTPS” στην μπάρα διευθύνσεων. Αν το URL της σελίδας δεν αρχίζει από το “HTTPS”, καλύτερα να μην το χρησιμοποιήσεις και φυσικά να μην αναφέρεις εκεί προσωπικές πληροφορίες ή τον κωδικό σου .

ΣΥΜΒΟΥΛΗ

Αν οι γονείς σου διστάζουν να σου επιτρέψουν να πάρεις δική σου συσκευή ακολούθησε τις παρακάτω συμβουλές για να κερδίσεις την εμπιστοσύνη τους.

Υπάρχουν εφαρμογές και εργαλεία που μπορούν να σε προστατέψουν αλλά χρειάζεται να συνεργάζεσαι με τις οδηγίες τους για παραμένεις ασφαλής.

Εφαρμογές όπως το Qustodio, προσφέρουν τη δυνατότητα φιλτραρίσματος μέσω του Safe Search κάθε ενοχλητικού περιεχομένου και της επείγουσας ειδοποίησης κάποιου ενήλικα που εμπιστεύεσαι, μέσω του Panic Button. Αν δεν θέλεις να μιλήσεις στους γονείς σου, σκέψου κάποιον άλλον που μπορεί να σε βοηθήσει σε περίπτωση που συναντήσεις στο διαδίκτυο μια δυσάρεστη εμπειρία. Η ασφάλεια σου είναι προτεραιότητα.

Section 02

Διαδικτυακές αλληλοεπιδράσεις

Τι μπορεί να αλλάξει στο διαδίκτυο;

Η επικοινωνία με σεβασμό δημιουργεί ευχάριστη ατμόσφαιρα και χτίζει ισχυρές κοινωνίες, εντός και εκτός διαδικτύου. Στο διαδίκτυο όμως, λόγω της απόστασης, χρειάζεται να είμαστε ακόμη πιο ευγενικοί. Αν νιώθεις θυμωμένος ή αναστατωμένος, απομακρύνσου για λίγο από το τηλέφωνο ή τον υπολογιστή σου μέχρι να ηρεμήσεις. Διάβασε μια δεύτερη φορά αυτό που έγραψες πριν πατήσεις το «Αποστολή» και υπολόγισε την επίδραση που θα έχουν τα λόγια σου στους άλλους. Πριν πεις κάτι αρνητικό, σκέψου αν αυτό θα τολμούσες να το πεις στους άλλους κατά πρόσωπο.

Είναι εξίσου σημαντικό να υπερασπίζεσαι τους άλλους. Αν δεις κάποιο περιστατικό εκφοβισμού, προσβολής ή κακοποίησης θα πρέπει να το καταγγείλεις. Εδώ θα βρεις τις πληροφορίες που χρειάζεσαι για να αναφέρεις και να καταγγείλεις τη διαδικτυακή παρενόχληση.

Γιατί πρέπει να σκεφτόμαστε πριν κοινοποιήσουμε κάτι;

Οποιαδήποτε διαδικτυακή δημοσίευση αφήνει «ψηφιακά αποτυπώματα» για μεγάλο χρονικό διάστημα για αυτό θα πρέπει να είσαι σίγουρος πριν κοινοποιήσεις οτιδήποτε. Αναρωτήσου αν το περιεχόμενο διέπεται από σεβασμό, είναι ειλικρινές και αν έχεις τη συναίνεση που χρειάζεται για να το δημοσιεύσεις. Η κοινοποίηση ψευδών πληροφοριών μπορεί να προκαλέσει ζημιά σε άλλα άτομα, να πλήξει την υπόληψη τους ή ακόμη και να επιφέρει νομικές συνέπειες. Οι αλγόριθμοι των κοινωνικών δικτύων προωθούν πολλές φορές «προβληματικό» περιεχόμενο, που σημαίνει ότι η παραπληροφόρηση διαδίδεται γρήγορα και ευρέως. Για αυτό αξίζει να χρησιμοποιούμε τα εργαλεία όπως τα FactCheck.org, ή το GoogleFactCheck για να διασταυρώνουμε πληροφορίες.

