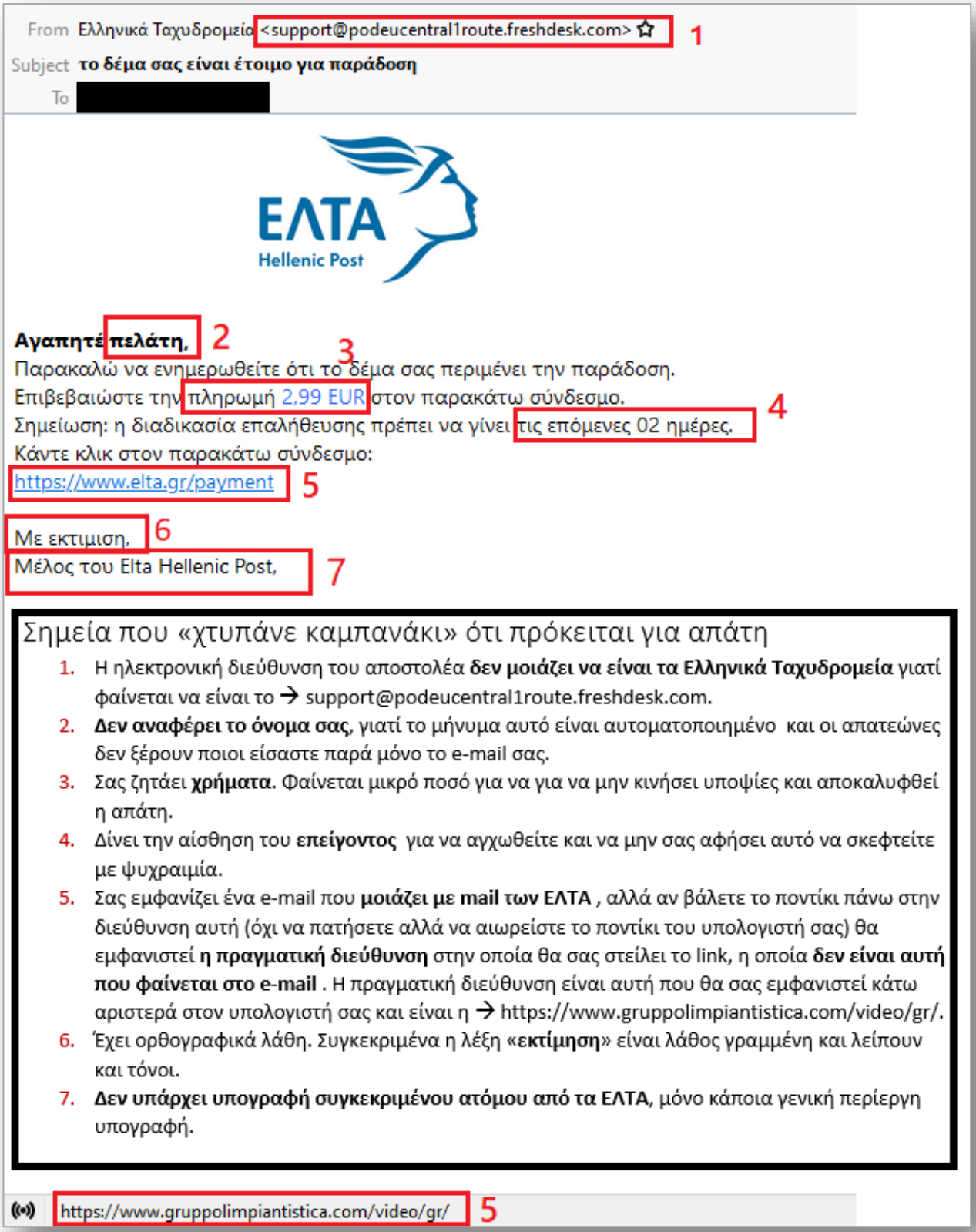
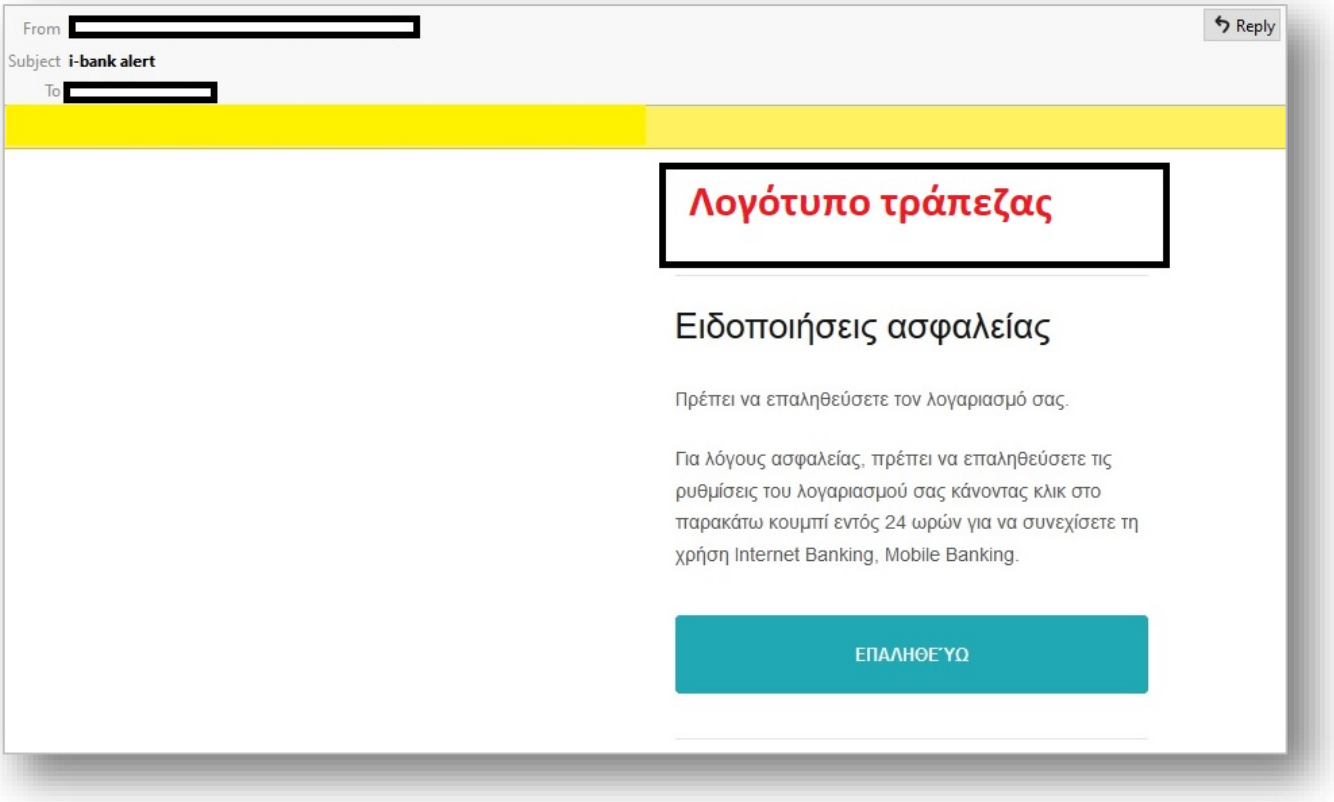
Την προσοχή των χρηστών εφιστά το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου του Ιδρύματος Τεχνολογίας και Έρευνας σε σχέση με τις διαδικτυακές απάτες οι οποίες λόγω της κατάστασης που έχει διαμορφωθεί και της υπερχρήσης που παρατηρείται έχουν αυξηθεί αισθητά από την αρχή της πανδημίας. Η γραμμή καταγγελιών για το παράνομο περιεχόμενο στο διαδίκτυο SafeLine.gr έχει δεχτεί από το Μάρτιο του 2020 έως σήμερα μεγάλο αριθμό αναφορών που αφορούν σε οικονομικές απάτες σε εξ' αποστάσεως συναλλαγές και ηλεκτρονικές αγορές.

