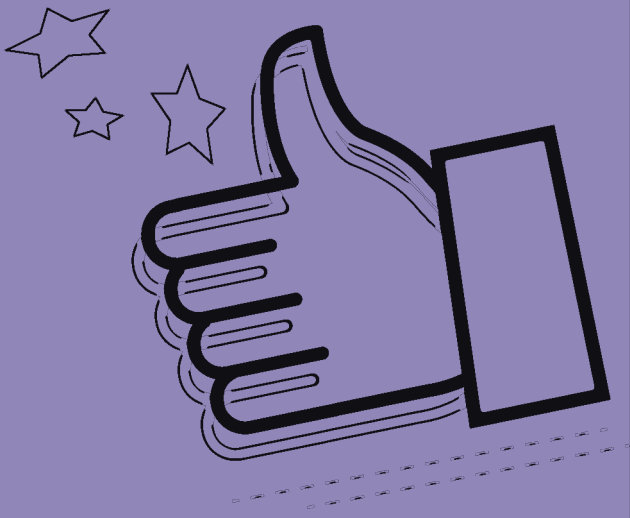
#social_media_&_facebook

κίνδυνοι και συμβουλές σχετικά
με τα δημοφιλή κοινωνικά δίκτυα στο Internet



Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Προστασίας του Πολίτη

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Τι είναι οι ιστοσελίδες κοινωνικής δικτύωσης;

Πρόκειται για ιστοσελίδες που προσφέρουν στους χρήστες τους τη δυνατότητα να δημιουργήσουν το προσωπικό τους προφίλ, να παρουσιάσουν τον εαυτό τους και να επικοινωνήσουν με άλλους χρήστες στο Διαδίκτυο. Τους χρήστες αυτούς μπορεί να τους γνωρίζουμε στην πραγματική μας ζωή ή να είναι και εντελώς άγνωστοι.

Μέσα από αυτή την επικοινωνία δημιουργούνται online κοινότητες, όπου άνθρωποι με κοινά ενδιαφέροντα μπορούν να μοιράζονται πληροφορίες και να εκφράζουν τις απόψεις τους. Δεν χρειάζονται ιδιαίτερες τεχνικές γνώσεις για να δημιουργήσει κάποιος το προφίλ του και να ανεβάσει περιεχόμενο (σχόλια, φωτογραφίες, βίντεο), το οποίο θα μοιραστεί αργότερα με άλλους χρήστες.

Οι πιο δημοφιλείς ιστοσελίδες κοινωνικής δικτύωσης είναι το Facebook, το Twitter, το Instagram και το TikTok.

Όπως ισχύει γενικά για το Διαδίκτυο, λέμε ΝΑΙ στη χρήση των Μέσων Κοινωνικής Δικτύωσης, αλλά ακολουθώντας βασικούς κανόνες.

Η γνώση των κανόνων ασφαλείας, η ανάπτυξη κριτικής και αντιληπτικής ικανότητας και η ικανότητα αναγνώρισης των κινδύνων είναι βασικά εφόδια για την ασφαλή πλοήγησή μας στα Μέσα Κοινωνικής Δικτύωσης.

Κίνδυνοι Μέσων Κοινωνικής Δικτύωσης

Ορισμένοι από τους κινδύνους που ελλοχεύουν στα μέσα κοινωνικής δικτύωσης και θα πρέπει να γνωρίζουμε:

• Η πληροφορία μένει για πάντα στο Διαδίκτυο

Μια φωτογραφία ή ένα σχόλιο που ανεβαίνει σε μια σελίδα κοινωνικής δικτύωσης δημοσιεύεται σε έναν αριθμό χρηστών. Ακόμα κι αν επιλέξετε να αποσύρετε αυτή την πληροφορία, αυτή παραμένει αποθηκευμένη στα αρχεία της εταιρείας όπου ανήκει η σελίδα, απλώς δεν εμφανίζεται στο Διαδίκτυο. Επίσης, οποιοσδήποτε από τους χρήστες που τη βλέπει, μπορεί να την αντιγράψει και να τη χρησιμοποιήσει στο μέλλον.

