

ΠΡΟΣΟΧΗ ΣΤΑ ΜΗΝΥΜΑΤΑ PHISHING – ΟΔΗΓΙΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

📅 19/05/2021 📁 ΔΕΛΤΙΑ ΤΥΠΟΥ



Πολλαπλασιάζονται το τελευταίο χρονικό διάστημα τα φαινόμενα αποστολής ηλεκτρονικών μηνυμάτων από επιτήδειους, τα λεγόμενα «phishing». Το πότε μιλάμε για «phishing», το καταλαβαίνουμε όταν λάβουμε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, κείμενο ή άλλη μορφή ηλεκτρονικής επικοινωνίας που φαίνεται να προέρχεται από τράπεζα ή κάποια άλλη δημοφιλή ηλεκτρονική υπηρεσία που μας ζητά ευαίσθητες πληροφορίες όπως έναν αριθμό πιστωτικής κάρτας κλπ. Αν τυχόν πέσουμε στη σχετική παγίδα, τότε οι πληροφορίες που εν αγνοία μας θα παρέχουμε, θα πουληθούν ή θα αξιοποιηθούν από τους επιτιθέμενους για εξαπάτηση, εκβιασμό, κλοπή χρημάτων, ή υποκλοπή ταυτότητας.

Η πιο κοινή τεχνική ηλεκτρονικού “φαρέματος” είναι να μιμηθεί κάποιος μια τράπεζα ή ένα χρηματοπιστωτικό ίδρυμα μέσω ηλεκτρονικού ταχυδρομείου, προκαλώντας το θύμα να συμπληρώσει τα στοιχεία του λογαριασμού του σε μια ψεύτικη φόρμα μέσα στο κείμενο του μηνύματος, σε ένα επισυναπτόμενο αρχείο, ή παραπέμποντάς τον σε μια ιστοσελίδα.

Πώς αντιμετωπίζουμε μια τέτοιου είδους κυβερνοεπίθεση;

1. **Ελέγχουμε πάντοτε το όνομα του αποστολέα** και συγκεκριμένα την κατάληξη του domain (πχ @eeke.com) και εφόσον η κατάληξη δεν μας είναι γνωστή, ή δεν υπάρχει σε μια μηχανή αναζήτησης, τότε προκύπτει για απώληση



2. Παρατηρούμε και δεν παραπλανούμαστε από το θέμα του μηνύματος, αφού οι επιτήδευτοι χρησιμοποιούν βαρύγδουπους τίτλους, όπως π.χ. περί δήθεν οφειλής μας, περί ύπαρξης ιού στο λογισμικό του υπολογιστή, ότι είμαστε κληρονόμοι ενός τεράστιου ποσού από το εξωτερικό, ότι κάποιος θέλει να μας αποστείλει χρήματα κλπ.
3. Δεν ανοίγουμε ποτέ, πριν σιγουρευτούμε για την ασφάλειά τους, τους συνδέσμους που επισυνάπτονται στο mail. Κι αυτό γιατί μπορεί να οδηγηθούμε σε έναν κακόβουλο ιστότοπο ή να μολυνθεί ο υπολογιστής, τάμπλετ, κινητό μας κλπ. με κακόβουλο λογισμικό
4. Ελέγχουμε τον τρόπο γραφής του mail καθώς και την ορθογραφία του, είμαστε δε πάντα υποψιασμένοι όταν δεν αναφέρει συγκεκριμένα το όνομά μας εντός του κειμένου
5. Καμία τράπεζα δεν ζητάει προσωπικά στοιχεία μέσω mail, γι'αυτό δεν δίνουμε ποτέ τέτοιου είδους πληροφορίες ηλεκτρονικά.
6. Ελέγχουμε τακτικά τους λογαριασμούς μας στο διαδίκτυο (τραπεζικούς, on line λογαριασμούς κλπ.) προκειμένου να έχουμε ανά πάσα στιγμή πλήρη εικόνα για αυτούς

Οι καταναλωτές που αντιμετωπίζουν οποιοδήποτε πρόβλημα τέτοιου είδους ή έχουν πέσει θύμα phishing, μπορούν να επικοινωνούν με την Ένωση Εργαζομένων Καταναλωτών Ελλάδας για περαιτέρω συμβουλές και οδηγίες στα ακόλουθα στοιχεία επικοινωνίας:

- **Tel:** 210-8817730
- **Web:** www.eeke.gr
- **e-mail:** info@eeke.gr
- **fb:** www.facebook.com/enosikatanaloton/

Μοιράσου το: