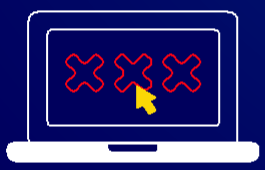
CYBER CRIME DIVISION

ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΠΟΡΝΟΓΡΑΦΙΑ ΑΝΗΛΙΚΩΝ



Από τα συχνότερα αδικήματα που αντιμετωπίζει η Υπηρεσία μας με την πάροδο των τελευταίων ετών είναι αυτά **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 κάποια γνωστά. 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.

CYBER CRIME DIVISION

ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΠΟΡΝΟΓΡΑΦΙΑ ΑΝΗΛΙΚΩΝ

ΥΜΒΟΥΛΕΣ

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 κανονικά περιεχόμενα, 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.

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

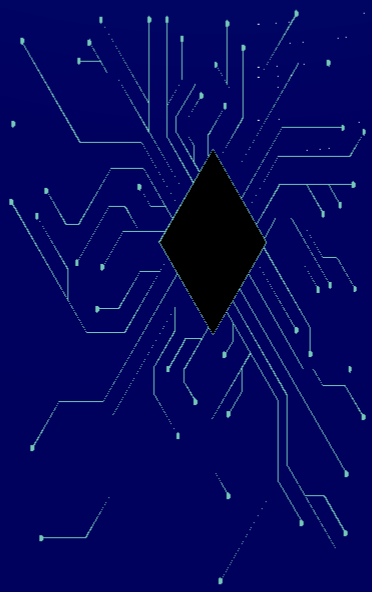
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION

ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

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' αυτά αν, πατώντας σε κάποιο διαφημιστικό μήνυμα, βρεθείτε σε σελίδα που ζητά προσωπικά σας δεδομένα, ελέγξτε τα προσεκτικά.



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

CYBER CRIME DIVISION

ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΔΙΑΚΙΝΗΣΗ ΦΑΡΜΑΚΩΝ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

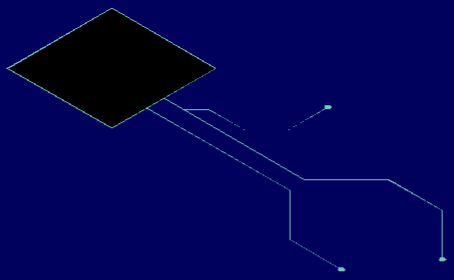
Στα διαδίκτυα διακινούνται παράνομα φαρμακευτικά σκευάσματα και ιατροτεχνολογικά προϊόντα.

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.).



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

CYBER CRIME DIVISION

ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΓΟΡΕΣ

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

Μην αποθηκεύεις ή σημειώνεις τον κωδικό σου PIN.

Ποτέ μην αποκαλύπτεις τα 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 καταναείς 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.