Απάτες μέσω ηλεκτρονικού ταχυδρομείου (phishing)

Τον τελευταίο καιρό μάλιστα έχουν πληθήνει οι καταγγελίες για επιθέσεις ηλεκτρονικού ψαρέματος (phishing) προκειμένου επιτήδειοι να αποσπάσουν προσωπικά στοιχεία. Το «ηλεκτρονικό ψάρεμα» γίνεται κυρίως μέσω ηλεκτρονικού ταχυδρομείου, διαφημίσεων ή από ιστότοπους που έχουν παρόμοια εμφάνιση με ιστότοπους που τα θύματα χρησιμοποιούν ήδη (Εικόνα 1). Για παράδειγμα, τα θύματα λαμβάνουν μήνυμα ηλεκτρονικού ταχυδρομείου που μοιάζει να έχει σταλεί από την τράπεζά τους (Εικόνα 2) το οποίο τους ζητά να επιβεβαιώσουν τον αριθμό του τραπεζικού τους λογαριασμού. Πληροφορίες που μπορεί να ζητηθούν είναι τα ονόματα χρηστών και κωδικοί πρόσβασης, αριθμοί κοινωνικής ασφάλισης, αριθμοί τραπεζικών λογαριασμών, αριθμοί πιστωτικών καρτών, ημερομηνία γέννησης κ.α.



Εικόνα 1 Παράδειγμα απάτης με ΕΛΤΑ



Εικόνα 2 Παράδειγμα απάτης με Τράπεζα

Απάτες με spam μηνύματα εκβιαστικού περιεχομένου

Επιπρόσθετα, συχνές είναι οι καταγγελίες για περιστατικά spam μηνυμάτων εκβιαστικού περιεχομένου (Εικόνα 3) , που αποστέλλονται μαζικά σε διάφορους αποδέκτες με σκοπό την εξαπάτησή τους. Ειδικότερα, επιτήδειοι στέλνουν μαζικά μηνύματα σε αποδέκτες και τους ενημερώνουν ότι διαθέτουν πρόσβαση στη συσκευή τους ενώ κάποιες φορές το μήνυμα φαίνεται ψευδώς να έχει αποσταλεί από τον ίδιο προσωπικό λογαριασμό του παραλήπτη.

Παράλληλα τους γνωστοποιούν ότι δήθεν έχει εγκατασταθεί κακόβουλο λογισμικό, μετά από την επίσκεψή τους σε κάποιον ιστότοπο, το οποίο έχει ενεργοποιήσει την κάμερα και τους έχει καταγράψει σε προσωπικές στιγμές. Στη συνέχεια αναφέρεται ότι το κακόβουλο λογισμικό έχει συλλέξει όλες τις επαφές των χρηστών από τα μέσα κοινωνικής δικτύωσης και οι δράστες απειλούν με την αποστολή του επίμαχου υλικού στις επαφές τους, σε περίπτωση που δεν λάβουν bitcoins.

Σημειώνεται ότι στα εκβιαστικά αυτά μηνύματα ηλεκτρονικού ταχυδρομείου κάποιες φορές γίνεται και αναφορά σε πραγματικούς κωδικούς (ή και παλαιότερους κωδικούς) ώστε οι χρήστες να πεισθούν για το αληθές της απειλής (δείτε περισσότερα για την απάτη αυτή εδώ https://saferinternet4kids.gr/nea/mail-scam/.

