Χρήσιμες Πληροφορίες για τη χρήση καρτών και ασφάλεια συναλλαγών καρτών στο διαδίκτυο («Χρήσιμες Πληροφορίες Συναλλαγών Καρτών στο διαδίκτυο»)

Οι «Χρήσιμες Πληροφορίες Συναλλαγών Καρτών στο διαδίκτυο» εκδίδονται από καιρό εις καιρό με στόχο την παροχή πληροφοριών στους πελάτες για τον τρόπο χρήσης καρτών και ασφάλεια διενέργειας συναλλαγών καρτών στο διαδίκτυο.

Συναλλαγές καρτών στο διαδίκτυο περιλαμβάνουν οποιεσδήποτε συναλλαγές κατά τις οποίες αποκτώνται αγαθά ή υπηρεσίες από τη χρήση της κάρτας, του αριθμού της κάρτας ή με οποιονδήποτε άλλο τρόπο προτείνεται από τον κάτοχο της κάρτας για χρέωση του λογαριασμού της κάρτας.

Α. Εξοπλισμός / Προγράμματα και Προστασία υπολογιστή (από «Ιούς Δολιοφθοράς», «Virus», «Spyware») / Τοίχος Προστασίας (Firewall)

1. Για εκτέλεση συναλλαγών καρτών στο διαδίκτυο, απαιτείται η χρήση ηλεκτρονικού υπολογιστή ή έξυπνου (smart) τηλεφώνου με σύνδεση στο διαδίκτυο.
2. Σε περίπτωση ασύρματης πρόσβασης στο διαδίκτυο, σας προτρέπουμε να φροντίσετε ώστε να εγκαταστήσετε σωστά τον ασύρματο (wireless) εξοπλισμό σας. Εισηγούμαστε να διαβάσετε τις οδηγίες εγκατάστασης του προσεκτικά και να ακολουθείτε τις προτεινόμενες οδηγίες ασφάλειας της κατασκευάστριας εταιρείας.
3. Εγκαταστήστε στον υπολογιστή σας προγράμματα anti-virus και προγράμματα για καταπολέμηση ιών spyware και malware. Χρησιμοποιείτε τακτικά τα προγράμματα αυτά για εντοπισμό κινδύνων και καταπολέμηση spyware, malware και spam.
4. Επιβεβαιώνετε ότι τα προγράμματα anti-virus και anti-spyware είναι επικαιροποιημένα.
5. Επιβεβαιώστε ότι τα λειτουργικά συστήματα και προγράμματα του υπολογιστή σας είναι επικαιροποιημένα με τις τελευταίες προσθήκες ασφαλείας.
6. Χρησιμοποιείτε firewall (ή προσωπικό firewall) για να αποτρέπετε εξωτερικούς χρήστες να εισβάλουν στον υπολογιστή σας.

Β. Ασφαλή Χρήση των Κωδικών Πρόσβασης/Ασφαλείας για τη χρήση της Υπηρεσίας Safe@Web

1. Ποτέ μην αποκαλύψετε τον Κωδικό Πρόσβασης/Ασφαλείας σας σε οποιονδήποτε.
2. Μην γράφετε τον Κωδικό Πρόσβασης/Ασφαλείας σας κάπου που μπορεί να εντοπιστεί από τρίτους.
3. Τα μέλη του προσωπικού της Τράπεζας Κύπρου δεν θα σας ζητήσουν ποτέ να αποκαλύψετε τον Κωδικό Πρόσβασης/Ασφαλείας σας, είτε από το τηλέφωνο ή μέσω του ηλεκτρονικού ταχυδρομείου.
4. Μην αφήσετε κανένα να σας παρακολουθεί ενώ πληκτρολογείτε τον Κωδικό Πρόσβασης/Ασφαλείας κατά την πρόσβασή σας σε οποιαδήποτε ιστοσελίδα.
5. Πάντοτε να αποσυνδέεστε από την κάθε ιστοσελίδα. Μην κλείνετε απλά τον περιηγητή σας ή την εφαρμογή στο τηλέφωνο σας.
6. Ενεργοποιήστε τη δυνατότητα “time out” για να κλειδώνετε τον υπολογιστή σας όταν απομακρύνεστε.
7. Για μεγαλύτερη ασφάλεια, εισηγούμαστε όπως αλλάζετε τον Κωδικό Πρόσβασης/Ασφαλείας σας τακτικά.