• Εντοπισμός θέσης

Πολλοί χρήστες επιλέγουν να δημοσιεύσουν στις ιστοσελίδες κοινωνικής δικτύωσης πού βρίσκονται κάθε στιγμή. Είτε γίνεται συνειδητά, με την επιλογή της δημοσίευσης της θέσης μέσα από την ιστοσελίδα, είτε αυτόματα με τη χρήση εφαρμογών στο κινητό μας, πρέπει να θυμόμαστε ότι η δημοσίευση της θέσης μας μπορεί να χρησιμοποιηθεί από κακόβουλους χρήστες, για να μας εντοπίσουν, ή από επίδοξους διαρρήκτες για να γνωρίζουν πότε λείπουμε από το σπίτι.

• Κλοπή Ταυτότητας

Πρόκειται για την περίπτωση που κάποιος χρήστης του Διαδικτύου παριστάνει άλλους χρήστες και παραπλανά ή παρενοχλεί. Μπορεί να εκδηλωθεί με δύο τρόπους: α) με την κλοπή του πραγματικού σας προφίλ, β) με τη δημιουργία ενός νέου προφίλ που θα περιλαμβάνει τα δικά σας στοιχεία, όπως ονοματεπώνυμο ή φωτογραφίες.

• Παραχώρηση των δεδομένων σε τρίτες εταιρείες

Οι εταιρείες που κατέχουν τις ιστοσελίδες κοινωνικής δικτύωσης έχουν πρόσβαση στις πληροφορίες που δημοσιεύετε σε αυτές αλλά και σε δεδομένα που προκύπτουν από τη σύνδεσή σας, όπως η IP διεύθυνση, η γεωγραφική περιοχή όπου ανήκετε, και ο browser που χρησιμοποιείτε. Οι πληροφορίες αυτές μπορούν να παραχωρηθούν σε τρίτες εταιρείες και να χρησιμοποιηθούν σε μεθόδους στοχευμένης διαφήμισης.

• Εξειδικευμένες απάτες

Οι πληροφορίες που δημοσιεύουμε στο προφίλ μας μπορούν να χρησιμοποιηθούν από επιτήδειους, ώστε να εξειδικεύσουν τις επιθέσεις ηλεκτρονικού «ψαρέματος» (phishing) και να έχουν μεγαλύτερη πιθανότητα να εξαπατήσουν εσάς ή τους φίλους σας.

Συμβουλές προστασίας
Και όσα δεν γνωρίζατε...

- Δεν δημοσιεύουμε πληροφορίες που μπορεί να βοηθήσουν κάποιον άγνωστο να μας εντοπίσει. Η διεύθυνση και το τηλέφωνό μας, η επιχείρηση όπου εργαζόμαστε ή το σχολείο στο οποίο φοιτούμε, μπορεί να χρησιμοποιηθούν από αγνώστους για να μας πλησιάσουν. Πριν αναρτήσουμε κάποιο «story», το σκεφτόμαστε καλά, διότι εκείνη τη στιγμή δηλώνουμε το πού και με ποιους είμαστε.
- Δεν χρησιμοποιούμε τα μέσα κοινωνικής δικτύωσης ως ημερολόγιο. Δεν είναι ανάγκη το προφίλ μας να περιέχει όλες τις πληροφορίες για την καθημερινή μας δραστηριότητα.
- Ελέγχουμε τις ρυθμίσεις ασφαλείας και απορρήτου για το προφίλ μας. Ρυθμίζουμε έτσι ώστε οι πληροφορίες μας να είναι ορατές μόνο στους φίλους μας.
- Δεν επιτρέπουμε σε εφαρμογές (applications) που δεν γνωρίζουμε να χρησιμοποιούν τα στοιχεία του λογαριασμού μας πέρα από το ονοματεπώνυμό μας, εάν δεν είναι απολύτως απαραίτητο για την παρεχόμενη υπηρεσία, ή να δημοσιεύουν σχόλια στον λογαριασμό μας.
- Τα social media συχνά προβάλλουν έναν τέλειο τρόπο ζωής, ένα τέλειο πρότυπο ανθρώπου που είναι «μέσα σε όλα». Δεν αλλάζουμε τη συμπεριφορά μας προκειμένου να προσαρμοστούμε στα «πρότυπα» των social media και δεν νιώθουμε αδύναμοι αν δεν ταυτιζόμαστε με τις τάσεις των άλλων χρηστών.
- Στα social media διαδίδονται συχνά παραπλανητικές ή πλήρως ψευδείς ειδήσεις (fake news). Επιλέγουμε να ενημερωνόμαστε από αξιόπιστες πηγές και να διασταυρώνουμε τις πληροφορίες που εμφανίζονται.
- Σκεφτόμαστε πριν δημοσιεύσουμε ένα σχόλιο ή μια φωτογραφία: Μήπως θα μας έφερνε σε δύσκολη θέση εάν το έβλεπαν τα μέλη της οικογένειάς μας ή ο μελλοντικός εργοδότης μας;
- Πριν δημοσιεύσουμε μια πληροφορία στα μέσα κοινωνικής δικτύωσης, σκεφτόμαστε ότι δεν «σβήνουμε» ποτέ από το Διαδίκτυο. Θα μπορούσε να επηρεάσει αρνητικά τη μελλοντική μας ζωή;

