Πώς μπορώ να κάνω το Online Banking μου ασφαλές;

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 online ασφάλεια

Ξέρετε με ποιον έχετε να κάνετε;

Πάντα πρέπει να κάνετε είσοδο στην πύλη για Online Banking, εισάγοντας τη διεύθυνση Διαδικτύου της Τράπεζας στο πεδίο του Browser σας **https://probanking.procreditbank.gr/**.

Ποτέ δεν πρέπει να επισκέπτεστε ιστοσελίδα και να εισάγετε τα προσωπικά σας δεδομένα, χρησιμοποιώντας link από email. Αν έχετε αμφιβολίες, επικοινωνήστε με την ProCredit Bank σε: **(+30) 801 100 71 71**.

Φυλάξτε τους κωδικούς σας πρόσβασης

Πρέπει να είστε πάντα προσεκτικοί με μη εξουσιοδοτημένα μηνύματα ηλεκτρονικού ταχυδρομείου ή με τηλεφωνήματα που θέλουν από σας να αποκαλύψετε προσωπικές πληροφορίες ή τους αριθμούς των τραπεζικών σας καρτών. Η ProCredit Bank ή η αστυνομία ποτέ δεν θα επικοινωνούσαν με σας για να ζητήσουν να τους δώσετε προσωπικά σας δεδομένα ή να αποκαλύψετε πληροφορίες για τους κωδικούς πρόσβασης που χρησιμοποιείτε. Κρατήστε μυστικές αυτές τις πληροφορίες. Πρέπει να είστε προσεκτικοί, όταν δίνετε τα προσωπικά σας δεδομένα σε κάποιον, ιδιαίτερα αν δεν τον γνωρίζετε.

Φροντίστε για την ασφάλεια τον υπολογιστή σας

Χρησιμοποιείτε τις τελευταίες εκδόσεις λογισμικού προστασίας από ιούς και προσωπικά τείχη προστασίας (firewall). Χρησιμοποιείτε πάντα την τελευταία έκδοση του Browser σας, η οποία έχει όλες τις τρέχουσες ενημερώσεις κατά τη στιγμή. Πρέπει να είστε ιδιαίτερα προσεκτικοί, αν χρησιμοποιείτε το Διαδίκτυο σε δημόσιους χώρους – σε καφετέριες, βιβλιοθήκες ή σε οποιονδήποτε ξένο υπολογιστή, πάνω στο οποίο δεν έχετε έλεγχο.

Φυλάξτε τα χρήματά σας!

Μην ξεγελιέστε από email μηνύματα που φαίνονται ειλικρινά και που σας προτείνουν τη δυνατότητα να κερδίσετε κάποια εύκολα χρήματα. Αυτό που φαίνεται πάρα πολύ καλό είναι πολύ πιθανό να μην είναι αλήθεια. Πρέπει να είστε ιδιαίτερα προσεκτικοί με email μηνύματα από άλλα κράτη, επειδή είναι πολύ πιο δύσκολο να ελέγξετε αν στάλθηκαν από τους ανθρώπους που παρουσιάζονται ως αποστολείς τους.

Για περισσότερες πληροφορίες μπορείτε να επισκεφτείτε εξειδικευμένες ιστοσελίδες όπως:

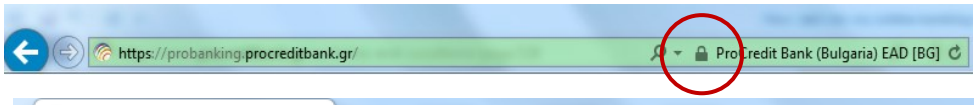
http://www.staysafeonline.org/stay-safe-online

