

Covid-19: Προστατέψτε τα χρήματά σας

Αγαπητέ πελάτη,

Σε μια περίοδο που η χρήση των ψηφιακών μας δικτύων είναι απολύτως απαραίτητη για εσάς, θέλουμε να σας διαβεβαιώσουμε ότι προτεραιότητά μας είναι η ασφάλεια των ηλεκτρονικών σας συναλλαγών.

Δυστυχώς, κάποιοι χρησιμοποιούν το ξέσπασμα του Κορωνοϊού ως ευκαιρία εξαπάτησης του κοινού. Για παράδειγμα μπορεί να προσφέρουν ιατρικά προϊόντα ή να προτείνουν οδηγίες για «ασφαλές καταφύγιο» χρημάτων.

Για αυτό θα θέλαμε να σας δώσουμε επικαιροποιημένες πληροφορίες για τις συνήθεις τακτικές ηλεκτρονικής απάτης και κάποιες βασικές πληροφορίες και τι μπορείτε να κάνετε για να προστατευτείτε.

Τι επιδιώκουν οι επιτιήδαιοι;

- να «μολύνουν» τη συσκευή σας (υπολογιστή ή κινητό) με κακόβουλο λογισμικό (malware) και να υποκλέψουν την ταυτότητά σας
- να σας στείλουν ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου (spam emails) ή μηνύματα που σχετίζονται με απάτες (scam emails)
- να σας οδηγήσουν σε «ψεύτικους» ιστότοπους και να αποσπάσουν προσωπικές σας πληροφορίες
- να παραβιάσουν το ασύρματο δίκτυό σας για να εντοπίσουν δεδομένα σας όπως ονόματα χρήστη και κωδικούς
- να πάρουν τον έλεγχο του υπολογιστή σας για να επιτεθούν σε υπολογιστές άλλων χρηστών.

Ποιες είναι οι τακτικές που χρησιμοποιούνται πιο συχνά;

Οι επιτιήδαιοι χρησιμοποιούν παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου (phishing emails), τηλεφωνήματα (vishing) ή γραπτά μηνύματα (smishing). Με αυτά επιδιώκουν να αποσπάσουν πληροφορίες από τα υποψήφια θύματά τους ή να τα οδηγήσουν στο να ακολουθήσουν έναν υπερσύνδεσμο (link) σε ιστοσελίδα, η οποία φαίνεται αξιόπιστη.

Συμβουλές και οδηγίες για ασφαλείς συναλλαγές

Η HSBC:

- δεν θα σας ζητήσει ποτέ και με κανένα τρόπο το όνομα χρήστη και τους κωδικούς σας
- δεν θα στείλει ποτέ κάποιον εκπρόσωπό της σπίτι σας για να παραλάβει μετρητά, κάρτες ή οτιδήποτε άλλο.

Αποφύγετε να:

- απαντάτε σε e-mails που σας ζητούν προσωπικά σας στοιχεία, διαγράψτε τα αμέσως
- ακολουθείτε υπερσυνδέσμους (links) που σας έχουν σταλεί μέσω e-mail ή δημοσιεύονται σε μέσα κοινωνικής δικτύωσης, ιστοσελίδες άλλων εταιρειών, μηχανών αναζήτησης, κλπ.
- προβαίνετε σε κάποια πληρωμή όταν λαμβάνετε e-mails από συνεργάτες σας, στα οποία σας δίνονται διαφορετικοί από τους συνηθισμένους Τραπεζικούς λογαριασμούς. Πάντα να επιβεβαιώνετε τα στοιχεία πληρωμών με τους συνεργάτες σας προηγουμένως
- εμπιστεύεστε επικοινωνίες που δεν προέρχονται από τα επίσημα κανάλια της Τράπεζας και πάντα να διασταυρώνετε τυχόν προσφορές για δάνεια, κάρτες κλπ.

Βεβαιωθείτε ότι:

- οι μυστικοί σας κωδικοί είναι σύνθετοι και δεν τους μοιράζετε με τρίτους
- χρησιμοποιείτε πάντα τις πιο ενημερωμένες εκδόσεις Internet browsers, οι οποίοι πληρούν προηγμένο σχεδιασμό ασφαλείας
- ο Internet browser που χρησιμοποιείτε δεν αποθηκεύει αυτόματα κωδικούς User ID & Passwords σε ιστοσελίδες που επισκέπτεστε (εμπόρων, Τραπεζών, κοινωνικής δικτύωσης, κλπ)

Πώς μπορώ να αναφέρω στην HSBC πιθανή απόπειρα εξαπάτησης

Σε περίπτωση που υποπτεύεστε απόπειρα κακόβουλης επίθεσης ή απάτη παρακαλώ ενημερώστε την HSBC στο τηλέφωνο 210-6962190, 24 ώρες την ημέρα, καθημερινές και αργίες, ή ηλεκτρονικά με e-mail στο [**phonebanking.requests-gr@hsbc.com**](mailto:phonebanking.requests-gr@hsbc.com)

Με εκτίμηση,

Στέλιος Πιρπινιάς,

Head of Wealth Management & Personal Banking (WPB)
HSBC Continental Europe, Greece