ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Προστασίας του Πολίτη

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ
CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΔΙΕΥΘΥΝΣΗ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Με το άρθρο 31 του Π.Δ. 178/2014 (ΦΕΚ 281/Α/31-12-2014) προβλέφθηκε η ίδρυση και η διάρθρωση της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος και της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, ενώ με το Π.Δ. 82/2020 έγινε η αναδιάρθρωσή τους. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος έχει έδρα την Αθήνα και τοπική αρμοδιότητα που εκτείνεται στη χωροταξική διάταξη του «Τομέα Νοτίου Ελλάδος», ο οποίος περιλαμβάνει την εδαφική δικαιοδοσία των αστυνομικών υπηρεσιών της Γενικής Αστυνομικής Διεύθυνσης Αττικής και των Γενικών Περιφερειακών Αστυνομικών Διευθύνσεων Δυτικής Ελλάδος, Ιονίων Νήσων, Κρήτης, Νοτίου Αιγαίου, Πελοποννήσου, Στερεάς Ελλάδος. Η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος έχει έδρα τη Θεσσαλονίκη και τοπική αρμοδιότητα, η οποία εκτείνεται στη χωροταξική διάταξη του «Τομέα Βορείου Ελλάδος», ο οποίος περιλαμβάνει την εδαφική δικαιοδοσία των αστυνομικών υπηρεσιών της Γενικής Αστυνομικής Διεύθυνσης Θεσσαλονίκης και των Γενικών Περιφερειακών Αστυνομικών Διευθύνσεων Ανατολικής Μακεδονίας και Θράκης, Κεντρικής Μακεδονίας, Δυτικής Μακεδονίας, Ηπείρου, Θεσσαλίας και Βορείου Αιγαίου.

Η αποστολή της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος είναι αυτοτελής κεντρική Υπηρεσία και υπάγεται απευθείας στον κ. Αρχηγό της Ελληνικής Αστυνομίας.

Στην εσωτερική της δομή, αποτελείται από πέντε τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου. Έτσι, στη νέα αναβαθμισμένη δομή της αποτελείται από:

α. Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών,

β. Τμήμα Καινοτόμων Δράσεων και Στρατηγικής,

γ. Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων,

δ. Τμήμα Διαδικτυακής Προστασίας Ανηλίκων,

ε. Τμήμα Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων.

ΔΙΑΔΙΚΤΥΟ

ΕΝΑ ΠΑΓΚΟΣΜΙΟ ΘΑΥΜΑ!

Η μεγάλη ανάπτυξη του τομέα της πληροφορικής και η αυξημένη συμμετοχή των πολιτών στη νέα εποχή της Κοινωνίας της Πληροφορίας, επέφεραν σημαντικά τεχνολογικά επιτεύγματα και εξυπηρετήσεις στην κοινωνία, που αφενός διευκολύνουν την καθημερινότητα, αφετέρου δημιουργούν πεδίο κατάλληλο και για την εμφάνιση μορφών εγκληματικής δραστηριότητας με τη χρήση των τεχνολογιών πληροφορικής και επικοινωνιών.

Η πιο εντυπωσιακή, ωστόσο, δυνατότητα που προσφέρει το Διαδίκτυο, είναι η περιήγηση στον παγκόσμιο ιστό, η άντληση πληροφοριών και η ενημέρωση που προσφέρουν οι διάφοροι ιστότοποι. Έτσι, οι χρήστες μπορούν να επισκέπτονται τους ιστοτόπους αυτούς και να ενημερώνονται για θέματα που τους ενδιαφέρουν, για παρεχόμενες υπηρεσίες, για προϊόντα τα οποία θέλουν να αγοράσουν, για δραστηριότητες εκπαιδευτικών ιδρυμάτων, για νόμους και κανονισμούς κυβερνητικών υπηρεσιών, και πολλά άλλα. Επίσης, ο χρήστης μπορεί απλώς με ένα «κλικ» από την άνεση του σπιτιού του, να ανατρέξει σε κατάλληλες πηγές ή βιβλία που ίσως να μην είχε πριν άμεσα στη διάθεσή του, και μέσα σε λίγα δευτερόλεπτα να βρει πληροφορίες για οποιοδήποτε θέμα μπορεί να τον ενδιαφέρει!

Μέσα από το Διαδίκτυο μπορούμε, να ψυχαγωγηθούμε: να παίξουμε παιχνίδια, να ακούσουμε τραγούδια, να βρούμε παραστάσεις που μας ενδιαφέρουν, να κλείσουμε εισιτήρια για τον κινηματογράφο. Κι όλα αυτά από την άνεση του σπιτιού μας!

Χρησιμοποιώντας το Διαδίκτυο, με ένα μόνο «κλικ» μπορούμε να βρεθούμε σε οποιαδήποτε χώρα! Να δούμε ξένους πολιτισμούς, εικόνες από άλλες χώρες, να διαβάσουμε για την ιστορία ξένων λαών! Παράλληλα, μπορούμε να οργανώσουμε τα ταξίδια μας! Να κλείσουμε εισιτήρια και ξενοδοχεία σε χαμηλές τιμές, να διαβάσουμε ταξιδιωτικές εμπειρίες άλλων ανθρώπων και να γράψουμε τις δικές μας!

Μέσα από την ψηφιοποίηση των δεδομένων, μπορούμε να αναζητήσουμε δημόσια έγγραφα που μας αφορούν, σε λίγα μόλις δευτερόλεπτα! Να υποβάλλουμε αιτήσεις και να αποστείλουμε έγγραφα, γλιτώνοντας χρόνο, κόπο και χρήματα.

Πολύ σημαντικές είναι και οι δυνατότητες που προσφέρει το Διαδίκτυο για μόρφωση και επιμόρφωση. Όλο και περισσότερες βιβλιοθήκες διαθέτουν on-line τους

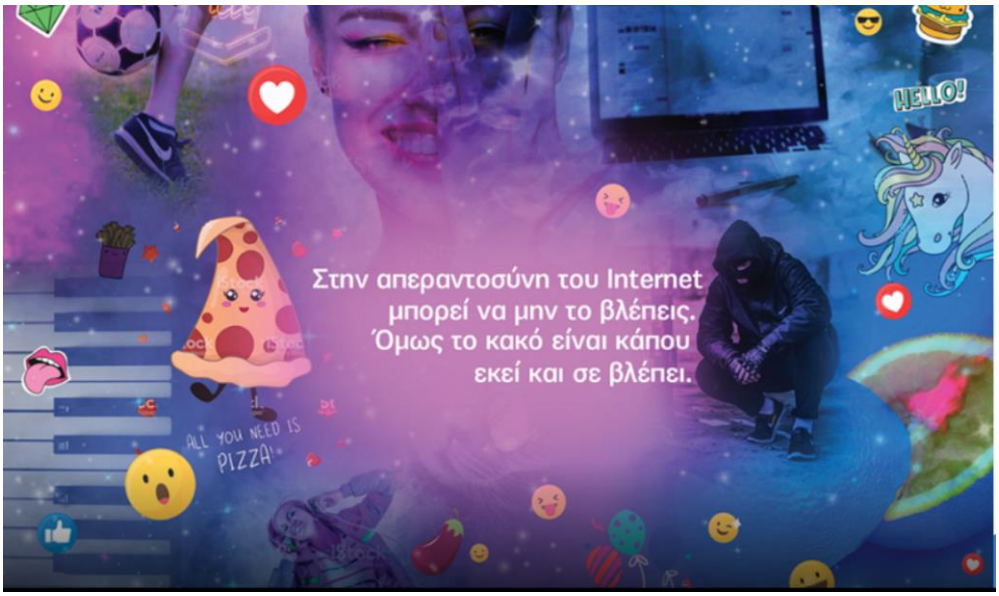
καταλόγους των βιβλίων τους. Όσοι ενδιαφέρονται, μπορούν με τη βοήθεια της μηχανής αναζήτησης να βρουν πού υπάρχει το βιβλίο που χρειάζονται. Ορισμένες μάλιστα βιβλιοθήκες επιτρέπουν ακόμα και να δανείζεται κάποιος βιβλία on-line. Παράλληλα, πρωτοποριακές και αποτελεσματικές μέθοδοι διδασκαλίας επιστρατεύουν το Διαδίκτυο και συντελούν στην καλύτερη δυνατή γνώση και μάθηση μέσω εξελιγμένων συστημάτων τηλεκπαίδευσης.

Ειδικά στην εποχή που διανύουμε, η πανδημία του COVID-19 και η ανάγκη για την απρόσκοπτη συνέχιση της λειτουργίας του δημόσιου και ιδιωτικού τομέα, επιτάχυνε τον ψηφιακό μετασχηματισμό τους προκειμένου να προσαρμοστούν στα νέα δεδομένα αξιοποιώντας τεχνολογίες απομακρυσμένης πρόσβασης. Στον εκπαιδευτικό τομέα εφαρμόστηκε η τηλεκπαίδευση αξιοποιώντας τις ώριμες τεχνολογίες ομαδικών τηλεδιασκέψεων και διαμοιρασμού υλικού, ώστε να διασφαλιστεί η συνέχεια της εκπαιδευτικής διαδικασίας. Έτσι ακόμη και παιδιά κάθε ηλικίας, ξεκινώντας από 4 ετών, συμμετέχουν σε πολλές από αυτές τις δραστηριότητες «συνδεδεμένα ψηφιακά».

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος συστήνει:

ΝΑΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ αλλά ΜΕ ΠΡΟΫΠΟΘΕΣΕΙΣ!

Βάζουμε όρια στη χρήση του διαδικτύου, επενδύουμε σε ένα σφαλές μέλλον για τα παιδιά μας.



ΕΠΙΣΦΑΛΕΙΣ ΔΙΑΔΙΚΤΥΑΚΕΣ ΣΥΜΠΕΡΙΦΟΡΕΣ

#CYBERBULLYING

όταν η ψυχολογική βία στο διαδίκτυο απειλεί κάθε παιδί

Ψηφιακή παρενόχληση (cyberbullying)

Σύμφωνα με τον Νορβηγό ψυχολόγο, DanielOlweus, το φαινόμενο του εκφοβισμού εκλαμβάνεται ως «μια σειρά επαναλαμβανόμενων επιθετικών πράξεων και/ή συμπεριφορών προς κάποιο λιγότερα ισχυρό άτομο»

Ο ψηφιακός εκφοβισμός είναι οποιαδήποτε **επαναλαμβανόμενη** πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής

συμπεριφοράς, που πραγματοποιείται μέσω της χρήσης ψηφιακών συσκευών (Η/Υ, κινητών τηλεφώνων). Ο ψηφιακός εκφοβισμός μοιάζει πολύ με τον απλό εκφοβισμό, αφού υπάρχει αυτός που το κάνει, αυτός που το υφίσταται και οι παρατηρητές. Έχει, όμως, και μερικές σημαντικές διαφορές με τον παραδοσιακό εκφοβισμό όπως:

- ✓ Μπορεί να φτάσει σε πολύ λίγο χρόνο σε πολλούς παραλήπτες,
- ✓ Τα ηλεκτρονικά μηνύματα είναι σχεδόν αδύνατον να ελεγχθούν,
- ✓ Αυτός που το κάνει νιώθει ότι μπορεί να παραμείνει ανώνυμος,
- ✓ Η έλλειψη προσωπικής επαφής με αυτόν που το παθαίνει κάνει τον δράστη σκληρότερο,
- ✓ Αυτός που το παθαίνει πλήττεται παντού, ακόμα και μέσα στο σπίτι και στον προσωπικό του χώρο.
- ✓ Η έλλειψη προσωπικής επαφής αυτού που το υφίσταται μειώνει τις αναστολές αυτού που το κάνει.

✓ Παρατηρείται εξαναγκασμός αυτού που το παθαίνει σε αποτρόπαιες πράξεις και επικίνδυνες προκλήσεις.

Πως εκδηλώνεται το cyberbullying

- Αποστολή κειμένων, e-mail, ή άμεσων μηνυμάτων με προσβλητικό περιεχόμενο.
- Κακόβουλη δημοσίευση φωτογραφιών σε μέσα κοινωνικής δικτύωσης (social media) ή άλλες ιστοσελίδες με μοναδικό σκοπό την παρενόχληση.
- Διάδοση φημών και ψευδών γεγονότων με σκοπό την δυσφήμιση σε τρίτους σε μέσα κοινωνικής δικτύωσης, ιστολόγια, ιστοσελίδες κ.λπ.
- Ανώνυμες κλήσεις και μηνύματα με σκοπό τον φόβο και την ταραχή.
- Χρήση του ονόματος ξένου χρήστη με σκοπό τη διάδοση φημών και ψεμάτων για κάποιον τρίτο (κλοπή ταυτότητας).
- Δημιουργία ιστοσελίδων που στοχοποιούν συγκεκριμένα άτομα καλώντας άλλους να δημοσιεύσουν μηνύματα μίσους.
- Αποστολή ειδικών προγραμμάτων trojan horses (δούρειοι ίπποι) σκόπιμα για να δημιουργήσουν πρόβλημα, με την υποκλοπή κωδικών.
- Εκφοβισμός στη διάρκεια ενός διαδραστικού online παιχνιδιού.

Προφίλ ατόμου που κάνει και που υφίσταται τον ψηφιακό εκφοβισμό

Ο καθένας μας μπορεί να εμπλακεί σε ένα περιστατικό ψηφιακής παρενόχλησης ως το άτομο που υφίσταται αντίστοιχες συμπεριφορές ή τις πραγματοποιεί αλλά ακόμη πιο συχνά, και ως παρατηρητής. Η ψηφιακή παρενόχληση ίσως ελκύει παιδιά που δεν έχουν παρενοχλήσει ποτέ στην πραγματική ζωή επειδή πιστεύουν ότι καλύπτονται από την ψευδαίσθηση της ανωνυμίας όταν χρησιμοποιούν το διαδίκτυο ή το κινητό τους. Με τον τρόπο αυτό πιστεύουν ότι θα μπορούσαν να προβούν σε συμπεριφορές που δεν θα διανοούνταν στις διαπροσωπικές τους σχέσεις, και να χρησιμοποιήσουν τις νέες τεχνολογίες για να αναστατώσουν άτομα από το σχολικό και το οικογενειακό τους περιβάλλον. Πολλές φορές μπορεί ακόμα και να ενδώσουν

στην πίεση συνομηλίκων τους και να προωθήσουν ένα e-mail με εκφοβιστικό περιεχόμενο χωρίς να αναλογιστούν τις συνέπειες.

Ιδιαίτερα κρίσιμος είναι και ο ρόλος του παρατηρητή καθώς μπορεί να βοηθήσει στην αποκλιμάκωση ενός περιστατικού.

Για ποιους λόγους μπορεί κάποιος να εκφοβίζει μέσω του Διαδικτύου;

- Ανάγκη για επιβολή δύναμης
- Θυμός
- Ζήλια
- Διασκέδαση
- Ψυχολογική καταπίεση
- Λόγοι αντεκδίκησης
- Ανάγκη για προσοχή

Πως αισθάνονται αυτοί που το παθαίνουν;

- Θυμό
- Αγανάκτηση
- Θλίψη
- Ντροπή
- Φόβο

Σε περίπτωση που υφίστασαι εκφοβισμό μέσω διαδικτύου, είναι σημαντικό να προβείς σε μια σειρά ενεργειών:

- Απόφυγε να απαντήσεις στις απειλές του δράστη. Απαντώντας επιθετικά, φέρνουμε νέες απειλές και την ικανοποίηση στον δράστη ότι η παρενόχληση λειτουργεί.
- Άλλαξε λογαριασμό e-mail ή «κατέβασε» τη σελίδα δικτύωσής σου και, αν είναι εφικτό, δημιούργησε νέους λογαριασμούς.
- Διατήρησε αποδεικτικά της δράσης, συμπεριλαμβάνοντας όσα περισσότερα στοιχεία μπορείς όπως ημερομηνίες και ώρες, λογαριασμούς ηλεκτρονικού ταχυδρομείου και λοιπά. Καλό θα είναι τα στοιχεία αυτά να υπάρχουν και σε εκτυπωμένη μορφή.
- Αφαίρεσε από τις λίστες των «φίλων» αυτόν που σε παρενόχλησε και ρύθμισε το προφίλ κοινωνικής δικτύωσης ώστε να είναι «απόρρητο», αν δεν είναι ήδη.
- Εάν αυτός που σε παρενοχλεί είναι γνωστό σου πρόσωπο, ζήτησέ του να σβήσει τα μηνύματα και να αποκαταστήσει την αλήθεια σε περίπτωση διάδοσης φημών. Είναι σημαντικό να ενημερωθούν οι γονείς του παιδιού για τη συμπεριφορά του με βασικό σκοπό να περιοριστεί το άτομο που εκφοβίζει.
- Σε περίπτωση που η παρενόχληση πραγματοποιηθεί σε κάποια ιστοσελίδα κοινωνικής δικτύωσης (π.χ. Facebook) κάνε αναφορά (report) για το περιστατικό στους διαχειριστές της ιστοσελίδας.
- Μην κρατάς τον εκφοβισμό για τον εαυτό σου. Δεν είσαι μόνος/μόνη! Ό,τι σε προσβάλει σε μειώνει και σε ενοχλεί στο διαδίκτυο πρέπει να το πεις και όχι να το υποστείς! Πρέπει οπωσδήποτε να αναφέρεις το περιστατικό σε έναν ενήλικα, είτε πρόκειται για τους γονείς σου είτε για κάποιον εκπαιδευτικό ή άλλο κοντινό και έμπιστο άτομο, και, φυσικά να το καταγγείλεις, ακόμα και μόνος σου, καλώντας στη Διεύθυνση Δίωξη Ηλεκτρονικού Εγκλήματος μέσω του CYBERALERT.

