

**Την προσοχή των χρηστώ ν εφιστά το Ελληνικό Κέντρο Α-σφαλούς Διαδικτύου του Ιδρύματος Τεχνολογίας και Έρε-υνας σε σχέση με τις διαδικτυακές απάτες οι οποίες,...**

**όπως αναφέρει σε ανακοίνωσή του, λόγω της κατάστασης που έχει διαμορφωθεί και της υπερχρήσης που παρατηρείται έχουν αυξηθεί αισθητά από την αρχή της πανδημίας.**
**Η γραμμή καταγγελιώ ν για το παράνομο περιεχόμενο στο διαδίκτυο SafeLine.gr έχει δεχτεί από το Μάρτιο του 2020 έως σήμερα μεγάλο αριθμό αναφορώ ν που αφορούν σε οικονομικές απάτες σε εξ' αποστάσεως συναλλαγές και ηλεκτρονικές αγορές.**
**Πιο αναλυτικά στην ανακοίνωση αναφέρονται τα εξής:**
**Απάτες μέσω ηλεκτρονικού ταχυδρομείου (phishing)**
**Τον τελευταίο καιρό μάλιστα έχουν πληθύνει 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. Για παράδειγμα, (σχετική φωτό επισυνάπτεται) τα θύματα λαμβάνουν μήνυμα ηλεκτρονικού ταχυδρομείου που μοιάζει να έχει σταλεί από την τράπεζά τους το οποίο τους ζητά να επιβεβαιώ σουν τον αριθμό του τραπεζικού τους λογαριασμού. Πληροφορίες που μπορεί να ζητηθούν είναι τα ονόματα χρηστώ ν και κωδικοί πρόσβασης, αριθμοί κοινωνικής ασφάλισης, αριθμοί τραπεζικώ ν λογαριασμώ ν, αριθμοί πιστωτικώ ν καρτώ ν, ημερομηνία γέννησης κ.α.**

**Απάτες με spam μηνύματα εκβιαστικού περιεχομένου**

**Επιπρόσθετα, συχνές είναι οι καταγγελίες για περιστατικά spam μηνυμάτων εκβιαστικού περιεχομένου, που αποστέλλονται μαζικά σε διάφορους αποδέκτες με σκοπό την εξαπάτησή τους. Ειδικότερα, επιτήδειοι στέλνουν μαζικά μηνύματα σε αποδέκτες και τους ενημερώ νουν ότι διαθέτουν πρόσβαση στη συσκευή τους ενώ κάποιες φορές το μήνυμα φαίνεται ψευδώ ς 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 χρηστώ ν από τα μέσα κοινωνικής δικτύωσης και οι δράστες απειλούν με την αποστολή του επίμαχου υλικού στις επαφές τους, σε περίπτωση που δεν λάβουν bitcoins.**

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

**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 επαφώ ν 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 κώ δικα.**

**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 ώ στε 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 τηλεφώ νου 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 πιστωτικώ ν καρτώ ν. Να βεβαιώ νεστε 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 καταναλωτώ ν που έχουν ήδη αγοράσει από το κατάστημα.
• Να μην πείθεστε από υπερβολικά δελεαστικές τιμές των προϊόντων σε σχέση με τον ανταγωνισμό.

Romance scams

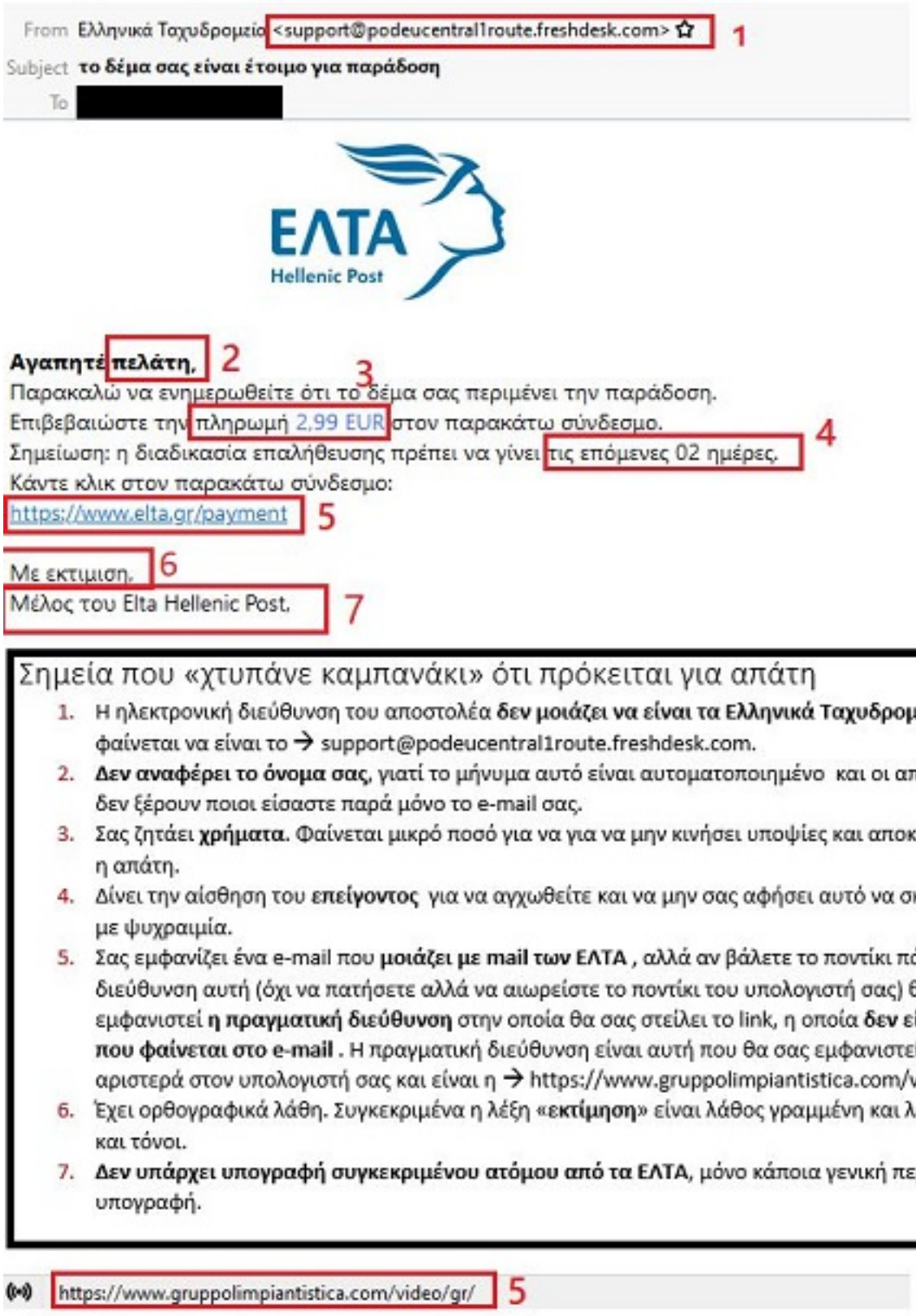
Ιδιαίτερη προσοχή εφιστάται στους χρήστες και για οργανωμένα κυκλώ ματα εγκληματιώ ν που προκειμένου να αποσπάσουν χρήματα από τα θύματά τους εκμεταλλεύονται τη μοναξιά και την ανάγκη επικοινωνίας κατά τη διάρκεια του lockdown (romance scam).