Πρόσθετες συμβουλές για online ασφάλεια

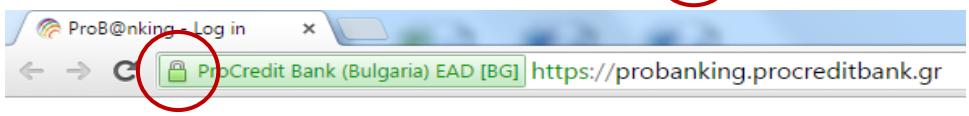
Ξέρετε με ποιον έχετε να κάνετε

- Πάντα χρησιμοποιείτε την **ασφαλή υπηρεσία της ProCredit Bank για e-banking**. Πριν μπείτε στην ιστοσελίδα της Τράπεζας, ελέγξτε αν υπάρχει κλειδωμένο λουκέτο ή ολόκληρο κλειδί κάτω δεξιά στο παράθυρο του Browser σας. Η αρχική καταγραφή της διεύθυνσης Διαδικτύου της Τράπεζας θα αλλάξει από “http” σε “https”, όταν πραγματοποιηθεί ασφαλής σύνδεση.
- Μπορείτε να ελέγξετε το Πιστοποιητικό Ασφάλειας της ιστοσελίδας της ProCredit Bank, πατώντας το λουκέτο που εμφανίζεται στο browser σας.

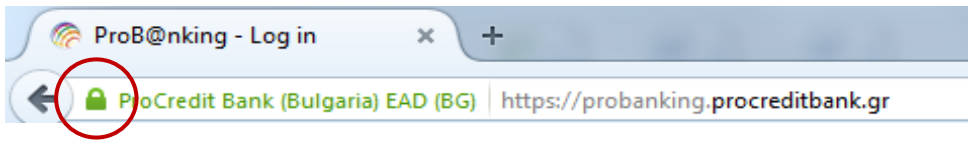
Internet Explorer:



Chrome:



Firefox:



Φυλάξτε τον κωδικό σας πρόσβασης

- Πάντα θυμάστε τους κωδικούς σας πρόσβασης ή άλλες πληροφορίες σχετικά με την ασφάλειά σας και καταστρέφετε το συντομότερο δυνατόν τα έγγραφα που περιέχουν τέτοιες πληροφορίες.
- Πρέπει να είστε υπεύθυνοι κατά την διατήρηση της εμπιστευτικότητας του κωδικού σας πρόσβασης ή άλλων πληροφοριών που έχουν σχέση με την ασφάλειά σας – μην τα αποκαλύπτετε ποτέ σε μέλη της οικογένειας, σε φίλους και άλλους.
- Όταν επικοινωνείτε με την Τράπεζα, πρέπει να ξέρετε ποιες πληροφορίες θα ζητηθούν από σας. Να έχετε υπόψη ότι η Τράπεζα που σας εξυπηρετεί ποτέ δεν θα ζητήσει από σας να της δώσετε τους κωδικούς πρόσβασής σας.
- Αφού έχετε τελειώσει με το Online Banking, πάντα ελέγχετε αν έχετε βγει από την πύλη και αν έχετε αποσυνδεθεί από το προφίλ σας.
- Μην αποθηκεύετε ποτέ τον κωδικό πρόσβασης στον υπολογιστή σας, εκτός εάν είναι προστατευμένος (π.χ. Password manager).
- Μην αφήνετε ποτέ τον υπολογιστή σας αφύλακτο, όταν έχετε μπει στο Internet Banking σας.
- Σας συμβουλεύουμε να αλλάζετε περιοδικά τον κωδικό σας πρόσβασης. Όταν αλλάζετε τον κωδικό σας πρόσβασης, πάντα επιλέγετε τέτοιο που δύσκολο μπορεί να αναμένεται.
- Μην χρησιμοποιείτε τον κωδικό πρόσβασης για το Internet Banking για άλλες ιστοσελίδες.

