ΑΠΑΤΗΛΑ ΜΗΝΥΜΑΤΑ SMS (SMISHING)

Ο όρος "smishing" (ένας συνδυασμός των λέξεων "SMS" και "Phishing") αναφέρεται στην προσπάθεια των απατεώνων να αποκτήσουν προσωπικές και οικονομικές πληροφορίες ή κωδικούς ασφαλείας μέσω μηνυμάτων SMS.

ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ;

Το μήνυμα κειμένου συνήθως θα σας ζητά να κάνετε κλικ σε έναν ηλεκτρονικό σύνδεσμο (link) ή να καλέσετε έναν αριθμό τηλεφώνου, προκειμένου να επαληθεύσετε, ενημερώσετε ή επανανεργοποιήσετε τον λογαριασμό σας. Αλλά...ο ηλεκτρονικός σύνδεσμος οδηγεί σε ψεύτικη ιστοσελίδα και ο αριθμός τηλεφώνου οδηγεί στον απατεώνα που ισχυρίζεται ότι εκπροσωπεί τη νόμιμη επιχείρηση.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

- Μην κάνετε κλικ σε ηλεκτρονικούς συνδέσμους (links), συνημμένα αρχεία ή εικόνες που λαμβάνετε με μηνύματα κειμένου (sms) δίχως να έχετε επαληθεύσει τον αποστολέα.
- Μην βιάζεστε. Πάρτε τον χρόνο σας και πραγματοποιήστε τους απαραίτητους ελέγχους προτού απαντήσετε.
- Ποτέ μην απαντάτε σε μήνυμα κειμένου (sms) που σας ζητά τον κωδικό "PIN" ή τον κωδικό πρόσβασης ("password") στον τραπεζικό σας λογαριασμό ή οποιαδήποτε άλλα εξατομικευμένα διαπιστευτήρια ασφαλείας (π.χ. e-banking user name).
- Εάν νομίζετε ότι ενδέχεται να έχετε απαντήσει σε ένα απατηλό μήνυμα κειμένου (sms) και παρείχατε τα στοιχεία των τραπεζικών σας λογαριασμών, επικοινωνήστε αμέσως με την τράπεζα συνεργασίας σας.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ | 90 YEARS 1928-2018 HELLENIC BANK ASSOCIATION

#CyberScams