ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΔΙΕΥΘΥΝΣΗ ΔΙΩΞΗΣ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ
ΠΡΟΛΗΨΗ • ΕΡΕΥΝΑ • ΚΑΤΑΣΤΟΛΗ

Ένας κόσμος **συνδεδεμένος**

Ένας κόσμος **προστατευμένος**

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Προστασίας του Πολίτη

Αρχηγείο Ελληνικής Αστυνομίας

CYBER ALERT

Όπως συμβαίνει στον πραγματικό κόσμο, έτσι και στο Διαδίκτυο, υπάρχουν **κακόβουλοι χρήστες** που έχουν σκοπό να **κλέψουν** τα προσωπικά σας **στοιχεία**, τα **χρήματά** σας, **ή και τα δύο**.

Κυριότερες μορφές διαδικτυακής απάτης:

- **Phishing/Smishing:** λήψη email/SMS από υποτιθέμενο υπαρκτό και νόμιμο οργανισμό, το οποίο περιλαμβάνει ύποπτο link ή συνημμένο αρχείο.
- **Επενδυτικές Απάτες:** επικοινωνούν μαζί σας και σας υπόσχονται γρήγορο κέρδος από διαδικτυακές επενδύσεις, πιέζοντάς σας χρονικά καθώς η προσφορά λήγει άμεσα.
- **Σε διαδικτυακές αγορές:** δημοσίευση προσφορών, οι οποίες είναι πολύ καλές για να είναι αληθινές και είναι διαθέσιμες για περιορισμένο χρονικό διάστημα.
- **Συσχετιζόμενες με εταιρικά emails:** στοχεύουν υπαλλήλους εταιρειών για να καταθέσουν χρήματα σε απατηλούς τραπεζικούς λογαριασμούς με διάφορες προφάσεις.
- **Με αγγελίες μέσω διαδικτύου:** δημοσίευση απατηλών αγγελιών στο διαδίκτυο για μίσθωση κατοικιών, εύρεση εργασίας ή αγοραπωλησίες προϊόντων.
- **Μεταφορέας παράνομου χρήματος (Money Mule):** άτομα που εν αγνοία τους αναλαμβάνουν να μεταφέρουν παράνομα αποκτηθέντα χρήματα σε λογαριασμούς τρίτων.
- **Με πρόφαση τις διαδικτυακές γνωριμίες:** προσέγγιση μέσω σελίδων κοινωνικής δικτύωσης, δήθεν για δημιουργία γνωριμίας και δεσμού.
- **Παραβιάσεις ψηφιακών πορτοφολιών:** με σκοπό την κλοπή κρυπτονομισμάτων και τη μεταφορά τους σε έτερα πορτοφόλια.
- **Με χρήση τεχνητής νοημοσύνης-Deep-fake οπτικοακουστικό υλικό:** πλαστογράφηση φωνών και προσώπων με στόχο π.χ. να πείσουν τα υποψήφια θύματα να προβούν σε δήθεν αποδοτικές επενδύσεις ή σε αγορά σκευασμάτων.

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

- **Με ψευδείς διαγωνισμούς:** χρησιμοποιώντας ονόματα εταιρειών υπόσχονται δώρα μέσω διαγωνισμών (δωροεπιταγές, αεροπορικά εισιτήρια κ.ά.).
- **Με προγνωστικά αθλητικών αγώνων:** χρησιμοποιώντας τα μέσα κοινωνικής δικτύωσης, υπόσχονται έναντι αμοιβής προγνωστικά αγώνων.
- **Με χορήγηση δανείων από μη αδειοδοτημένους φορείς:** αναρτήσεις σε σελίδες κοινωνικής δικτύωσης για δάνεια με ευνοϊκούς όρους από μη αδειοδοτημένους φορείς.
- **Vishing:** τηλεφωνικές κλήσεις με σκοπό να σας αποσπάσουν στοιχεία της πιστωτικής σας κάρτας ή του e-banking.

