



**Τα εργαλεία AI
αλλάζουν το παιχνίδι
των εισβολέων.**

Είσαι έτοιμοι;



Προηγουμένως...

Οι ιδιαίτερα παραπλανητικές επιθέσεις απαιτούσαν πολύ χρόνο και κόπο και μπορούσαν να δημιουργηθούν από ικανούς εισβολείς.

Ως εκ τούτου, **οι περισσότερες προσπάθειες ηλεκτρονικού ψαρέματος ήταν χαμηλού επιπέδου** (π.χ., με ορθογραφικά λάθη, ύποπτο σχεδιασμό, λανθασμένη γλώσσα, κτλ), επομένως ήταν εύκολο να εντοπίσεις την απάτη.



Σήμερα...

Τα εργαλεία AI επιτρέπουν στους εισβολείς να δημιουργήσουν ιδιαιτέρως επαγγελματικά email και περιεχόμενο γρήγορα και εύκολα.

Γι' αυτό το λόγο, στα εισερχόμενα μηνύματά μας αρχίζουμε να βλέπουμε όλο και πιο πολύπλοκες επιθέσεις. Αυτές οι πολύ παραπλανητικές επιθέσεις είναι δυσκολότερο να εντοπιστούν ως απειλές, αυξάνοντας το ρίσκο να πέσουμε θύματά τους.

Πώς μπορείτε να εντοπίσετε σήμερα το ηλεκτρονικό ψάρεμα;

- Στα email, επιβεβαιώστε ότι η **διεύθυνση του αποστολέα** εμφανίζεται ακριβώς όπως θα την περιμένατε. Οι εισβολείς δεν μπορούν να αντιγράψουν αυτή τη λεπτομέρεια.
- Κάντε κατάδειξη με το ποντίκι πάνω σε **συνδέσμους** πριν πατήσετε πάνω τους για να επαληθεύσετε ότι είναι έγκυροι. Οι εισβολείς μπορούν να μιμηθούν τον σχεδιασμό γνωστών εταιριών, αλλά δεν μπορούν να χρησιμοποιήσουν τον γνήσιο domain τους.



Τι δεν αποτελεί πλέον αξιόπιστο σημάδι αυθεντικότητας;

- Επαγγελματίες σχεδιασμός
- Καλογραμμένο κείμενο
- Ηχογραφημένη φωνή γνωστού σας προσώπου
- Βίντεο υψηλής ποιότητας

Μην ξεχάσετε: Η ασφάλειά μας βρίσκεται στα χέρια μας.

Να σας γίνει συνήθεια να ελέγχετε κάθε email πριν πατήσετε πάνω σε οποιονδήποτε σύνδεσμο και να μην ελέγχετε ποτέ email όταν είστε αφηρημένοι.