Πρόσεχε το περιεχόμενο που κοινοποιείς όσον αφορά στην προσωπική σου ασφάλεια και ιδιωτικότητα. Όσον αφορά τους άλλους είναι σημαντική η συναίνεση τους, ειδικά σε ευαίσθητα ζητήματα. Πριν δημοσιεύσεις φωτογραφίες ή πληροφορίες άλλων ρώτα αν επιτρέπεται και σεβάσου την απόφαση τους, όποια και αν είναι. Αν κατά λάθος κοινοποιήσεις μια ψευδή πληροφορία ή επιβλαβές περιεχόμενο, θα πρέπει να αντιδράσεις άμεσα και γρήγορα. Διέγραψε τη δημοσίευση σου και διόρθωσε το λάθος, καθιστώντας το διαδικτυακό χώρο υγιή και αξιόπιστο.

Πώς μπορείς να χρησιμοποιείς την Τεχνητή Νοημοσύνη με ασφάλεια;

Η τεχνητή νοημοσύνη μπορεί να δημιουργήσει εικόνες, βίντεο, ιστορίες ή φωνητικά μηνύματα κατά παραγγελία του χρήστη. Η χρήση της μπορεί να γίνει από διασκεδαστική έως επικίνδυνη, αν δημιουργηθεί βίαιο, προσβλητικό ή παράνομο περιεχόμενο, το οποίο μπορεί να επιφέρει σοβαρές νομικές συνέπειες.

Για παράδειγμα τα deepfakes βίντεο που δείχνουν κάποιους να κάνουν ή να λένε πράγματα που δεν έκαναν ποτέ. Τα Deepfakes ξεγελούν το κόσμο, δημιουργούν σύγχυση και μπορούν να καταστρέψουν μόνιμα την υπόληψη ή τις σχέσεις κάποιου. Για το δικό σου, αλλά και το κοινό καλό, πρόσεχε στη δημιουργία ή την αναδημοσίευση περιεχομένου που έχει δημιουργηθεί από την Τεχνητή Νοημοσύνη, καθώς μπορεί να είναι επιβλαβές και να επιφέρει πολύ σοβαρές συνέπειες.

Με ποιους τρόπους μπορεί να ξεγελαστούμε από την Τεχνητή Νοημοσύνη;

- Να μας υποδυθεί κάποιος άλλος μέσω φωνής, εικόνας ή βίντεο.
- Να δημιουργήσει κάποιος άλλος γυμνές φωτογραφίες ή βίντεο (deepfakes) με εμάς με σκοπό τον εκβιασμό.
- Να δημιουργήσει παράνομο και αρνητικό περιεχόμενο που μπορεί να προκαλέσει ψυχικό τραύμα σε όσους το δουν.

Με αυτές τις γνώσεις, ελπίζουμε ότι αντιλαμβάνεσαι πόσο σημαντικό είναι να είσαι προσεκτικός/ή με ό,τι συναντήσεις στο διαδίκτυο και ότι δεν πρέπει να πιστεύεις όσα βλέπεις ή ακούς εκεί. Να έχεις κριτική σκέψη για να εντοπίζεις το περιεχόμενο που έχει δημιουργηθεί από την τεχνητή Νοημοσύνη.

Image generated by AI

Πώς μπορούμε να εντοπίσουμε το περιεχόμενο που έχει δημιουργηθεί από Τεχνητή Νοημοσύνη;

Είναι δύσκολο αλλά με λίγη προσοχή μπορούμε να το εντοπίσουμε. Αρχικά ψάχνουμε για οτιδήποτε φαίνεται «περίεργο», «χωρίς ατέλειες» ή με παράξενα λάθη που οι άνθρωποι συνήθως δεν κάνουν, όπως περίεργα χέρια ή ασύντακτες προτάσεις. Τα εργαλεία της Τεχνητής Νοημοσύνης μπορούν να παράγουν περιεχόμενο που φαίνεται ή ακούγεται σαν αληθινό.

