Πώς να αναγνωρίσεις τις διαδικτυακές απάτες

EUROPEAN CYBER SECURITY MONTH

Λαμβάνεις ένα SMS από το δράστη Γιώργο, ο οποίος υποδύεται ότι εργάζεται στην τράπεζα συνεργασίας σου. Κάνεις κλικ στον ηλεκτρονικό σύνδεσμο του SMS.

Ανακατευθύνεσαι σε ιστοσελίδα που μοιάζει με εκείνη της τράπεζας συνεργασίας σου. Εισάγεις τα διαπιστευτήρια ασφαλείας σου (user name & password).

Ο δράστης Γιώργος πλέον έχει πρόσβαση στα οικονομικά σου στοιχεία και στο ιστορικό των πρόσφατων ηλεκτρονικών σου συναλλαγών.

Σου τηλεφωνεί υποδυόμενος τον τραπεζικό υπάλληλο και παραθέτει τα στοιχεία σου.

Ο δράστης Γιώργος σε πείθει να προχωρήσεις στη μεταφορά χρημάτων σε άλλο τραπεζικό λογαριασμό τον οποίο ελέγχει ο ίδιος.

Προστατεύσου από τις διαδικτυακές απάτες!

1. Προσοχή σε ανεπιθύμητα μηνύματα κειμένου ή μηνύματα ηλεκτρονικού ταχυδρομείου που ισχυρίζονται ότι προέρχονται από την τράπεζα συνεργασίας σου.
2. Εάν περιέχουν ηλεκτρονικούς συνδέσμους (links) και συνημμένα αρχεία, μην τα ανοίξεις.
3. Εάν λάβεις μια ύποπτη κλήση από την τράπεζα με την οποία συνεργάζεσαι, κλείσε το τηλέφωνο και επαλήθευσέ την κλήση καλώντας το τμήμα εξυπηρέτησης πελατών της τράπεζας.
4. Ποτέ μην κοινοποιείς τα διαπιστευτήρια ασφαλείας σου (user name & password) ή τους κωδικούς για την εκτέλεση συναλλαγής πληρωμής (π.χ. SMS OTP).
5. Εάν νομίζεις ότι έχεις πέσει θύμα απάτης, επικοινώνησε αμέσως με την τράπεζα συνεργασίας σου και ανέφερε το σχετικό περιστατικό στην αστυνομία.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ · ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