CYBER CRIME DIVISION

ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται σε ένα άτομο και το περιγράφει, όπως ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση, εκπαίδευση, οικονομική κατάσταση, κ.ά. Τα προσωπικά σου δεδομένα χρησιμοποιούνται σε καθημερινή βάση, καθώς εσύ περιηγείσαι στο Διαδίκτυο.

ΤΙ ΝΑ ΠΡΟΣΕΧΕΤΕ;

Η ανωνυμία στο Διαδίκτυο και η δυνατότητα δημιουργίας ψεύτικων προφίλ, οδηγεί στο να μην ξέρουμε πραγματικά με ποιόν επικοινωνούμε. Άντρες χρησιμοποιούν προφίλ με γυναικεία χαρακτηριστικά και το αντίστροφο, προσπαθώντας να αποσπάσουν τα προσωπικά στοιχεία ενός παιδιού και να το παρασύρουν.

Προτρέψτε το παιδί να μην χρησιμοποιεί εύκολους κωδικούς πρόσβασης στις ιστοσελίδες που εγγράφεται, όπως ημερομηνίες γέννησης.

Διαβάστε τους όρους χρήσης των ιστοσελίδων που επισκέπτεται και εγγράφεται το παιδί σας (ιστοσελίδες κοινωνικής δικτύωσης, στα forums και τα ιστολόγια). Στη συνέχεια συστήστε και στο παιδί σας να κάνει το ίδιο.

Συμβουλεύστε το παιδί σας να μη δημοσιεύει φωτογραφίες ή βίντεο που δε θα έδειχνε σε ανθρώπους στον «πραγματικό κόσμο» ή που θα μπορούσε να το φέρει σε δύσκολη θέση όταν μεγαλώσει.

Τονίστε του ότι η δημοσιοποίηση υλικού (φωτογραφίες ή βίντεο) που αφορά τρίτους, απαιτεί σε κάθε περίπτωση την άδειά τους.

Εφόσον το παιδί διαθέτει το δικό του ιστολόγιο, βεβαιωθείτε ότι το περιεχόμενό του δεν είναι υβριστικό ή ρατσιστικό.

Και μην ξεχνάτε ότι πρέπει πρώτα εσείς οι γονείς να ακολουθείτε τους κανόνες ασφαλούς πλοήγησης ώστε να δίνετε το παράδειγμα στα παιδιά σας... σκεφτείτε πώς θα ένιωθε το παιδί σας αν ενώ το παροτρύνετε να προφυλάσσει τις προσωπικές του φωτογραφίες εσείς τις ανεβάζετε στο Facebook; Διδάξτε στο παιδί πως όπως συμπεριφέρεται στην πραγματική ζωή, έτσι θα πρέπει να συμπεριφέρεται και στο Διαδίκτυο.

CHAT ROOMS

Με τον όρο **chat rooms (δωμάτια επικοινωνίας)** αναφερόμαστε σε διαδικτυακούς χώρους που επιτρέπουν την άμεση και σε πραγματικό χρόνο επικοινωνία μεταξύ δύο ή περισσότερων χρηστών.

ΧΡΗΣΙΜΕΣ ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΝΑ ΒΟΗΘΗΣΟΥΜΕ ΤΑ ΠΑΙΔΙΑ ΜΑΣ ΝΑ ΑΠΟΦΥΓΟΥΝ ΤΟΥΣ ΚΙΝΔΥΝΟΥΣ ΣΤΑ CHAT ROOMS:

Ενημερωθείτε για το πρωτόκολλο επικοινωνίας που χρησιμοποιείται στα chat rooms (emoticons, greeklish, ακρωνύμια). Ακόμη καλύτερα ζητήστε από το παιδί σας να σας εκπαιδεύσει!!!

Συζητήστε με τα παιδιά σας για την δραστηριότητά τους στα chat rooms, ποια chat rooms επισκέπτονται ή ποια θα ήθελαν να επισκεφτούν, για τι θέματα συζητάνε κ.λπ..

Ενθαρρύνετε τα παιδιά σας να σας μιλήσουν για τους νέους εικονικούς τους φίλους.

Εξηγήστε τους γιατί στο Διαδίκτυο δεν πρέπει να εμπιστεύονται άτομα που δε γνωρίζουν στην πραγματική τους ζωή και δεν πρέπει να τους αποκαλύπτουν πληροφορίες (π.χ. αριθμό τηλεφώνου, διεύθυνση κατοικίας ή όνομα σχολείου) για τα ίδια ή την οικογένειά τους.