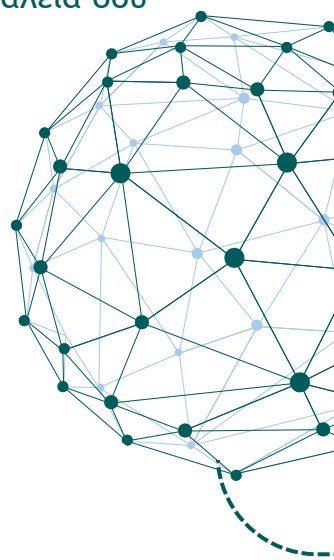
Άλλη μια συμβουλή είναι να διασταυρώνουμε τα γεγονότα. Το περιεχόμενο της Τεχνητής Νοημοσύνης, κυρίως τα κείμενα, ίσως παρουσιάζουν πληροφορίες που δεν είναι ακριβείς ή εξακριβωμένες. Χρησιμοποίησε εργαλεία αντίστροφης αναζήτησης εικόνων για να ελέγξεις αν μια εικόνα έχει δημιουργηθεί ή τροποποιηθεί. Ιδιαίτερη προσοχή χρειάζεται το viral ή το ερωτικό περιεχόμενο καθώς διαδίδεται γρήγορα ενώ μπορεί να είναι παραπλανητικό ή ψευδές.

Σε αυτή την περίπτωση μην το αγνοήσεις, κάνε μια αναφορά στην πλατφόρμα που εμφανίστηκε, προκειμένου να εμποδίσεις την περαιτέρω διάδοση του.

Ασφαλή διαδικτυακά παιχνίδια

Τα παιχνίδια σχετίζονται με ικανότητες, προκλήσεις και την επικοινωνία με άλλα άτομα που έχουν κοινά ενδιαφέροντα. Για να παραμένεις ασφαλής όσο παίζεις, χρειάζεται να συμπεριφέρεσαι υποστηρικτικά προς τους άλλους και με σεβασμό. Αυτό σημαίνει να είσαι ευγενικός/ή, δίκαιος/η και να σέβεσαι τη συμμετοχή των άλλων, με σκοπό όλοι να διασκεδάσουν κατά το παιχνίδι σας.

Γνωρίζουμε όμως ότι δε θα παίξουν όλοι δίκαια. Να είσαι σε ετοιμότητα, να προσέχεις τα προειδοποιητικά σημάδια και να μην εμπιστεύεσαι εύκολα όσους γνωρίζεις στο διαδίκτυο. Οι προσωπικές σου πληροφορίες όπως το όνομα σου, η διεύθυνση ή το σχολείο σου θα πρέπει να παραμένουν ιδιωτικές. Αν κάποιος σε κάνει να νιώσεις αμήχανα βγες από το παιχνίδι ή κάνε του μπλοκ. Η ασφάλεια σου είναι πάντα προτεραιότητα.