Πώς πρέπει να δράσουν οι γονείς σε περίπτωση που το παιδί τους υφίσταται 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 εξοικειωθείτε

και οι ίδιοι με το διαδίκτυο, καθώς αποτελεί αναπόσπαστο πλέον κομμάτι της ζωής μας, αλλά και να επισκεφτείτε τις ιστοσελίδες που το παιδί σας επισκέπτεται. Η δαιμονοποίηση του διαδικτύου σίγουρα δεν ωφελεί κανέναν και ας μην ξεχνάμε ότι είναι ένα πολύ σημαντικό εργαλείο της τεχνολογίας που ήρθε και θα μείνει στη ζωή μας.

- Πολύ συχνά, αρκετοί γονείς, ως απάντηση σε ένα περιστατικό cyberbullying, απαγορεύουν στα παιδιά τους να επισκέπτονται διάφορες ιστοσελίδες, αλλά έτσι μπορεί ενδεχομένως να τα προφυλάσσουν από κάποια ενοχλητικά μηνύματα, ωστόσο τα κρατούν μακριά από την εξέλιξη της τεχνολογίας και την προσωπική τους ανάπτυξη.
- Θα πρέπει να κρατήσετε όλα τα αποδεικτικά στοιχεία κι όχι να τα διαγράψετε γιατί είναι χρήσιμα σε μια πιθανή ψηφιακή διερεύνηση τους από τη ΔΙ.Δ.Η.Ε. Είναι πολύ σημαντικό να έχετε ενημερώσει τα παιδιά εκ των προτέρων ότι εάν δεχτούν απειλητικά ή προσβλητικά μηνύματα πρέπει να τα αποθηκεύσουν και όχι να τα διαγράψουν, να κρατήσουν δηλαδή όλα τα αποδεικτικά στοιχεία. Επιπλέον καλό θα ήταν να μάθετε στα παιδιά ότι πρέπει ακόμα και να εκτυπώσουν τα απειλητικά μηνύματα που ενδεχομένως λάβουν και βεβαίως να σας τα δείξουν.
- Συχνά το άτομο που εκφοβίζει και που υφίσταται τον ψηφιακό εκφοβισμό είναι γνωστοί μεταξύ τους. Σε αυτήν την περίπτωση είναι σημαντικό να ενημερωθούν οι γονείς του παιδιού για τη συμπεριφορά του, το σχολείο του αν τα παιδιά πηγαίνουν στο ίδιο σχολείο, με βασικό στόχο να νιώσει μεγαλύτερη ασφάλεια αυτός που το παθαίνει και να ελεγχθεί αλλά και να περιοριστεί αυτός που το υφίσταται. Σημαντική είναι και η ενημέρωση του Συλλόγου Γονέων και Κηδεμόνων για το περιστατικό και κυρίως για τη διερεύνηση του κατά πόσο υπάρχουν και άλλα αντίστοιχα περιστατικά, τα οποία δεν είχαν γίνει γνωστά.
- Σε περιπτώσεις όπου η παρενόχληση επιμένει και προέρχεται από άγνωστο αποστολέα, μπορείτε να καταγγείλετε το περιστατικό στη ΔΙ.Δ.Η.Ε. προκειμένου να ενημερωθεί ο Εισαγγελέας και να κινηθεί η ποινική διαδικασία.

- Εάν το παιδί συνεχίζει να εμφανίζεται αγχωμένο, απομονωμένο, φοβισμένο, είναι σημαντικό να ζητήσετε τη βοήθεια ενός ειδικού σε θέματα ψυχικής υγείας.

Πώς πρέπει να δράσουν οι γονείς σε περίπτωση που το παιδί τους είναι αυτό που εκφοβίζει;

- Μιλήστε στο παιδί σας.
- Μείνετε ήρεμοι. Δώστε έμφαση στη συμπεριφορά, όχι στο παιδί.
- Προσπαθήστε να καταλάβετε τους λόγους.
- Συνεργαστείτε με το σχολείο για να λύσετε το πρόβλημα.
- Προβληματιστείτε σχετικά με τις συμπεριφορές στην οικογένειάς σας.

Ποιες είναι οι συνέπειες του Cyber bullying:

- Τα παιδιά παραμελούν τις σχολικές τους υποχρεώσεις, αποτυγχάνουν και πολλές φορές αποφεύγουν το σχολείο. Εάν αυτός που το παθαίνει είναι ενήλικας, παρουσιάζονται αντίστοιχα προβλήματα στη δουλειά του.
- Ψυχοσωματικά προβλήματα (προβλήματα υγείας που προκαλούνται από ψυχολογικές αιτίες), διατροφικές και αναπτυξιακές διαταραχές, στομαχόπονοι, διαταραχή του ύπνου.
- Αίσθημα ντροπής, αμηχανίας, εξευτελισμού, λύπης, κατάθλιψη, αγωνία.
- Συνεχής φόβος και αίσθημα διακινδύνευσης.
- Αίσθημα αποτυχίας, έλλειψη αυτοπεποίθησης και εμπιστοσύνης σε άλλους ανθρώπους.
- Απελπισία και απόγνωση.
- Βία σε άλλα άτομα και εκδικητικότητα
- Αυτοτραυματισμοί και αυτοκτονίες.

Μέτρα Προστασίας

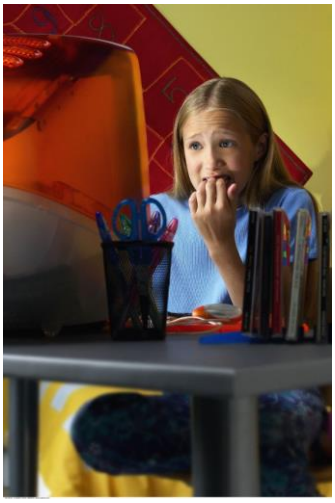
- Προστασία προσωπικών δεδομένων από ιστοσελίδες κοινωνικής δικτύωσης. Περιορίζοντας τις διαθέσιμες πληροφορίες για τον εαυτό μας ή την οικογένειά μας, μειώνουμε τις πιθανότητες να μπούμε στο στόχαστρο αγνώστων δραστών.
- Δεν είναι σωστό να κάνουμε φίλους τους πάντες σε ιστοσελίδες κοινωνικής δικτύωσης.

- Να συμπεριφέρεσαι στους άλλους online, όπως θα έκανες στην πραγματική ζωή. Αν κάποιος σε αντιμετωπίζει με αγένεια ή είναι απότομος, δεν είσαι υποχρεωμένος να απαντήσεις. Θα δει ότι δεν έχει αποτελέσματα και θα σταματήσει τα προσβλητικά μηνύματα. Αν όχι, και τα μηνύματα συνεχιστούν, ζήτα βοήθεια από έναν έμπιστο ενήλικα.
- Ποτέ μην ανοίγεις ένα μήνυμα από κάποιον που δε γνωρίζεις.
- Απόφυγε να αναρτάς stories που μαρτυρούν την τοποθεσία σου (σχολείο ή μέρη τα οποία επισκέπτεσαι).
- Διάγραψε περίεργα μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα κειμένου από ανθρώπους που δεν γνωρίζεις. Σε περίπτωση αμφιβολίας, ζήτα συμβουλές από έναν έμπιστο ενήλικα.
- «Google yourself!». Χρησιμοποίησε μια μηχανή αναζήτησης ανά τακτά διαστήματα και πραγματοποίησε αναζήτηση μαζί με έναν ενήλικα με το όνομά σου ή το ψευδώνυμο που χρησιμοποιείς στο Διαδίκτυο. Έτσι θα μπορείς να εποπτεύεις την ηλεκτρονική σου παρουσία.
- Δεν χρειάζεται να είσαι «πάντα συνδεδεμένος» - αποσυνδέσου και κλείσε τον υπολογιστή. Δώσε στον εαυτό σου ένα διάλειμμα. Μη μένεις online για πάρα πολύ χρόνο.
- Βάλε τη φαντασία σου να δουλέψει όταν δημιουργείς κωδικούς πρόσβασης. Μη χρησιμοποιείς κωδικούς που εύκολα μπορεί κανείς να φανταστεί (ημερομηνία γέννησης κ.ά.)
- Αν δεις κάτι στο διαδίκτυο ή λάβεις ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή μήνυμα κειμένου που σε κάνει να αισθανθείς άβολα, κλείσε τον υπολογιστή ή το τηλέφωνο και ζήτα συμβουλές από έναν ενήλικα, τον οποίο εμπιστεύεσαι.

Η ΔΙ.Δ.Η.Ε. επεμβαίνει σε αστυνομική και ποινική διερεύνηση σοβαρών περιπτώσεων όπου απειλείται η ψυχική και σωματική υγεία του παιδιού. Σε κάθε άλλη περίπτωση λειτουργεί μεσολαβητικά και συμβουλευτικά ώστε να επιλυθεί το ζήτημα εντός της σχολικής κοινότητας.

#ΠΟΡΝΟΓΡΑΦΙΑ ΑΝΗΛΙΚΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

όταν η παιδική αξιοπρέπεια κινδυνεύει και ηλεκτρονικά



Η παραγωγή υλικού πορνογραφίας ανηλίκων είναι ένα παγκόσμιο φαινόμενο με τεράστια κέρδη. Τα κυκλώματα πορνογραφίας ανηλίκων δραστηριοποιούνται καθημερινά σε όλο τον κόσμο.

Τα «αρπακτικά», προσποιούμενοι ότι είναι έφηβοι, χρησιμοποιούν τα δωμάτια ανοιχτής επικοινωνίας (chat rooms), τις ιστοσελίδες κοινωνικής δικτύωσης και άλλους χώρους διαδικτυακής επικοινωνίας για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν.

Συχνά τέτοιου είδους ιστότοποι θεωρούνται από τα παιδιά ασφαλείς τόποι συνομιλίας στο διαδίκτυο, τόσο εξαιτίας της δημόσιας φύσης της συζήτησης, αλλά και της λανθασμένης εκτίμησης ότι διατηρείται η ανωνυμία. Τα «αρπακτικά» ξεκινούν συζητήσεις με τα πιθανά θύματα με σκοπό να αναπτύξουν φιλική σχέση με αυτά και να αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον τόπο διαμονής τους, τα ενδιαφέροντα, τα χόμπι και τις σεξουαλικές τους εμπειρίες.

Οι συζητήσεις μπορεί να διαρκέσουν ημέρες, εβδομάδες, ακόμη και μήνες, μέχρι το

«αρπακτικό» να αποκτήσει την εμπιστοσύνη του παιδιού. Στην συνέχεια προκαλούν σιγά-σιγά συζητήσεις σεξουαλικής φύσεως και τους στέλνουν φωτογραφίες ως κάτι το αποδεκτό και φυσιολογικό. Πρόκειται για μια τακτική που υπονομεύει την απροθυμία των παιδιών στο να λάβουν μέρος σε σεξουαλική επαφή, αλλά και που έχει σκοπό να αποτρέψει το θύμα από το να ζητήσει προστασία από τους γονείς και τους δασκάλους του, αφού καταλήγει να νιώθει ένοχο που έχει ανταλλάξει τέτοιου είδους φωτογραφίες.

Τα «αρπακτικά» μπορεί να είναι και άτομα υπεράνω πάσης υποψίας: μορφωμένοι, επιφανείς, οικονομικά ευκατάστατοι, οι οποίοι πιθανόν να έχουν και δική τους οικογένεια, φιλήσυχοι, ευυπόληπτοι. Δεν θα διστάσουν να εκμεταλλευτούν τη θέση

τους, αλλά και τη σχέση τους (συγγενείς) για να ικανοποιήσουν το αρρωστημένο τους πάθος.

Συμβουλές

- Συμβουλευτείτε τους γονείς σας, όταν έχει προκύψει κάποιο πρόβλημα με κάποιον ο οποίος σας προσέγγισε στο Διαδίκτυο.
- Αν διαθέτετε λογαριασμό σε κάποια ιστοσελίδα κοινωνικής δικτύωσης, αποφεύγετε να βάζετε τα προσωπικά σας στοιχεία (ονοματεπώνυμο, διεύθυνση, τηλέφωνο, σχολείο), καθώς επίσης και φωτογραφίες σας ή των συμμαθητών σας.
- Αν θέλετε να βάλετε φωτογραφίες σας σε διάφορες σελίδες, καλό είναι να μην απεικονίζουν ευαίσθητα σημεία του σώματός σας ή το πρόσωπό σας και να είναι με μακρινή λήψη.
- Χρησιμοποιήστε σύνθετο κωδικό πρόσβασης στο λογαριασμό σας και όχι κάποιον τον οποίο μπορεί εύκολα να μαντέψει κάποιος άλλος. Καλό, επίσης, είναι τον κωδικό πρόσβασης να τον γνωρίζουν οι γονείς σας, για λόγους ασφαλείας.
- Μην αποδέχεστε αιτήματα φιλίας από αγνώστους.
- Αποφεύγετε να μπαίνετε σε σελίδες στις οποίες συνομιλείτε με αγνώστους ή απαιτείται η χρήση κάμερας.
- Μην ανοίγετε ποτέ την κάμερα σε αγνώστους.
- Αν κάποιος χρήστης σε μια συνομιλία σας ζητήσει να βγάλετε κάποια φωτογραφία που να δείχνει το σώμα σας ή γενικότερα εσάς, και να τη στείλετε, μην το κάνετε σε καμία περίπτωση και ειδοποιήστε αμέσως τους γονείς σας.
- Μην ανοίγετε μηνύματα και κυρίως συνδέσμους (links) που υπάρχουν σε αυτά, κι ας τα έχει στείλει κάποιος φίλος ή φίλη σας, αφού δεν ξέρετε σε ποια σελίδα σας οδηγούν. Μπορεί, για παράδειγμα, πίσω από το σύνδεσμο αυτό να κρύβεται κάποιος ιός.
- Αν κάποιος άγνωστος χρήστης σάς προσέγγισε σε μια συνομιλία και μιλάει με σεξουαλικά υπονοούμενα, μη συνεχίσετε να μιλάτε μαζί του.

- Αν για οποιονδήποτε λόγο αισθάνεστε ανασφάλεια ή φόβο, καλό είναι να ειδοποιήσετε τους γονείς σας ή την Υπηρεσία μας στο τηλέφωνο 11188 για οποιαδήποτε βοήθεια.

Συμβουλές για γονείς

Ανεξάρτητα του πώς μπορεί να λειτουργεί κάποιο άτομο που σκοπεύει να προσεγγίσει τα παιδιά, παρατηρούνται τα εξής:

1. Η επίτευξη σωστής επικοινωνίας μεταξύ γονέα και παιδιού είναι πρωταρχικός παράγοντας, ενώ σε περίπτωση οποιασδήποτε απορίας ή αδυναμίας καλό είναι να ζητηθεί η συμβουλή ειδικού σε θέματα ψυχικής υγείας.
2. Οι γονείς θα πρέπει να έχουν την εποπτεία των συσκευών, με τις οποίες τα παιδιά εισέρχονται σε ιστοσελίδες, εφαρμογές και υπηρεσίες. Αν δεν υπάρχει η απαραίτητη τεχνογνωσία από πλευράς γονέων, καλό είναι να ζητηθεί η συμβουλή ειδικού. Επιπλέον, καλό είναι να γνωρίζουν από πριν τους κωδικούς πρόσβασης στα εκάστοτε προφίλ-λογαριασμούς στα οποία εισέρχεται το παιδί. Σε καμία περίπτωση όμως το παιδί δε θα πρέπει να νιώθει ότι παρακολουθείται από το γονιό. Θα πρέπει να χτιστεί μια σχέση εμπιστοσύνης γονιού-παιδιού αναφορικά με την πλοήγηση του στο διαδίκτυο.
3. Καλό είναι παιδιά νεαρής ηλικίας (κάτω των δεκατριών ετών) να μη διαθέτουν λογαριασμούς σε ιστοσελίδες κοινωνικής δικτύωσης ή, εφόσον δεν μπορεί να αποφευχθεί αυτό, να υπάρχει καλή επικοινωνία και η κατάλληλη ρύθμιση για την πρόσβαση από τρίτα άτομα σε αυτούς.
4. Προτείνεται να αποφεύγεται το «ανέβασμα» (upload) ή η αναφορά σε κάποια συζήτηση προσωπικών στοιχείων (ονοματεπώνυμα, διευθύνσεις κατοικίας, τηλεφωνικοί αριθμοί, κ.λπ.), φωτογραφιών, ακόμα και e-mail στις εκάστοτε ιστοσελίδες, εφαρμογές και υπηρεσίες. Σε περίπτωση «ανεβάσματος» φωτογραφίας, να μην απεικονίζονται ευδιάκριτα σε αυτήν τα πρόσωπα των παιδιών ή να είναι μακρινή λήψη, πολύ περισσότερο δε όταν τα παιδιά είναι κάτω των δεκατριών ετών.
5. Συμβουλεύουμε τα παιδιά για την αποφυγή χρήσης κάμερας, κυρίως όταν η συνομιλία γίνεται με άγνωστα άτομα ή χωρίς την παρουσία των γονέων και των κηδεμόνων.

6. Σημαντικό είναι οι γονείς να μην ξεχνάνε ότι εκτός από τα παιδιά τους πρέπει να προστατεύουν και τους εαυτούς τους, ενώ δεν πρέπει να ανεβάζουν (upload) φωτογραφίες των ανήλικων παιδιών τους καθώς και προσωπικές και οικογενειακές τους στιγμές.

#ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΒΙΑΣΜΟΣ ΚΑΙ ΕΞΑΝΑΓΚΑΣΜΟΣ ΠΑΙΔΙΩΝ - SEXTORTION

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 δράστες των εγκλημάτων αυτής της μορφής έχουν κυρίως δύο κίνητρα:

- Σεξουαλικό ενδιαφέρον για ανήλικα άτομα, ώστε να επιδιώκουν την παραγωγή πρωτότυπου υλικού πορνογραφίας ανηλίκων από τα θύματά τους ή συνάντηση στον πραγματικό κόσμο με αυτά και
- Οικονομικό ενδιαφέρον, ώστε να επιδιώκουν οικονομικό όφελος από τη δράση τους.

Πολλά από τα προναφερθέντα περιστατικά διαδικτυακού εκβιασμού και εξαναγκασμού δεν καταγγέλλονται στις Αρχές Επιβολής του Νόμου γιατί το θύμα είτε αισθάνεται ντροπή για το υλικό που κλήθηκε να παράγει, είτε δε γνωρίζει ότι έχει διαπραχθεί έγκλημα σε βάρος του.

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 και προχώρησαν στην εκστρατεία ενημέρωσης "#Say NO" ("Πες ΟΧΙ").

Στην ανωτέρω εκστρατεία ενημέρωσης, στην οποία λαμβάνει μέρος και η χώρα μας, περιλαμβάνεται ένα σύντομο βίντεο, διαθέσιμο σε όλες τις επίσημες γλώσσες των Κρατών Μελών της Ε.Ε., που σκοπό έχει να βοηθήσει τους πολίτες να αναγνωρίσουν

τις παραβατικές συμπεριφορές σε βάρος τους. Ταυτόχρονα, παρέχονται συμβουλές πρόληψης και τονίζεται η σημασία της καταγγελίας των εγκλημάτων στις αρμόδιες Αρχές.

Σχετικοί σύνδεσμοι:

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

Συμβουλές για παιδιά και εφήβους:

- Κάνω φίλους μόνο όσους γνωρίζω καλά. Δεν ανταγωνίζομαι με την παρέα ποιος θα κάνει τους περισσότερους φίλους.
- Ορίζω στις Ρυθμίσεις Απορρήτου της συσκευής μου τι θέλω να φαίνεται στους άλλους.
- Αποφεύγω το "check-in" στο σχολείο, στη βόλτα ή μέρη που επισκέπτομαι συχνά.
- Δε δημοσιεύω φωτογραφίες μου που "μαρτυράνε" τοποθεσίες, π.χ. το σπίτι μου, το σχολείο μου.
- Ποτέ δεν κάνω chat με κάποιον που δε γνωρίζω.
- Προσέχω τις κινήσεις μου στην κάμερα.
- Σκέφτομαι πολύ πριν δημοσιεύσω κάποιο video μου.

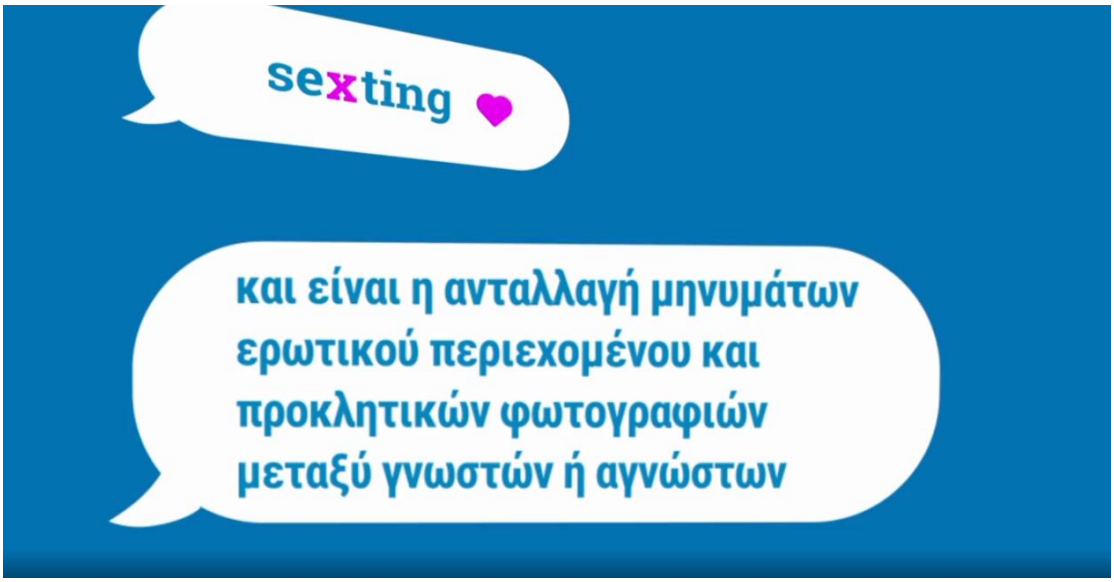
Σε περίπτωση που κάποιος πολίτης πέσει θύμα διαδικτυακού εκβιασμού και εξαναγκασμού δεν πρέπει να πληρώσει και να ντραπεί να αναφέρει το γεγονός στις Αστυνομικές Αρχές. Συγκεκριμένα προτείνεται να ακολουθήσει τα παρακάτω βήματα:

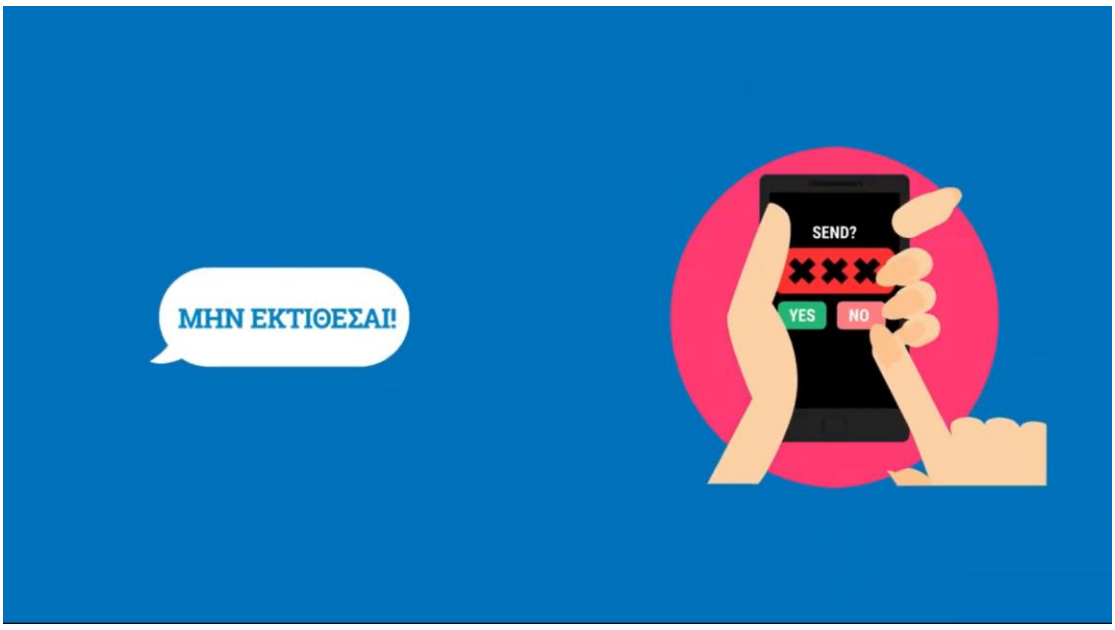
- Να μην υποκύψει στους εκβιασμούς και να μην πληρώσει τίποτα.
- Να αναζητήσει βοήθεια.
- Να συλλέξει τις αποδείξεις και να μη διαγράψει τίποτα.
- Να σταματήσει την επικοινωνία και να μπλοκάρει το άτομο.
- Να καταγγείλει το περιστατικό.

#SEXTING

Sexting ονομάζεται η ανταλλαγή μηνυμάτων και φωτογραφιών σεξουαλικού περιεχομένου μέσω κινητών τηλεφώνων. Το φαινόμενο αυτό γνωρίζει μεγάλη έξαρση το τελευταίο χρονικό διάστημα και στη χωρά μας! Συγκεκριμένα, η Υπηρεσία μας δέχεται πλήθος καταγγελιών όπου έφηβοι, αλλά και ενήλικες, εκβιάζονται με λεκτικό ή φωτογραφικό υλικό που αντάλλαξαν μέσω sexting.

Τονίζεται ότι η κατοχή και η διακίνηση πορνογραφικού υλικού ανηλίκων αποτελεί ποινικό αδίκημα. Ακόμη και εάν βρεθεί στην κατοχή ανήλικου/-ης γυμνή ή ημίγυμνη φωτογραφία ανήλικου/-ης είναι ποινικό αδίκημα «πορνογραφία ανηλίκων» και έχει νομικές συνέπειες.





#ΕΠΙΣΦΑΛΕΙΣ ΣΥΜΠΕΡΙΦΟΡΕΣ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ (SOCIAL MEDIA)

Τα Μέσα Κοινωνικής Δικτύωσης είναι ιστοσελίδες που προσφέρουν στους χρήστες τους τη δυνατότητα να δημιουργήσουν το προσωπικό τους προφίλ, να παρουσιάσουν τον εαυτό τους, να αναζητήσουν παλιούς φίλους και να επικοινωνήσουν με άλλους χρήστες στο Διαδίκτυο. Οι χρήστες αυτοί μπορεί να είναι

γνωστοί από την καθημερινή ζωή τους ή εντελώς άγνωστοι. Μέσα από αυτήν την επικοινωνία δημιουργούνται online κοινότητες, όπου άνθρωποι με κοινά ενδιαφέροντα μπορούν να μοιράζονται πληροφορίες και να εκφράζουν τις απόψεις τους. Δε χρειάζονται ιδιαίτερες τεχνικές γνώσεις για να δημιουργήσει κανείς το προφίλ του και να ανεβάσει περιεχόμενο (σχόλια, φωτογραφίες, βίντεο), το οποίο θα μοιραστεί αργότερα με άλλους χρήστες. Οι ιστοσελίδες κοινωνικής δικτύωσης είναι ιδιαίτερα δημοφιλείς στην Ελλάδα, με πιο γνωστές τις: Facebook, TikTok, Twitter, Youtube, Instagram.

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.

Σημεία ενδιαφέροντος στα μέσα κοινωνικής δικτύωσης

- Χρήση της πληροφορίας για άλλο σκοπό. Στα κοινωνικά δίκτυα ο χρήστης έχει τη λανθασμένη αίσθηση ότι οι πληροφορίες που ανεβάζει είναι διαθέσιμες μόνο στους φίλους του. Στην πραγματικότητα, έχουν πρόσβαση σε αυτές και άλλοι χρήστες της ιστοσελίδας, οι οποίοι μπορούν να τις χρησιμοποιήσουν με σκοπό διαφορετικό από αυτόν που αρχικά θέλατε, επηρεάζοντας την καθημερινότητά σας εντός και εκτός του διαδικτύου. Για παράδειγμα, ένα σχόλιο που απευθύνεται σε φίλους, θα μπορούσε να διαβαστεί από τον εργοδότη σας και να δημιουργήσει λανθασμένες εντυπώσεις για την επαγγελματική σας ζωή.

- Η πληροφορία μένει για πάντα στο διαδίκτυο. Ανεβάζοντας μια φωτογραφία ή ένα σχόλιο σε μια σελίδα κοινωνικής δικτύωσης δημοσιεύεται σε έναν αριθμό χρηστών. Ακόμη και αν επιλέξετε να αποσύρετε αυτή την πληροφορία, αυτή παραμένει αποθηκευμένη στα αρχεία της εταιρίας όπου ανήκει η σελίδα, απλά

δεν εμφανίζεται στο διαδίκτυο. Επίσης, οποιοσδήποτε από τους χρήστες που την βλέπουν μπορεί να την αντιγράψει και να τη χρησιμοποιήσει στο μέλλον.

- Αποποίηση των πνευματικών δικαιωμάτων. Σε αρκετά από τα μέσα κοινωνικής δικτύωσης, τίθεται ως όρος για την εγγραφή του χρήστη η αποποίηση των πνευματικών δικαιωμάτων από το περιεχόμενο που ανεβάζει. Ως αποτέλεσμα, οι φωτογραφίες που δημοσιοποιείτε περνούν στην ιδιοκτησία της εταιρίας που κατέχει την ιστοσελίδα και μπορούν να χρησιμοποιηθούν από οποιονδήποτε.
- Παρενόχληση - Stalking - Cyberbullying. Δημοσιοποιώντας πληροφορίες όπως το ονοματεπώνυμο, η διεύθυνση, ο αριθμός τηλεφώνου ή ακόμη το όνομα του σχολείου ή της επιχείρησης όπου εργάζεστε, κάνετε γνωστή σε κάθε χρήστη την πραγματική σας ταυτότητα. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν από κακόβουλους χρήστες για να σας παρακολουθήσουν ή ακόμη και να σας απειλήσουν. Ιδιαίτερη προσοχή χρειάζεται και κατά τη δημοσιοποίηση φωτογραφιών, οι οποίες μπορούν να παραποιηθούν με ψηφιακό τρόπο και να διανεμηθούν με σκοπό να σας δυσφημίσουν ή να σας απειλήσουν.
- Εντοπισμός θέσης. Πολλοί χρήστες επιλέγουν να δημοσιεύσουν στα μέσα κοινωνικής δικτύωσης που βρίσκονται κάθε στιγμή, επιλέγοντας τη δημοσίευση της θέσης μέσα από την ιστοσελίδα (check-in) ή αναρτώντας ιστορίες (stories) με προσθήκη τοποθεσίας. Πρέπει να θυμάστε ότι η δημοσίευση της θέσης σας μπορεί να χρησιμοποιηθεί από κακόβουλους χρήστες για να σας εντοπίσουν ή από επίδοξους διαρρήκτες για να γνωρίζουν πότε λείπετε από το σπίτι.
- Κλοπή Ταυτότητας. Πρόκειται για την περίπτωση όπου κάποιος χρήστης του διαδικτύου παριστάνει εσάς και παραπλανά ή παρενοχλεί άλλους χρήστες. 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.
- Δημοσιοποίηση προσωπικών δεδομένων από τρίτους χρήστες. Όσο προσεκτικός και να είναι ένας χρήστης σχετικά με τις πληροφορίες που δημοσιοποιεί στα μέσα κοινωνικής δικτύωσης, δεν είναι πάντα σε θέση να ελέγξει τις πληροφορίες που άλλοι χρήστες δημοσιοποιούν για αυτόν. Για παράδειγμα, ένας φίλος σας

μπορεί να δημοσιεύσει στο προφίλ του μια φωτογραφία που μεταξύ άλλων περιλαμβάνει και εσάς, σε άσεμνες πόζες ή σε ένα μέρος που δεν θα θέλατε να ξέρουν άλλοι ότι έχετε επισκεφθεί. Επίσης, δηλώνοντας κάποιος ότι είναι συμμαθητής σας και γνωστοποιώντας το σχολείο που πηγαίνει, αυτομάτως αποκαλύπτει μια διεύθυνση όπου μπορεί κάποιος να σας εντοπίσει.

- Παραχώρηση των δεδομένων σε τρίτες εταιρίες. Οι εταιρίες που κατέχουν τα μέσα κοινωνικής δικτύωσης έχουν πρόσβαση στις πληροφορίες που δημοσιεύετε σε αυτά, αλλά και σε δεδομένα που προκύπτουν από τη σύνδεσή σας, όπως η IP διεύθυνση, η γεωγραφική περιοχή που ανήκετε και ο browser που χρησιμοποιείτε. Οι πληροφορίες αυτές μπορούν να παραχωρηθούν σε τρίτες εταιρίες και να χρησιμοποιηθούν σε μεθόδους στοχευμένης διαφήμισης.
- Παραχώρηση στοιχείων σε εφαρμογές. Σε αρκετά μέσα κοινωνικής δικτύωσης, πέρα από τη δημοσίευση πληροφορίας στο προφίλ του, ο χρήστης έχει τη δυνατότητα να χρησιμοποιήσει εφαρμογές. Καθώς οι εφαρμογές δεν πιστοποιούνται πάντα για την ασφάλειά τους, ενδέχεται να αποκτούν πρόσβαση σε προσωπικές πληροφορίες από το προφίλ σας, όπως τα στοιχεία διεύθυνσής σας ή να περιέχουν κακόβουλο λογισμικό (ιούς κτλ.).
- Εξειδικευμένες απάτες. Οι πληροφορίες που δημοσιεύετε στο προφίλ σας μπορούν να χρησιμοποιηθούν από επιτήδειους, ώστε να εξειδικεύσουν τις επιθέσεις ηλεκτρονικού «ψαρέματος» (phishing) τους και να έχουν μεγαλύτερη πιθανότητα να εξαπατήσουν εσάς ή τους φίλους σας.

Συμβουλές προστασίας στα μέσα κοινωνικής δικτύωσης

Προσωπικά Δεδομένα

- Μη δημοσιεύετε πληροφορίες που μπορούν να βοηθήσουν κάποιον άγνωστο να σας εντοπίσει. Η διεύθυνσή και το τηλέφωνό σας, η επιχείρηση που εργάζεστε ή το σχολείο που πηγαίνετε μπορούν να χρησιμοποιηθούν από αγνώστους για να σας πλησιάσουν.
- Μην ξεχνάτε ότι τη διεύθυνσή σας μπορούν να προδώσουν και οι προσωπικές πληροφορίες των γειτόνων ή των συμμαθητών σας. Μη δημοσιεύετε φωτογραφίες με ευκρινή τα στοιχεία διεύθυνσή σας.

