



## Η ΕΛ.ΑΣ. για την ΕΛΛΑΔΑ

Ερμούπολη Σύρου, 31 Μαρτίου 2022

### ΔΕΛΤΙΟ ΤΥΠΟΥ

Η Γενική Περιφερειακή Αστυνομική Διεύθυνση Νοτίου Αιγαίου στο πλαίσιο προληπτικής δράσης συμβουλευτικών ενημερώσεων προς αποφυγή τυχόν εξαπάτησης από επιτήδειους, σε συνέχεια [σχετικής ανακοίνωσης](#) και εν γνώσει έναρξης της θερινής τουριστικής περιόδου επιστὰ στους υπευθύνους καταλυμάτων διαμονής να είναι ιδιαίτερα προσεκτικοί κατά τις οικονομικές τους συναλλαγές που αφορούν στην κράτηση δωματίων.

Ειδικότερα, κάποιες γνωστές μορφές εξαπάτησης όπως αυτές που πραγματοποιούνται με τη μέθοδο της αποστολής απατηλών μηνυμάτων SMS (smishing) μπορεί να παρουσιάσουν παραλλαγές στο πρόσχημα που επικαλούνται οι απατεώνες.

Ενδέχεται επιτήδειοι να προσποιηθούν ότι επιθυμούν να προβούν σε κράτηση δωματίων και στο πλαίσιο της δήθεν πραγματοποίησης πληρωμής του συμφωνηθέντος ποσού να αποσπάσουν τεχνηέντως τους αριθμούς και κωδικούς PIN τραπεζικών καρτών ή τους προσωπικούς κωδικούς e-banking. Ακολουθώντας με τη χρήση των υποκλεμμένων στοιχείων να πραγματοποιήσουν μεταφορές χρηματικών ποσών από τους τραπεζικούς λογαριασμούς των παθόντων σε δικούς τους ή συνεργών τους.

Συνοπτικά συνίσταται:

- Να μην γνωστοποιούνται αριθμοί τραπεζικών καρτών και προσωπικοί κωδικοί πρόσβασης ή επαλήθευσης σε τραπεζικούς λογαριασμούς
- Να μην συμπληρώνονται στοιχεία πρόσβασης τραπεζικών λογαριασμών σε φόρμες που αποστέλλονται από ηλεκτρονικές διευθύνσεις ή μηνύματα
- Για πρόσβαση σε ιστοσελίδα τράπεζας να πληκτρολογείται η διεύθυνση στον browser και να μην πραγματοποιείται είσοδος μέσω υπερσυνδέσμων.
- Σε περίπτωση ύποπτης διαδικασίας να γίνεται επαλήθευση μέσω τραπεζής.



## Η ΕΛ.ΑΣ. για την ΕΛΛΑΔΑ

Ενδεικτικές μορφές πραγματοποίησης απάτης είναι οι:

- απάτες σε αγορές μέσω διαδικτύου (online shopping scams)

### 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 πωλησών, 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.

Ειδική προσφορά  
**ΣΟΥΠΕΡ ΠΡΟΣΦΟΡΑ**  
70%  
\$\$

EUROPOL  
ΕΟ3  
Ευρωπαϊκή Οργανισμός  
Επιβολής του Νόμου

ΕΒΡ  
ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ

CYBER  
CRIME  
DIVISION  
ΒΟΥΛΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

#CyberScams



## Η ΕΛ.ΑΣ. για την ΕΛΛΑΔΑ

- απατηλές τηλεφωνικές κλήσεις (vishing)

### ΑΠΑΤΗΛΕΣ ΤΗΛΕΦΩΝΙΚΕΣ ΚΛΗΣΕΙΣ

Ο όρος "Vishing" (συνδυασμός των λέξεων "Voice" και "Phishing") είναι απάτη μέσω τηλεφώνου, που σκοπό έχει να εξαπατηθεί το θύμα προκειμένου να αποκαλύψει τις προσωπικές και οικονομικές του πληροφορίες ή κωδικούς ασφαλείας του ή και να μεταφέρει χρήματα στους απατεώνες.

#### ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

- > Να είστε προσεκτικοί με αιφνιδιαστικές και απροειδοποίητες τηλεφωνικές κλήσεις.
- > Κρατήστε τον αριθμό τηλεφώνου από τον οποίο σας έχουν καλέσει και ενημερώστε ότι θα τους επιστρέψετε εσείς την τηλεφωνική κλήση.
- > Για να επαληθεύσετε την ταυτότητά τους, αναζητήστε τον αριθμό τηλεφώνου της επιχείρησης και επικοινωνήστε απευθείας μαζί τους.
- > Μην επαληθεύετε το άτομο που σας καλεί με τον αριθμό τηλεφώνου που σας έδωσε (μπορεί να είναι ψεύτικος ή πλαστογραφημένος αριθμός).
- > Οι απατεώνες μπορούν να βρουν τα βασικά στοιχεία επικοινωνίας σας μέσω διαδικτύου (π.χ. από τα μέσα κοινωνικής δικτύωσης). Μην υποθέσετε ότι το άτομο που σας καλεί δηλώνει την αληθινή του ιδιότητα επειδή έχει στη διάθεσή του τέτοιες πληροφορίες.
- > Μην δίνετε τον κωδικό "PIN" της πιστωτικής ή χρεωστικής σας κάρτας ή τον κωδικό πρόσβασης του τραπεζικού σας λογαριασμού μέσω e-banking. Η τράπεζα συνεργασίας σας δεν θα ζητήσει ποτέ τέτοιου είδους πληροφορίες.
- > Μην μεταφέρετε χρήματα σε άλλο τραπεζικό λογαριασμό κατόπιν αιτήματός τους. Η τράπεζα συνεργασίας σας δεν θα σας ζητήσει ποτέ να προβείτε σε τέτοια ενέργεια.
- > Αν νομίζετε ότι πρόκειται για απατηλή τηλεφωνική κλήση, αναφέρετέ το στην τράπεζα συνεργασίας σας.



**EUROPOL** Ευρωπαϊκό Κέντρο για την Εγκληματολογία  
**EC3** European Cybercrime Centre  
**EBF** European Bank Fraud  
**CYBER CRIME DIVISION** ΔΙΟΤΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ  
**9 YEARS** 1928-2018  
**HELLENIC BANK ASSOCIATION**  
**#CyberScams**





## Η ΕΛ.ΑΣ. για την ΕΛΛΑΔΑ

- απατηλά μηνύματα SMS (smishing)

### 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.
- > Μην 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 παρέχετε τα στοιχεία των τραπεζικών σας λογαριασμών, επικοινωνήστε αμέσως με την τράπεζα συνεργασίας σας.



## Η ΕΛ.ΑΣ. για την ΕΛΛΑΔΑ

### • απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου (phishing)

**ΑΠΑΤΗΛΑ ΜΗΝΥΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ (PHISHING)**

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 μηνυμάτων ηλεκτρονικού ταχυδρομείου.
- 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 απίπειρα ηλεκτρονικού "φαρέματος" από το κινητό τηλέφωνο ή το tablet σας.

**ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;**

- Διατηρείτε το λογισμικό ενημερωμένο, περιλαμβανομένου του φιλτράριστη ιστοσελίδων (browser), του αντικού προγράμματος (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 πραγματικά μηνύματα από την τράπεζα συνεργασίας σας. Ελέγξτε για ορθογραφικά λάθη και λάθη γραμματικής ή σύνταξης.
- Μην απαντάτε σε οποιοδήποτε 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 πραγματοποιείτε λήψη (download) του επισυναπτόμενου αρχείου, αντίθετα πληκτρολογήστε τη διεύθυνση του ηλεκτρονικού συνδέσμου στον φιλτράριστη ιστοσελίδων (browser) που χρησιμοποιείτε.
- Σε περίπτωση οποιασδήποτε αμφιβολίας, ελέγξτε την ιστοσελίδα ή τηλεφωνήστε στην τράπεζα συνεργασίας σας.

**#CyberScams**





## Η ΕΛ.ΑΣ. για την ΕΛΛΑΔΑ

- απατηλές ιστοσελίδες τραπεζών (spoofed bank websites)

### ΑΠΑΤΗΛΕΣ ΙΣΤΟΣΕΛΙΔΕΣ ΤΡΑΠΕΖΩΝ

Τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου περιλαμβάνουν ηλεκτρονικούς συνδέσμους (links), οι οποίοι θα σας ανακατευθύνουν σε μια ψεύτικη ιστοσελίδα, δήθεν της τράπεζας συνεργασίας σας, όπου θα σας ζητηθεί να αποκαλύψετε τα οικονομικά και προσωπικά σας στοιχεία.




