

Πώς θα διακρίνετε τα μηνύματα «ψαρέματος»



Οδηγός από τα

Εργαστήρια Kaspersky

Οι ειδικοί των Εργαστηρίων Kaspersky διακρίνουν μερικές ενδείξεις που φανερώνουν προσπάθεια υποκλοπής προσωπικών δεδομένων μέσω ειδοποιήσεων ηλεκτρονικού ταχυδρομείου από δήθεν επίσημους φορείς. Διαβάστε τι πρέπει να προσέξετε πριν κάνετε κλικ σε ένα link που περιέχεται σε μήνυμα ηλεκτρονικού ταχυδρομείου.

Σύμφωνα με την Darya Gudkova, επικεφαλής του τμήματος Ανάλυσης Περιεχομένου και Έρευνας στο Kaspersky Lab, να θυμάστε ότι τα επίσημα email:

- δεν ζητούν ποτέ από τους πελάτες να εισάγουν και να επιβεβαιώσουν προσωπικές πληροφορίες ή στοιχεία των τραπεζικών τους λογαριασμών **μέσα από links** (παραπομπές) που περιέχονται σε αυτά.
- Δεν απειλούν **να μπλοκάρουν** τους λογαριασμούς των πελατών.
- Μην κλικάρετε ποτέ σε ένα link αν το πρόγραμμα antivirus ή ο browser σας το **αποκλείσει**.
- Πρέπει να δείχνετε ιδιαίτερη προσοχή στα links που περιέχονται στο μήνυμα.

Αν το link που περιλαμβάνεται στο e-mail οδηγεί σε μια **ανεπίσημη ιστοσελίδα** ή

- αν το κείμενο του email υποδεικνύει τη διεύθυνση μιας επίσημης ιστοσελίδας ενώ **το link οδηγεί σε μια άλλη σελίδα**, αυτό αποτελεί στοιχείο ότι ενδέχεται να έχετε ένα phishing email μπροστά σας.
- Αν έχετε αμφιβολίες για την αυθεντικότητα του email, **επικοινωνήστε με το τμήμα εξυπηρέτησης πελατών** του οργανισμού που υποτίθεται ότι σας έστειλε το email για να ανακαλύψετε αν το συγκεκριμένο μαζικό email όντως στάλθηκε.

Διαβάστε περισσότερα για το λεγόμενο phishing (παραφράζοντας το fishing) στο tech.in.gr

Θέματα: [Χάκινγκ](#)

- [Kaspersky Lab: «Προσοχή στους Ιούς των Ταξιδιών»](#)
 - [Υπερδιπλασιάστηκαν οι απόπειρες εξαπάτησης στα κοινωνικά δίκτυα](#)
 - [Μην κάνετε κλικ | Hello this user is making really bad rumors about you...](#)
 - [«Στείλτε αυτό το μήνυμα σε φίλους σας»... και καλά ξεμπερδέματα](#)
 - [Μεταλλαγμένος επιστρέφει ο Ιός της Αστυνομίας στην Ελλάδα για λύτρα](#)
 - [«Κοιτάξτε τη γραμμή διευθύνσεων πριν μπείτε στο Facebook», λέει η ESET](#)
-
- [Τα νέα εργαλεία κυβερνο-εγκλήματος και πώς να προστατευτείτε](#)

Ξέρατε ότι ένα κλικ σε ένα συντετμημένο URL αρκεί για να μολύνει τον υπολογιστή σας με κακόβουλο λογισμικό, ότι η αναζήτηση για καυτά θέματα της επικαιρότητας σε μηχανές αναζήτησης μπορεί να σας οδηγήσει σε παγίδες ή ότι μπορείτε να ακολουθείτε δικτυακούς τόπους με βάση τη καλή τους φήμη;

Πηγή: [In.gr Τεχνολογία](#)