- Μη χρησιμοποιείτε τα μέσα κοινωνικής δικτύωσης ως ημερολόγιο. Το προφίλ σας δεν είναι ανάγκη να περιέχει όλες τις πληροφορίες για την καθημερινή σας δραστηριότητα
- Ελέγξτε τις ρυθμίσεις ασφαλείας και απορρήτου για το προφίλ σας. Ρυθμίστε τις έτσι ώστε οι πληροφορίες σας να είναι ορατές μόνο στους φίλους σας.
- Μην επιτρέπετε σε εφαρμογές (applications) που δε γνωρίζετε να χρησιμοποιούν τα στοιχεία του λογαριασμού σας.

Αποφυγή Καταστάσεων Αμηχανίας

- Σκεφτείτε πριν δημοσιεύσετε ένα σχόλιο ή μια φωτογραφία. Μήπως θα σας έφερνε σε δύσκολη θέση εάν το έβλεπαν τα μέλη της οικογένειάς σας ή ο μελλοντικός εργοδότης σας;
- Πριν δημοσιεύσετε μια πληροφορία στα μέσα κοινωνικής δικτύωσης σκεφτείτε ότι θα μείνει για πάντα στο διαδίκτυο. Μήπως θα μπορούσε να επηρεάσει αρνητικά τη μελλοντική σας ζωή;
- Ελέγξτε το περιεχόμενο που δημοσιεύουν οι φίλοι σας στα μέσα κοινωνικής δικτύωσης.
- Σεβαστείτε τους φίλους σας. Εάν η πληροφορία που πρόκειται να δημοσιεύσετε αφορά κάποιο φίλο σας, π.χ. πρόκειται για μια κοινή σας φωτογραφία, επικοινωνήστε μαζί του και ζητήστε την άδειά του για τη δημοσίευση.

Δεν εμπιστευόμαστε αγνώστους

- Μη δέχεστε αιτήματα φιλίας από αγνώστους. Μην εμπιστεύεστε τα στοιχεία που δηλώνει κάποιος στο προφίλ του στα μέσα κοινωνικής δικτύωσης. Το όνομα, η ηλικία, ακόμη και οι φωτογραφίες του προφίλ μπορεί να μην είναι αληθινά.
- Όταν δέχεστε αιτήματα φιλίας από άτομα που γνωρίζετε στην πραγματική σας ζωή, επικοινωνήστε τηλεφωνικά μαζί τους και ρωτήστε αν το προφίλ τους ανήκει, πριν αποδεχθείτε το αίτημα.

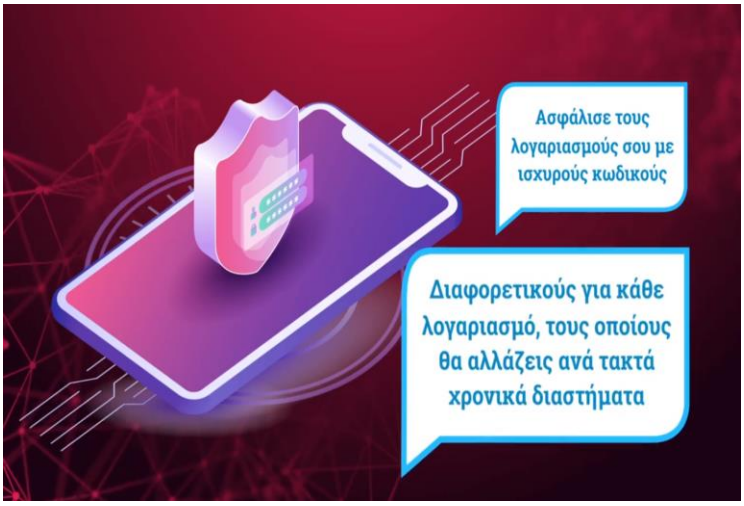
Απόπειρες Απάτης

- Αν κάποιος φίλος σας επικοινωνήσει μαζί σας και σας ζητήσει χρήματα, επικοινωνήστε πρώτα μαζί του τηλεφωνικά. Ενδέχεται να έχει κλαπεί το προφίλ του από απατεώνες.

- Κανένα μέσο κοινωνικής δικτύωσης δεν πρόκειται να σας αποστείλει e-mail ζητώντας να επιβεβαιώσετε τον κωδικό σας, συμπληρώνοντάς τον σε κάποια φόρμα. Εάν λάβετε ένα τέτοιο e-mail πιθανόν να πρόκειται για επίθεση ηλεκτρονικού «ψαρέματος» (phishing).

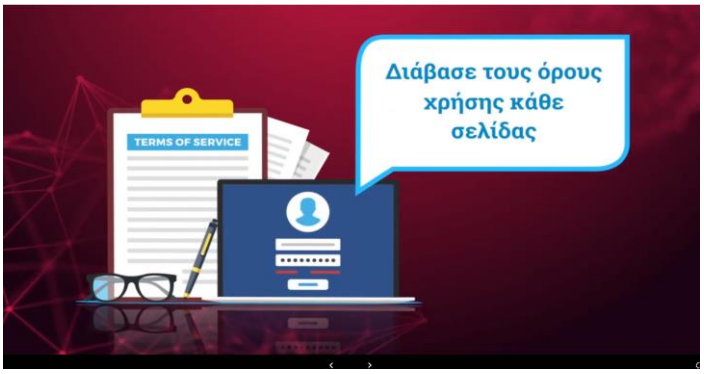
Ασφάλεια Λογαριασμού

- Σιγουρευτείτε ότι ο κωδικός ασφαλείας για το λογαριασμό σας είναι «δυνατός». Μη χρησιμοποιείτε κωδικούς που εύκολα μπορεί κανείς να μαντέψει, όπως η ημερομηνία γέννησής σας.
- Μη χρησιμοποιείτε τον ίδιο κωδικό με άλλους λογαριασμούς και θυμηθείτε να αλλάζετε τον κωδικό σας σε τακτά χρονικά διαστήματα.
- Όπως με κάθε άλλο κωδικό ασφαλείας μην αποκαλύπτετε τον κωδικό ασφαλείας του προφίλ σας σε τρίτα άτομα και μην τον συμπληρώνετε σε φόρμες στο διαδίκτυο, εκτός από τη σελίδα του log-in.
- Αν αντιληφθείτε ότι ο λογαριασμός σας έχει κλαπεί αναφέρετέ το άμεσα στο διαχειριστή του μέσου κοινωνικής δικτύωσης, μέσω της προτεινόμενης από αυτό διαδικασίας (report).
- Μελετήστε τις διαδικασίες προστασίας της ιδιωτικότητας και ασφάλειας λογαριασμού που παρέχει το μέσο κοινωνικής δικτύωσης και ενεργοποιήστε τις.



Όροι χρήσης

- Πριν δημιουργήσετε λογαριασμό σε κάποιο μέσο κοινωνικής δικτύωσης διαβάστε προσεχτικά τους όρους χρήσης και την πολιτική ασφαλείας του.



- Ξαναδιαβάστε τους όρους χρήσης και την πολιτική ασφαλείας ανά τακτά χρονικά διαστήματα. Κατά τη δημιουργία του λογαριασμού σας έχετε αποδεχθεί ότι ενδέχεται να αλλάξουν χωρίς προειδοποίηση.

Social Media & Πρότυπα

- Τα social media συχνά προβάλλουν έναν τέλειο τρόπο ζωής, ένα τέλειο πρότυπο ανθρώπου που είναι "μέσα σε όλα".
- Άνθρωποι, κυρίως έφηβοι αλλάζουν συμπεριφορά προκειμένου να προσαρμοστούν στα «πρότυπα» των social media.
- Νιώθουν αδύναμοι, αν δεν προσαρμοστούν στα πρότυπα των άλλων χρηστών.

#ΕΘΙΣΜΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Τι είναι ο Εθισμός στο Διαδίκτυο

- νέα μορφή εξάρτησης
- ορίζεται ως «ενασχόληση με το Διαδίκτυο για άντληση αισθήματος ικανοποίησης που συνοδεύεται με αύξηση του χρόνου που καταναλώνεται για την άντληση αυτού του αισθήματος»
- αποτελεί μια κατάσταση, που προκαλεί σημαντική έκπτωση στην κοινωνική και επαγγελματική ή ακαδημαϊκή λειτουργικότητα του ατόμου
- οι ειδικοί της ψυχικής υγείας όλο και συχνότερα καλούνται, να προσεγγίσουν θεραπευτικά άτομα με προβληματική χρήση του Διαδικτύου

Λόγοι που οδηγούν στον Εθισμό στο Διαδίκτυο

- Στο διαδίκτυο δεν υπάρχουν άμεσες συνέπειες των πράξεων, ο χρήστης μπορεί να μπει και να βγει όποτε θέλει, ενώ μπορεί να καλύψει την όποια εξωτερική εμφάνιση, αφού δεν υπάρχει, πολλές φορές, οπτική επαφή.
- Ο έφηβος μπορεί να ενσαρκώσει διαφορετικούς ρόλους, ή να υιοθετήσει διαφορετικές ταυτότητες ανάλογα με την εκάστοτε διαδικτυακή εμπειρία, εξαιτίας της ανωνυμίας, που συνιστά κατεξοχήν χαρακτηριστικό του διαδικτύου.
- Ο εθισμός των εφήβων στο διαδίκτυο μπορεί, επίσης να είναι το αποτέλεσμα άλλων ψυχικών διαταραχών, όπως κατάθλιψη, αγχώδεις διαταραχές, διαταραχές προσωπικότητας, υπερκινητικότητα και κοινωνική φοβία.

Συμπτώματα που πρέπει να σας προβληματίσουν

- Το παιδί ασχολείται συνεχώς με το διαδίκτυο ή με δραστηριότητες σχετικές με αυτό, παραμελώντας συχνά τις υποχρεώσεις του στο σπίτι και στο σχολείο.
- 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.
- Πτώση στις σχολικές επιδόσεις.
- Το διαδίκτυο το απασχολεί ακόμα και την ώρα που τρώτε ή την ώρα που διαβάζει.
- Αντιδρά πολύ νευρικά, θυμωμένα ή επιθετικά όταν κάποιος το διακόπτει από το παιχνίδι ή από τη συζήτηση που είχε online.
- Ξενυχτά συχνά για να μένει συνδεδεμένος / συνδεδεμένη στο διαδίκτυο.
- Δείχνει άγχος, ανησυχία, εξάρσεις θυμού ή βίας ή καταθλιπτική συμπεριφορά όταν δεν παίζει στο διαδίκτυο.

Ρόλος γονέων

- Οριοθετούμε από την αρχή τις ώρες που τα παιδιά μπορούν να είναι στο Διαδίκτυο, εξηγώντας πάντα τους λόγους που γίνεται αυτό, και ορίζουμε από την αρχή τις συνέπειες που θα υπάρξουν αν τα παιδιά παραβούν τους κανόνες αυτούς.
- Ο σκοπός μας είναι να βοηθήσουμε τα παιδιά μας να αναπτύξουν τα ίδια τον απαραίτητο αυτοέλεγχο και αυτοπειθαρχία αναφορικά με τη χρήση του Διαδικτύου.
- Είναι σημαντικό να μη χρησιμοποιούμε την πρόσβαση στο Διαδίκτυο σαν ανταμοιβή μιας καλής συμπεριφοράς του παιδιού ή να απαγορεύουμε την πρόσβαση στον υπολογιστή σαν τιμωρία.
- Ας εξερευνήσουμε τις δικές μας διαδικτυακές συνήθειες, καθώς ως γονείς ή εκπαιδευτικοί αποτελούμε από τα πιο σημαντικά πρότυπα προς μίμηση.
- Καλό είναι να έχουμε τους υπολογιστές που έχουν πρόσβαση στο διαδίκτυο σε κοινόχρηστους χώρους, ώστε να μπορούμε να επιβλέψουμε τις ώρες που αφιερώνουν στη χρήση του.
- Ας θυμόμαστε ότι ο προτεινόμενος καθημερινός χρόνος μπροστά στην οθόνη του υπολογιστή δε θα πρέπει να ξεπερνάει τη μιάμιση (1,5) ώρα.
- Ας αφιερώσουμε χρόνο στα παιδιά μας. Το διαδίκτυο και ο υπολογιστής δεν μπορεί και δεν πρέπει να υποκαταστήσει τη δική μας παρουσία.
- Καλό είναι να εγκαταστήσουμε φίλτρα γονικού ελέγχου σε όλες τις συσκευές που συνδέονται στο διαδίκτυο. Ας έχουμε όμως υπόψη ότι από μόνα τους τα φίλτρα δεν είναι η λύση ή η απάντηση για την ασφάλεια των παιδιών, αλλά αποτελούν ένα καλό ξεκίνημα.
- Ας ενθαρρύνουμε τα παιδιά να ασχολούνται με νέες δραστηριότητες και χόμπι που δεν περιλαμβάνουν τον υπολογιστή και ας ενθαρρύνουμε τις κοινωνικές τους αλληλεπιδράσεις.

- Παρόλα αυτά, αν τα συμπτώματα επιμένουν, θα ήταν καλό να ζητήσουμε άμεσα βοήθεια από κάποιον ειδικό.

Χαρακτηριστικά διαδικτυακών παιχνιδιών:

- Ο κόσμος που περιγράφουν δεν σταματά ποτέ και υφίσταται ακόμα και όταν ο παίκτης δεν είναι συνδεδεμένος. Ως εκ τούτου, ο παίκτης παύει να είναι ο πρωταγωνιστής και γίνεται απλά ένα μέλος του κόσμου.

- Οι διαδικτυακές δυνατότητες επιτρέπουν την ταυτόχρονη επικοινωνία χιλιάδων παικτών, από διαφορετικές χώρες και πολιτισμικό υπόβαθρο, και την αλληλεπίδραση τους.
- Επίσης προσφέρουν ένα ισχυρότατο σύστημα συνεχών ανταμοιβών (ολοκληρώνω μια αποστολή, παίρνω ένα βραβείο και πηγαίνω για την επόμενη αποστολή και το επόμενο βραβείο), 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 για τους νέους (και όχι μόνο) ανθρώπους.

Διαδικτυακά παιχνίδια και εθισμός

- Οι έρευνες δείχνουν ότι μεγάλο ποσοστό των χρηστών του διαδικτύου που παρουσιάζουν κατάχρηση ή εθισμό σε αυτό, είναι παίκτες διαδικτυακών παιχνιδιών.
- Τα χαρακτηριστικά των παιχνιδιών και των κινήτρων για τα οποία παίζει κανείς, έχουν ταυτιστεί με τον εθισμό στο διαδίκτυο, αφού στα παιχνίδια συγκεντρώνονται τόσο διαδικτυακές, όσο διαδραστικές-κοινωνικές συνθήκες, που αυξάνουν πολύ τις πιθανότητες για ανάπτυξη εθισμού.
- Τα άτομα που παρουσιάζουν εθισμό στα παιχνίδια έχουν προβλήματα στην καθημερινότητα τους και τη ψυχική τους διάθεση. Επηρεάζεται η εργασία τους (για τους ενήλικες), η ακαδημαϊκή πορεία ή επίδοση στο σχολείο, οι σχέσεις τους με γονείς και συνομηλίκους, αφού το παιχνίδι γίνεται, όχι απλά η κύρια ασχολία, αλλά το μοναδικό πράγμα που απασχολεί τη σκέψη τους.
- Σε επίπεδο συμπεριφοράς, πολύ συχνά είναι τα ξεσπάσματα θυμού, τα οποία μπορούν να λάβουν και ακραίες μορφές (σωματική επίθεση στους γονείς, αυτοτραυματισμοί) σε περίπτωση βίαιης διακοπής του διαδικτύου. Τα παραπάνω φαινόμενα, να σημειωθεί, αποτελούν αρκετά σπάνια περιστατικά.
- Ένα είναι το βασικό γνώρισμα της απαρχής μιας προβληματικής συμπεριφοράς (κατάχρηση, εθισμός) από τον παίκτη: το άτομο αρχίζει να αντιλαμβάνεται και να συμπεριφέρεται στο παιχνίδι σαν κάτι περισσότερο από αυτό που είναι, δηλαδή ένα απλό παιχνίδι.
- Η επικοινωνία με το παιδί είναι ο ακρογωνιαίος λίθος της εμπιστοσύνης που πρέπει να υπάρχει, η οποία θα φέρει τους γονείς συμμάχους στην προσπάθεια για απεγκλωβισμό από τον διαδικτυακό κόσμο.
- Οι κίνδυνοι του διαδικτύου και των διαδικτυακών παιχνιδιών δεν θα πρέπει να αποτελούν αποτρεπτικό παράγοντα για τη χρήση τους. Άλλωστε, η μεγάλη πλειοψηφία των παικτών δεν παρουσιάζουν εθισμό.
- Τα διαδικτυακά παιχνίδια δεν είναι εγγενώς αρνητικά. Ο αντίκτυπος που θα έχουν στο παιδί, τον έφηβο, ακόμα και τον ενήλικα, εξαρτάται από τη συνετή και υπεύθυνη χρήση, την ενημέρωση των οικείων του ανήλικου για αυτά και τη δυνατότητα διακριτικής παρακολούθησης που χρειάζεται, τη θέσπιση

κανόνων ορθής χρήσης, τη δημιουργία δραστηριοτήτων και κινήτρων στην πραγματική ζωή και, φυσικά, τη σχέση αμοιβαίας εμπιστοσύνης μεταξύ γονιού- παιδιού ή δάσκαλου- παιδιού.

#ΑΠΑΤΕΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

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. Βασική αρχή στις απάτες που διαπράττονται μέσω Διαδικτύου είναι να πείσουν το θύμα να καταβάλλει ένα μικρό, αρχικό χρηματικό ποσό, με σκοπό να εξασφαλίσει ένα πολύ μεγαλύτερο στο μέλλον ή γενικότερα να πείσουν το θύμα για την ασφάλεια των διαδικτυακών συναλλαγών με σκοπό στη συνέχεια να του αποσπάσουν μεγάλα χρηματικά ποσά.

Τα περιστατικά απάτης με τη χρήση πιστωτικών καρτών σε online αγορές αυξάνονται με ραγδαίο ρυθμό. Η έλλειψη επαφής πρόσωπο-με-πρόσωπο στο διαδίκτυο, τείνει να κάνει τους απατεώνες πιο τολμηρούς. Online αγορές προϊόντων που ποτέ δεν παραδόθηκαν (κινητά τηλέφωνα κ.α), υπέρογκες χρεώσεις πιστωτικών καρτών για υπηρεσίες που ποτέ δεν ζητήθηκαν ή είχαν αρχικά παρουσιαστεί ότι προσφέρονται δωρεάν, παραπλανητική πληροφόρηση για προϊόντα που αγοράζονται μέσω διαδικτύου, είναι μόνο μερικές από τις καταγγελίες πολιτών που δέχονται καθημερινά οι διωκτικές αρχές της χώρας μας.

Χαρακτηριστικά, αναφέρουμε περιπτώσεις ανθρώπων οι οποίοι, ενδιαφερόμενοι να αγοράσουν κάποιο αυτοκίνητο, μηχανή κ.τ.λ., αναζητούν στο διαδίκτυο την αγγελία που θα καλύψει τις ανάγκες τους. Στη συνέχεια, και αφού έχουν αναπτύξει σχετική επικοινωνία με τον κάτοχο - δράστη (email, τηλεφωνικά), καταβάλλουν κάποια προκαταβολή, συνήθως μέσω εταιρείας πληρωμών. Εκεί ξεκινούν τα προβλήματα, καθώς ο δράστης προφασίζεται πλέον διάφορες δικαιολογίες για να εισπράξει επιπλέον χρήματα, για να καθυστερήσει και, τελικά, να μην παραδώσει ποτέ το

προϊόν. Έχει παρατηρηθεί οι εγκληματίες να αποστέλλουν στα θύματα τους με email ακόμα και ψεύτικα έγγραφα του υπό πώληση αντικειμένου με τα οποία περιγράφουν τα διάφορα χαρακτηριστικά του. Οι εγκληματίες επίσης πολλές φορές για να πετύχουν τους σκοπούς τους χρησιμοποιούν παραπλανητικές ιστοσελίδες εταιρειών μεταφοράς οι οποίες εγγυώνται την ασφαλή μεταφορά του προϊόντος. Όταν όμως γίνει η πληρωμή οι ιστοσελίδες αυτές παύουν να υπάρχουν.

Τα ψηφιακά – εικονικά νομίσματα (με πιο γνωστό μεταξύ αυτών το bitcoin[1]), χρησιμοποιούνται ολοένα και περισσότερο σε νόμιμες αλλά και παράνομες δραστηριότητες. Η ιδιαιτερότητα των ψηφιακών / εικονικών / κρυπτο- νομισμάτων είναι ότι η κυκλοφορία τους δεν ελέγχεται κεντρικά από κάποιο φορέα, ούτε απαιτείται η δήλωση / παροχή πραγματικών στοιχείων από τους συναλλασσόμενους προς κάποια ρυθμιστική Αρχή. Οι κυβερνοεγκληματίες πραγματοποιούν μεταφορές χρημάτων ή νομιμοποιούν έσοδα από παράνομες δραστηριότητες βασιζόμενοι στα ψηφιακά νομίσματα και την ανωνυμία που αυτά παρέχουν. Αναμένεται στο προσεχές μέλλον να υπάρξουν νομοθετικές εξελίξεις στο συγκεκριμένο ζήτημα, καθώς παρατηρείται ότι όλο και περισσότερα κράτη αναζητούν τρόπους ελέγχου της χρήσης ψηφιακών νομισμάτων από τους πολίτες τους.

#ηλεκτρονική απάτη- Phising

Ο όρος "phishing" αναφέρεται στα απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου, που σκοπό έχουν να εξαπατηθούν οι παραλήπτες τους και να γνωστοποιήσουν στους απατεώνες προσωπικές και οικονομικές τους πληροφορίες ή κωδικούς ασφαλείας τους.

ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ;

Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου: μπορεί να μοιάζουν πάρα πολύ με τα μηνύματα που στέλνουν στους πελάτες τους οι τράπεζες.

- αντιγράφουν το λογότυπο, τα χαρακτηριστικά και το ύφος των πραγματικών

[1] https://www.ecb.europa.eu/explainers/tell-me/html/what-is-bitcoin.el.html

μηνυμάτων ηλεκτρονικού ταχυδρομείου

- σας ζητούν να κατεβάσετε στη συσκευή σας ένα επισυναπτόμενο αρχείο ή να κάνετε κλικ σε έναν ηλεκτρονικό σύνδεσμο (link)
- κάνουν χρήση ορολογίας που δίνει την αίσθηση του κατεπείγοντος

Οι εγκληματίες στον κυβερνοχώρο βασίζονται στο γεγονός ότι οι άνθρωποι είναι απασχολημένοι και βιαστικοί.

Καταρχήν, αυτά τα απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου μοιάζουν να είναι νόμιμα.

Προσέξτε ιδιαίτερα όταν χρησιμοποιείτε μια φορητή συσκευή. Ενδεχομένως να είναι πιο δύσκολο να εντοπίσετε μια απόπειρα ηλεκτρονικού "ψαρέματος" από το κινητό τηλέφωνο ή το tablet σας.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

- Διατηρείτε το λογισμικό ενημερωμένο, περιλαμβανομένου του φυλλομετρητή ιστοσελίδων (browser), του αντιικού προγραμμάτος (antivirus) και του λειτουργικού συστήματος.
- Να είστε ιδιαίτερα προσεκτικοί εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου "τράπεζας" σας ζητά ευαίσθητες πληροφορίες (π.χ. τον κωδικό πρόσβασης του τραπεζικού σας λογαριασμού μέσω internet banking).
- Ελέγξτε προσεκτικά το μήνυμα ηλεκτρονικού ταχυδρομείου: συγκρίνετε τη διεύθυνση με τα προηγούμενα πραγματικά μηνύματα από την τράπεζα συνεργασίας σας. Ελέγξτε για ορθογραφικά λάθη και λάθη γραμματικής ή σύνταξης.
- Μην απαντάτε σε ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου, αντίθετα προωθήστε το στην τράπεζα συνεργασίας σας, πληκτρολογώντας την ηλεκτρονική της διεύθυνση μόνοι σας.
- Μην κάνετε απευθείας κλικ στον ηλεκτρονικό σύνδεσμο (link) και μην πραγματοποιείστε λήψη (download) του επισυναπτόμενου αρχείου, αντίθετα πληκτρολογήστε τη διεύθυνση του ηλεκτρονικού συνδέσμου στον φυλλομετρητή ιστοσελίδων (browser) που χρησιμοποιείτε.
- Σε περίπτωση οποιασδήποτε αμφιβολίας, ελέγξτε την ιστοσελίδα ή τηλεφωνήστε στην τράπεζα συνεργασίας σας.

#ΑΠΑΤΗΛΑ ΜΗΝΥΜΑΤΑ SMS (SMISHING)

Ο όρος "smishing" (ένας συνδυασμός των λέξεων "SMS" και "Phishing") αναφέρεται στην προσπάθεια των απατεώνων να αποκτήσουν προσωπικές και οικονομικές πληροφορίες ή κωδικούς ασφαλείας μέσω μηνυμάτων SMS

ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ;

Το μήνυμα κειμένου συνήθως θα σας ζητά να κάνετε κλικ σε έναν ηλεκτρονικό σύνδεσμο (link) ή να καλέσετε έναν αριθμό τηλεφώνου, προκειμένου να επαληθεύσετε, ενημερώσετε ή επανανεργοποιήσετε τον λογαριασμό σας. Αλλά…ο ηλεκτρονικός σύνδεσμος οδηγεί σε ψεύτικη ιστοσελίδα και ο αριθμός τηλεφώνου οδηγεί στον απατεώνα που ισχυρίζεται ότι εκπροσωπεί τη νόμιμη επιχείρηση.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

- Μην κάνετε κλικ σε ηλεκτρονικούς συνδέσμους (links), συνημμένα αρχεία ή εικόνες που λαμβάνετε με μηνύματα κειμένου (sms) δίχως να έχετε επαληθεύσει τον αποστολέα.
- Μη βιάζεστε. Πάρτε τον χρόνο σας και πραγματοποιήστε τους απαραίτητους ελέγχους προτού απαντήσετε.
- Ποτέ μην απαντάτε σε μήνυμα κειμένου (sms) που σας ζητά τον κωδικό "PIN" ή τον κωδικό πρόσβασης ("password") στον τραπεζικό σας λογαριασμό ή οποιαδήποτε άλλα εξατομικευμένα διαπιστευτήρια ασφαλείας (π.χ. e-banking user name).
- Εάν νομίζετε ότι ενδέχεται να έχετε απαντήσει σε ένα απατηλό μήνυμα κειμένου (sms) και παρείχατε τα στοιχεία των τραπεζικών σας λογαριασμών, επικοινωνήστε αμέσως με την τράπεζα συνεργασίας σας.

#ηλεκτρονική απάτη-Θέσεις εργασίας

Η παγκόσμια οικονομική κατάσταση έχει φέρει στο προσκήνιο ένα ακόμη είδος απάτης. Πρόκειται για απατηλές διαδικτυακές αγγελίες που αναρτώνται σε ιστοσελίδες εύρεσης εργασίας ή αποστέλλονται μέσω e-mail στο θύμα και περιγράφουν ιδιαίτερα ελκυστικές θέσεις εργασίας συνήθως στο εξωτερικό, ενώ οι δράστες δεν διστάζουν να δημιουργήσουν ιστοσελίδα της εταιρείας-εργοδότη, στην

οποία αναρτούν πληροφορίες για την απατηλή αγγελία προκειμένου να γίνουν ακόμη πιο πειστικοί. Ζητείται από τους ανυποψίαστους υποψήφιους εργαζόμενους να γνωστοποιήσουν τα προσωπικά τους στοιχεία, ακόμη και να αποστείλουν αντίγραφα εγγράφων τους, όπως το δίπλωμα οδήγησης, την ταυτότητά τους και όποιο άλλο θεωρηθεί «χρήσιμο» και «απαραίτητο» για την διεκδίκηση της εν λόγω θέσης εργασίας. Στη συνέχεια, ο εργαζόμενος ενημερώνεται ότι μιας και η εργοδότρια εταιρεία δεν κατέχει τραπεζικό λογαριασμό στην δική του χώρα, ένας από τους πιστωτές της θα του χορηγήσει επιταγή για τα έξοδα και το μισθό του. Η επιταγή συνήθως υπερβαίνει κατά πολύ τα συμφωνηθέντα και ζητείται από τον υποψήφιο να αποστείλει με έμβασμα το επιπλέον ποσό στον εργοδότη. Αφού η διαδικασία ολοκληρωθεί, ο εργαζόμενος αντιλαμβάνεται ότι η επιταγή είναι πλαστή. Σε άλλες περιπτώσεις, το θύμα πείθεται να καταβάλει ένα ποσό για να κατοχυρώσει την εν λόγω «κάλπικη» θέση εργασίας.

<u>Συμβουλές</u>

- Να διασταυρώνετε τα στοιχεία κάθε ενδεχόμενου εργοδότη και μέσω δεύτερης πηγής και στη συνεχεία να απευθύνεστε απευθείας στον εργοδότη.
- Να μην εμπιστεύεστε όσους, μέσω διαδικτύου, σας ζητούν χρήματα εκ των προτέρων για να σας βρούνε εργασία ή να σας προσφέρουν μια θέση εργασίας.
- Ποτέ μην δεχθείτε να πληρώσετε για «αποκλειστικές» πληροφορίες για θέσεις εργασίας.
- Να αξιολογούνται προσεκτικά τα στοιχεία επαφής, που δίνονται σε αγγελίες εργασίας μέσω διαδικτύου ή σε σχετικά e-mail και να προσέχετε εάν υπάρχουν ανορθογραφίες ή κάποια διεύθυνση e-mail που δεν αναφέρει το όνομα της εταιρείας.
- Να δίνεται προσοχή στη σύνταξη του κειμένου, όπου εάν υπάρχουν πολλά ορθογραφικά λάθη και άλλες ανακρίβειες, αυτό αποτελεί συνηθισμένη ένδειξη που παραπέμπει σε ψεύτικη αγγελία εργασίας.
- Να πληκτρολογούνται οι διευθύνσεις των ιστοσελίδων (URL) στον περιηγητή (browser) αντί των υπερσυνδέσμων (links) όταν ελέγχετε τις πηγές των θέσεων εργασίας.

- Να δίνετε ιδιαίτερη προσοχή όταν απευθύνεστε σε εταιρείες που βρίσκονται στο εξωτερικό ή γίνεστε αποδέκτης μηνυμάτων από φερόμενες εταιρείες του εξωτερικού.
- Εάν κάποια θέση εργασίας υπόσχεται υπερβολικά υψηλές αποδοχές, οι οποίες μάλιστα σε σύντομο χρονικό διάστημα θα διπλασιαστούν, πιθανότατα πρόκειται για απατηλό-παραπλανητικό μήνυμα, το οποίο πρέπει να ελεγχθεί.

#ηλεκτρονική απάτη - Spamming

Η λέξη «Spam» περιγράφει τη μαζική αποστολή μηνυμάτων ηλεκτρονικού υπολογιστή (e-mails), τα οποία έχουν συνήθως απρόκλητο και εμπορικό χαρακτήρα, και αποστέλλονται αδιακρίτως. Όταν ο στόχος του αποστολέα των μηνυμάτων αυτών είναι να εξαπατήσει τον αποδέκτη και να χρησιμοποιήσει με κακόβουλο τρόπο τα δεδομένα που θα υποκλέψει, τότε έχουμε να κάνουμε με τη διαδικασία του «Scamming». Πρόκειται για τον πλέον διαδεδομένο τρόπο δράσης σε πολλά είδη ηλεκτρονικών οικονομικών εγκλημάτων (phishing, εικονικές θέσεις εργασίας στο εξωτερικό, διαφημίσεις για χάσιμο βάρους κ.τ.λ.).

Συμβουλές

- Μην ανοίγετε τα spam μηνύματα.
- Μην απαντάτε στα spam μηνύματα, ώστε ο αποστολέας να μην αντιληφθεί ότι η διεύθυνσή σας είναι υπαρκτή και ενεργή.
- Διατηρείτε δύο (2) e-mail διευθύνσεις, μία για τους οικείους σας και μία για κάθε άλλο σκοπό.
- Ποτέ μην αγοράζετε κάτι που σας αποστέλλεται μέσω ενός απομονωμένου e-mail.

ΑΠΑΤΕΣ ΣΕ ΑΓΟΡΕΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

Οι προσφορές μέσω διαδικτύου συνιστούν συχνά επικερδείς αγορές, αλλά χρειάζεται ιδιαίτερη προσοχή στα περιστατικά απάτης.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

- Να κάνετε χρήση εγχώριων ιστοσελίδων λιανικών πωλήσεων, όταν είναι δυνατόν - είναι πιθανότερο να λύσετε τυχόν προβλήματα που θα ανακύψουν.
- Πραγματοποιήστε την έρευνα σας - ελέγξτε τις κριτικές προτού προβείτε σε κάποια αγορά.
- Χρησιμοποιήστε πιστωτικές κάρτες - έχετε περισσότερες πιθανότητες να σας επιστραφούν τα χρηματικά ποσά σε περίπτωση απάτης.
- Πληρώστε μόνο μέσω μιας ασφαλούς υπηρεσίας πληρωμών - Σας ζητούν μεταφορά χρημάτων; Σκεφτείτε το διπλά!
- Πληρώστε μόνο εφόσον είστε συνδεδεμένοι στο διαδίκτυο μέσω ασφαλών συνδέσεων - αποφεύγετε τη χρήση δωρεάν ή ανοικτών δημόσιων δικτύων WiFi.
- Πληρώστε μόνο μέσω ασφαλούς συσκευής - Διατηρείτε το λειτουργικό σας σύστημα και λογισμικό ασφαλείας ενημερωμένο.
- Προσοχή στις διαφημίσεις που προσφέρουν εξωφρενικές προσφορές ή θαυματουργά προϊόντα - Εάν ακούγεται πολύ καλό για να είναι αληθινό, τότε κατά πάσα πιθανότητα είναι ψεύτικο!
- Αναδυόμενο παράθυρο που ισχυρίζεται ότι έχετε κερδίσει βραβείο; Σκεφτείτε το ξανά. Ενδεχομένως να κερδίσατε κακόβουλο λογισμικό.
- Εάν δεν παραλάβετε το προϊόν σας, επικοινωνήστε με τον έμπορο/πωλητή. Εάν δεν λάβετε απάντηση, επικοινωνήστε με την τράπεζα συνεργασίας σας.