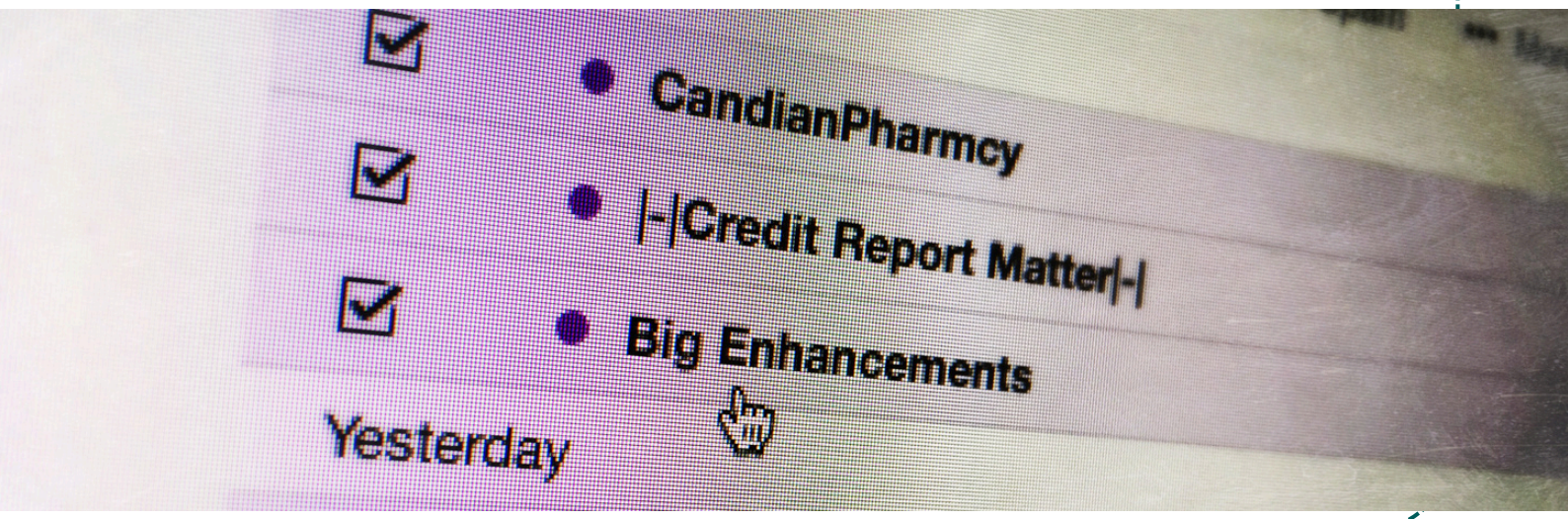
Να θυμάσαι ότι οι διακρίσεις εμφανίζονται συχνά στις κοινότητες των παιχνιδιών και ίσως γίνουν στόχοι συγκεκριμένα άτομα από περιθωριοποιημένες ομάδες. Είναι σημαντικό να φροντίζουμε ο ένας τον άλλον και να υποστηρίζουμε εκείνους που είναι πιο ευάλωτοι. Αν παρατηρήσεις κάποια ρατσιστική συμπεριφορά ή παρενόχληση θα πρέπει να αντιδράσεις και να αναζητήσεις βοήθεια. Μίλα σε κάποιον που εμπιστεύεσαι, είτε είναι φίλος, οικογένεια ή ειδικός. Αν αντιδρούμε σαν ομάδα και αντιμετωπίζουμε τα προβλήματα στην αρχή τους μπορούμε να δημιουργήσουμε χαρούμενη ατμόσφαιρα για όλους στο χώρο των διαδικτυακών παιχνιδιών.

Τι είναι το Phishing;

Το Phishing είναι μια αθέμιτη πρακτική κατά την οποία οι απατεώνες προσποιούνται ότι είναι μια αξιόπιστη εταιρεία ή πρόσωπο για να μας εξαπατήσουν ώστε να μοιραστούμε τις προσωπικές μας πληροφορίες ή τους κωδικούς μας, μέσω των emails, μηνυμάτων ή πλαστών ιστότοπων. Συνήθως προσποιούνται ότι είναι φίλοι που μας χρειάζονται ή μια αξιόπιστη εταιρία που θέλει να μας δώσει ένα βραβείο.

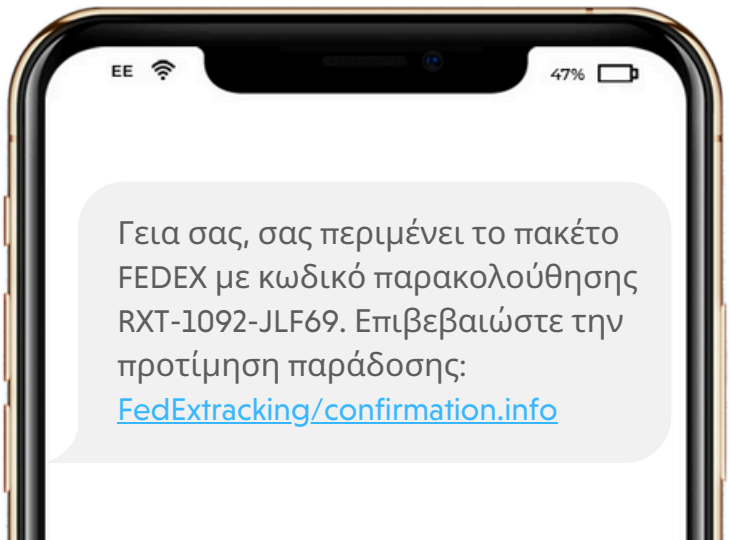
Να προσέχεις:

- Τις επείγουσες καταστάσεις, καθώς δημιουργείται επίτηδες πανικός για βιαστικές κινήσεις.
- Γενικευμένοι χαιρετισμοί που δε χρησιμοποιούν το όνομα σου.
- Γραμμένα λάθος URLs ή μικρές παραλλαγές στην επωνυμία μιας εταιρίας.
- Απρόσμενα δώρα ή βραβεία που μπορούν να διεκδικηθούν μέσω κάποιου συνδέσμου.



