Πώς μπορώ να προστατεύσω τον εαυτό μου από «phishing»;

Η ProCredit Bank δεσμεύεται με μια σειρά μέτρων για την προστασία των online πληρωμών σας και για την διατήρηση της ακεραιότητας των δεδομένων στο τραπεζικό σας λογαριασμό. Για την επίτευξη του σκοπού αυτού χρησιμοποιούμε την τελευταία έκδοση του λογισμικού ασφάλειας και εφαρμόζουμε διάφορες διαδικασίες ασφάλειας. Παρόλα αυτά σας παρακαλούμε να έχετε υπόψη ότι το Internet και το ηλεκτρονικό σας ταχυδρομείο μπορούν να χρησιμοποιούνται ως μέσο παράνομων δραστηριοτήτων. Για τον λόγο αυτό σας συμβουλεύουμε να πάρετε κάποια απλά μέτρα ασφάλειας που θα κάνουν το Online Banking σας πιο ασφαλές.

Συμβουλές για αποφυγή του «phishing»

Τι είναι «phishing»;

Το «phishing» είναι προσπάθεια να μαζευτούν προσωπικές σας πληροφορίες μέσω αποστολής email. Τα μηνύματα συνήθως ισχυρίζονται ότι έχουν σταλεί από γνήσιες εταιρείες που αναπτύσσουν δραστηριότητα στο Internet, ο σκοπός τους όμως είναι να δελεάσουν τους πελάτες αυτών των εταιρειών να αποκαλύψουν πληροφορίες σε πλαστή ιστοσελίδα που χρησιμοποιείται από απατεώνες.

Ποιες πληροφορίες θα ζητήσουν από σας;

Τα email «phishing» συνήθως ισχυρίζονται ότι πρέπει να ανανεώσετε ή να επαληθεύσετε το προφίλ σας και σας προσκαλούν να κάνετε κλικ σε link από το μήνυμα που σας οδηγεί σε πλαστή ιστοσελίδα. Κάθε πληροφορία που εισάγεται στην ιστοσελίδα αυτή χρησιμοποιείται από εγκληματίες για απάτες.

Πώς να αποφύγουμε να γίνουμε θύματα phishing;

Πρέπει να είστε δύσπιστοι προς όλα τα μη ζητούμενα ή απροσδόκητα μηνύματα ηλεκτρονικού ταχυδρομείου που λαμβάνετε, ακόμα και όταν φαίνεται να προέρχονται από αξιόπιστη πηγή. Τα μηνύματα ηλεκτρονικού ταχυδρομείου στέλνονται με σκοπό να φτάσουν σε πραγματικές διευθύνσεις email που ανήκουν σε χρήστες με τραπεζικό λογαριασμό στο ίδρυμα που είναι και ο στόχος της απάτης και το αντικείμενο ενδιαφέροντος των απατεώνων.

Τι πρέπει να κάνετε, αν λάβετε email «phishing»;

Αν έχετε αμφιβολίες σχετικά με τη γνησιότητα κάποιου μηνύματος ηλεκτρονικού ταχυδρομείου που ισχυρίζεται ότι αποστάλθηκε από την ProCredit Bank, ενημερώστε μας αμέσως σε τηλέφωνο (+30) 801 100 71 71 και στείλτε το μήνυμα αυτό στη διεύθυνση: probanking@procreditbank.bg