Μιλήστε τους σχετικά με τους πιθανούς κινδύνους του διαδικτυακού εκφοβισμού, της αποπλάνησης, της υποκλοπής προσωπικών δεδομένων και της ανταλλαγής ανάρμοστων φωτογραφιών.

Προτρέψτε τα να σας αναφέρουν κάθε περίπτωση που έχουν υποστεί οποιουδήποτε είδους παρενόχληση ή συμπεριφορά που τα έκανε να αισθανθούν αμηχανία ή φόβο.

Παρακινείστε τα παιδιά σας να χρησιμοποιούν ψευδώνυμο το οποίο όμως δεν παραπέμπει στην ηλικία ή το φύλο τους.

Διδάξτε τα παιδιά σας πώς να σώζουν αντίγραφο μιας συνομιλίας και πώς να αποκλείουν/να αγνοούν κάποιον και να αναφέρουν κάτι ανάρμοστο στον διαχειριστή του chat room.

Σε κάθε περίπτωση **το κλειδί είναι η επικοινωνία με τα παιδιά!!!** Δεν θα πρέπει να αισθάνονται ότι εάν τους συμβεί κάτι κακό θα θεωρηθούν υπεύθυνα. Αντίθετα, πρέπει να αισθάνονται ότι οι γονείς τους θα δείξουν κατανόηση και θα τα βοηθήσουν να αντιμετωπίσουν τους κινδύνους και να χρησιμοποιήσουν το Διαδίκτυο με ασφάλεια.

CYBERBULLYING

Ο ψηφιακός εκφοβισμός είναι οποιαδήποτε πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς που πραγματοποιείται μέσω του Διαδικτύου και των κινητών τηλεφώνων, η οποία επαναλαμβάνεται ανά τακτά ή άτακτα χρονικά διαστήματα. Στόχος του επιτιθέμενου είναι να προκαλέσει ζημιά ή να βλάψει το θύμα του.

ΠΩΣ ΕΚΔΗΛΩΝΕΤΑΙ

Αποστολή ανεπιθύμητων μηνυμάτων με υβριστικό-προσβλητικό-σεξουαλικό-απειλητικό-εκβιαστικό περιεχόμενο.

Διάδοση προσβλητικών φημών online (π.χ. ιστοσελίδες κοινωνικής δικτύωσης).

Δυσφήμηση σε τρίτους κάνοντας αναρτήσεις ή στέλνοντας email χρησιμοποιώντας τους κωδικούς πρόσβασης του θύματος.

Ανάρτηση φωτογραφιών-βίντεο στο Διαδίκτυο, ιστοσελίδες, blogs, chat rooms.

Ενοχλητικές κλήσεις και sms στο κινητό τηλέφωνο.

Η δημιουργία ιστοσελίδων που στοχοποιούν συγκεκριμένα άτομα καλώντας άλλους να δημοσιεύσουν μηνύματα μίσους.

Η αποστολή ιών (ειδικών κακόβουλων προγραμμάτων trojan horses (δούρειοι ίπποι) με σκοπό την υποκλοπή κωδικών.

Εκφοβισμός στη διάρκεια ενός διαδραστικού online παιχνιδιού.

ΤΙ ΠΡΟΤΕΙΝΟΥΜΕ ΣΕ ΠΕΡΙΠΤΩΣΕΙΣ ΕΚΔΗΛΩΣΗΣ CYBERBULLYING;

Η επικοινωνία με το παιδί είναι το κλειδί! Είναι σημαντικό να ακούσετε προσεκτικά τι λέει το παιδί για τις online εμπειρίες του και να επισκεφτείτε τις ιστοσελίδες που το παιδί σας επισκέπτεται.

Θα πρέπει να κρατήσετε όλα τα αποδεικτικά στοιχεία κι όχι να τα διαγράψετε. Είναι χρήσιμα σε μια πιθανή ψηφιακή διερεύνησή τους από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.

Συχνά, αυτός που κάνει cyberbullying είναι κάποιος γνωστός αυτού που το υφίσταται. Σε αυτήν την περίπτωση είναι σημαντικό να ενημερωθούν οι γονείς του παιδιού για τη συμπεριφορά του και το σχολείο του (διευθυντής-καθηγητής).

Σε περιπτώσεις όπου η παρενόχληση επιμένει και προέρχεται από άγνωστο αποστολέα, μπορείτε να καταγγείλετε το περιστατικό στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.

Ζητήστε τη βοήθεια ενός ειδικού σε τέτοιου είδους θέματα (ψυχολόγου).

ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

Με τον όρο Μέσα Κοινωνικής Δικτύωσης αναφερόμαστε σε ιστοτόπους, στους οποίους οι χρήστες μπορούν να δημιουργήσουν προσωπικές σελίδες, να ανταλλάξουν πληροφορίες και περιεχόμενο, να επικοινωνήσουν και να διασκεδάσουν μέσω εφαρμογών και παιχνιδιών, χωρίς να διαθέτουν εξειδικευμένες τεχνικές γνώσεις.

Οι πιο δημοφιλείς ιστοσελίδες κοινωνικής δικτύωσης είναι το Facebook, το Twitter, το Instagram και το Youtube. Λέμε **ΝΑΙ στη χρήση των Μέσων Κοινωνικής Δικτύωσης**, αλλά ακολουθώντας βασικούς κανόνες.

ΑΚΟΛΟΥΘΟΥΝ ΧΡΗΣΙΜΕΣ ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΝΑ ΒΟΗΘΗΣΟΥΜΕ ΤΑ ΠΑΙΔΙΑ ΝΑ ΑΠΟΦΥΓΟΥΝ ΤΟΥΣ ΚΙΝΔΥΝΟΥΣ ΤΩΝ ΜΕΣΩΝ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ:

Μείνετε κοντά στα παιδιά σας και εμπλακείτε σε κάθε διαδικτυακή τους δραστηριότητα στα Μέσα Κοινωνικής Δικτύωσης με τον ίδιο τρόπο που κάνετε στις δραστηριότητες του σχολείου.

Αφιερώστε λίγο από το χρόνο σας για να περιηγηθείτε σε αυτά.

Θυμηθείτε ότι η απαγόρευση οδηγεί, συνήθως, σε αντίθετα αποτελέσματα.

Εξηγήστε στα παιδιά σας γιατί δε δημοσιοποιούμε υλικό με προσωπικά δεδομένα μας στο Διαδίκτυο.

Να έχετε υπόψη σας ότι για ο,τιδήποτε δημοσιεύουμε στα Μέσα Κοινωνικής Δικτύωσης αποποιούμαστε τα πνευματικά δικαιώματα.

Συμβουλεύστε τα παιδιά σας να μην δημοσιοποιούν την καθημερινή τους δραστηριότητα στα Μέσα Κοινωνικής Δικτύωσης μέσω της διαδικασίας check in. Το ίδιο ισχύει και για την ανάρτηση φωτογραφιών, στις οποίες φαίνεται καθαρά το σπίτι τους, το σχολείο ή το μέρος που συχνάζουν.

Τονίστε στα παιδιά σας ότι δεν εμπιστευόμαστε άτομα τα οποία δεν γνωρίζουμε και στην πραγματική ζωή.

Προσοχή απαιτείται και στις πληροφορίες που δίνουμε και στο περιεχόμενο (αρχεία, εικόνες, βίντεο) που ανταλλάσσουμε με οποιονδήποτε χρήστη του Διαδικτύου. Ακόμη και οι γνωστοί μπορεί να αποδειχθούν άγνωστοι!

Αποτρέψτε τα παιδιά σας να συναντηθούν με άτομα που γνώρισαν μέσω των Μέσων Κοινωνικών Δικτύωσης.

Κατά τη δημιουργία του λογαριασμού, συμβουλέψτε τα παιδιά σας να επιλέγουν ασφαλείς κωδικούς και να πραγματοποιήσουν τις απαραίτητες ρυθμίσεις απορρήτου ώστε ο λογαριασμός τους να είναι περισσότερο ασφαλής.

Αν αντιληφθείτε ότι έχουν κλέψει τον λογαριασμό σας ή των παιδιών σας, αναφέρετε την κλοπή του λογαριασμού στο μέσο κοινωνικής δικτύωσης μέσω της προτεινόμενης από αυτό διαδικασίας (report).

ΔΙΑΔΙΚΤΥΑΚΑ ΠΑΙΧΝΙΔΙΑ

Τα διαδικτυακά παιχνίδια είναι δισδιάστατα ή τρισδιάστατα παιχνίδια που παίζονται στον ηλεκτρονικό υπολογιστή ή στις παιχνιδομηχανές και, μέσω του διαδικτύου, ο χρήστης μπορεί να παίζει και να αλληλεπιδρά σε έναν ενιαίο, εικονικό κόσμο.