Γειά σου!
Είμαι χάκερ και εισέβαλα επιτυχώς στο λειτουργικό σας σύστημα. Πρέπει να αποδεχτείτε αυτό το γεγονός και να το λάβετε στα σοβαρά.
Έχω πλήρη πρόσβαση στους λογαριασμούς σας.
Σε παρατήρησα κρυφά για αρκετούς μήνες.
Έχω αντιγράψει τον τηλεφωνικό σας κατάλογο, εξέτασα τη διαδικτυακή σας συμπεριφορά, τα κείμενα.
Το γεγονός είναι ότι, λόγω ενός ιστότοπου για ενήλικες που επισκεφτήκατε, το μηχάνημά σας έχει μολυνθεί από κακόβουλο λογισμικό. Από αυτό έχω αποκτήσει πρόσβαση σε πιο σημαντικά μέρη της ζωής σας (και όπως γνωρίζετε όλα αποθηκεύονται σε ψηφιακή μορφή αυτές τις μέρες).
Μπορεί να μην καταλαβαίνετε τι σημαίνει αυτό, επιτρέψτε μου να σας το εξηγήσω.
Ο ιός Trojan horse μου επιτρέπει να αποκτήσω πλήρη πρόσβαση σε έναν υπολογιστή και σε άλλες συσκευές.
Αυτό σημαίνει ότι μπορώ να δω τα πάντα στην οθόνη σας και να ενεργοποιήσω την κάμερα και το μικρόφωνό σας χωρίς να το γνωρίζετε, μεταξύ άλλων, όπως η αντιγραφή αρχείων και φωτογραφιών.
Μπορώ ακόμα να δω όλα τα στοιχεία επικοινωνίας σας και όλα τα email σας.
Γιατί δεν εντοπίζει το λογισμικό προστασίας από ιούς αυτό το κακόβουλο λογισμικό;
Απάντηση: Χρησιμοποιώ κακόβουλο λογισμικό που βασίζεται σε προγράμματα οδήγησης. Ενημερώνω την υπογραφή του κάθε τέσσερις ώρες, οπότε το λογισμικό προστασίας από ιούς δεν μπορεί να εντοπίσει την παρουσία του. Είμαι επαγγελματίας.
Έφτιαξα ένα βίντεο, το αριστερό μισό αυτού του βίντεο δείχνει ότι ευχαριστείς τη δική σου σκηνή και το δεξί μισό δείχνει το βίντεο που παρακολουθούσες.
Με ένα κλικ του ποντικιού, μπορώ να στείλω αυτό το βίντεο σε όλες τις διευθύνσεις email με τις οποίες έχετε επαφές και σε όλες τις επαφές στα κοινωνικά σας δίκτυα, στο τηλέφωνό σας. Είμαι βέβαιος ότι δεν θέλετε να το δει κανείς.
Μπορώ επίσης να δημοσιεύσω όλα τα email σας και το ιστορικό συνομιλιών στο λογισμικό συνομιλίας που χρησιμοποιείτε.
Εάν δεν θέλετε να συμβεί αυτό, μεταφέρετε bitcoin αξίας 700 ευρώ στον λογαριασμό μου bitcoin (εάν δεν ξέρετε πώς να το κάνετε, απλώς αναζητήστε στο Google: "αγορά bitcoin").
Οι πληροφορίες λογαριασμού bitcoin μου (πορτοφόλι bitcoin, BTC) είναι:
[redacted]
Είναι μόνο ένα μικρό ποσό 700 ευρώ μόνο (περίπου 785 δολάρια USD). Δεν συγκρίνεται πολύ με αυτό που έχω.
Αφού λάβω τα χρήματα, θα διαγράψω όλες τις πληροφορίες για εσάς, θα διαγράψω αμέσως το trojan horse και το βίντεο και θα εξαφανιστούν για πάντα από τη ζωή σας.
Δεν θέλω να καταστρέψω τη ζωή σας, αλλά η ζωή μας εδώ έγινε πολύ δύσκολη. Δεν θα έχω άλλη επιλογή αν δεν παραπονεθείτε.
Ολοκληρώστε την πληρωμή εντός 60 ωρών (σας δίνω περισσότερες από 2 ημέρες για να μου μεταφέρετε 700 ευρώ σε Bitcoin). Αφού δείτε αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου, θα λάβω αμέσως μια υπενθύμιση και θα ξεκινήσει η αντίστροφη μέτρηση των 60 ωρών.
Η εύρεση κάποιου παραπονούμενου είναι εντελώς άσκοπη, γιατί όπως και ο λογαριασμός μου στο Bitcoin, αυτό το email δεν μπορεί να παρακολουθείται. Πρέπει να αποδεχτείτε το γεγονός ότι δεν υπάρχει άλλη επιλογή.
Είμαι πολύ προσεκτικός και δεν κάνω ποτέ λάθη.
Εάν διαπιστώσω ότι έχετε μοιραστεί αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου με άλλους, τότε θα το δημοσιεύσω αμέσως.
Καλή τύχη! Και να είστε σε καλή υγεία!

