Κάρτα Phishing

Πώς αναγνωρίζω ένα ύποπτο μήνυμα — και τι κάνω

7 σημάδια ότι ένα μήνυμα είναι ύποπτο

- Ο αποστολέας δεν είναι αυτός που δηλώνει — ελέγξτε το πραγματικό domain (π.χ. «aade-gov-gr.com» αντί για «aade.gr»).
- Επείγον ή απειλή: «λήγει σε 24 ώρες», «ο λογαριασμός θα κλειδωθεί».
- Ζητά κωδικό, στοιχεία κάρτας ή σύνδεση μέσω συνδέσμου.
- Γενικός χαιρετισμός («Αγαπητέ χρήστη») αντί για το όνομά σας.
- Σύνδεσμος που οδηγεί αλλού απ' ό,τι γράφει — σταθείτε με τον δείκτη πάνω του πριν κλικάρετε.
- Απρόσμενο συνημμένο ή αίτημα εκτός διαδικασίας (π.χ. «ο διοικητής» ζητά πληρωμή από προσωπικό email).
- Περίεργη διατύπωση ή ορθογραφικά, και σύνδεση «http» αντί για «https».

ΝΑ κάνετε	ΝΑ ΜΗΝ κάνετε
• Σταθείτε με τον δείκτη πάνω στους συνδέσμους και ελέγξτε το domain. • Επαληθεύστε με άλλο κανάλι — τηλεφωνήστε στο γνωστό εσωτερικό. • Αναφέρετε το ύποπτο μήνυμα στην πληροφορική ή στον ΥΑΣΠΕ. • Σε αμφιβολία, μην κάνετε τίποτα και ρωτήστε.	• Μην κάνετε κλικ σε συνδέσμους/συνημμένα που δεν περιμένατε. • Μην δίνετε ποτέ κωδικό ή στοιχεία κάρτας μέσω email. • Μην απαντάτε στον αποστολέα «για επιβεβαίωση». • Μην συνδέετε άγνωστα USB.

Αν αμφιβάλλετε: ΜΗΝ κλικάρετε. Ανέφερετε αμέσως στην πληροφορική ή στον ΥΑΣΠΕ. Καλύτερα μία περιττή αναφορά, παρά μία παράβλεψη.

Γρήγορος έλεγχος πριν από κάθε κλικ

- Περίμενα αυτό το μήνυμα; Ξέρω τον αποστολέα;
- Μου ζητά κάτι επείγον, μυστικό ή οικονομικό;
- Ταιριάζει το domain του αποστολέα και του συνδέσμου;
- Αν όχι σε κάποιο — σταματώ και επαληθεύω.