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 κοινωνικώ ν δικτύων ή ιστοσελίδων γνωριμιώ ν για πιθανά θύματα, περνώ ντας εβδομάδες ή μήνες για να δημιουργήσουν μια σχέση. Για να ισχυροποιήσουν τις ψεύτικες ιστορίες τους, συχνά παίρνουν φωτογραφίες και ονόματα πραγματικώ ν στρατιωτώ ν 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 πληρώ σει 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 χώ ρας, 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 γνωριμιώ ν όπου το συναντήσατε.**



From Ελληνικά Ταχυδρομεία <support@podeucentral1route.freshdesk.com> ☆ 1
Subject **το δέμα σας είναι έτοιμο για παράδοση**
To [redacted]

ΕΛΤΑ
Hellenic Post

**Αγαπητέ πελάτη,** 2
Παρακαλώ να ενημερωθείτε ότι το δέμα σας περιμένει την παράδοση. 3
Επιβεβαιώστε την πληρωμή 2,99 EUR στον παρακάτω σύνδεσμο.
Σημείωση: η διαδικασία επαλήθευσης πρέπει να γίνει τις επόμενες 02 ημέρες. 4
Κάντε κλικ στον παρακάτω σύνδεσμο:
https://www.elta.gr/payment 5

Με εκτιμιση, 6
Μέλος του Elta Hellenic Post. 7

Σημεία που «χτυπάνε καμπανάκι» ότι πρόκειται για απάτη

1. Η ηλεκτρονική διεύθυνση του αποστολέα **δεν μοιάζει να είναι τα Ελληνικά Ταχυδρομεία** γιατί φαίνεται να είναι το → support@podeucentral1route.freshdesk.com.
2. **Δεν αναφέρει το όνομα σας**, γιατί το μήνυμα αυτό είναι αυτοματοποιημένο και οι απατεώνες δεν ξέρουν ποιοι είσαστε παρά μόνο το e-mail σας.
3. Σας ζητάει **χρήματα**. Φαίνεται μικρό ποσό για να για να μην κινήσει υποψίες και αποκαλυφθεί η απάτη.
4. Δίνει την αίσθηση του **επείγοντος** για να αγχωθείτε και να μην σας αφήσει αυτό να σκεφτείτε με ψυχραιμία.
5. Σας εμφανίζει ένα e-mail που **μοιάζει με mail των ΕΛΤΑ** , αλλά αν βάλετε το ποντίκι πάνω στην διεύθυνση αυτή (όχι να πατήσετε αλλά να αιωρείστε το ποντίκι του υπολογιστή σας) θα εμφανιστεί **η πραγματική διεύθυνση** στην οποία θα σας στείλει το link, η οποία **δεν είναι αυτή που φαίνεται στο e-mail** . Η πραγματική διεύθυνση είναι αυτή που θα σας εμφανιστεί κάτω αριστερά στον υπολογιστή σας και είναι η → https://www.gruppolimpiantistica.com/video/gr/.
6. Έχει ορθογραφικά λάθη. Συγκεκριμένα η λέξη «**εκτίμηση**» είναι λάθος γραμμένη και λείπουν και τόνοι.
7. **Δεν υπάρχει υπογραφή συγκεκριμένου ατόμου από τα ΕΛΤΑ**, μόνο κάποια γενική περίεργη υπογραφή.

https://www.gruppolimpiantistica.com/video/gr/ 5