Εικόνα 3 Παράδειγμα απάτης εκβιαστικού περιεχομένου

Emails με κακόβουλο λογισμικό

Καταγγελίες στην ανοιχτή γραμμή για το παράνομο περιεχόμενο στο διαδίκτυο SafeLine.gr αναφέρονται και σε λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου (emails) που εμπεριέχουν αρχεία κακόβουλου λογισμικού (malware).

Ειδικότερα, το θύμα λαμβάνει μήνυμα από άγνωστη διεύθυνση ηλεκτρονικού ταχυδρομείου, στο οποίο:

- το εμφανιζόμενο όνομα αποστολέα είναι υπαρκτό και ανήκει στη λίστα επαφών του,
- το περιεχόμενο του μηνύματος αποτελεί απόσπασμα προγενέστερης συνομιλίας μεταξύ του εμφανιζόμενου αποστολέα και άλλης επαφής (ή και του ίδιου του θύματος),
- περιέχει σύνδεσμο ή έχει επισυναφθεί αρχείο, το οποίο εμπεριέχει (συγκεκαλυμμένο) κακόβουλο εκτελέσιμο κώδικα.

Συμβουλές για προστασία από διαδικτυακές απάτες

- Να παρατηρείτε πάντα τη διεύθυνση του αποστολέα ενός μηνύματος ηλεκτρονικού ταχυδρομείου και ιδιαίτερα τις διαφορές στο εμφανιζόμενο όνομα και το email του αποστολέα.
- Να μην απαντάτε ποτέ σε ύποπτα email. Καμία υπηρεσία π.χ. τράπεζα **δε** θα ζητήσει διαδικτυακή ενημέρωση για προσωπικά δεδομένα.
- Να δημιουργείτε αντίγραφα ασφαλείας των αρχείων (backup) σε τακτά χρονικά διαστήματα, σε εξωτερικό μέσο αποθήκευσης έτσι ώστε να είναι δυνατή η αποκατάστασή τους.
- Σε περίπτωση όπου λάβετε μήνυμα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς ή άγνωστη προέλευση, να μην ανοίγετε τους συνδέσμους (links) και να μην κατεβάζετε συνημμένα αρχεία που περιέχονται στα μηνύματα αυτά.
- Να χρησιμοποιείτε λογισμικά προγράμματα, ενημερωμένα στην τελευταία τους έκδοση, ενώ θα πρέπει να υπάρχει πάντα ενημερωμένο πρόγραμμα προστασίας από κακόβουλο λογισμικό του ηλεκτρονικού υπολογιστή.
- Να πραγματοποιείτε αγορές από αξιόπιστα και γνωστά ηλεκτρονικά καταστήματα. Σημαντική ένδειξη αξιοπιστίας είναι η μακρόχρονη λειτουργία των καταστημάτων στην αγορά και η ύπαρξη φυσικής έδρας.
- Να ελέγχετε τις βασικές πληροφορίες που παρέχονται για το ηλεκτρονικό κατάστημα από τον ιστότοπό του. Να αναζητάτε, ειδικότερα, την επωνυμία της εταιρείας και τα πλήρη στοιχεία επικοινωνίας, συμπεριλαμβανομένης ταχυδρομικής διεύθυνσης. Η ύπαρξη μόνο ηλεκτρονικής διεύθυνσης (e-mail) και κινητού τηλεφώνου δεν αρκεί και αποτελεί, μάλιστα, ένδειξη απάτης.
- Να ελέγχετε, πριν από την πληρωμή ότι ο ιστότοπος παρέχει ασφαλή σύνδεση για τη μετάδοση ευαίσθητων δεδομένων, όπως στοιχείων πιστωτικών καρτών. Να βεβαιώνεστε ότι το σύμβολο ασφαλούς μετάδοσης δεδομένων εμφανίζεται στο πεδίο «διεύθυνση του προγράμματος περιήγησης» – browser με τη μορφή HTTPS.
- Να αναζητάτε και να διαβάζετε σχόλια, εμπειρίες ή συστάσεις άλλων καταναλωτών που έχουν ήδη αγοράσει από το κατάστημα.
- Να μην πείθεστε από υπερβολικά δελεαστικές τιμές των προϊόντων σε σχέση με τον ανταγωνισμό.

