

Ηλεκτρονικό Ψάρεμα

Μάθε να αναγνωρίζεις το Phishing!



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης

Τι είναι το Phishing;

Το phishing αποτελεί μία από τις πλέον διαδεδομένες και επιβλαβείς μορφές διαδικτυακής απάτης. Πρόκειται για την προσπάθεια εξαπάτησης χρηστών, ώστε να αποκαλύψουν ευαίσθητες πληροφορίες — όπως κωδικούς πρόσβασης, αριθμούς τραπεζικών λογαριασμών, πιστωτικών καρτών ή ακόμα και προσωπικά δεδομένα (ΑΦΜ, διευθύνσεις, στοιχεία ταυτότητας).

Η λέξη phishing προέρχεται από το αγγλικό fishing (ψάρεμα) – οι επιτήδριοι «ρίχνουν το δόλωμα» ελπίζοντας ότι κάποιος θα «τσιπήσει». Το δόλωμα μπορεί να είναι ένα μήνυμα ηλεκτρονικού ταχυδρομείου, ένα SMS, μια τηλεφωνική κλήση ή ακόμη και ένα QR code.

Οι κυβερνοεγκληματίες εκμεταλλεύονται τη φυσική περιέργεια και την εμπιστοσύνη των ανθρώπων, καθώς και την έλλειψη χρόνου ή προσοχής. Συνήθως παριστάνουν ότι εκπροσωπούν γνωστές εταιρείες, τράπεζες, υπηρεσίες courier ή δημόσιους οργανισμούς, ζητώντας να «επιβεβαιώσεις» τα στοιχεία σου ή να «ενημερώσεις» το λογαριασμό σου.

60% των κυβερνοεπιθέσεων ξεκινούν με phishing, σύμφωνα με στοιχεία του ENISA (Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας).



Πώς λειτουργεί;

1. Ο αποστολέας στέλνει ένα παραπλανητικό μήνυμα που φαίνεται αληθινό, χρησιμοποιώντας λογότυπα, ύφος και σχεδιασμό που μιμούνται τον πραγματικό οργανισμό.
2. Το μήνυμα σε ωθεί να ενεργήσεις γρήγορα («ο λογαριασμός σου κινδυνεύει», «έχεις απλήρωτο υπόλοιπο», «κέρδισες ένα δώρο»).
3. Ο σύνδεσμος οδηγεί σε ψεύτικη ιστοσελίδα, πανομοιότυπη με την κανονική.
4. Μόλις εισαγάγεις τα στοιχεία σου, αυτά αποστέλλονται στους δράστες, που μπορούν να τα χρησιμοποιήσουν για κλοπή χρημάτων, πρόσβαση σε λογαριασμούς ή παραβίαση εταιρικών δεδομένων.

Τι μπορεί να συμβεί;

Μια επίθεση phishing μπορεί να έχει σοβαρές συνέπειες:

- ➡ Κλοπή χρημάτων ή οικονομική απώλεια.
- ➡ Παραβίαση επαγγελματικών λογαριασμών.
- ➡ Διαρροή προσωπικών ή εταιρικών δεδομένων.
- ➡ Κακόβουλη χρήση των στοιχείων σου για άλλες απάτες.

Η πρόληψη είναι η καλύτερη άμυνα: ενημέρωση, επαγρύπνηση και σκέψη πριν από κάθε κλικ.



Μορφές Phishing

Οι κυβερνοεγκληματίες χρησιμοποιούν πολλές διαφορετικές μεθόδους για να «ψαρέψουν» τα δεδομένα μας. Κάθε μορφή έχει τον δικό της τρόπο δράσης, αλλά όλες μοιράζονται τον ίδιο στόχο: να σε πείσουν να αποκαλύψεις πληροφορίες ή να εγκαταστήσεις κακόβουλο λογισμικό.

Email phishing: Αποστολή ψεύτικων emails που μιμούνται γνωστούς οργανισμούς και περιέχουν κακόβουλους συνδέσμους.

Smishing: Παραπλανητικά μηνύματα SMS που οδηγούν σε ψεύτικες ιστοσελίδες ή ζητούν προσωπικά στοιχεία.

Vishing: Τηλεφωνικές κλήσεις από άτομα που προσποιούνται υπαλλήλους τραπεζών ή αρχών για να αποσπάσουν πληροφορίες.

Quishing: Χρήση QR codes που οδηγούν σε κακόβουλες σελίδες ή ενεργοποιούν εγκατάσταση λογισμικού.

Spear phishing: Στοχευμένες επιθέσεις με εξατομικευμένα μηνύματα που μοιάζουν απολύτως πειστικά.