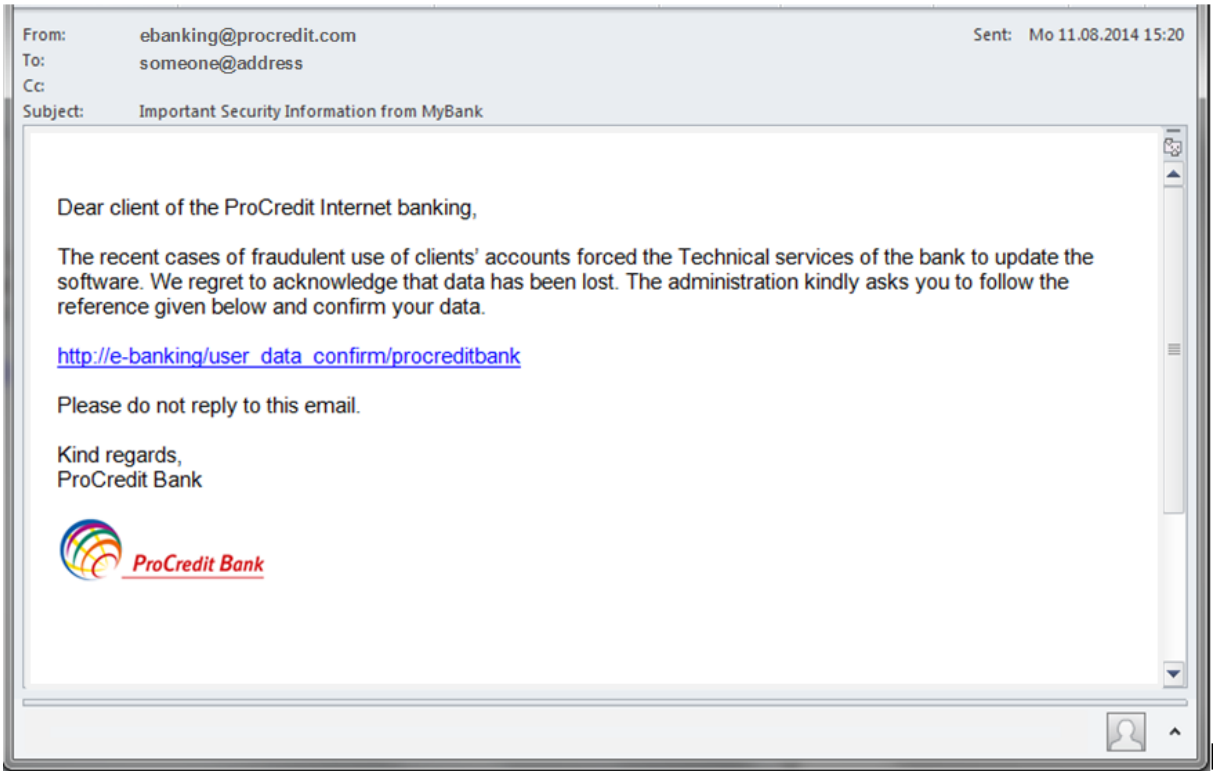
Για περισσότερες πληροφορίες επισκεφθείτε το ακόλουθο link:
http://www.staysafeonline.org/stay-safe-online/keep-a-clean-machine/spam-and-phishing

Πρόσθετες συμβουλές για online ασφάλεια

Πώς να ξεχωρίσω ένα «phishing» email;

Το μήνυμα «phishing» μπορεί να φαίνεται σαν να προέρχεται από τη διεύθυνση ηλεκτρονικού ταχυδρομείου της γνήσιας ProCredit Bank. Δυστυχώς, λόγω του τρόπου δημιουργίας του email, είναι πάρα πολύ εύκολο οι απατεώνες να δημιουργήσουν πλαστό αποστολέα στο πεδίο «Από: (From)» ή να αποκρύψουν τον πραγματικό αποστολέα.

Παράδειγμα για παραπλανητικό email μήνυμα



Παρόλο που η ProCredit Bank μπορεί να επικοινωνήσει μαζί σας μέσω email, το email αυτό δεν θα περιέχει ποτέ link σε κάποια ιστοσελίδα, η οποία να ζητήσει να εισάγετε προσωπικές πληροφορίες (κωδικό πρόσβασης, sms, TAN κ.α.)

Αν έχετε κάποιες αμφιβολίες σχετικά με τη γνησιότητα κάποιου μηνύματος ηλεκτρονικού ταχυδρομείου που ισχυρίζεται ότι αποστάλθηκε από την ProCredit Bank, ενημερώστε μας αμέσως σε τηλέφωνο (+30) 801 100 71 71 και στείλτε τα ύποπτα μηνύματα στη διεύθυνση: probanking@procreditbank.bg.