- Ελέγχουμε το περιεχόμενο που δημοσιεύουν οι φίλοι μας στα μέσα κοινωνικής δικτύωσης. Μήπως δεν αρμόζει στο προφίλ που θέλουμε να προβάλλουμε στον υπόλοιπο κόσμο;
- Σεβόμαστε τους φίλους μας. Εάν η πληροφορία που πρόκειται να δημοσιεύσουμε αφορά κάποιον φίλο μας, π.χ. πρόκειται για μια κοινή φωτογραφία, τότε επικοινωνούμε με τον φίλο μας και ζητάμε την άδειά του για τη δημοσίευση.
- Δεν δεχόμαστε αιτήματα φιλίας από αγνώστους. Δεν εμπιστευόμαστε τα στοιχεία που δηλώνει κάποιος στο προφίλ του στα μέσα κοινωνικής δικτύωσης. Το όνομα, η ηλικία, ακόμα και οι φωτογραφίες του προφίλ μπορεί να μην είναι αληθινά.
- Δίνουμε ιδιαίτερη σημασία στα παιδιά. Μιλάμε για τους κινδύνους στα μέσα κοινωνικής δικτύωσης και δεν τους επιτρέπουμε να συναντούν άτομα που γνώρισαν μέσα από αυτά.
- Όταν δεχόμαστε αιτήματα φιλίας από άτομα που γνωρίζουμε στην πραγματική μας ζωή, επικοινωνούμε τηλεφωνικά μαζί τους και ρωτάμε αν το προφίλ τούς ανήκει, πριν αποδεχθούμε το αίτημα.
- Αν κάποιος φίλος επικοινωνήσει μαζί μας και μας ζητήσει χρήματα, επικοινωνούμε πρώτα μαζί του τηλεφωνικά. Ενδέχεται να έχει κλαπεί το προφίλ από κακόβουλους χρήστες.
- Καμία ιστοσελίδα κοινωνικής δικτύωσης δεν πρόκειται να σας αποστείλει e-mail ζητώντας να επιβεβαιώσετε τον κωδικό μας, συμπληρώνοντάς τον σε κάποια φόρμα. Εάν λάβουμε ένα τέτοιο e-mail, πιθανόν να πρόκειται για επίθεση ηλεκτρονικού «ψαρέματος» (phishing).
- Σιγουρευόμαστε ότι ο κωδικός ασφαλείας για τον λογαριασμό μας είναι «δυνατός». Δεν χρησιμοποιούμε κωδικούς που εύκολα μπορεί κανείς να μαντέψει, όπως η ημερομηνία γέννησής μας.
- Δεν χρησιμοποιούμε τον ίδιο κωδικό με άλλους λογαριασμούς, όπως το e-mail μας, και θυμόμαστε να αλλάζουμε τον κωδικό μας σε τακτά χρονικά διαστήματα.
- Αν αντιληφθούμε ότι ο λογαριασμός μας έχει κλαπεί, το αναφέρουμε το συντομότερο στο διαχειριστή του μέσου κοινωνικής δικτύωσης, μέσω της προτεινόμενης από αυτό διαδικασίας (report).