Να αναφέρετε πάντοτε τυχόν ύποπτη απόπειρα απάτης στην αστυνομία, ακόμα και αν δεν είστε θύμα αυτής.

Βασικές συμβουλές για ασφαλείς online συναλλαγές

- Πραγματοποιούμε έρευνα αγοράς πριν προβούμε σε οποιαδήποτε συναλλαγή.
- Αγοράζουμε από αξιόπιστες πηγές. Πραγματοποιούμε αγορές από εταιρείες και καταστήματα που γνωρίζουμε ή που έχουμε αγοράσει ξανά και ελέγχουμε τις αξιολογήσεις κάθε πωλητή.

- Ελέγχουμε τις επαναλαμβανόμενες χρεώσεις. Πριν δώσουμε τα στοιχεία της κάρτας μας για την πληρωμή μιας επαναλαμβανόμενης υπηρεσίας μέσω διαδικτύου, γνωρίζουμε εκ των προτέρων τον τρόπο διακοπής αυτής.
- Πολλά διαδικτυακά καταστήματα ζητούν την αποθήκευση των στοιχείων πληρωμής. Είμαστε επιφυλακτικοί σε αυτό και σκεφτόμαστε διπλά πριν προβούμε σ'αυτή την ενέργεια κατανοώντας τους κινδύνους που ελλοχεύουν.
- Βεβαιωνόμαστε για την ασφαλή διαδικασία μεταφοράς δεδομένων. Αναζητούμε το σύμβολο του λουκέτου στη γραμμή URL και τη χρήση των πρωτοκόλλων HTTPS και SSL κατά την περιήγηση στο διαδίκτυο και αποφεύγουμε διαδικτυακές αγορές σε ιστοσελίδες που δεν χρησιμοποιούν πλήρη αυθεντικοποίηση (Verified by Visa / Mastercard Secure Code).
- Αποθηκεύουμε 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.
- Όταν αγοράζουμε μέσω διαδικτύου από ιδιώτη, δε στέλνουμε χρήματα προκαταβολικά στον πωλητή. Εάν είναι δυνατό, διατηρούμε το δικαίωμα της πρότερης παραλαβής των προϊόντων (διαδικασία αντικαταβολής).
- Δεν στέλνουμε χρήματα σε κάποιον που δε γνωρίζουμε. Εάν κάποιος μας προσεγγίσει μέσω διαδικτύου και μας ζητήσει χρήματα σκεφτόμαστε εάν θα δίναμε μετρητά σε άγνωστο πρόσωπο στο δρόμο.
- Προστατεύουμε τις κάρτες μας, όπως θα προστατεύαμε τα μετρητά μας. Πάντα διατηρούμε την κάρτα μας στην κατοχή μας, ορίζουμε όρια ανάληψης και αγορών στην κάρτα μας που ανταποκρίνεται στις ανάγκες μας και δεν αποθηκεύουμε ή σημειώνουμε τον κωδικό μας PIN. Δεν αποκαλύπτουμε το PIN μας σε οποιονδήποτε. Ποτέ δεν δίνουμε τον αριθμό της κάρτας μας, το PIN ή οποιαδήποτε άλλη πληροφορία για την κάρτα, μέσω ηλεκτρονικού ταχυδρομείου (e-mail).
- Μόνο κακόβουλοι χρήστες θα ζητήσουν τους κωδικούς της ηλεκτρονικής τραπεζικής μας ή τα στοιχεία της κάρτας μας μέσω ηλεκτρονικού

ταχυδρομείου ή τηλεφώνου. Ούτε η τράπεζά μας ούτε οι αστυνομικές αρχές θα ζητήσουν ποτέ κάτι τέτοιο. Αν έχουμε αποκαλύψει τους κωδικούς της ηλεκτρονικής τραπεζικής μας ή τα στοιχεία της κάρτας μας σε άγνωστο άτομο, ακυρώνουμε την κάρτα και επικοινωνούμε αμέσως με την τράπεζά μας.

- Φροντίζουμε να έχουμε εγκατεστημένο στον υπολογιστή σας κάποιο πρόγραμμα προστασίας από ιούς (antivirus), το οποίο να αναβαθμίζουμε συχνά ή ακόμη καλύτερα έχουμε επιλέξει να λαμβάνουμε τις ενημερώσεις αυτόματα.
- Αποφεύγουμε να κάνουμε τις αγορές μέσω κοινόχρηστων υπολογιστών.
- Τις περισσότερες φορές για να πραγματοποιήσουμε μια αγορά ή συναλλαγή σε κάποιο ηλεκτρονικό κατάστημα, το πιθανότερο είναι ότι θα χρειαστεί να δημιουργήσουμε ένα λογαριασμό και να επιλέξουμε κωδικό πρόσβασης (password). Για όλα τα passwords που χρησιμοποιούμε ισχύουν τα εξής:
  - ✓ Δημιουργούμε ισχυρό κωδικό πρόσβασης.
  - ✓ Φροντίζουμε να τα αλλάζετε τακτικά.
  - ✓ Δε χρησιμοποιούμε το ίδιο όνομα χρήστη και κωδικό σε διαφορετικές υπηρεσίες του Διαδικτύου, ώστε αν κάποιος παραβιάσει τον κωδικό μας σε μία υπηρεσία, να μην έχει πρόσβαση παντού.
  - ✓ Τα ονόματα, οι ημερομηνίες γέννησης και οι αριθμοί τηλεφώνου μπορεί να φαίνονται ως η κατάλληλη λύση για να θυμόμαστε τους κωδικούς μας αλλά δεν είναι ασφαλή γι' αυτό χρησιμοποιούμε συνδυασμό λέξεων, αριθμών και συμβόλων ή και ολόκληρες φράσεις.
- Θα πρέπει να είμαστε επιφυλακτικοί όταν συναντάμε «μεγάλες» προσφορές που λήγουν άμεσα, καθώς συνήθως κρύβουν παγίδες. Επίσης, ιδιαίτερη προσοχή θα πρέπει να δίνουμε εάν υπάρχει ασυνταξία ή ορθογραφικά λάθη στην ιστοσελίδα του ηλεκτρονικού καταστήματος.

Σε περίπτωση που προκύψει πρόβλημα με τη διαδικτυακή μας αγορά..

- Η πρώτη μας ενέργεια είναι πάντα η επικοινωνία με τον πωλητή για την επίλυση του θέματος.
- Εάν προσφύγουμε στην τράπεζα, προσκομίζουμε αντίγραφο της ηλεκτρονικής αλληλογραφίας με τον πωλητή.

- Εάν επιστρέψουμε ελαττωματικά ή κατεστραμμένα προϊόντα, πάντα το κάνουμε μέσω συστημένου ταχυδρομείου. Διατηρούμε την απόδειξη με τον αριθμό αποστολής καθώς μπορεί να το χρειασθούμε αργότερα.

Σε περίπτωση που πέσουμε θύματα διαδικτυακής απάτης…

- Εάν το προϊόν πληρώθηκε με πιστωτική, χρεωστική ή προπληρωμένη κάρτα, το αναφέρουμε στην τράπεζά μας. Ίσως να έχουμε το δικαίωμα επιστροφής των χρημάτων.
- Δεδομένου ότι η απάτη είναι κατ' έγκληση διωκόμενο αδίκημα, προσφεύγουμε στην πλησιέστερη στον τόπο κατοικίας μας αστυνομική ή εισαγγελική αρχή προκειμένου να καταγγείλουμε σχετικά, προσκομίζοντας τα απαραίτητα αποδεικτικά στοιχεία.

ΤΙ ΝΑ ΚΑΝΕΙΣ

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.

https

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.

ΧΡΥΣΟΙ ΚΑΝΟΝΕΣ

ΑΣΦΑΛΕΙΣ ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΓΟΡΕΣ

EUROPOL EC3 European Cybercrime Centre

CYBER CRIME DIVISION

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών

ΤΙ ΝΑ ΑΠΟΦΕΥΓΕΙΣ

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 δεν γνωρίζεις.

Εάν κάποιος σε προσεγγίσει μέσω διαδικτύου και σου ζητήσει χρήματα, σκέψου εάν θα έδινες μετρητά σε άγνωστο πρόσωπο στο δρόμο.

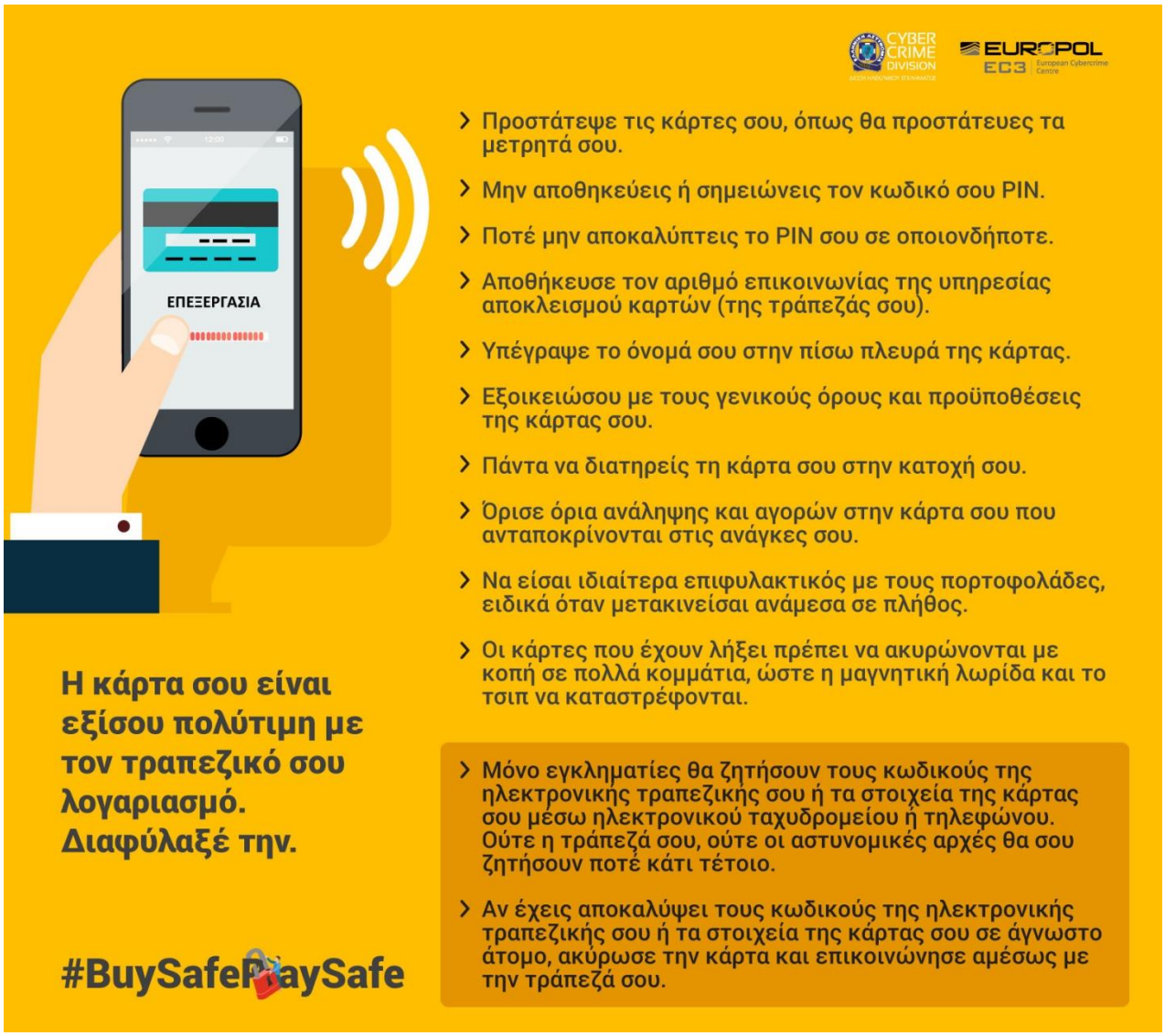
Ποτέ μην δίνεις τον αριθμό της κάρτας σου, το PIN ή οποιαδήποτε άλλη πληροφορία για την κάρτα, μέσω ηλεκτρονικού ταχυδρομείου (e-mail).

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.


CYBER CRIME DIVISION
ΔΙΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ
EUROPOL
EC3 European Cybercrime Centre
Διάβασε τα δικαιώματα των εφαρμογών, ειδικά αν ζητείται η καταχώρηση των στοιχείων της κάρτας σου.
Έλεγξε το είδος δεδομένων που η εφαρμογή μπορεί να έχει πρόσβαση και αν διαμοιράζει τις πληροφορίες σου με τρίτους φορείς.
Χρησιμοποίησε προπληρωμένες κάρτες για να εγγραφείς σε συνδρομητικές υπηρεσίες μέσω εφαρμογής.
Επιβεβαίωσε ότι οι αγορές παιχνιδιών (εντός εφαρμογής) με χρήση της πιστωτικής σου κάρτας είναι δυνατές μόνο με τη χρήση του κωδικού PIN.
Έλεγξε τον εκδότη της εφαρμογής. Να είσαι επιφυλακτικός – οι εγκληματίες μπορεί να χρησιμοποιήσουν όμοια ονόματα.
Έλεγξε τη βαθμολογία και τις αξιολογήσεις άλλων χρηστών.
Έλεγξε την ημερομηνία έκδοσης και το πλήθος των φορών που έχει κατέβει η εφαρμογή.
Αναζήτησε ορθογραφικά λάθη στον τίτλο ή στην περιγραφή.
Όταν υπάρχει αμφιβολία, κατέβασε την εφαρμογή από την επίσημη ιστοσελίδα του πωλητή.
Αποθηκευτικός Χώρος
Επέλεξε μέθοδο πληρωμής
Εισήγαγε αριθμό πιστωτικής ή χρεωστικής κάρτας
Άλλη μέθοδος
ΟΡΟΙ & ΠΡΟΥΠΟΘΕΣΕΙΣ
Πριν προχωρήσεις διάβασε και αποδέξου τους Όρους και τις Προϋποθέσεις
Ακύρωση
OK
Αυτή η εφαρμογή θα έχει πρόσβαση σε:
Επαφές
Τηλεφωνικές κλήσεις
Μηνύματα
Μικρόφωνο
Κάμερα
Τοποθεσία
Αποθηκευτικό χώρο
#BuySafePlaySafe



Κινητά τηλέφωνα και Διαδικτυακές Παγίδες

Η χρήση των κινητών τηλεφώνων -και δη των smartphones- αυξάνεται συνεχώς και όλο και περισσότεροι χρήστες χρήζουν αυτά ως απαραίτητα εργαλεία για την καθημερινότητά τους. Επιτήδειοι εκμεταλλευόμενοι την τάση αυτή, προκαλούν απάτες αρκετών εκατομμυρίων ευρώ από την αγοραπωλησία εφαρμογών λογισμικού για κινητά τηλέφωνα, όπως, για παράδειγμα, ο εντοπισμός του κινητού τηλεφώνου κάποιου αγαπημένου προσώπου. Συνήθως ζητείται από τον ανυποψίαστο χρήστη, να εισάγει το κινητό του τηλέφωνο προκειμένου να αποκτήσει την εφαρμογή που έχει επιλέξει. Στη συνέχεια, ξεκινούν οι υπέρογκες χρεώσεις στον αριθμό του, τις οποίες ο ίδιος αποδέχτηκε, καθώς αυτές περιγράφονται στα ψιλά γράμματα των όρων χρήσης που η πλειοψηφία των καταναλωτών δεν διαβάζουν.


ΕΦΑΡΜΟΓΕΣ
ΔΕΝ ΕΙΝΑΙ ΠΑΙΧΝΙΔΙ!
Εγκαταστήστε εφαρμογές μόνο μέσω των επίσημων καταστημάτων εφαρμογών.
Πριν κατεβάσετε μια εφαρμογή, βρείτε πληροφορίες γι' αυτή και τους δημιουργούς της. Προσοχή στους συνδέσμους που λαμβάνετε μέσω email ή SMS, που μπορεί να σας παραπλανήσουν ώστε να εγκαταστήσετε εφαρμογές από τρίτες ή μη έμπιστες πηγές.
Άγνωστο κατάστημα
Sketchy εφαρμογές
by TrustMe :-) Developers
Μοναδική εφαρμογή με την οποία θα κερδίσετε 20.000 ευρώ σε δύο ώρες. Κατεβάστε την τώρα!
ΕΛΕΓΞΤΕ ΤΙΣ ΚΡΙΤΙΚΕΣ ΚΑΙ ΤΙΣ ΒΑΘΜΟΛΟΓΙΕΣ ΑΛΛΩΝ ΧΡΗΣΤΩΝ.
ΑΞΙΟΛΟΓΗΣΕΙΣ (9,458)
Χρήστης 1
Malware
Χρήστης 2
Malware 100%
Χρήστης 3
Μείνετε μακριά!
Χρήστης 4
Μην την κατεβάσετε
ΔΙΑΒΑΣΤΕ ΤΙΣ ΑΔΕΙΕΣ ΠΡΟΣΒΑΣΗΣ ΠΟΥ ΖΗΤΑ Η ΕΦΑΡΜΟΓΗ
Ελέγξτε σε ποιες κατηγορίες δεδομένων θα μπορεί να έχει πρόσβαση, καθώς και αν θα μοιράζεται πληροφορίες για εσάς με εξωτερικές οντότητες.
Χρειάζεται όλες αυτές τις άδειες; Αν όχι, τότε μην την κατεβάσετε!
Αυτή η εφαρμογή θα έχει πρόσβαση σε:
Επαφές
Τηλεφωνικές κλήσεις
Μηνύματα
Μικρόφωνο
Κάμερα
Τοποθεσία
Αποθηκευτικό χώρο
ΑΔΕΙΕΣ ΕΦΑΡΜΟΓΗΣ
ΕΓΚΑΤΑΣΤΗΣΤΕ ΜΙΑ ΕΦΑΡΜΟΓΗ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΦΟΡΗΤΕΣ ΣΥΣΚΕΥΕΣ.
Θα εξετάσει όλες τις εφαρμογές της συσκευής καθώς και κάθε επόμενη που θα εγκαταστήσετε και θα σας προειδοποιεί σε περίπτωση εντοπισμού κακόβουλου λογισμικού.
EUROPOL
EC3 European Cybercrime Centre
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ
#MobileMalware

ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ
MOBILE BANKING

ΤΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΘΑ ΣΑΣ ΚΟΣΤΙΣΕΙ!