Whaling: Εξειδικευμένες επιθέσεις εναντίον ανώτερων στελεχών ή διοικητικών υπευθύνων.

BEC (Business Email Compromise): Πλαστογράφηση εταιρικών emails για την υποκλοπή χρημάτων ή δεδομένων.

AI-based scams: Απάτες που αξιοποιούν τεχνητή νοημοσύνη ή deepfakes για ρεαλιστικά και δύσκολα ανιχνεύσιμα επιβλαβή μηνύματα.

Πριν ανοίξεις έναν σύνδεσμο ή ένα συνημμένο αρχείο, σκέψου δύο φορές
— ακόμα κι αν φαίνεται να προέρχεται από γνωστή πηγή.

Η κυβερνοασφάλεια ξεκινά από ένα απλό βήμα: μην κάνεις κλικ αν δεν είσαι σίγουρος!

Πώς να αναγνωρίσετε ένα μήνυμα phishing

Σκεφτείτε πριν κάνετε κλικ!

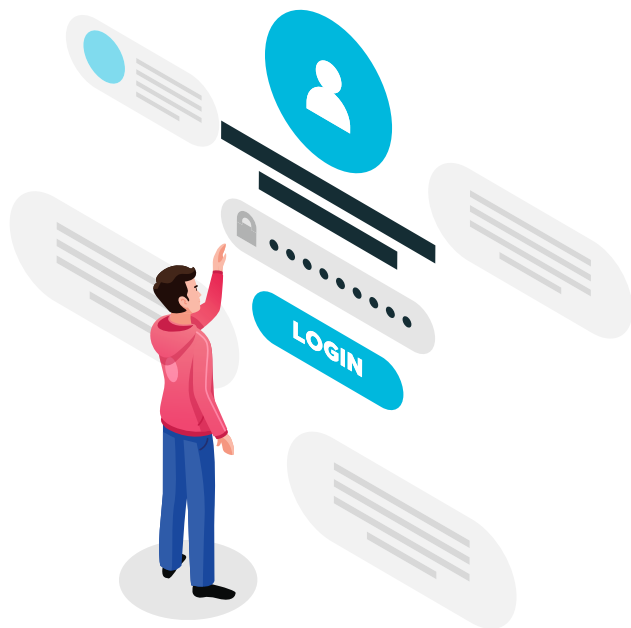
Τα ψεύτικα μηνύματα συχνά έχουν κοινά χαρακτηριστικά:

- ➡ Επείγουσα ή απειλητική γλώσσα («Ο λογαριασμός σας θα απενεργοποιηθεί άμεσα!»).
- ➡ Ορθογραφικά ή συντακτικά λάθη.
- ➡ Ύποπτοι σύνδεσμοι ή επισυναπτόμενα αρχεία.
- ➡ Αποστολέας με ύποπτη διεύθυνση email.
- ➡ Αιτήματα για προσωπικά δεδομένα ή πληρωμές.

Αν πέσετε θύμα phishing...

Αν πιστεύετε ότι έχετε αποκαλύψει προσωπικά στοιχεία:

- ➡ Αλλάξτε άμεσα τους κωδικούς πρόσβασης.
- ➡ Επικοινωνήστε με την τράπεζά σας ή τον πάροχο υπηρεσίας.
- ➡ Ενημερώστε τη Δίωξη Ηλεκτρονικού Εγκλήματος (cyberalert.gr).
- ➡ Κάντε καταγγελία στην Ανοιχτή Γραμμή Παράνομου Περιεχομένου στο Διαδίκτυο, [Safeline.gr](https://safeline.gr).
- ➡ Μάθετε περισσότερα στο [Saferinternet4kids.gr](https://saferinternet4kids.gr).





**Μην κάνετε ποτέ κλικ σε
συνδέσμους ή QR codes από
άγνωστες ή μη επαληθευμένες
πηγές. Αν έχετε αμφιβολία,
επικοινωνήστε απευθείας με τον
οργανισμό μέσω των επίσημων
καναλιών του.**



SaferInternet4Kids.gr
ΓΙΑ ΕΝΑ ΑΣΦΑΛΕΣΤΕΡΟ ΔΙΑΔΙΚΤΥΟ



ITE

ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης

«Την αποκλειστική ευθύνη της παρούσας έκδοσης φέρει ο συγγραφέας της. Η Ευρωπαϊκή Ένωση δεν φέρει καμία ευθύνη για οποιαδήποτε χρήση των περιεχομένων σ' αυτήν πληροφοριών.»