



Νέα κομπίνα έχουν σκαρφιστεί επιτήδριοι για να αποσπά-σουν στοιχεία από κάρτες από εναλλακτικές τράπεζες, και να αποσπάσουν τα χρήματα του λογαριασμού. ...

«Όλες οι κάρτες απενεργοποιούνται προσωρινά για διαδικτυακές πληρωμές μέχρι να εγγραφείτε στα αναβαθμισμένα μέτρα ασφαλείας. Για να το ενεργοποιήσετε, ακολουθήστε τα ακόλουθα απλά βήματα».

Αυτό είναι ένα από τα μηνύματα που λαμβάνει μία ομάδα χρηστών των εναλλακτικών ψηφιακών τραπεζικών δικτύων που σε καμία περίπτωση δεν θα πρέπει να προχωρήσουν στην ενεργοποίηση του και στην παροχή προσωπικών στοιχείων τους, καθώς πρόκειται για κλασική μορφή της απάτης του «ηλεκτρονικού ψαρέματος».

Όπως έχουν επισημάνει σε δημόσιες παρεμβάσεις αρμόδια τραπεζικά στελέχη, με την μεγάλη αύξηση της χρήσης των ψηφιακών δικτύων η προληπτική ενημέρωση για τα θέματα ασφαλείας είναι απαραίτητη, ώστε οι καταναλωτές να μην πέφτουν θύματα επίδοξων απατεώνων. Μια από τις απάτες που γνωρίζει έξαρση είναι το «ηλεκτρονικό ψάρεμα» στοιχείων (phishing), μια μορφή απάτης που μέσω emails ή sms που στέλνονται στους καταναλωτές έχει ως στόχο την υποκλοπή των προσωπικών δεδομένων του ατόμου.

Παριστάνουν οργανισμούς, εταιρείες, τράπεζες

Τα μηνύματα αυτά, όπως αναφέρεται στο blog της Τράπεζας Πειραιώς, περιέχουν παραπλανητικό περιεχόμενο και οι αποστολές τους υποδύονται την ταυτότητα ενός νόμιμου οργανισμού/εταιρίας/τράπεζας.

Στόχο έχουν να αποσπάσουν απόρρητα προσωπικά και οικονομικά δεδομένα όπως, το όνομα του χρήστη ηλεκτρονικής τραπεζικής, κωδικούς πρόσβασης, στοιχεία χρεωστικών / πιστωτικών καρτών κ.ο.κ. Στη συνέχεια, τα δεδομένα αυτά μπορούν να χρησιμοποιηθούν για την πραγματοποίηση μη εξουσιοδοτημένων οικονομικών

συναλλαγών με αποτέλεσμα την πρόκληση οικονομικής ζημίας. Η πλειοψηφία των phishing μηνυμάτων επικαλείται είτε κάποιο πρόβλημα στον λογαριασμό του χρήστη, είτε απαιτεί την επιβεβαίωσή του για εκτέλεση συναλλαγής (η οποία δεν έχει λάβει επίσημη εντολή από τον χρήστη), είτε ενέργεια αναβάθμισης υπηρεσίας, είτε επιβεβαίωση προσωπικών δεδομένων.

Όσον αφορά στον τρόπο που υποκλέπτονται τα στοιχεία των καταναλωτών, συνήθως πρακτική αποτελεί η υποκλοπή τους μέσω email ή sms που αποστέλλονται και ζητούν από τον χρήστη/καταναλωτή να επισκεφθεί την ιστοσελίδα του Οργανισμού, επιλέγοντας έναν σύνδεσμο (link) που περιλαμβάνεται στο κείμενο. Σε περίπτωση που ο συναλλασσόμενος επιλέξει να επισκεφτεί τον σύνδεσμο θα παρατηρήσει ότι η σελίδα αυτή προσομοιάζει ή και αντιγράφει πλήρως οικεία ηλεκτρονικά περιβάλλοντα, όπως την ηλεκτρονική τραπεζική της τράπεζας του κάθε καταναλωτή. Ωστόσο, σε καμία περίπτωση το «ψεύτικο» περιβάλλον δεν αποτελεί επίσημη σελίδα του Οργανισμού που γνωρίζει.

Συστάσεις προς τους καταναλωτές

Για την ασφάλειά των καταναλωτών, όπως αναφέρεται στο ενημερωτικό σημείωμα, συστήνεται προς τους συναλλασσόμενους να μην επιλέξουν τον σύνδεσμο και δηλώσουν προσωπικά στοιχεία και κωδικούς, καθώς άμεσα οι επιτήδριοι θα προχωρήσουν σε συναλλαγές, προκαλώντας οικονομική ζημία (στον συναλλασσόμενο).

Ειδικότερα, όπως επισημαίνεται προς τους καταναλωτές, σε περίπτωση που λάβουν κάποιο ύποπτο email/sms, συστήνεται να μην εισέλθουν στο σύνδεσμο που προτρέπεται. Στη συνέχεια και για την ασφάλειά τους θα πρέπει να επικοινωνήσουν άμεσα με τον Οργανισμό. Μετά τη δήλωση του περιστατικού και ακολουθώντας τις οδηγίες εξουσιοδοτημένου αντιπροσώπου, θα πρέπει να διαγράψουν το email ή sms, που έχουν λάβει, χωρίς να το προωθήσουν σε κάποιον παρά μόνο σε αρμόδια υπηρεσία της τράπεζας τους, εφόσον ζητηθεί.

Όπως έχουν κατ' επανάληψη αναφέρει οι τράπεζες προς τους καταναλωτές, από πλευράς τραπεζών δεν θα τους ζητηθεί ποτέ και με κανέναν τρόπο οι κωδικοί πρόσβασης τους σε υπηρεσίες ηλεκτρονικής τραπεζικής, ή στοιχεία και κωδικοί καρτών, αλλά ούτε θα προβούν (οι τράπεζες) σε διαδικασία επικαιροποίησης -επαλήθευσης προσωπικών στοιχείων, γεγονός που αποκλείει κάθε πιθανότητα το email ή sms που λαμβάνουν να προέρχεται από την τράπεζα τους.