Πώς μπορούμε να προστατευτούμε

- Διατηρούμε το **λογισμικό ενημερωμένο**, συμπεριλαβανομένου του φυλλομετρητή ιστοσελίδων (browser), του αντιικού προγράμματος (antivirus) και του λειτουργικού συστήματος.
- **Είμαστε ιδιαίτερα προσεκτικοί**, εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου «Οργανισμού», μας ζητά ευαίσθητες πληροφορίες (π.χ. τον κωδικό πρόσβασης).
- Επικοινωνούμε άμεσα με το αρμόδιο τραπεζικό ίδρυμα σε περίπτωση πραγματοποίησης συναλλαγών που δεν αναγνωρίζουμε.
- Χρησιμοποιούμε τη **μέθοδο SLAM** (ελέγχουμε Sender - Links - Attachment - Message) για να εντοπίσουμε ύποπτα μηνύματα ψαρέματος. Συγκρίνουμε τη διεύθυνση με τα προηγούμενα πραγματικά μηνύματα από τον αποστολέα. Ελέγχουμε για ορθογραφικά, γραμματικά και συντακτικά λάθη.
- **Δεν κάνουμε απευθείας κλικ σε ηλεκτρονικούς συνδέσμους (link)** και δεν πραγματοποιούμε λήψη (download) του επισυναπτόμενου αρχείου, αντίθετα πληκτρολογούμε τη διεύθυνση του ηλεκτρονικού συνδέσμου στον φυλλομετρητή ιστοσελίδων (browser) που χρησιμοποιούμε.

- Πριν ολοκληρώσουμε μια διαδικτυακή αγορά **ελέγχουμε τις διαθέσιμες αξιολογήσεις για τον πωλητή.**
- Δεν μεταφέρουμε χρήματα μέσω των λογαριασμών μας και αν μας υποκλέψουν τους κωδικούς τραπεζικής **ελέγχουμε τις πραγματοποιηθείσες συναλλαγές** καθώς μπορεί να εμπλακούμε σε μεταφορά παράνομων χρημάτων.
- **Ασφαλίζουμε το οικιακό μας δίκτυο.**
- Χρησιμοποιούμε **ισχυρούς κωδικούς πρόσβασης** (εάν είναι εφικτό password manager ή two-step verification).
- Τα γνωστά «στικάκια» είναι μία πηγή μόλυνσης, ενώ είναι πολύ εύκολο ακόμη και να χαθούν! **Χρησιμοποιούμε πρόγραμμα κρυπτογράφησης ή κλειδώματος των αρχείων.**
- Δίνουμε **ιδιαίτερη προσοχή στη χρήση των μέσων κοινωνικής** δικτύωσης και ειδικότερα αν το επάγγελμά μας συνδέεται με διαχείριση ευαίσθητων δεδομένων. Γνωρίζουμε ποιες πληροφορίες μοιραζόμαστε στα μέσα κοινωνικής δικτύωσης.
- Χρησιμοποιούμε **ένα VPN.**
- Δεν ξεχνάμε τη **φυσική ασφάλεια.**

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

Για περισσότερες πληροφορίες :

ΕΠΙΚΟΙΝΩΝΙΑ

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος – Cyber Crime Division
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11522
e-mail: **ccu@cybercrimeunit.gov.gr**, Τηλ.: **11188**

Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδας
Μοναστηρίου 326, Θεσσαλονίκη, Τ.Κ. 54121
e-mail: **ydheve@cybercrimeunit.gov.gr**, Τηλ.: **11188**

Ενημερωθείτε για θέματα ασφαλούς πλοήγησης στο Διαδίκτυο στο **cyberkid.gov.gr** και στο **www.cyberalert.gr**

Cyberkid.gov.gr
CyberAlertGR
Cyberalert.gr
CyberAlertGR
Cyber Alert

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Προστασίας του Πολίτη

ΕΛΑΣ Επόμενο βήμα

Αρχηγείο Ελληνικής Αστυνομίας

#θύμα_διαδικτυακής_απάτης

όταν το σερφάρισμα οδηγεί στην εξαπάτηση

Οι κυριότερες μορφές διαδικτυακής απάτης είναι οι ακόλουθες:

Phishing/Smishing

Λήψη e-mails/SMS, εστιασμένων στα ενδιαφέροντα του χρήστη, από υποτιθέμενο υπαρκτό και νόμιμο οργανισμό, τα οποία περιλαμβάνουν ύποπτο link ή συνημμένο αρχείο. Vishing: τηλεφωνικές κλήσεις με σκοπό να σας αποσπάσουν στοιχεία της πιστωτικής κάρτας ή του e-banking σας.
Στόχος είναι η απόκτηση πρόσβασης στα στοιχεία ηλεκτρονικής τραπεζικής ή κάρτας τραπέζης.

Tip: ***Η τράπεζα δεν θα ζητήσει ποτέ τους κωδικούς και τα προσωπικά μας δεδομένα μέσω e-mail ή sms ή τηλεφωνικά. Δεν γνωστοποιούμε τα στοιχεία της τραπεζικής μας κάρτας σε τρίτους.***

Ιστοσελίδα κλώνος e-banking

Κατά την αναζήτηση της ιστοσελίδας του e-banking σε μηχανές αναζήτησης (π.χ. google, bing) εμφανίζεται ως πρώτη επιλογή, ιστοσελίδα κλώνος τραπέζης. Στόχος: η υποκλοπή των κωδικών σας.