Romance scams

Ιδιαίτερη προσοχή εφιστάται στους χρήστες και για οργανωμένα κυκλώματα εγκληματιών που προκειμένου να αποσπάσουν χρήματα από τα θύματά τους **εκμεταλλεύονται τη μοναξιά και την ανάγκη επικοινωνίας** κατά τη διάρκεια του lockdown (romance scam). Η SafeLine.gr έχει δεχτεί καταγγελίες που αφορούν σε τέτοιου είδους οικονομικής εξαπάτησης. Επιτήδειοι εμφανιζόμενοι **κυρίως ως Αμερικάνοι στρατιωτικοί γιατροί** οι οποίοι υπηρετούν στο Αφγανιστάν ή τη Συρία, πείθουν τα θύματα τους να τους στείλουν χρήματα αναπτύσσοντας μια φιλία ή ένα ειδύλλιο. Αναζητούν μέσω κοινωνικών δικτύων ή ιστοσελίδων γνωριμιών για πιθανά θύματα, περνώντας εβδομάδες ή μήνες για να δημιουργήσουν μια σχέση. Για να ισχυροποιήσουν τις ψεύτικες ιστορίες τους, συχνά παίρνουν φωτογραφίες και ονόματα πραγματικών στρατιωτών που συλλέγουν από ιστότοπους στο διαδίκτυο. Αυτές οι απάτες αναφέρονται ως **romance scams.**

Συμβουλές για προστασία από romance scams

Πριν στείλετε χρήματα, ελέγξτε αν αναγνωρίζετε κάποια από τα προειδοποιητικά σημάδια, διότι ενδέχεται να είστε πιθανό θύμα απάτης:

- Δεν έχετε γνωρίσει ποτέ τον φίλο/φίλη σας και όλη η επικοινωνία σας ήταν αυστηρά διαδικτυακή.
- Το άτομο ισχυρίζεται ότι υπέστη σοβαρό τραυματισμό και χρειάζεται βοήθεια για να επιστρέψει στην πατρίδα του ή ισχυρίζεται ότι χρειάζεται χρήματα για να ταξιδέψει στο σπίτι του για να επισκεφθεί έναν άρρωστο συγγενή.
- Το άτομο ισχυρίζεται ότι θέλει να σας επισκεφτεί κατά τη διάρκεια της άδειας του, αλλά χρειάζεται να στείλετε χρήματα για να αγοράσει αεροπορικά εισιτήρια.
- Το άτομο ισχυρίζεται ότι χρειάζεται τη βοήθειά σας για να πληρώσει το «τέλος εξόδου» από το Αφγανιστάν/Συρία.
- Το άτομο ισχυρίζεται ότι γεννήθηκε και μεγάλωσε στις Ηνωμένες Πολιτείες, αλλά χρησιμοποιεί κακή γραμματική και ορθογραφία.
- Το άτομο ισχυρίζεται ότι βρίσκεται στο Αφγανιστάν, αλλά σας ζητά να στείλετε χρήματα σε λογαριασμό τρίτης χώρας, όπως η Νιγηρία.