Όταν επιλέγουμε συνδέσμους που είναι απάτη υπάρχει κίνδυνος να παραχωρήσουμε σε κάποιον τα στοιχεία της ταυτότητας μας ή τους λογαριασμούς μας. Επομένως θα πρέπει να σιγουρευόμαστε για τη διεύθυνση URL πριν την πατήσουμε, αλλά και για τον αποστολέα των μηνυμάτων και των emails πριν τα διαβάσουμε.

Το phishing που γίνεται μέσω κειμένου, γνωστό και ως «smishing» είναι ιδιαίτερα συχνό και εμφανίζεται ως επείγον μήνυμα από γνωστούς ή εταιρίες, που επιδιώκουν την ευκαιρία να αποσπάσουν τις προσωπικές μας πληροφορίες.



Τι πρέπει να γνωρίζουμε για το Sexting;

Το φλερτ μέσω μηνυμάτων και η αποστολή αποκαλυπτικών φωτογραφιών θεωρείται φυσικό μέσο εξερεύνησης της σεξουαλικότητας και της επικοινωνίας μας με άλλους. Όταν γίνεται με τη συναίνεση όλων των εμπλεκόμενων και με σεβασμό μπορεί να είναι μια πολύ θετική εμπειρία, αλλά υπάρχουν μερικές συμβουλές για να τις έχεις στο μυαλό σου.

ΣΥΝΑΙΝΕΣΗ

Όλοι οι εμπλεκόμενοι θα πρέπει να συμφωνούν με το sexting. Αν κάποιος δε νιώθει καλά, θα πρέπει να σταματήσετε αμέσως.

ΕΠΙΚΟΙΝΩΝΙΑ

Να είστε ειλικρινείς. Να συμφωνήσετε από πριν για τα όρια και να συζητήσετε με ποιο τρόπο θα προστατέψετε το περιεχόμενο που θα ανταλλάξετε.

ΑΝΑΔΡΟΜΗ

Να αναλογίζεστε τα συναισθήματά σας σχετικά με το sexting. Αν αρχίσετε να έχετε αμφιβολίες, πρέπει να αισθάνεστε άνετα να σταματήσετε ανά πάσα στιγμή.

Καλό θα ήταν επίσης να μην δείχνετε ποτέ σε άλλους τα προσωπικά σας μηνύματα και να φροντίζετε ώστε το προσωπικό σας περιεχόμενο να μην είναι προσβάσιμο σε άλλους.

Η κακοποίηση μέσω Sexting

Το Sexting είναι εξ ορισμού προσωπική διαδικασία αλλά κάποιες φορές τα πράγματα δεν πάνε όπως τα θέλουμε. Είτε κατά λάθος, είτε επίτηδες, αν κάποιος διαρρεύσει τις προσωπικές σου φωτογραφίες χωρίς τη συναίνεση σου, διαπράττει κακοποίηση μέσω sexting. Είναι παράνομο και απόλυτη ευθύνη του ατόμου που διέρρευσε χωρίς την άδεια σου. Σε περίπτωση που συμβεί κάτι τέτοιο, είναι λογικό να νιώσεις θυμό, απόγνωση ή ντροπή, αλλά θα πρέπει να θυμάσαι ότι δεν το προκάλεσες εσύ και μπορείς να ζητήσεις βοήθεια.

Υπάρχουν υπηρεσίες για να σε βοηθήσουν σε μία τέτοια δύσκολη στιγμή, όπως μια Γραμμή Βοήθειας που μπορεί να σου προσφέρουν συναισθηματική υποστήριξη αλλά και συμβουλές για να αφαιρεθούν οι εικόνες σου από το διαδίκτυο άμεσα.

Αν κάποιος σε απειλεί ότι θα δημοσιεύσει τις προσωπικές σου φωτογραφίες ή μηνύματα, σε κακοποιεί μέσω sextortion. Συνήθως απαιτούν χρήματα, υπηρεσίες ή επιπλέον αποκαλυπτικό περιεχόμενο προκειμένου να μην διαρρεύσουν τις εικόνες σου. Όλο αυτό είναι πολύ αγχωτικό αλλά υπάρχει πάντα διαθέσιμη υποστήριξη.