Φροντίστε για την ασφάλεια του υπολογιστή σας

- Πρέπει να είστε ιδιαίτερα προσεκτικοί με όλα τα μη ζητούμενα μηνύματα ηλεκτρονικού ταχυδρομείου, ιδιαίτερα αν έχουν σταλεί από άγνωστες διευθύνσεις. Μην ανοίγετε ποτέ link σε τέτοια μηνύματα που σας προσκαλούν να επισκεφθείτε άγνωστες ιστοσελίδες.
- Μην ανοίγετε, μην κατεβάζετε ή αποσυμπιέζετε άγνωστα συνημμένα αρχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου που έχουν ληφθεί από άγνωστες, ύποπτες ή αβέβαιες πηγές.
- Εγκαταστήστε λογισμικό προστασίας από ιούς, ενημερώνετέ το τακτικά και σαρώνετε περιοδικά τον υπολογιστή σας για τη δική σας ασφάλεια.

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.

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

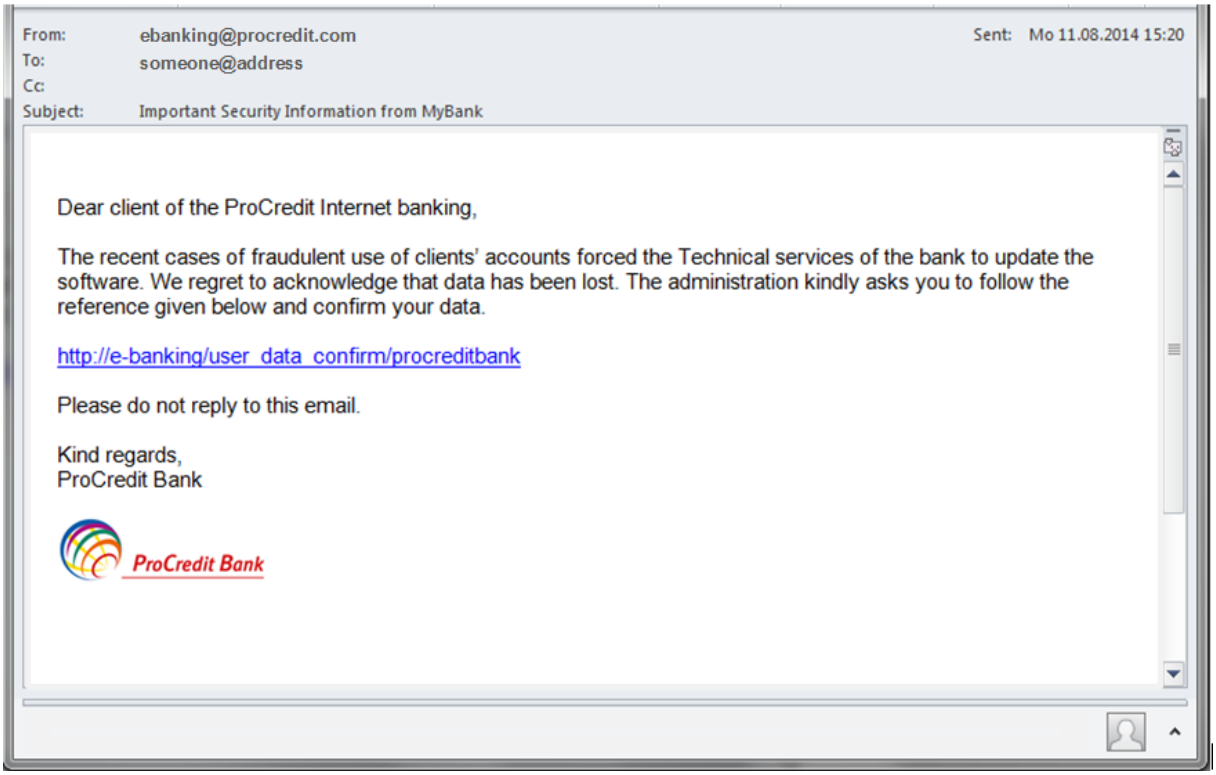
Για περισσότερες πληροφορίες επισκεφθείτε το ακόλουθο link:
http://www.staysafeonline.org/stay-safe-online/keep-a-clean-machine/spam-and-phishing

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.