Εάν πιστεύετε ότι είστε θύμα διαδικτυακής απάτης:

- Μη στείλετε χρήματα.
- Διακόψτε κάθε επικοινωνία. Μην επιχειρήσετε να επιλύσετε την κατάσταση μόνοι σας. Εάν αισθάνεστε απειλή, επικοινωνήστε αμέσως με την αστυνομία. Μην επιχειρήσετε να ανακτήσετε προσωπικά τα χαμένα χρήματα.
- Κάντε άμεσα αναφορά στη Δίωξη Ηλεκτρονικού Εγκλήματος ή στη SafeLine.gr
- Αναφέρετε το άτομο/κατάστημα στο κοινωνικό δίκτυο ή στην ιστοσελίδα γνωριμιών όπου το συναντήσατε.

Σας υπενθυμίζουμε ότι το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου, είναι επίσημος εκπρόσωπος στην Ελλάδα των Πανευρωπαϊκών Οργανισμών INSAFE / INHOPE που χαράσσουν την ευρωπαϊκή στρατηγική για ένα ασφαλές και ποιοτικό διαδίκτυο και παρέχει ενημέρωση, βοήθεια και υποστήριξη στους μικρούς και μεγάλους χρήστες του διαδικτύου με την ανάπτυξη τριών διακριτών δράσεων:

Μέσω της ιστοσελίδας SaferInternet4Kids.gr μπορεί κανείς να ενημερωθεί και να αντλήσει υλικό σχετικό με την ασφαλή χρήση του Ίντερνετ και τη χρήση των κοινωνικών δικτύων με το οποίο μπορεί με τη σειρά του να ενημερώσει διαδραστικά παιδιά και νέους κάθε ηλικίας. Το ενημερωτικό αυτό portal απευθύνεται τόσο σε γονείς και εκπαιδευτικούς όσο και σε εφήβους και παιδιά και περιλαμβάνει κατάλληλο πολυμεσικό υλικό.

Μέσω της συμβουλευτικής γραμμής Βοήθειας Help-line (διαθέσιμη τηλεφωνικά στο 210-6007686 και μέσω του ιστοχώρου www.help-line.gr), εξειδικευμένοι ψυχολόγοι παρέχουν υποστήριξη και συμβουλές για εξειδικευμένα θέματα που σχετίζονται με τη υπερβολική ενασχόληση στο διαδίκτυο, τον διαδικτυακό εκφοβισμό, την έκθεση σε ακατάλληλο περιεχόμενο και άλλους προβληματισμούς σχετικά με τη χρήση του διαδικτύου, του κινητού τηλεφώνου και των διαδικτυακών παιχνιδιών.

Και μέσω της Ανοιχτής Γραμμής Καταγγελιών για το παράνομο περιεχόμενο του διαδικτύου SafeLine (http://www.safeline.gr), δέχεται καταγγελίες για παιδική κακοποίηση και παράνομη χρήση του διαδικτύου και συνεργάζεται τόσο με την Ελληνική αστυνομία όσο και με την INTERPOL μέσω του Ευρωπαϊκού οργανισμού INHOPE. Η SafeLine είναι δηλαδή ένα κομμάτι ενός μεγάλου παζλ, μιας και η καταπολέμηση του παράνομου περιεχομένου του Ίντερνετ είναι υπόθεση παγκόσμιας κλίμακας και δεν περιορίζεται από εθνικά σύνορα.

Μάθετε νέα και άλλες ενδιαφέρουσες πληροφορίες από τη σελίδα μας στο Facebook και ακολουθήστε μας στο Twitter .