Ο κόσμος που περιγράφουν δε σταματά ποτέ και υφίσταται ακόμα και όταν ο παίκτης δεν είναι συνδεδεμένος. Οι διαδικτυακές δυνατότητες επιτρέπουν την ταυτόχρονη επικοινωνία χιλιάδων παικτών, από διαφορετικές χώρες και πολιτισμικό υπόβαθρο, και την αλληλεπίδρασή τους.
Επίσης, προσφέρουν ένα ισχυρότατο σύστημα συνεχών ανταμοιβών μέσα από πίστες και ανταμοιβές, μέσα σε έναν κόσμο που συνεχώς εξελίσσεται και εμπλουτίζεται. Τα διαδικτυακά παιχνίδια κρατάνε τους παίκτες σε εγρήγορση, και είναι σχεδιασμένα για να προσελκύουν μεγάλους αριθμούς παικτών, ενώ τα τελευταία χρόνια αποτελούν μια ξεχωριστή μόδα.

ΕΘΙΣΜΟΣ

Οι έρευνες δείχνουν ότι η συντριπτική πλειοψηφία των χρηστών του διαδικτύου που παρουσιάζουν κατάχρηση ή εθισμό σε αυτό, είναι παίκτες διαδικτυακών παιχνιδιών.

ΣΥΜΠΤΩΜΑΤΑ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΜΑΣ ΠΡΟΒΛΗΜΑΤΙΣΟΥΝ

Το παιδί ασχολείται συνεχώς με το διαδίκτυο, παραμελώντας συχνά τις υποχρεώσεις του.

Το παιδί ξεχνιέται συχνά στον υπολογιστή και δεν έχει συναίσθηση του χρόνου που αναλώνει σε αυτόν.

Προτιμά τα παιχνίδια στο διαδίκτυο, από το να συναντά φίλους του, με αποτέλεσμα να απομονώνεται.

Πέφτει η απόδοση του στο σχολείο.

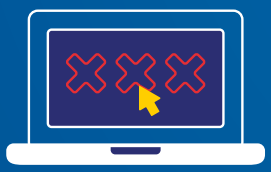
Το διαδίκτυο το απασχολεί ακόμα και την ώρα του φαγητού ή την ώρα που διαβάζει.

Αντιδρά πολύ νευρικά, θυμωμένα ή επιθετικά όταν κάποιος το διακόπτει από το παιχνίδι ή από τη συζήτηση που έχει online.

Ξενυχτά συχνά για να μένει συνδεδεμένος/ συνδεδεμένη στο διαδίκτυο.

Θα πρέπει λοιπόν να παρατηρήσουμε τα προειδοποιητικά σημάδια, να αντιδράσουμε και να βρούμε έναν τρόπο διαχείρισης της κατάστασης, θέτοντας ένα πλαίσιο ώστε να απομακρύνουμε το παιδί ή τον έφηβο από τη μόνιμη ασχολία του με το διαδίκτυο.
Επιπλέον, είναι απαραίτητο να έχουν τεθεί κάποιες βάσεις ώστε όταν το παιδί φτάνει στην εφηβεία, να υπάρχουν όρια. Για να υπάρξουν ωστόσο όρια θα πρέπει και οι γονείς να μπορούν να διαθέσουν τον απαραίτητο χρόνο για να συμβουλέψουν και να κατευθύνουν κατάλληλα το παιδί. Ο σκοπός μας είναι να βοηθήσουμε τα παιδιά μας να αναπτύξουν τα ίδια τον απαραίτητο αυτοέλεγχο και αυτοπειθαρχία αναφορικά με τη χρήση του Διαδικτύου.

ΠΟΡΝΟΓΡΑΦΙΑ ΑΝΗΛΙΚΩΝ



Από τα συχνότερα αδικήματα που αντιμετωπίζει η Υπηρεσία μας με την πάροδο των τελευταίων ετών είναι αυτό **της πορνογραφίας ανηλίκων, της προσβολής της γενετήσιας αξιοπρέπειας ανηλίκων και ο διαδικτυακός εκβιασμός και εξαναγκασμός παιδιών (sextortion)**.