TIP!

Πλέον οι δράστες προτρέπουν ολοένα και συχνότερα τα θύματα τους να χρησιμοποιήσουν κρυπτονομίσματα.

Πώς μπορείτε να προστατευτείτε:

- **Μην αποκαλύπτετε** τους **κωδικούς** της ηλεκτρονικής τραπεζικής ή τα **στοιχεία της κάρτας** σας μέσω ηλεκτρονικού ταχυδρομείου ή τηλεφώνου.
- Παρατηρήστε τη **σύνταξη** του κειμένου σε ένα email. Ενδεχομένως να υπάρχουν πολλά **ορθογραφικά λάθη** και άλλες **ανακρίβειες**.
- Εάν λάβετε ύποπτο email, **μην απαντήσετε**, **μην ακολουθήσετε** τυχόν υποδεικνυόμενο σύνδεσμο (link) και **μην ανοίξετε** τυχόν συνημμένο αρχείο.
- Να είστε ιδιαίτερα **επιφυλακτικοί** με διαφημίσεις ή αγγελίες που αφορούν θέσεις εργασίας με μεγάλες οικονομικές απολαβές ή εξαιρετικές προσφορές προϊόντων.
- **Μην εμπιστεύεστε** όσους σας ζητούν χρήματα εκ των προτέρων για να σας προσφέρουν μια θέση εργασίας.
- Όταν αγοράζετε μέσω διαδικτύου από ιδιώτη, **μη στέλνετε χρήματα προκαταβολικά** στον πωλητή.
- Πραγματοποιείστε αγορές από **εταιρείες που γνωρίζετε** ή ελέγξτε τις αξιολογήσεις.
- Επικοινωνήστε **άμεσα** με το αρμόδιο τραπεζικό ίδρυμα σε περίπτωση πραγματοποίησης συναλλαγών που δεν αναγνωρίζετε.

Αν πέσετε θύμα, μη διστάσετε να το καταγγείλετε:

- Στη Διεύθυνση Δίωξης Κυβερνοεγκλήματος, μέσω τηλεφώνου στο **11188** ή μέσω email 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 Κυβερνοεγκλήματος βάσει των προβλεπόμενων διατάξεων του Κώδικα Ποινικής Δικονομίας περί υποβολής εγκλήσεως.

ΤΑΥΤΟΠΟΙΗΣΗ ΔΥΟ ΠΑΡΑΓΟΝΤΩΝ (2FA)

Η ταυτοποίηση δύο παραγόντων (2FA) είναι μια ηλεκτρονική μέθοδος ταυτοποίησης, κατά την οποία ένας χρήστης αποκτά πρόσβαση σε έναν ιστότοπο ή μια εφαρμογή μόνο αφού παρουσιάσει επιτυχώς τουλάχιστον δύο διαφορετικά στοιχεία επαλήθευσης.

ΧΡΗΣΙΜΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

- **ΔΙΕΥΘΥΝΣΗ ΔΙΩΞΗΣ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ**
  Λ. Αλεξάνδρας 173, Αμπελόκηποι, Τ.Κ. 11522
  Αθήνα,
  e-mail: **ccu@cybercrimeunit.gov.gr**,
  Τηλ.: **11188**

- **ΥΠΟΔΙΕΥΘΥΝΣΗ ΔΙΩΞΗΣ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ ΒΟΡΕΙΟΥ ΕΛΛΑΔΑΣ**
  Μοναστηρίου 326, Τ.Κ. 54121
  Θεσσαλονίκη,
  e-mail: **ydheve@cybercrimeunit.gov.gr**
  Τηλ.: **11188**

CyberAlertGR
CyberAlertGR
Cyberalert.gr
Cyber Alert

11188

Ενημερωθείτε για θέματα ασφαλούς πλοήγησης στο διαδίκτυο στο: **www.cyberalert.gr**