- Μελετάμε τις διαδικασίες προστασίας της ιδιωτικότητας και ασφάλειας λογαριασμού που παρέχει το μέσο κοινωνικής δικτύωσης, και τις ενεργοποιούμε. Επιλέγουμε εναλλακτικούς τρόπους για ανάκτηση του λογαριασμού μας ή περιορισμό των ατόμων που βλέπουν το προφίλ μας. Επισκεπτόμαστε τις ρυθμίσεις του λογαριασμού μας ανά τακτά χρονικά διαστήματα για να ανακαλύψουμε νέες προσφερόμενες υπηρεσίες.
- Διαβάζουμε αναλυτικά τους όρους χρήσης πριν δημιουργήσουμε έναν λογαριασμό (sign up). Εάν δεν συμφωνούμε με κάποιον από τους όρους χρήσης, δεν προχωράμε στη δημιουργία του λογαριασμού. Επισκεπτόμαστε ξανά τους όρους χρήσης ανά τακτά χρονικά διαστήματα, ώστε να ενημερωθούμε για τυχόν αλλαγές.
- Πριν επιτρέψουμε σε μια εφαρμογή να αποκτήσει πρόσβαση στο προφίλ μας, διαβάζουμε προσεκτικά τις πληροφορίες στις οποίες θα έχει πρόσβαση και τις ενέργειες που θα μπορεί να πραγματοποιήσει στο προφίλ.
- Εάν κάποιος χρήστης μάς ενοχλεί, τον αναφέρουμε στον διαχειριστή της ιστοσελίδας πατώντας την επιλογή «Αναφορά/Μπλοκάρισμα» (Report/Block). Στο μενού ενεργειών της αναφοράς μπορούμε να δηλώσουμε την αιτία για την οποία μας παρενοχλεί, π.χ. παριστάνει εμάς (κλοπή ταυτότητας), μας προσβάλλει. Μπορούμε, επίσης, να επιλέξουμε να μπλοκάρουμε κάποιον χρήστη που μας ενοχλεί, ώστε να μην λαμβάνουμε μηνύματά του.
- Ασφαλίζουμε τους λογαριασμούς μας (χρησιμοποιούμε την επιλογή two-step authentication, ισχυρούς κωδικούς πρόσβασης και διαφορετικούς ανά λογαριασμό).

Θυμηθείτε:

Μπορεί να πάρει χρόνια
να δημιουργηθεί ένας λογαριασμός
και λίγα δευτερόλεπτα για να χαθεί.

ΕΠΙΚΟΙΝΩΝΙΑ

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος – Cyber Crime Division
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11522
e-mail: **ccu@cybercrimeunit.gov.gr**, Τηλ.:**11188**, Fax: **2131527471**

Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδας
Μοναστηρίου 326, Τ.Κ. 54 121 Θεσσαλονίκη
e-mail: **ydheve@cybercrimeunit.gov.gr**, Τηλ.:**11188**, Fax: **2131527666**

Ενημερωθείτε για θέματα ασφαλούς πλοήγησης στο Διαδίκτυο στο **https://www.cyberkid.gov.gr** και στο **https://www.cyberalert.gr**

Για άμεση ενημέρωση που αφορά θέματα
της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος
ακολουθήστε μας στα μέσα κοινωνικής δικτύωσης:

https://www.facebook.com/cyberkid.gov.gr/
https://www.facebook.com/CyberAlertGR/
https://www.instagram.com/cyberalert.gr/
https://twitter.com/CyberAlertGR
Youtube channel: Cyber Alert