Τα παιδιά πολλές φορές συνομιλούν διαδικτυακά με άτομα που δε γνωρίζουν νομίζοντας ότι μιλάνε με κάποιο γνωστό. Στη συνέχεια, αποστέλλουν τα προσωπικά τους στοιχεία, όπως ονοματεπώνυμο, διευθύνσεις, τηλεφωνικούς αριθμούς, ανεβάζουν (upload) ή αποστέλλουν (send) φωτογραφίες τους κάποιες φορές με προκλητικό περιεχόμενο ή ακόμα συναντιούνται με τα άτομα αυτά.
Τα συγκεκριμένα άτομα, τα οποία χαρακτηρίζονται ως «αρπακτικά», εκμεταλλεύονται την παιδική άγνοια, προκειμένου να ικανοποιήσουν μελλοντικά τις απεχθείς ορέξεις τους.
Ο διαδικτυακός εκβιασμός και εξαναγκασμός παιδιών έχει λάβει μεγάλες διαστάσεις τα τελευταία χρόνια. Το φαινόμενο, γνωστό και ως **«sextortion»**, αναφέρεται σε χρήση πληροφοριών ή εικόνων σεξουαλικής φύσεως από τους κυβερνοεγκληματίες με σκοπό το θύμα να παράγει πρωτότυπο υλικό, να καταβάλει χρήματα ή να προβεί σε άλλες ενέργειες.

ΟΙ ΔΡΑΣΤΕΣ ΤΩΝ ΕΓΚΛΗΜΑΤΩΝ ΑΥΤΗΣ ΤΗΣ ΜΟΡΦΗΣ ΕΧΟΥΝ ΚΥΡΙΩΣ ΔΥΟ ΚΙΝΗΤΡΑ

- Σεξουαλικό ενδιαφέρον
- Οικονομικό ενδιαφέρον

Προκειμένου να αντιμετωπιστεί το ως άνω φαινόμενο, οι Αρχές Επιβολής του Νόμου στο σύνολο των Κρατών – Μελών της Ευρωπαϊκής Ένωσης ένωσαν τις δυνάμεις τους με εταιρείες του ιδιωτικού τομέα προχώρησαν στην εκστρατείας ενημέρωσης **«#Say NO» («Πες ΟΧΙ»)**.

Σχετικοί σύνδεσμοι:
https://www.europol.europa.eu/sayno (Εκστρατεία της Europol)
https://www.youtube.com/watch?v=cZAiW61p9DQ (Βίντεο της εκστρατείας)

Σε περίπτωση που κάποιος πολίτης πέσει θύμα διαδικτυακού εκβιασμού και εξαναγκασμού δεν πρέπει να πληρώσει και να ντραπεί να αναφέρει το γεγονός στις Αστυνομικές Αρχές.

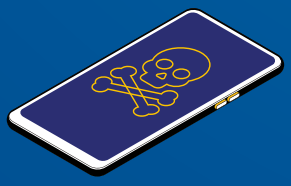
ΣΥΓΚΕΚΡΙΜΕΝΑ ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ ΑΚΟΛΟΥΘΗΣΕΙ ΤΑ ΠΑΡΑΚΑΤΩ ΒΗΜΑΤΑ

- Να μην υποκύψει στους εκβιασμούς και να μην πληρώσει τίποτα.
- Να αναζητήσει βοήθεια.
- Να συλλέξει τις αποδείξεις και να μη διαγράψει τίποτα.
- Να σταματήσει την επικοινωνία και να μπλοκάρει το άτομο.
- Να καταγγείλλει το περιστατικό.

ΣΥΜΒΟΥΛΕΣ

- Η επίτευξη σωστής επικοινωνίας μεταξύ γονιών και παιδιών είναι πρωταρχικός παράγοντας.
- Σημαντική είναι η εποπτεία των συσκευών και των αποθηκευτικών μέσων αυτών.
- Καλό είναι να γνωρίζετε από πριν τους κωδικούς πρόσβασης στα εκάστοτε προφίλ- λογαριασμούς στα οποία εισέρχεται το παιδί.
- Καλό είναι παιδιά νεαρής ηλικίας μικρότερα των δεκατεσσάρων (14) ετών, να μη διαθέτουν λογαριασμούς σε ιστοσελίδες κοινωνικής δικτύωσης.
- Να αποφεύγεται «το ανέβασμα» (upload) ή η αναφορά σε κάποια συζήτηση, προσωπικών στοιχείων.
- Αποφυγή ανεβάσματος ή αποστολής φωτογραφιών με άσεμνο περιεχόμενο.
- Σε περίπτωση «ανεβάσματος» απλής φωτογραφίας με κανονικό περιεχόμενο, να μην απεικονίζονται ευδιάκριτα σε αυτή τα πρόσωπα των παιδιών, ή νχα είναι με μακρινή λήψη.
- Να μη γίνεται αποδοχή ως φίλος/η, άγνωστων ατόμων, σε προφίλ ή λογαριασμούς που τυχόν διαθέτουν τα παιδιά.
- Οι φίλοι που διαθέτει το παιδί σε κάποιο προφίλ να είναι μόνο γνωστοί και στην πραγματική ζωή.
- Αποφυγή ανοίγματος οποιουδήποτε συνδέσμου (link), άγνωστης προέλευσης.
- Συμβουλεύετε τα παιδιά για την αποφυγή χρήσης κάμερας, κυρίως όταν η συνομιλία γίνεται με άγνωστα άτομα, χωρίς την παρουσία σας.