Τι να προσέχουμε με τους άγνωστους στο διαδίκτυο;

Σίγουρα σου έχει τύχει να γνωρίσεις κάποιον στο διαδίκτυο και να νιώθεις ότι τον ξέρεις πολύ καιρό. Υπάρχει όμως η πιθανότητα να μην είναι αυτό που υποστηρίζει ότι είναι. Αν αρχίσει να κάνει ερωτήσεις για προσωπικές πληροφορίες ή προσπαθεί να δημιουργήσει ερωτικό κλίμα, πιθανώς να έχεις συναντήσει έναν groomer.

Οι Groomers είναι ενήλικες που υποδύονται τους διαδικτυακούς φίλους σου ώστε να σε χειραγωγήσουν για να συνάψεις μια σεξουαλική σχέση μαζί τους. Είναι ειδικοί στην απάτη και για αυτό είναι δύσκολο να εξακριβώσεις τους αληθινούς σκοπούς τους. Όλοι μπορούν να γίνουν στόχοι ενός groomer αλλά εκείνοι που έχουν περισσότερες πιθανότητες να εξαπατηθούν είναι τα ευάλωτα άτομα, όπως τα μέλη της ΛΟΑΤΚΙ κοινότητας.

Πρόσεχε να εντοπίσεις προειδοποιητικά σημάδια όπως την απαίτηση να κρατήσεις μυστική τη διαδικτυακή σας σχέση, καθώς αυτό είναι σημάδι χειραγώγησης και ελέγχου. Οι υγιείς σχέσεις με αλληλοσεβασμό δεν απαιτούν μυστικότητα. Οι αληθινοί φίλοι δε σου λένε ψέματα ή δε σε πιέζουν σε κάτι με το οποίο νιώθεις άβολα. Αν δεν είσαι σίγουρος/η για κάποιον μην του αποκαλύψεις προσωπικές πληροφορίες και προσπάθησε να διασταυρώνεις όσα σου λέει. Αν σκοπεύεις να συναντήσεις κάποιον που γνώρισες στο διαδίκτυο, ενημέρωνε πάντα τους γονείς σου και πάρε μαζί σου έναν φίλο που εμπιστεύεσαι.

Τι θα πρέπει να προσέχεις;

Προσέχουμε για περίεργα σημάδια, όπως το να μας πιέζει κάποιος να κάνουμε κάτι με το οποίο δε νιώθουμε άνετα, είτε πρόκειται για cyberbullying, παρενόχληση, ή αποστολή ανεπιθύμητων εικόνων, έως και πιο ύπουλη χειραγώγηση. Οποιαδήποτε παρόμοια συμπεριφορά θεωρείται κακοποιητική και απαράδεκτη και θα πρέπει να αναφέρεται στις αρχές.

ΣΥΜΒΟΥΛΗ

Αν κάποιος φίλος/η σας εμφανίσει ξαφνικές αλλαγές στη συμπεριφορά του, όπως μυστικοπάθεια, απομόνωση ή υπερβολική προσκόλληση στο κινητό του/της, θα πρέπει να σε ενημερώσουμε ότι μάλλον έχει κάποια προβλήματα στο διαδίκτυο. Αν αντιληφθείς ότι κάτι δεν πάει καλά, πήγαινε και μίλησέ του/της με ενσυναίσθηση, δείχνοντας του/της ότι δε θα πρέπει να φοβάται να σου μιλήσει.

Μπορείς να αρχίσεις με το «Βλέπω ότι δεν είσαι καλά τελευταία, αν θέλεις να μιλήσεις, είμαι εδώ.»
Η υποστήριξη σου μπορεί να αλλάξει πολλά.

