

24 Οκτωβρίου 2021

Δείτε πώς απατεώνες κλέβουν κωδικούς τραπεζικών λογαριασμών με email και SMS

Επιστήμες, Τέχνες & Πολιτισμός / Οικονομία & εξ-οικονομώ



Email προς τους πελάτες της έστειλε η τράπεζα Eurobank για να τους προειδοποιήσει για τις τεχνικές που εφαρμόζουν απατεώνες στο Διαδίκτυο, όταν επιχειρούν να υποκλέψουν κωδικούς και στοιχεία, στοχεύοντας σε πιστωτικές κάρτες και τραπεζικούς λογαριασμούς.



«Οι τρέχουσες συνθήκες έχουν δημιουργήσει πρόσφορο έδαφος για τους απατεώνες του διαδικτύου. Εκμεταλλούνται την αυξημένη χρήση ηλεκτρονικών υπηρεσιών για να εξαπατούν, να διαδίδουν κακόβουλο λογισμικό και να υποκλέπτουν ευαίσθητα στοιχεία ή κωδικούς με email, SMS, μηνύματα στα κοινωνικά μέσα και άλλα τεχνάσματα phishing» εξηγεί η τράπεζα.

Ποιες είναι οι τακτικές των απατεώνων του διαδικτύου:

-Απατηλά μηνύματα με email και SMS (phishing ή ηλεκτρονικό ψάρεμα)

Οι απατεώνες στέλνουν απατηλά email ή SMS προσποιούμενοι ότι αποστολέας είναι η τράπεζα των παραληπτών. Σε αυτά τα μηνύματα συνήθως αναφέρουν ότι «έχει παρατηρηθεί ύποπτη δραστηριότητα» στον λογαριασμό ή την κάρτα του αποδέκτη ή ότι «έχει κλειδωθεί ή απενεργοποιηθεί» ο λογαριασμός ή η κάρτα του.

Τα μηνύματα δίνουν κάποιον σύνδεσμο και προτρέπουν τους αποδέκτες να ακολουθήσουν αμέσως τις οδηγίες σε αυτόν για να λυθεί το πρόβλημά τους.

Ωστόσο, ο σύνδεσμος οδηγεί σε απατηλή ιστοσελίδα πανομοιότυπη με αυτήν της

τράπεζας των παραληπτών. Οι παραλήπτες δεν αντιλαμβάνονται τη διαφορά κι έτσι συμπληρώνουν κωδικούς e-Banking, Κωδικούς μιας Χρήσης (OTP) και άλλα στοιχεία τους.

-Εξαπάτηση μέσω αγγελιών για αγορά ή πώληση προϊόντων

Οι απατεώνες τηλεφωνούν προφασιζόμενοι ότι ενδιαφέρονται να αγοράσουν το προϊόν για το οποίο κάποιος έχει αναρτήσει αγγελία (συνήθως διαδικτυακά). Ζητούν από τον πωλητή να τους δώσει στοιχεία κάρτας ή κωδικούς e-Banking και Κωδικό μιας Χρήσης (OTP) που λαμβάνει εκείνη τη στιγμή στο κινητό του ώστε δήθεν να καταθέσουν τα χρήματα.

-Εξαπάτηση για διαμεσολάβηση στη μεταφορά παράνομου χρήματος (money muling)

Οι απατεώνες ζητούν από κάποιο άτομο να μεσολαβήσει στη μεταφορά χρημάτων και προσφέρουν αμοιβή για να γίνει κατάθεση χρημάτων σε λογαριασμό του. Στη συνέχεια, ζητούν από το θύμα είτε να τους δώσει τα χρήματα κάνοντας ανάληψη από κάποιο ATM ή κατάστημα είτε να τα μεταφέρει σε λογαριασμό άλλου ατόμου.