ΔΙΑΦΗΜΙΣΤΙΚΕΣ ΠΑΓΙΔΕΣ



Εμφανίστηκε μήνυμα-διαφήμιση που σας ζητάει να καταχωρήσετε το κινητό σας για να λάβετε μέρος σε διαγωνισμό;
Πολλές φορές τα μηνύματα αυτά μπορεί να είναι παραπλανητικά με σκοπό να σας χρεώσουν. Γι' αυτό αν, πατώντας σε κάποιο διαφημιστικό μήνυμα, βρεθείτε σε σελίδα που ζητά προσωπικά σας δεδομένα, ελέγξτε το προσεκτικά.

ΔΙΑΚΙΝΗΣΗ ΦΑΡΜΑΚΩΝ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

Στο διαδίκτυο διακινούνται παράνομα φαρμακευτικά σκευάσματα και ιατροτεχνολογικά προϊόντα.

Κάθε διαδικτυακή πηγή αγοράς φαρμάκων είναι παράνομη και μη εγκεκριμένη από τους αρμόδιους φορείς.

Η διαδικτυακή αγορά φαρμάκων ενέχει σοβαρούς κινδύνους για την υγεία των καταναλωτών.

Πάνω από το 50% των φαρμάκων που πωλούνται μέσω διαδικτύου είναι πλαστά, νοθευμένα, αμφιβόλου ποιότητας, αποτελεσματικότητας και επικίνδυνα για την υγεία των καταναλωτών.

Όλα τα φάρμακα που κυκλοφορούν νόμιμα στην Ελλάδα πρέπει να έχουν ταινία γνησιότητας την οποία χορηγεί ο Εθνικός Οργανισμός Φαρμάκων (Ε.Ο.Φ.).

ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΓΟΡΕΣ

Προστατέψτε τις κάρτες σου, όπως θα προστάτευες τα μετρητά σου.

Μην αποθηκεύεις ή σημειώνεις τον κωδικό σου PIN.

Ποτέ μην αποκαλύπτεις το PIN σου σε οποιονδήποτε.

Αποθήκευσε τον αριθμό επικοινωνίας της Υπηρεσίας αποκλεισμού καρτών (της τράπεζάς σου).

Εξοικειώσου με τους γενικούς όρους και προϋποθέσεις της κάρτας σου.

Πάντα να διατηρείς την κάρτα σου στην κατοχή σου.

Όρισε όρια ανάληψης και αγορών στην κάρτα σου που ανταποκρίνονται στις ανάγκες σου.

Οι κάρτες που έχουν λήξει πρέπει να ακυρώνονται με κοπή σε πολλά κομμάτια, ώστε η μαγνητική λωρίδα και το chip να καταστρέφονται.

Μόνο εγκληματίες θα ζητήσουν τους κωδικούς της ηλεκτρονικής τραπεζικής σου ή τα στοιχεία της κάρτας σου μέσω ηλεκτρονικού ταχυδρομείου ή τηλεφώνου. Ούτε η τράπεζά σου ούτε οι αστυνομικές αρχές θα σου ζητήσουν ποτέ κάτι τέτοιο.

Αν έχεις αποκαλύψει τους κωδικούς της ηλεκτρονικής τραπεζικής σου ή τα στοιχεία της κάρτας σου σε άγνωστο άτομο, ακύρωσε την κάρτα και επικοινώνησε αμέσως με την τράπεζά σου.

ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΑΣΦΑΛΗΣ ONLINE ΣΥΝΑΛΛΑΓΕΣ

Αγόρασε από αξιόπιστες πηγές.
Πραγματοποίησε αγορές από εταιρείες και καταστήματα που γνωρίζεις ή που έχεις αγοράσει ξανά και έλεγξε τις αξιολογήσεις κάθε πωλητή σε ιστοσελίδες όπως Amazon και EBay.

Έλεγξε τις επαναλαμβανόμενες χρεώσεις.
Πριν δώσεις τα στοιχεία της κάρτας σου για την πληρωμή μιας επαναλαμβανόμενης υπηρεσίας μέσω διαδικτύου, ψάξε τον τρόπο διακοπής αυτής.