Tip: ***Για την είσοδό μας στο e-banking πληκτρολογούμε τον υπερσύνδεσμο (url) μόνοι μας στον περιηγητή (browser) ή ακολουθούμε σελιδοδείκτη (bookmark) που έχουμε αποθηκεύσει.***

Επενδυτικές Απάτες

Επικοινωνούν μαζί μας και μας υπόσχονται γρήγορο κέρδος από διαδικτυακές επενδύσεις, πιέζοντάς μας χρονικά καθώς η προσφορά λήγει άμεσα, ενώ μας εισάγουν σε πλατφόρμα όπου μπορούμε να βλέπουμε online τις αποδόσεις.

Tip: ***Δεν ανταποκρινόμαστε σε αναρτήσεις-αγγελίες στο Διαδίκτυο, κλήσεις, μηνύματα sms που υπόσχονται επενδυτικές ευκαιρίες και είμαστε επιφυλακτικοί σε επενδύσεις υποσχόμενες υπέρογκα κέρδη. Λαμβάνουμε αμερόληπτες συμβουλές πριν επενδύσουμε τα χρήματά μας.***

Απάτες σε διαδικτυακές αγορές

Δημοσίευση προσφορών, οι οποίες είναι πολύ καλές για να είναι αληθινές και είναι διαθέσιμες για περιορισμένο χρονικό διάστημα.

Tip: Κάνουμε έρευνα για την έδρα του καταστήματος και τις αξιολογήσεις του πριν αγοράσουμε. Θαυματουργά προϊόντα ή εξωφρενικές προσφορές ίσως είναι πολύ καλές για να είναι αληθινές.

Απάτες σχετιζόμενες με εταιρικά e-mail (Business E-mail Compromise-BEC)

Στοχεύουν υπαλλήλους εταιρειών για να πραγματοποιήσουν εταιρικές συναλλαγές προς απατηλούς τραπεζικούς λογαριασμούς με διάφορες προφάσεις.

Tips:

- *Για επιχειρήσεις:*
  - *Ορίζουμε εσωτερικές διαδικασίες για τη διενέργεια πληρωμών και εφαρμόζουμε την επαλήθευση νομιμότητας για αυτές.*
  - *Καθιερώνουμε διαδικασίες υποβολής αναφορών σε περίπτωση απάτης.*
  - *Αναβαθμίζουμε και ενημερώνουμε το λογισμικό.*
  - *Ενημερώνουμε τους υπαλλήλους της εταιρείας.*
- *Για εργαζόμενους:*
  - *Εφαρμόζουμε αυστηρά διαδικασίες ασφαλείας για διενέργεια πληρωμών και καταβολής προμηθειών.*
  - *Ελέγχουμε links, urls, επισυναπτόμενα αρχεία ειδικά αν χειριζόμαστε ευαίσθητες πληροφορίες.*
  - *Αποφεύγουμε κοινοποίηση πληροφοριών σχετικά με την ιεραρχία και τη θέση μας στην εταιρεία που θα μας στοχοποιήσουν σε κακόβουλους χρήστες.*

Απάτες με αγγελίες μέσω Διαδικτύου

Δημοσίευση απατηλών αγγελιών στο διαδίκτυο για μίσθωση κατοικιών, εύρεση εργασίας ή αγοραπωλησίες προϊόντων.

Tip: Δεν δίνουμε τα στοιχεία της τραπεζικής μας κάρτας.

Απάτες με πρόφαση τις διαδικτυακές γνωριμίες

Προσέγγιση μέσω σελίδων κοινωνικής δικτύωσης ή εφαρμογών γνωριμιών, δήθεν για δημιουργία προσωπικής σχέσης. Στόχος είναι η υπεξαίρεση χρηματικού ποσού.

Tip: ***Προσέχουμε τα ορθογραφικά, γραμματικά και συντακτικά λάθη. Δεν στέλνουμε χρήματα και προσωπικά έγγραφα, όσο αληθοφανείς κι αν είναι οι ιστορίες τους.***

Απάτες με πρόφαση επιδιόρθωση υπολογιστή

Προσποιούμενοι τεχνικούς σε μεγάλες εταιρείες πληροφορικής ζητούν να εγκαταστήσουν λογισμικό απομακρυσμένης πρόσβασης, με την πρόφαση ότι ο υπολογιστής ή η φορητή συσκευή μας έχει μολυνθεί από κακόβουλο λογισμικό. Στόχος τους είναι η υποκλοπή προσωπικών και τραπεζικών δεδομένων.

Tip: ***Δεν εγκαθιστούμε αμφιβόλου ασφαλείας λογισμικό στις συσκευές μας.***

Απάτες με χορήγηση δανείων από μη αδειοδοτημένους φορείς

Αναρτήσεις σε σελίδες κοινωνικής δικτύωσης για δάνεια με ευνοϊκούς όρους από μη αδειοδοτημένους φορείς.

Tip: ***Είμαστε ιδιαίτερα επιφυλακτικοί με αυτόκλητα e-mails ή διαφημίσεις που προβάλλονται στα μέσα κοινωνικής δικτύωσης και υπόσχονται εξαιρετικές ευκαιρίες δανείων.***

Δεν διστάζουμε να καταγγείλουμε:

- Στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, μέσω τηλεφώνου στο 11188 ή μέσω e-mail στο ccu@cybercrimeunit.gov.gr ή με φυσική παρουσία.
- Σε οποιαδήποτε αστυνομική ή δικαστική αρχή ανά την Επικράτεια.
- Στην ψηφιακή πύλη της Δημόσιας Διοίκησης gov.gr, στην ενότητα «Πολίτης και καθημερινότητα» και στην υποενότητα «Καταγγελίες». Σημειώνεται ότι είναι πιθανόν να απαιτηθεί περαιτέρω επικοινωνία με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος βάσει των προβλεπόμενων διατάξεων του Κώδικα Ποινικής Δικονομίας περί υποβολής εγκλήσεων.