Το κακόβουλο λογισμικό mobile banking είναι σχεδιασμένο ώστε να υποκλέπτει τραπεζικά δεδομένα που είναι αποθηκευμένα στη συσκευή σας.

ΠΩΣ ΔΙΑΔΙΔΕΤΑΙ;

- **Κατά την επίσκεψη σε μολυσμένους ή κακόβουλους ιστοτόπους**
- **Κατεβάζοντας κακόβουλες εφαρμογές**
- **Με τη μέθοδο του phishing**

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

- **Υποκλοπή προσωπικών πληροφοριών αυθεντικοποίησης**
- **Χωρίς δικαίωμα αναλήψεις και μεταφορές χρημάτων**

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

- Κατεβάστε την επίσημη εφαρμογή για φορητές συσκευές της τράπεζάς σας και βεβαιωθείτε ότι επισκέπτεσθε τον επίσημο ιστότοπο της τράπεζας κάθε φορά.
- Αποφύγετε την αυτόματη είσοδο (log in) στον ιστότοπο ή την εφαρμογή της τράπεζας.
- Μην μοιράζεστε με κανέναν δεδομένα που αφορούν τον τραπεζικό σας λογαριασμό και ιδίως τον κωδικό πρόσβασης.
- Αν υπάρχει διαθέσιμη, εγκαταστήστε μια εφαρμογή ασφαλείας που θα σας προειδοποιεί εγκαίρως για οποιαδήποτε ύποπτη δραστηριότητα.
- Αν χάσετε το κινητό σας τηλέφωνο, ή αλλάξετε αριθμό, επικοινωνήστε με την τράπεζά σας, ώστε να γίνει επικαιροποίηση των στοιχείων σας.
- Μην μοιράζεστε οποιαδήποτε πληροφορία για τον τραπεζικό σας λογαριασμό μέσω SMS ή email.
- Χρησιμοποιήστε πάντα μια ασφαλή σύνδεση Wi-Fi για τη σύνδεσή σας στον ιστότοπο ή την εφαρμογή της τράπεζάς σας. Μην το κάνετε μέσω ελεύθερου Wi-Fi!
- Ελέγχετε τακτικά τους έντυπους τραπεζικούς σας λογαριασμούς – εφόσον λαμβάνετε τέτοιους.

EUROPOL EC3 European Cybercrime Centre

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#MobileMalware

Ασφάλεια Πληροφοριών

Είναι ένα σύγχρονο πρόβλημα που αντιμετωπίζουν όλα τα πληροφοριακά συστήματα και επηρεάζουν άμεσα την πληροφοριακή υποδομή. Τα ζητήματα ασφάλειας πληροφοριών παρουσιάζονται σε όλες τις περιοχές εφαρμογών όπως: στις επιχειρήσεις – οργανισμούς, στην δημόσια διοίκηση και σε ατομικό επίπεδο καθώς το προσωπικό απόρρητο μπορεί να διασφαλισθεί σήμερα μόνο με συστήματα ασφάλειας πληροφοριών και κρυπτογραφίας.

Η ασφάλεια πληροφοριών είναι ένα από τα πιο καίρια και σύγχρονα ζητήματα στο χώρο της τεχνολογίας και της πληροφορικής. Η συνεχώς αυξανόμενη εξάρτηση τόσο του δημόσιου όσο και του ιδιωτικού τομέα από τα πληροφοριακά συστήματα καθιστά κρίσιμη και αναγκαία προϋπόθεση την συνεχή και αδιάλειπτη παρακολούθηση των συστημάτων τους προκειμένου να διασφαλίσουν απόρρητες πληροφορίες και υψηλής σημασίας συναλλαγές.

Ειδικοί σε όλο τον κόσμο ασχολούνται με θέματα ασφάλειας πληροφοριών και προσπαθούν μέσω έρευνας και τεχνικών αναλύσεων να εντοπίσουν αδυναμίες σε εφαρμογές και συστήματα, μεθόδους παράκαμψης των υπαρχόντων μέτρων ασφαλείας και να αναπτύξουν νέες μεθόδους ή μέτρα προστασίας για να ενισχύσουν την ασφάλεια των συστημάτων και εφαρμογών ενάντια σε επιθέσεις.

ΑΠΕΙΛΕΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΙΣΤΟΥ

ΕΛΕΓΞΤΕ ΔΙΠΛΑ ΠΡΙΝ ΚΑΝΕΤΕ ΚΛΙΚ.

Θα μπορούσατε να χάσετε χρήματα, προσωπικά δεδομένα ή ακόμα και αποθηκευμένα αρχεία, αν η συσκευή σας σταματήσει να λειτουργεί. Μην τσιμπάτε!

ΠΩΣ ΘΑ ΜΠΟΡΟΥΣΕ ΝΑ ΣΥΜΒΕΙ;

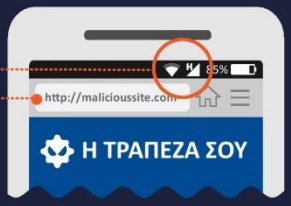
ΕΠΙΘΕΣΕΙΣ PHISHING: Εγκληματίες εξαπατούν τους χρήστες ώστε να δώσουν προσωπικές πληροφορίες, προσποιούμενοι έμπιστες οντότητες. Επιθέσεις γίνονται μέσω email, μηνυμάτων SMS ή ιστοτόπων κοινωνικής δικτύωσης.

ΠΕΡΙΗΓΗΣΗ ΣΕ ΙΣΤΟΤΟΠΟ: Η συσκευή σας μπορεί να μολυνθεί κατά τη διάρκεια μιας απλής επίσκεψης σε έναν μη ασφαλή ιστότοπο.

ΜΕΤΑΦΟΡΤΩΣΗ ΑΡΧΕΙΩΝ: Σε ένα email μπορεί να εμπεριέχονται κακόβουλοι σύνδεσμοι ή μολυσμένα επισυναπτόμενα αρχεία.

ΓΙΑΤΙ ΕΙΝΑΙ ΑΠΟΤΕΛΕΣΜΑΤΙΚΟ;

Οι φορητές συσκευές είναι **ΔΙΑΡΚΩΣ ΣΥΝΔΕΔΕΜΕΝΕΣ** στο Διαδίκτυο.



Το **ΜΙΚΡΟ ΜΕΓΕΘΟΣ ΤΗΣ ΟΘΟΝΗΣ ΤΗΣ ΣΥΣΚΕΥΗΣ** συχνά δημιουργεί προβλήματα. Οι περιηγητές στις φορητές συσκευές προβάλλουν τα URLs σε περιορισμένο χώρο, δυσκολεύοντας έτσι τον έλεγχο για το αν ο ιστότοπος είναι ορθός.

Η ΑΝΕΠΙΦΥΛΑΚΤΗ ΕΜΠΙΣΤΟΣΥΝΗ ΤΟΥ ΧΡΗΣΤΗ στην προσωπική φύση της φορητής συσκευής.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

Θα πρέπει να σας βάλουν σε υποψίες ένα SMS ή μια τηλεφωνική κλήση από μια εταιρεία όπου σας ζητάνε προσωπικές πληροφορίες. Μπορείτε να επιβεβαιώσετε ότι το μήνυμα ή η κλήση είναι νόμιμα καλώντας απευθείας στην εταιρεία μέσω της επίσημης γραμμής επικοινωνίας της.

https://

Κατά την περιήγηση στο Διαδίκτυο από τη φορητή σας συσκευή, βεβαιωθείτε ότι η σύνδεση είναι ασφαλής (ένδειξη HTTPS). Μπορείτε πάντα να το ελέγχετε στην αρχή του URL.

Ποτέ μην κάνετε κλικ σε ένα σύνδεσμο ή ένα επισυναπτόμενο αρχείο που εμπεριέχονται σε μη ζητηθέν email ή SMS. Διαγράψτε το αμέσως.

^BE:%}
W@RY
*)Z#$=

Θα πρέπει να σας βάλει σε υποψίες ένας ιστότοπος που περιέχει ασύντακτες προτάσεις, ορθογραφικά λάθη ή χαμηλή ανάλυση.

Αν υπάρχει διαθέσιμη, εγκαταστήστε μια εφαρμογή ασφαλείας που θα σας προειδοποιεί εγκαίρως για οποιαδήποτε ύποπτη δραστηριότητα.

EUROPOL EC3 European Cybercrime Centre

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#MobileMalware

Κακόβουλο λογισμικό – Malware

Αποτελεί μείζον πρόβλημα για την ασφάλεια των Πληροφοριακών Συστημάτων. Το λογισμικό χαρακτηρίζεται ως κακόβουλο όταν βάσει των προθέσεων του προγραμματιστή το λογισμικό που προκύπτει διαθέτει τις απαιτούμενες εντολές προκειμένου να βλάψει ένα υπολογιστικό σύστημα.

MOBILE
RANSOMWARE

ΠΕΙΤΕ ΑΝΤΙΟ ΣΤΑ ΠΡΟΣΩΠΙΚΑ ΣΑΣ ΑΡΧΕΙΑ

Το ransomware κρατά ομήρους τη συσκευή σας και τα δεδομένα σας, απαιτώντας ανταλλάγματα. Αυτού του είδους το κακόβουλο λογισμικό κλειδώνει την οθόνη της συσκευής σας ή δε σας επιτρέπει να έχετε πρόσβαση σε αρχεία ή λειτουργίες.

ΠΩΣ ΔΙΑΔΙΔΕΤΑΙ;

Κατά την επίσκεψη σε μολυσμένους ή κακόβουλους ιστοτόπους.

Κατεβάζοντας απομιμήσεις νόμιμων εφαρμογών.

Κάνοντας κλικ σε συνδέσμους ή επισυναπτόμενα που εμπεριέχονται σε phishing emails.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Ίσως χρειαστεί να επαναφέρετε τη συσκευή στις εργοστασιακές της ρυθμίσεις, χάνοντας έτσι όλα τα δεδομένα σας.

Ένας επιτιθέμενος μπορεί να έχει πλήρη πρόσβαση στη συσκευή σας και να μοιραστεί τα δεδομένα σας με τρίτους.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

Δημιουργήστε σε τακτική βάση αντίγραφα ασφαλείας των δεδομένων σας και εγκαταστήστε όλες τις διαθέσιμες ενημερώσεις για το λειτουργικό σύστημα και τις εφαρμογές.

Αποφύγετε τις αγορές από καταστήματα εφαρμογών τρίτων.

Αν υπάρχει διαθέσιμη, εγκαταστήστε μια εφαρμογή ασφαλείας για φορητές συσκευές, που θα σας προειδοποιεί για κάθε περιστατικό ασφάλειας.

Προσέξτε τα emails και τους ιστοτόπους που φαίνονται ύποπτα ή υπερβολικά ωραία για να είναι αληθινά.

Μην παραχωρείτε σε κανέναν δικαιώματα διαχειριστή της συσκευής σας.

Μην πληρώσετε τα λύτρα. Χρηματοδοτείτε εγκληματίες και τους ενθαρρύνετε να συνεχίσουν τις έκνομες δραστηριότητές τους.

EUROPOL EC3 European Cybercrime Centre

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#MobileMalware

ΓΕΝΙΚΕΣ ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΗ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Συμβουλές για τους γονείς

- Δίνουμε το σωστό παράδειγμα με τη δική μας διαδικτυακή συμπεριφορά ακολουθώντας τους κανόνες ασφαλούς πλοήγησης. Οι ενήλικες λειτουργούν ως πρότυπα προς τα παιδιά.
- Συζητάμε με το παιδί για τη διαδικτυακή του ζωή και ενημερωνόμαστε για τα διαδικτυακά του ενδιαφέροντα, τους λογαριασμούς που διατηρεί σε μέσα κοινωνικής δικτύωσης, σε διαδικτυακά παιχνίδια και εφαρμογές. Αφιερώνουμε χρόνο στο να πλοηγηθούμε μαζί με το παιδί στο διαδίκτυο σε σελίδες και εφαρμογές ενδιαφέροντός του.
- Ελέγχουμε μαζί με το παιδί τις ρυθμίσεις ασφάλειας και απορρήτου των λογαριασμών του και βεβαιωνόμαστε ότι έχει ενεργοποιήσει την επιλογή διπλού ελέγχου ταυτότητας (two step verification), ενώ οι κωδικοί που χρησιμοποιεί είναι ασφαλείς (αποτελούνται από τουλάχιστον 8 σύμβολα, αριθμούς και γράμματα).
- Συζητάμε με τα παιδιά προκειμένου να συνειδητοποιήσουν ότι οι φίλοι τους σε κάποιο προφίλ θα πρέπει να είναι μόνο οι φίλοι τους και στην πραγματική ζωή. Σε καμία περίπτωση δε θα πρέπει να αποδέχονται άγνωστα άτομα, ούτε «φίλους φίλων».
- Συζητάμε με τα παιδιά για τους κινδύνους της έκθεσης των προσωπικών δεδομένων (ονοματεπώνυμα, διευθύνσεις κατοικίας, τηλεφωνικοί αριθμοί, σχολεία κ.λπ.), φωτογραφιών (άσεμνες και μη), ακόμα και e-mail στις εκάστοτε ιστοσελίδες, εφαρμογές και υπηρεσίες στο διαδίκτυο. Τονίζουμε ότι η ενδεχόμενη αποστολή φωτογραφιών σε γνωστό άτομο μια δεδομένη στιγμή μπορεί να έχει αρνητικές συνέπειες μελλοντικά.
- Καλό είναι να αποφεύγεται η είσοδος σε σελίδες, εφαρμογές ηλεκτρονικής συνδιάλεξης (chat) άγνωστες προς τα παιδιά στις οποίες δίνεται η δυνατότητα συνομιλίας με αγνώστους, καθώς και σ’ αυτές όπου γίνεται χρήση κάμερας.
- Καλό είναι να αποφεύγεται το άνοιγμα οποιουδήποτε συνδέσμου (link) αγνώστου προελεύσεως.

- Σε μικρές ηλικίες μπορούμε να υποστηρίξουμε τα παιδιά κατά την αυτονόμησή τους στο διαδίκτυο, εγκαθιστώντας εφαρμογή γονικού ελέγχου, που μπορεί να βοηθήσει τα παιδιά να πλοηγηθούν με ασφάλεια στο διαδίκτυο και τους γονείς να ελέγξουν το περιεχόμενο των ιστοσελίδων που επισκέπτονται.
- Θυμόμαστε ότι σε μεγαλύτερες ηλικίες η επικοινωνία βασίζεται στην εμπιστοσύνη.
- Αν αντιληφθούμε οποιοδήποτε πρόβλημα παραμένουμε ψύχραιμοι, ακούμε όλη την ιστορία χωρίς να διακόψουμε το παιδί, διαφυλάσσουμε τα όποια αποδεικτικά στοιχεία (screen shot φωτογραφιών/μηνυμάτων), αναφέρουμε το περιστατικό στις αρχές και ζητάμε τη βοήθεια των ειδικών.

Συμβουλές για παιδιά

- Τήρησε στο διαδίκτυο τους κανόνες που τηρείς και στην πραγματική ζωή.
- Συζήτησε με τους γονείς σου για τη διαδικτυακή σου ζωή, όπως κάνεις και για την πραγματική και πλοηγήσου μαζί τους στο διαδίκτυο προκειμένου να τους δείξεις τα ενδιαφέροντά σου.
- Βεβαιώσου για την ασφάλεια των λογαριασμών που διατηρείς στα μέσα κοινωνικής δικτύωσης, στα διαδικτυακά παιχνίδια και στις εφαρμογές, ελέγχοντας σχολαστικά τις ρυθμίσεις ασφάλειας αυτών και χρησιμοποιώντας σύνθετο κωδικό πρόσβασης και τη δυνατότητα διπλού ελέγχου ταυτότητας (two step verification).
- Αν έχεις λογαριασμό σε κάποια ιστοσελίδα κοινωνικής δικτύωσης, απόφυγε την ανάρτηση προσωπικών στοιχείων (ονοματεπώνυμο, διεύθυνση, τηλέφωνο, σχολείο), καθώς και δικών σου φωτογραφιών ή των συμμαθητών σου.
- Ρύθμισε τους λογαριασμούς σου προκειμένου να είναι ιδιωτικοί και μην αποδέχεσαι αιτήματα φιλίας από αγνώστους, ούτε από «φίλους φίλων». Θυμήσου ότι και στους ιδιωτικούς λογαριασμούς δεν υπάρχει απόλυτη ασφάλεια καθώς υπάρχει πάντα η πιθανότητα να παραβιαστεί τόσο ο λογαριασμός σου, όσο και κάποιου φίλου σου και να εκτεθεί και το υλικό που εσύ έχεις ανεβάσει.