Πολλά διαδικτυακά καταστήματα ζητούν την αποθήκευση των στοιχείων πληρωμής.
Σκέψου διπλά πριν αποφασίσεις και βεβαιώσου ότι κατανοείς τους κινδύνους που ελλοχεύουν.

Χρησιμοποίησε κάρτες κατά τις διαδικτυακές αγορές.
Οι περισσότερες κάρτες διαθέτουν ισχυρή πολιτική προστασίας πελάτη. Εάν δεν λάβεις το προϊόν που έχεις παραγγείλει, ο εκδότης της κάρτας θα σε αποζημιώσει.

Βεβαιώσου για την ασφαλή διαδικασία μεταφοράς δεδομένων.
Αναζήτησε το σύμβολο του λουκέτου στη γραμμή URL και τη χρήση των πρωτοκόλλων HTTPS και SSL κατά την περιήγηση στο διαδίκτυο.

Αποθήκευε πάντα όλα τα παραστατικά (έγγραφα) που σχετίζονται με διαδικτυακές αγορές.
Ενδέχεται να χρειαστούν για τον καθορισμό των όρων και προϋποθέσεων της αγοράς ή για την απόδειξη της πληρωμής των προϊόντων.

Εάν δεν αγοράζεις συγκεκριμένο προϊόν ή υπηρεσία, μην υποβάλλεις τα στοιχεία της κάρτας σου.

Όταν αγοράζεις μέσω διαδικτύου από ιδιώτη, μη στέλνεις χρήματα προκαταβολικά στον πωλητή. Εάν είναι δυνατό, διατήρησε το δικαίωμα της πρότερης παραλαβής των προϊόντων (διαδικασία αντικαταβολής).

Μην στέλνεις χρήματα σε κάποιον που δε γνωρίζεις.
Εάν κάποιος σε προσεγγίσει μέσω διαδικτύου και σου ζητήσει χρήματα σκέψου εάν θα έδινες μετρητά σε άγνωστο πρόσωπο στο δρόμο.

Ποτέ μη δίνεις τον αριθμό της κάρτας σου, το PIN ή οποιαδήποτε άλλη πληροφορία για την κάρτα, μέσω ηλεκτρονικού ταχυδρομείου (e-mail).

Απόφυγε διαδικτυακές αγορές σε ιστοσελίδες που δεν χρησιμοποιούν πλήρη αυθεντικοποίηση (Verified by Visa/Mastercard Secure Code).

Ποτέ μη στέλνεις στοιχεία της κάρτας σου, με μη κρυπτογραφημένο ηλεκτρονικό ταχυδρομείο (e-mail).
Μερικά διαδικτυακά καταστήματα εκτός Ευρώπης, ίσως αιτηθούν την αποστολή μέσω fax, αντιγράφου της κάρτας ή του διαβατηρίου σου, ως εγγύηση.

ΑΠΑΤΕΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

Όπως συμβαίνει στον πραγματικό κόσμο έτσι και στο Διαδίκτυο, υπάρχουν απατεώνες που έχουν σκοπό να κλέψουν τα προσωπικά σας στοιχεία (όνομα, τηλέφωνο, διεύθυνση κ.λπ.), τα χρήματά σας, ή και τα δύο. Γι' αυτό απαιτείται μεγάλη προσοχή όταν σερφάρουμε στο Διαδίκτυο.

Η απάτη στο συμβατικό κόσμο είναι ένα από τα πιο συνηθισμένα εγκλήματα. Η εμφάνιση, όμως, και ανάπτυξη του Διαδικτύου, μεγιστοποίησε τις δυνατότητες για διάπραξη νέων μορφών απάτης.

ΟΙ ΚΥΡΙΟΤΕΡΕΣ ΜΟΡΦΕΣ ΔΙΑΔΙΚΤΥΑΚΗΣ ΑΠΑΤΗΣ ΕΙΝΑΙ ΟΙ ΑΚΟΛΟΥΘΕΣ

Ισπανικό Λόττο

«Νιγηριανή» απάτη

Spamming

Phishing προσωπικών στοιχείων

Απάτες με ψευδείς διαγωνισμούς για δωροεπιταγές από γνωστές αλυσίδες καταστημάτων- σούπερ μάρκετ

Διαδικτυακή απάτη που υπόσχεται δωρεάν αεροπορικά εισιτήρια

Απάτη με ταξιδιωτικά πακέτα διακοπών.