Section 03

Αναζήτηση Βοήθειας

Αναζητώντας την υποστήριξη

Η ασφάλεια σου είναι προτεραιότητα. Αν εκφοβίζεσαι, εκβιάζεσαι, ή αν οι προσωπικές σου φωτογραφίες έχουν διαρρεύσει στο διαδίκτυο, μην διστάσεις να μιλήσεις σε κάποιον που εμπιστεύεσαι, είτε αυτός είναι φίλος, οικογένεια, καθηγητής ή κάποιος ειδικός. Να θυμάσαι ότι ο ειδικός/ σύμβουλος είναι δεσμευμένος για το απόρρητο και σκοπός του είναι να σε βοηθήσει χωρίς να σε κρίνει.

Αναζήτησε τις Γραμμές Βοήθειας

Οι διαδικτυακές απειλές μπορούν να σε οδηγήσουν να νιώθεις καταβεβλημένος, Η αναζήτηση υποστήριξης σε μια Γραμμή Βοήθειας μπορεί να σου παρέχει τον ασφαλή χώρο που χρειάζεσαι για να συζητήσεις τις ανησυχίες σου και να λάβεις τη βοήθεια που έχεις ανάγκη. Μπορείς να βρεις την εθνική γραμμή Βοήθειας εδώ: https://www.help-line.gr/

Αναφορά της τοξικότητας στις εφαρμογές

Τα κοινωνικά μέσα θα έπρεπε να είναι ασφαλείς χώροι επικοινωνίας με τους φίλους μας, χώροι έκφρασης και δημιουργικότητας. Αν συναντήσεις κάτι άσχημο, είτε πρόκειται για ακατάλληλο περιεχόμενο ή κακοποιητική συμπεριφορά πρέπει να το αναφέρεις στην πλατφόρμα που συνάντησες το περιστατικό.

Αναφορά Κακοποιητικού περιεχομένου

Οι Γραμμές Καταγγελίας προσπαθούν να αφαιρούν άμεσα οποιοδήποτε περιεχόμενο διαδικτυακής σεξουαλικής κακοποίησης που τους έχει αναφερθεί. Αν οι προσωπικές σας φωτογραφίες έχουν διαρρεύσει ή αν συναντήσετε ακατάλληλο περιεχόμενο με παιδιά θα πρέπει να το αναφέρετε αμέσως. Βρείτε την εθνική γραμμή καταγγελιών εδώ: https://www.safeline.gr/

Το εργαλείο Take it Down: Αν είσαι πάνω από 18 ετών και διέρρευσε στο διαδίκτυο μια προσωπική φωτογραφία σου όταν ήσουν ανήλικος το Take it Down μπορεί να σε βοηθήσει να προστατεύσεις την ιδιωτικότητα σου αφαιρώντας το περιεχόμενο αυτό από το διαδίκτυο.

Αν θέλεις να μάθεις περισσότερα σχετικά με τις επιλογές που έχεις για να διατηρήσεις τις εικόνες σου ασφαλείς, αναζήτησε βοήθεια στο Ελληνικό Κέντρο Ασφαλούς Διαδικτύου εδώ: https://saferinternet4kids.gr/.
Η συγκεκριμένη πλατφόρμα προσφέρει συμβουλές, πηγές, οδηγίες και καθοδήγηση για την ασφαλέστερη πλοήγηση στο διαδίκτυο.

Αναφορές

- 5 Reasons software updates are important
- App permissions explained: Which ones should you allow?
- 6 Tips to know if an app is safe
- How bad actors access webcams and other cameras
- Secret Selfies: Can Phones Take Pictures and Videos of You Without Your Knowledge?
- Location Services: A Quick Guide for iPhone and Android
- Family Sharing - Share your favourite things with your favourite people
- 5 Best Parental Controls for Teenagers in 2024
- Best private search engines that won't track you in 2024
- Share with Care: Staying Safe on Social Media
- How to Recognise and Avoid Phishing Scams
- Bullying, a guide for young people
- Child Safety in Gaming
- What is self-generated CSAM?
- The impact of online grooming
- 5 ways to Protect Yourself from Sexual Abuse Online
- Support and Safety through Helplines

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency. Neither the European Union nor the European Education and Culture Executive Agency can be held responsible for them.

INHOPE

Ένας Οδηγός Ψηφιακού Αλφαβητισμού για νέους, εκπαιδευτικούς, γονείς και γραμμές καταγγελιών.

Μάθετε περισσότερα και υποστηρίξτε μας στο inhope.org

Funded by the European Union