- Μην αποστέλλεις προσωπικές φωτογραφίες ακόμα και σε γνωστά σου άτομα.
- Απόφυγε ιστοσελίδες στις οποίες μπορείς να συνομιλήσεις με αγνώστους ή δεν εμφανίζεται το username τους ή απαιτείται χρήση κάμερας.
- Παίξε διαδικτυακά παιχνίδια με όρια και κανόνες, αποφεύγοντας τη συνομιλία με άγνωστους χρήστες.
- Μην ανοίγεις ποτέ την κάμερα για να συνομιλήσεις διαδικτυακά με αγνώστους.
- Οι κακόβουλοι χρήστες που προσεγγίζουν ανηλίκους διαδικτυακά είναι αρχικά πάντα διαθέσιμοι, υποστηρικτικοί και γνωρίζουν τα ενδιαφέροντά σου προκειμένου να σε προσεγγίσουν. Στόχος τους είναι να δώσουν την αίσθηση ότι «μπορείς να τους χειριστείς».
- Αν κάποιος χρήστης σε κάνει να αισθάνεσαι άβολα σε μια διαδικτυακή συνομιλία ή σου ζητήσει να βγάλεις φωτογραφία που να δείχνει το σώμα σου και να τη στείλεις, μην το κάνεις σε καμία περίπτωση και ειδοποίησε αμέσως έναν ενήλικο που εμπιστεύεσαι.
- Μην ανοίγεις μηνύματα/e-mail και κυρίως συνδέσμους (link), που υπάρχουν σ' αυτά, ακόμη κι αν σου τα έχει στείλει κάποιος φίλος ή φίλη σου.
- Θυμήσου: αν σου συμβεί κάτι που σε φέρνει σε δύσκολη θέση στο διαδίκτυο πρέπει να το πεις και όχι να το υποστείς. Συζήτησέ το με κάποιον ενήλικο που εμπιστεύεσαι, δείχνοντας θάρρος και αποθήκευσε τα όποια αποδεικτικά στοιχεία έχεις στη διάθεσή σου (screen shot φωτογραφιών/μηνυμάτων).

Ποια είναι, όμως, η ορθή χρήση του Διαδικτύου;

- Μη διακόπτετε τη χρήση, αλλά μάθετε να θέτετε όρια, και αρχίστε και πάλι την ενασχόληση με άλλες δραστηριότητες μακριά από τον υπολογιστή. Μια μέρα εκτός Διαδικτύου μπορεί να σας φανεί πιο ενδιαφέρουσα και πιο διασκεδαστική. Μιάμιση ώρα τη μέρα στο διαδίκτυο θεωρείται αρκετή για τη διαδικτυακή ενημέρωση και ψυχαγωγία του χρήστη. Μην ξεχνάτε ότι το χρόνο που περνάτε μπροστά στον υπολογιστή, συνήθως τον στερείτε από κάποιον αγαπημένο σας.
- Ο ρόλος των γονέων είναι πάρα πολύ σημαντικός τόσο για την πρόληψη, όσο και για την αντιμετώπιση του εθισμού των παιδιών τους στο Διαδίκτυο. Όσον αφορά την πρόληψη, το σημαντικότερο πράγμα που χρειάζεται να κάνουν οι

γονείς προκειμένου να μπορούν να ελέγχουν αποτελεσματικά τη χρήση του Διαδικτύου από τα παιδιά τους, είναι να γνωρίσουν οι ίδιοι το μέσο.

ΚΑΙΝΟΤΟΜΕΣ ΔΡΑΣΕΙΣ

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, εκτός από την καταστολή του Ηλεκτρονικού Εγκλήματος, δίνει ιδιαίτερη έμφαση και στην πρόληψή του. Στο πλαίσιο αυτό έχει αναπτύξει ένα σύνολο καινοτόμων δράσεων με στόχο την ενημέρωση και ευαισθητοποίηση των πολιτών, του εμπορικού κόσμου, των εταιριών καθώς και των δημόσιων και ακαδημαϊκών οργανισμών σε θέματα που αφορούν την ασφαλή πλοήγηση στο Διαδίκτυο, τους κινδύνους που ελλοχεύουν σε αυτό, καθώς και τους τρόπους προστασίας.

Συνοπτικά, οι καινοτόμες δράσεις που έχουν υλοποιηθεί από την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος είναι οι ακόλουθες:

- **Ημερίδες Ασφαλούς Πλοήγησης:** Το Αρχηγείο της Ελληνικής Αστυνομίας, μέσω της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, διοργανώνει ημερίδες σε όλη την Ελληνική Επικράτεια, έχοντας ως στόχο την ενημέρωση των πολιτών και ιδιαίτερα των μαθητών, των γονέων και των εκπαιδευτικών, για τα φαινόμενα διαδικτυακής βίας, τους κινδύνους που ελλοχεύουν στις ιστοσελίδες κοινωνικής δικτύωσης και γενικά την πρόληψη και την αντιμετώπιση των κινδύνων που σχετίζονται με τις νέες τεχνολογίες.
- **Τηλεδιασκέψεις:** Πραγματοποιούνται, ενημερώσεις ανά την επικράτεια, μέσω της υιοθέτησης της τεχνολογίας των τηλεδιασκέψεων. Η τηλεδιάσκεψη γίνεται σε πραγματικό χρόνο και επιτρέπει να πραγματοποιηθεί παρουσίαση, συνομιλία, ερωτήσεις και απαντήσεις μεταξύ ομιλητών και ακροατών που βρίσκονται σε απόσταση.
- **Εκπαιδευτικές Επισκέψεις:** Καθημερινά η ΔΙ.Δ.Η.Ε και η Υ.Δ.Η.Ε.Β.Ε γίνονται αποδέκτες πολλών αιτημάτων σχολείων και διάφορων φορέων που θέλουν να επισκεφτούν τις εγκαταστάσεις της και να ενημερωθούν για θέματα που αφορούν την ασφάλεια στο διαδίκτυο.

Κατά τη σχολική χρονιά 2020-2021 πραγματοποιήθηκαν συνολικά 126 ενημερωτικές ημερίδες σε όλη την Επικράτεια διαδικτυακά ή δια ζώσης, ενώ τη σχολική χρονιά 2021-2022 έχουν ήδη πραγματοποιηθεί συνολικά 238 ενημερωτικές ημερίδες και αναμένεται να ξεπεράσουν τις 270.

Τις ενημερώσεις παρακολούθησαν μαθητές, σπουδαστές, φοιτητές, γονείς, εκπαιδευτικοί, δικαστικοί λειτουργοί και πολίτες που επιθυμούσαν να ενημερωθούν για τους κινδύνους και τις απειλές του διαδικτύου αλλά και τις σύγχρονες μορφές κυβερνο-εγκλήματος και την προσαρμογή στα νέα δεδομένα.

Επιπλέον, η ΔΙ.Δ.Η.Ε. σε συνεργασία με το Υπουργείο Παιδείας και Θρησκευμάτων, ενημέρωσε παιδιά, εκπαιδευτικούς αλλά και γονείς, μέσω του Πανελλήνιου Σχολικού Δικτύου (my-school) την Παγκόσμια Ημέρα Ασφαλούς Πλοήγησης στο Διαδίκτυο (08-02-2022), κατά την οποία πραγματοποιήθηκαν 3 εκδηλώσεις με συμμετοχή περισσότερων από 1.500 σχολικών μονάδων και 80.000 μαθητών.

- **Τηλεοπτικά και ραδιοφωνικά «σποτ»:** Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος προχώρησε στην παραγωγή και προβολή μέσω ραδιοφωνικών και τηλεοπτικών σταθμών πανελλαδικής εμβέλειας, τηλεοπτικών και ραδιοφωνικών «σποτ» στο πλαίσιο της εκστρατείας πληροφόρησης ευαίσθητων κοινωνικών ομάδων για την προστασία τους από τις παγίδες του διαδικτύου.

- **Παραμύθι με τίτλο «ο Σίφης ο Ποντικός & το Διαδίκτυο»** το οποίο συνέγραψε η κ. Κάρμεν Ρουγγέρη σε συνεργασία με την Υπηρεσία μας. Στόχος του βιβλίου είναι να αποδώσει με εύσχημο και βιωματικό τρόπο τα περιστατικά που χειριζόμαστε καθημερινά και να βοηθήσει τα παιδιά να κατανοήσουν τους κινδύνους του διαδικτύου. Επιπλέον, δημιουργήθηκε οπτικοακουστικό υλικό με την αφήγηση του παραμυθιού από τη συγγραφέα του και την κα. Κουλουμπή το οποίο αναρτήθηκε στην ιστοσελίδα www.cyberkid.gr. Το μήνα Ιούλιο απεστάλησαν αντίγραφα του βιβλίου σε όλες τις παιδικές βιβλιοθήκες της Χώρας προκειμένου να προστεθούν στη συλλογή τους ενθαρρύνοντας τα παιδιά να διαβάσουν σε ένα κατάλληλα διαμορφωμένο χώρο.

Το παραμύθι είναι διαθέσιμο στον παρακάτω υπερσύνδεσμο:

https://www.cyberkid.gov.gr/wp-content/uploads/2021/02/O_SIFIS_KAI_O_PONTIKOS_2020.02.01_compressed.pdf

- **Συγγραφή και διαμοιρασμός ενημερωτικών φυλλαδίων:** Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος έχει προβεί στην έκδοση ενημερωτικών φυλλαδίων με δέκα (10) διαφορετικές θεματικές ενότητες για την παροχή συμβουλών για ασφαλέστερη πλοήγηση στο Διαδίκτυο. Επίσης από την Υπηρεσία μας δημιουργήθηκαν Φιλικές Συμβάσεις Γονιού-Παιδιού ανά ηλικιακή ομάδα αναφορικά με τη χρήση διαδικτύου και κινητού τηλεφώνου.
- **Από την Υπηρεσία μας αναπτύχθηκε εκπαιδευτικό υλικό σε συνεργασία με την εταιρεία "PLAYMOBIL HELLAS",** με θέμα την ασφαλή πλοήγηση των παιδιών στο διαδίκτυο. Στο πλαίσιο αυτό δημιουργήθηκε επιδαπέδιο παιχνίδι, βιβλίο δραστηριοτήτων και συνοδευτικό προωθητικό υλικό για την ευαισθητοποίηση των παιδιών μέσα από διαδραστικές και βιωματικές δραστηριότητες. Το σύνολο του υλικού αυτό ολοκληρώθηκε και παρουσιάστηκε στη Διεθνή Έκθεση Θεσσαλονίκης στο περίπτερο της Ελληνικής Αστυνομίας.
- **Συμμετοχή στο Πληροφοριακό Κέντρο της ΕΛ.ΑΣ. στη ΔΕΘ:** Περισσότεροι από 100.000 πολίτες επισκέφθηκαν το περίπτερο της Ελληνικής Αστυνομίας τα τελευταία χρόνια και ενημερώθηκαν σχετικά με την ασφαλή διαδικτυακή πλοήγηση, με αποτέλεσμα το περίπτερο να αποτελέσει σημαντικό πόλο έλξης.
- **Ιστότοπος cyberkid.gr και εφαρμογή Cyberkid:** Στο www.cyberkid.gr παρέχονται χρήσιμες πληροφορίες και συμβουλές σχετικά με το πως μπορεί να εκμεταλλευτεί όλη η οικογένεια τα θετικά των σύγχρονων τεχνολογιών που μας περιβάλλουν και φυσικά του διαδικτύου. Στο πλαίσιο της συνεχούς ενημέρωσης και ανάπτυξης του ιστότοπου www.cyberkid.gr δημιουργήθηκε η ενότητα «Ψηφιακή Αλάνα», όπου τα παιδιά μπορούν να παίζουν τα αγαπημένα τους ηλεκτρονικά παιχνίδια με απόλυτη προστασία από τους κινδύνους που παραμονεύουν στο διαδίκτυο.

Η εφαρμογή Cyberkid για κινητά δημιουργήθηκε με σκοπό να ενημερώνει καθημερινά τους γονείς και τα παιδιά κάθε οικογένειας για την ασφαλή πλοήγηση στο διαδίκτυο και τους κινδύνους που ελλοχεύουν σε αυτό. Παράλληλα, είναι μία διαδραστική εφαρμογή, η οποία δίνει την δυνατότητα άμεσης επικοινωνίας με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος μέσω της γραμμής CYBER ALERT αλλά και μέσω αποστολής άμεσου μηνύματος e-mail, με τη χρήση ενός κουμπιού, ενώ υπάρχει η δυνατότητα ψυχαγωγίας μέσω των διαφόρων παιχνιδιών.

- Ιστότοπος Cyberalert.gr – Feelsafe και εφαρμογή Feelsafe: Με την αυξανόμενη χρήση του διαδικτύου στις καθημερινές αγορές και τις εμπορικές συναλλαγές, κρίνεται επιβεβλημένη η διεύρυνση της ενημέρωσης ασφαλούς χρήσης του διαδικτύου και η περαιτέρω ενημέρωση μεταξύ άλλων και του εμπορικού κόσμου. Στο πλαίσιο αυτό, το Υπουργείο Εσωτερικών (πρώην Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης) σε συνεργασία με την Ελληνική Αστυνομία και τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος και η Ελληνική Συνομοσπονδία Εμπορίου και Επιχειρηματικότητας (Ε.Σ.Ε.Ε.), προχώρησαν στην υλοποίηση πλατφόρμας καινοτόμων δράσεων με την ονομασία «FeelSafe».

Στόχος είναι η από κοινού συστηματική και επιστημονική μελέτη των θεμάτων και προβλημάτων που προκύπτουν για το εμπόριο και τους καταναλωτές από τις ηλεκτρονικές συναλλαγές, με σκοπό την ενημέρωση εμπόρων και καταναλωτών για τους διαδικτυακούς κινδύνους και την ασφαλή χρήση του διαδικτύου στις εμπορικές συναλλαγές και τις διαδικτυακές αγορές.

Στο πλαίσιο αυτό, υλοποιήθηκε η ιστοσελίδα http://cyberalert.gr/feelsafe/ αλλά και η πρωτοποριακή εφαρμογή (application) "FeelSafe", οι οποίες αποτελούν βασικό βήμα ενημέρωσης των καταναλωτών αλλά και των μελών της Ε.Σ.Ε.Ε., μιας και το μεγαλύτερο μέρος των χρηστών, χρησιμοποιεί «έξυπνα» κινητά στην καθημερινότητά του.

Στην πλατφόρμα αυτή παρουσιάζονται με άμεσο τρόπο οδηγίες για την αποφυγή ηλεκτρονικών απατών ανά κατηγορία. Ο συνδυασμός αυτών των πληροφοριών με online γραμμή καταγγελιών (SOS) και η καθημερινή ενημέρωση από εξειδικευμένους αξιωματικούς της ΔΙ.Δ.Η.Ε. για τις τρέχουσες παγίδες – απάτες κρίνεται ως καθοριστική στην έγκυρη και έγκαιρη ενημέρωση των πολιτών.

- Παρουσία στα Μέσα Κοινωνικής Δικτύωσης (Facebook, Twitter, Instagram και YouTube): Η Σελίδα του Cyberkid στο Facebook δημιουργήθηκε τον Μάιο του 2014 με σκοπό να ενισχύσει την προβολή της ιστοσελίδας www.cyberkid.gr στα μέσα κοινωνικής δικτύωσης. Τον Απρίλιο του 2015 ξεκίνησε η λειτουργία του λογαριασμού Twitter «@CyberAlertGR» που έχει ως στόχο την άμεση και σε πραγματικό χρόνο (real time) ενημέρωση των πολιτών για τους κινδύνους που ανακύπτουν καθημερινά στο διαδίκτυο, ενώ ταυτόχρονα και οι ίδιοι θα μπορούν να ενημερώσουν τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος σε περίπτωση κινδύνου ή απειλής στο διαδίκτυο. Ενώ τον Αύγουστο 2015 δημιουργήθηκε αντίστοιχη σελίδα και στο Facebook «CYBER ALERT». Επίσης η Υπηρεσία μας διαθέτει στο YouTube το κανάλι CYBER ALERT και τον Φεβρουάριο του 2018 δημιουργήθηκε ο λογαριασμός Instagram "cyberalert.gr".

Στους παρακάτω υπερσυνδέσμους μπορείτε να βρείτε παρουσιάσεις που έχουν δημιουργηθεί από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος ανάλογα με το ακροατήριο:

1. Παρουσίαση Πρωτοβάθμιας:

   https://prezi.com/view/MN1PTUEGA1IXdxDQYrJu/

2. Παρουσίαση Δευτεροβάθμιας:

   https://prezi.com/view/A12ohUF1fRC20N2Q5Erq/

3. Παρουσίαση για ενήλικες:

   https://prezi.com/view/t7dLw7pTs3ofAHYc5r7Y/

Οι παρουσιάσεις της ΔΙ.Δ.Η.Ε. αναδιαμορφώνονται ανάλογα και με την επικαιρότητα αναφορικά με το διαδικτυακό έγκλημα.

Επικοινωνία με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

Πενταψήφιο τηλεφωνικό αριθμό 11188,

ccu@cybercrimeunit.gov.gr

www.facebook.com/cyberkid.gov.gr

www.facebook.com/CyberAlertGR

www.instagram.com/cyberalert.gr

https://www.youtube.com/channel/UCSECtiscTH8tkxzBzX8gVcQ

twitter.com@cyberalertgr

www.cyberalert.gr/feelsafe/

www.cyberkid.gr

μέσω των εφαρμογών CyberKid και FeelSafe.