Απάτες με δήθεν αγορές - πωλήσεις αυτοκινήτων

Απάτες με αγγελίες ενοικίασης σπιτιών μέσω διαδικτύου

Απάτες με προγνωστικά αθλητικών αγώνων

Απάτες με πρόφαση τις διαδικτυακές γνωριμίες

Απάτες με χορήγηση δανείων από μη αδειοδοτημενους φορείς

Απάτες με τη μέθοδο του «ενδιάμεσου» - εξαπάτηση επαγγελματιών στο διαδίκτυο (Business e-mail Compromise-BEC)

Απάτες με Θέσεις εργασίας

ΨΗΦΙΑΚΑ ΝΟΜΙΣΜΑΤΑ

Χαρακτηριστικό γνώρισμα των ψηφιακών νομισμάτων είναι το γεγονός πως η παραγωγή, αποθήκευση και διακίνησή τους καθώς και το σύνολο των συναλλαγών που πραγματοποιούνται με αυτά, γίνονται αποκλειστικά με ηλεκτρονικό τρόπο.

ΝΑ ΕΙΣΤΕ ΙΔΙΑΙΤΕΡΑ ΠΡΟΣΕΚΤΙΚΟΙ ΚΑΘΩΣ

Υπάρχει κίνδυνος απώλειας χρημάτων κατά την πραγματοποίηση συναλλαγών σε διαδικτυακά ανταλλακτήρια ψηφιακών νομισμάτων, καθόσον οι πλατφόρμες αυτές δεν υπόκεινται σε ρύθμιση και ορισμένες εξ' αυτών έπαυσαν να λειτουργούν ή καταρρεύσαν,

Η αξία ενός ψηφιακού-εικονικού νομίσματος δύναται να αλλάξει δυναμικά, είναι ιδιαίτερα ευμετάβλητη και μπορεί ακόμη και να μηδενιστεί,

Το ψηφιακό πορτοφόλι αποθήκευσης των εν λόγω εικονικών νομισμάτων, μπορεί να υποκλαπεί, ενώ η ανάκτηση του κλειδιού ή του κωδικού πρόσβασης στο ψηφιακό πορτοφόλι, καθίσταται τεχνικά ιδιαίτερα δυσχερής έως και αδύνατη.

ΕΦΑΡΜΟΓΕΣ ΣΕ ΚΙΝΗΤΑ ΤΗΛΕΦΩΝΑ

Πολλές δωρεάν εφαρμογές που κυκλοφορούν για έξυπνα κινητά τηλέφωνα (smartphones) μπορεί να κρύβουν πολλές παγίδες. Γι' αυτό πριν «κατεβάσετε» μια εφαρμογή διαβάστε τους όρους χρήσης και σε ποια στοιχεία του κινητού σας τηλέφωνου θα αποκτήσει πρόσβαση η συγκεκριμένη εφαρμογή (π.χ. λίστα επαφών, εντοπισμός θέσης) και ψάξτε σε κάποια διαδικτυακή μηχανή αναζήτησης κριτικές για τη συγκεκριμένη εφαρμογή.

Επίσης το «κατέβασμα» ύποπτων εφαρμογών μπορεί να μολύνει τη φορητή σας συσκευή (Mobile Malware) και έτσι να χάσετε προσωπικά σας στοιχεία.

ΠΩΣ ΝΑ ΑΠΟΤΡΕΨΕΙΣ ΜΙΑ ΕΠΙΘΕΣΗ RANSOMWARE;

Τήρησε αντίγραφα ασφαλείας.

Χρησιμοποίησε ένα ισχυρό λογισμικό προστασίας από ιούς.

Διατήρησε το σύνολο του λογισμικού στον υπολογιστή σου ενημερωμένο.

Ενεργοποίησε την επιλογή «Εμφάνιση επεκτάσεων αρχείων» στις ρυθμίσεις των Windows στον υπολογιστή σου.

Διαβάστε περισσότερα: ***www.nomoreransom.org***

ΕΠΙΚΟΙΝΩΝΙΑ

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος – Cyber Crime Division
Λ. Αλεξάνδρας 173, Αμπελόκηποι,Τ.Κ. 115 22, Αθήνα
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**

www.cyberkid.gov.gr
www.cyberalert.gr
https://www.facebook.com/cyberkid.gov.gr/
https://www.facebook.com/CyberAlertGR/
https://www.instagram.com/cyberalert.gr/
https://twitter.com/CyberAlertGR
https://www.youtube.com/channel/UCSECtiscTH8tkxzBzX8gVcQ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Προστασίας του Πολίτη

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