### ΠΟΙΕΣ ΕΙΝΑΙ ΟΙ ΕΝΔΕΙΞΕΙΣ;

Οι ψεύτικες ιστοσελίδες τραπεζών προσομοιάζουν αρκετά με τις νόμιμες ιστοσελίδες της τράπεζάς σας. Οι ψεύτικες ιστοσελίδες θα διαθέτουν συχνά ένα αναδυόμενο παράθυρο, με το οποίο θα σας ζητείται η εισαγωγή των εξατομικευμένων διαπιστευτηρίων ασφαλείας σας. Οι τράπεζες δεν κάνουν χρήση τέτοιων αναδυόμενων παραθύρων.

**Αυτές οι ιστοσελίδες συχνά εμφανίζουν:**

- Επείγον:** Δεν θα συναντήσετε ποτέ τέτοιους είδους μηνύματα σε νόμιμες ιστοσελίδες.
- Αναδυόμενα παραθύρα:** Χρησιμοποιούνται συνήθως για τη συλλογή ευαίσθητων προσωπικών σας πληροφοριών. Μην τα επιλέγετε και αποφεύγετε την υποβολή δεδομένων προσωπικού χαρακτήρα σε αυτά.
- Ελαττωματικός σχεδιασμός:** Να είστε προσεκτικοί σε ιστοσελίδες που παρουσιάζουν ελαττώματα στον σχεδιασμό τους ή ορθογραφικά λάθη και λάθη γραμματικής ή σύνταξης.

### ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

-  Μην κάνετε κλικ ποτέ σε ηλεκτρονικούς συνδέσμους (links) που περιλαμβάνονται σε μηνύματα ηλεκτρονικού ταχυδρομείου, τα οποία δήθεν σας ανακατευθύνουν στην ιστοσελίδα της τράπεζας συνεργασίας σας.
-  Πάντοτε να πληκτρολογείτε εσείς τον ηλεκτρονικό σύνδεσμο της τράπεζας σας ή να χρησιμοποιείτε υφιστάμενο ηλεκτρονικό σύνδεσμο από τον κατάλογο των αγαπημένων σας ελείδοδεικτών.
-  Χρησιμοποιείτε φυλλομετρητή ιστοσελίδων (browser) που σας επιτρέπει την επιλογή αποκλεισμού αναδυόμενων παραθύρων.
-  Εάν κάτι σημαντικό πραγματικά χρειάζεται την προσοχή σας θα ενημερωθείτε για αυτό από την τράπεζά σας όταν θα συνδεθείτε ηλεκτρονικά στον τραπεζικό σας λογαριασμό (π.χ. μέσω e-banking).

 #CyberScams



Υπουργείο Προστασίας του Πολίτη  
Ελληνική Αστυνομία  
Γενική Περιφερειακή Αστυνομική Διεύθυνση  
Νοτίου Αιγαίου

Γραφείο Ενημέρωσης Δημοσιογράφων  
Πλ. Ρεθύμνη, Τ.Κ. 841 00, Ερμούπολη Σύρου  
Τηλέφωνο: 22810-96110, 22810-96102  
e-mail: [press.gadpnaigaiou@hellenicpolice.gr](mailto:press.gadpnaigaiou@hellenicpolice.gr)

## Η ΕΛ.ΑΣ. για την ΕΛΛΑΔΑ

Σε κάθε περίπτωση οι πολίτες μπορούν να απευθύνονται στα Αστυνομικά Τμήματα και Υπηρεσίες Ασφαλείας της περιοχής τους.

Περισσότερες χρήσιμες συμβουλές-πληροφορίες για την προστασία των πολιτών έχουν αναρτηθεί στην ιστοσελίδα της Ελληνικής Αστυνομίας Ελληνικής Αστυνομίας [www.hellenicpolice.gr](http://www.hellenicpolice.gr) / Οδηγός του Πολίτη.