Γ. Ασφάλεια Διαδικτύου και Ηλεκτρονικού Ταχυδρομείου

1. Σε καμία περίπτωση μην αποκαλύψετε τους κωδικούς σύνδεσης σας στις ιστοσελίδες που έχετε καταχωρήσει αριθμούς καρτών σας.
2. Μην απομακρύνεστε από τον υπολογιστή σας προτού αποσυνδεθείτε από τις ιστοσελίδες στις οποίες έχετε καταχωρήσει στοιχεία για διενέργεια συναλλαγών με κάρτες.
3. Αποφεύγετε να χρησιμοποιείτε υπολογιστές δημόσιας χρήσης για εκτέλεση συναλλαγών καρτών στο διαδίκτυο.
4. Σε περίπτωση που σταματήσετε τη χρήση ενός υπολογιστή, συστήνουμε να διαγράφετε οποιεσδήποτε προσωπικές πληροφορίες που μπορεί να είναι φυλαγμένες σε αυτό, χρησιμοποιώντας κατάλληλα προγράμματα.
5. Από καιρό σε καιρό η Τράπεζα Κύπρου αποστέλλει προωθητικά ηλεκτρονικά μηνύματα (πχ μέσω email, SMS, κλπ). Ποτέ όμως δεν θα σας ζητήσουμε να αποκαλύψετε προσωπικές πληροφορίες ή κωδικούς ασφαλείας μέσω ηλεκτρονικού ταχυδρομείου, pop up windows και banners. Μην αποκαλύπτετε ποτέ μέσω διαδικτύου ή ηλεκτρονικού ταχυδρομείου (email), ή μέσω οποιασδήποτε ηλεκτρονικής συναλλαγής, προσωπικά σας στοιχεία όπως αριθμούς καρτών, User IDs, Κωδικούς Ασφαλείας, Κωδικούς digipass, αριθμούς τραπεζικών λογαριασμών κλπ.
6. Αν παραλάβετε ηλεκτρονικό μήνυμα που σας ζητά να «επιβεβαιώσετε την κάρτα σας», «να επιβεβαιώσετε τους κωδικούς πρόσβασης σας» ή με παρόμοιο περιεχόμενο, αυτό πιθανότατα να είναι μήνυμα απάτης.
7. Εάν παραλάβετε ηλεκτρονικά μηνύματα τύπου spam ή που να περιέχουν ύποπτα επισυνημμένα αρχεία, εισηγούμαστε όπως τα σβήσετε αμέσως χωρίς να ανταποκριθείτε.
8. Μην απαντάτε και μην κατεβάζετε (download) αρχεία στον υπολογιστή σας από άγνωστους αποστολείς ή ιστοσελίδες.
9. Εάν αμφιβάλλετε για την αυθεντικότητα κάποιας ιστοσελίδας, να θυμάστε να ελέγξετε το πιστοποιητικό της. Επιπρόσθετα, κάνοντας κλικ στην κλειδαριά (και πάλι στην μπάρα με τη διεύθυνση της ιστοσελίδας), θα δείτε το όνομα του δικαιούχου του πιστοποιητικού
10. Μην ανοίγετε μη αναμενόμενα επισυνημμένα αρχεία από γνωστές ή άγνωστες πηγές.

Δ. Διαδικασία που θα πρέπει να ακολουθείτε σε περίπτωση υποκλοπής κωδικού πρόσβασης/ασφαλείας ή καταχώρησης κωδικού πρόσβασης/ασφαλείας σε μη αυθεντική ιστοσελίδα

1. Σε περίπτωση που υποψιάζεστε ότι ο κωδικός πρόσβασής σας σε κάποια ιστοσελίδα από την οποία διενεργείτε συναλλαγές καρτών έχει κλαπεί ή αποκαλυφθεί σε τρίτους, αλλάξτε τον αμέσως με βάση τις οδηγίες που παρέχονται στη συγκεκριμένη ιστοσελίδα. Επικοινωνήστε μαζί μας το συντομότερο για να ακυρώσουμε την κάρτα σας και να σας εκδώσουμε νέα.
2. Αν έχετε παραλάβει μήνυμα τύπου «phishing» με σύνδεσμο που οδηγεί σε μη αυθεντική ιστοσελίδα, μην ανταποκριθείτε σε αυτό.
3. Αν έχετε απαντήσει σε οποιοδήποτε μήνυμα τύπου «Phishing» και έχετε καταχωρήσει προσωπικές πληροφορίες και άλλα στοιχεία σε ιστοσελίδα στην οποία έχετε δηλώσει στοιχεία της κάρτας σας, επικοινωνήστε με την Τράπεζα για ακύρωση της κάρτας και έκδοση νέας.

Ε. Πρόσθετη Πληροφόρηση

Επιπλέον των όσων αναφέρονται στις παραγράφους πιο πάνω, οι διατάξεις που αφορούν την προστασία της κάρτας και του PIN (κωδικού πρόσβασης), τις διαδικασίες που πρέπει να ακολουθούνται σε περίπτωση υποψίας για μη εξουσιοδοτημένη χρήση της κάρτας καθώς και οποιεσδήποτε άλλες πληροφορίες για την χρήση των καρτών και τις ευθύνες και υποχρεώσεις που διέπουν την σχέση της Τράπεζας και του Κατόχου Λογαριασμού Κάρτας και Κατόχου Κάρτας , περιγράφονται στο http://www.bankofcyprus.com.cy/Cards_Gr/