-Εξαπάτηση με πρόφαση επιδιόρθωση υπολογιστή

Οι απατεώνες τηλεφωνούν, συνήθως από το εξωτερικό, και υποδύονται τεχνικούς από μεγάλη εταιρεία πληροφορικής. Αρκετές φορές η συνομιλία γίνεται στα Αγγλικά. Ισχυρίζονται στον αποδέκτη ότι ο υπολογιστής ή η φορητή συσκευή του έχει μολυνθεί από κακόβουλο λογισμικό και ζητούν να εγκαταστήσουν λογισμικό απομακρυσμένης πρόσβασης για να επιδιορθώσουν το πρόβλημα.

-Επενδυτικές απάτες

Οι απατεώνες επικοινωνούν κυρίως μέσω τηλεφώνου με ανυποψίαστους πολίτες, υποδύμενοι εργαζομένους από μεγάλες επενδυτικές εταιρείες του εξωτερικού και μιλώντας σε άπταιστα Ελληνικά. Υπόσχονται υψηλές αποδόσεις με το άνοιγμα λογαριασμού σε διαδικτυακές επενδυτικές πλατφόρμες. Ωστόσο, αυτές οι πλατφόρμες είναι εικονικές. Οι περισσότεροι από όσους έχουν εξαπατηθεί αναφέρουν ότι όταν ζητούσαν να τους αποδοθούν τα κέρδη τους, διαπίστωναν ότι είχαν πέσει θύματα απάτης.

-Απατηλές εντολές πληρωμής με email

Οι απατεώνες αποκτούν μη εξουσιοδοτημένη πρόσβαση στην ηλεκτρονική αλληλογραφία ανάμεσα σε επαγγελματίες ή εμπόρους που συναλλάσσονται με επιχειρήσεις, είτε ως προμηθευτές είτε ως πελάτες. Παρεμβαίνουν σε αυτήν την

αλληλογραφία και προτρέπουν τους συναλλασσόμενους να καταθέσουν χρήματα σε απατηλούς τραπεζικούς λογαριασμούς, διαφορετικούς από αυτούς που είχαν συμφωνηθεί αρχικά.

Πώς να προστατευτείτε

-Να είστε ιδιαίτερα επιφυλακτικοί με μηνύματα που σας ενημερώνουν για δήθεν προβλήματα με λογαριασμούς, κάρτες ή το e-Banking σας.

-Μην αποκαλύπτετε σε κανέναν και για κανέναν λόγο κωδικούς σύνδεσης για το e-Banking, Κωδικούς μιας Χρήσης (OTP) που λαμβάνετε με μήνυμα στο κινητό σας (SMS, Viber), στοιχεία καρτών σας, καθώς και προσωπικά και οικονομικά στοιχεία σας, ακόμη και με πρόφαση ότι έτσι θα σας καταθέσουν χρήματα. Για κατάθεση χρημάτων, αρκεί να δώσετε τον IBAN του λογαριασμού σας.

-Μη δέχεστε να μεσολαβήσετε ως ενδιάμεσοι σε διακίνηση χρημάτων από άλλα άτομα, συνήθως άγνωστα σε εσάς. Μπορεί να υποστείτε σημαντικές επιπτώσεις, καθώς με αυτόν τον τρόπο εμπλέκεστε σε παράνομες ενέργειες, είτε το γνωρίζετε είτε όχι.

-Διακόψτε την κλήση εάν κάποιος σας καλεί από άγνωστο αριθμό, ειδικά από το εξωτερικό, και ισχυρίζεται ότι είναι από οποιαδήποτε εταιρεία πληροφορικής, χωρίς εσείς να έχετε δηλώσει βλάβη σε συσκευή σας.

-Ελέγξτε εάν μια διαδικτυακή επενδυτική πλατφόρμα είναι αδειοδοτημένη από κάποια υπαρκτή και αρμόδια εποπτική αρχή πριν ανοίξετε λογαριασμό σε αυτή.

-Διασταυρώστε τον αριθμό λογαριασμού με τον προμηθευτή ή τον πελάτη σας με τον οποίο συναλλάσσετε πριν κάνετε οποιαδήποτε πληρωμή.

Πηγή: iellada.gr