ΟΔΗΓΙΕΣ ΛΕΙΤΟΥΡΓΙΑΣ

Αυτές οι «Οδηγίες Λειτουργίας» εκδίδονται από καιρό εις καιρό με στόχο την παροχή πληροφοριών στους πελάτες για τον τρόπο λειτουργίας των ηλεκτρονικών καναλιών της Τράπεζας Κύπρου (1bank).

1. ΕΞΟΠΛΙΣΜΟΣ / ΠΡΟΓΡΑΜΜΑΤΑ

1.1. Για πρόσβαση στα ηλεκτρονικά κανάλια της 1bank, απαιτείται η χρήση ηλεκτρονικού υπολογιστή (για το internet banking) ή έξυπνου (smart) τηλεφώνου με σύνδεση στο διαδίκτυο (τόσο για το internet banking, όσο και για το mobile banking).

1.2. Για τη δική σας ασφάλεια εισηγούμαστε να κλειδώνετε το κινητό σας για διασφάλιση της μη εξουσιοδοτημένης πρόσβασης σε αυτό από τρίτα πρόσωπα. Εάν ο αριθμός κινητού σας άλλαξε, θα πρέπει να ειδοποιήσετε την Τράπεζα σε οποιοδήποτε κατάστημα ή τηλεφωνώντας στο Τηλεφωνικό Κέντρο της 1bank στον αριθμό που αναγράφεται στην Παράγραφο Λ πιο κάτω

1.3. Σε περίπτωση ασύρματης πρόσβασης στο διαδίκτυο, σας προτρέπουμε να φροντίσετε ώστε να εγκαταστήσετε σωστά τον ασύρματο (wireless) εξοπλισμό σας. Εισηγούμαστε να διαβάστε τις οδηγίες εγκατάστασης του προσεκτικά και να ακολουθείτε τις προτεινόμενες οδηγίες ασφάλειας της κατασκευάστριας εταιρείας.

1.4. Η λειτουργία των ηλεκτρονικών καναλιών της 1bank δεν επηρεάζεται από το λειτουργικό σύστημα ή τον περιηγητή που έχετε εγκατεστημένο στον υπολογιστή σας, συστήνουμε όμως τη χρήση των πιο κοινών περιηγητών. Για περισσότερες λεπτομέρειες κάντε κλικ εδώ.

1.5. Συνιστούμε (όπου εφαρμόζεται) να γίνουν οι πιο κάτω ρυθμίσεις στον περιηγητή σας:

- Διαγραφή Cookies και Αρχείων
- Η αποδοχή Cookies πρέπει να είναι ενεργοποιημένη
- Η χρήση Java Script πρέπει να επιτρέπεται
- Η χρήση Active Scripting πρέπει να επιτρέπεται
- Η χρήση των πρωτοκόλλων ασφάλειας TLS 1.0, TLS 1.1 και TLS 1.2 πρέπει να επιτρέπεται
- Δεν πρέπει να επιτρέπεται η αποθήκευση σελίδων Encrypted στο δίσκο.

1.6. Για τη χρήση των ειδικών mobile applications (Apps), θα χρειαστείτε λογαριασμό στο App Store (για να εγκαταστήσετε την iOS εφαρμογή) ή λογαριασμό στο Google Play Store (για να εγκαταστήσετε την Android εφαρμογή).

1.7. Αναφερθείτε στους Όρους και Προϋποθέσεις της 1bank για τις υποχρεώσεις και ευθύνες των διαφόρων μερών.

2. ΑΣΦΑΛΕΙΑ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

2.1. Φροντίζετε πάντα να αποκτάτε πρόσβαση στην υπηρεσία ηλεκτρονικής τραπεζικής της Τράπεζας Κύπρου (1bank), μέσω των επίσημων κεντρικών ιστοσελίδων στις διευθύνσεις www.bankofcyprus.com.cy, www.1bank.com ή μέσω του ειδικού App της Τράπεζας Κύπρου στο κινητό σας.

2.2. Σε καμία περίπτωση μην εμπιστεύεστε ιστοσελίδες στις οποίες δεν έχετε μεταβεί μέσω των πιο πάνω συνδέσμων ή να αποκαλύψετε σε αυτές τους κωδικούς σύνδεσης σας στην 1bank (User ID και Κωδικός Ασφαλείας).

2.3. Μην απομακρύνεστε από τον υπολογιστή σας την ώρα που χρησιμοποιείτε τις υπηρεσίες της 1bank.

2.4. Αποφεύγετε να χρησιμοποιείτε υπολογιστές δημόσιας χρήσης για πρόσβαση στην 1bank.

2.5. Περιορίστε τις οικονομικές σας πληροφορίες στον προσωπικό υπολογιστή σας.

2.6. Σε περίπτωση που σταματήσετε τη χρήση ενός υπολογιστή, συστήνουμε να διαγράφετε οποιεσδήποτε προσωπικές πληροφορίες που μπορεί να είναι φυλαγμένες σε αυτό, χρησιμοποιώντας κατάλληλα προγράμματα.

2.7. 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 User IDs, Κωδικούς Ασφαλείας, Κωδικούς digipass, αριθμούς καρτών, αριθμούς τραπεζικών λογαριασμών κλπ.

2.8. Αν παραλάβετε ηλεκτρονικό μήνυμα που σας ζητά να «επιβεβαιώσετε το λογαριασμό σας», «να επιβεβαιώσετε τους κωδικούς πρόσβασης σας» ή με παρόμοιο περιεχόμενο, αυτό πιθανότατα να είναι μήνυμα απάτης.

2.9. Εάν παραλάβετε ηλεκτρονικά μηνύματα τύπου spam ή που να περιέχουν ύποπτα επισυνημμένα αρχεία, εισηγούμαστε όπως τα σβήσετε αμέσως χωρίς να ανταποκριθείτε.

2.10. Μην απαντάτε και μην κατεβάζετε (download) αρχεία στον υπολογιστή σας από άγνωστους αποστολείς ή ιστοσελίδες.

2.11. Εάν αμφιβάλλετε για την αυθεντικότητα κάποιας ιστοσελίδας, να θυμάστε να ελέγξετε το πιστοποιητικό της. Μια ιστοσελίδα είναι αυθεντική αν η μπάρα με τη διεύθυνση της ιστοσελίδας είναι πράσινη (αυτό συμβαίνει όταν το πιστοποιητικό είναι EV). Επιπρόσθετα, κάνοντας κλικ στην κλειδαριά (και πάλι στην μπάρα με τη διεύθυνση της ιστοσελίδας), θα δείτε το όνομα του δικαιούχου του πιστοποιητικού (στην περίπτωση της Τράπεζας, δικαιούχος του πιστοποιητικού είναι: BANK OF CYPRUS PUBLIC COMPANY LTD)

2.12. Μην ανοίγετε μη αναμενόμενα επισυνημμένα αρχεία από γνωστές ή άγνωστες πηγές.

2.13. Αναφερθείτε στους Όρους και Προϋποθέσεις της 1bank για τις υποχρεώσεις και ευθύνες των διαφόρων μερών.

3. ΠΡΟΣΤΑΣΙΑ ΥΠΟΛΟΓΙΣΤΗ (ΑΠΟ «ΙΟΥΣ ΔΟΛΙΟΦΘΟΡΑΣ», «VIRUS», «SPYWARE») / ΤΟΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ (FIREWALL)

3.1. 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.

3.2. Επιβεβαιώνετε ότι τα προγράμματα anti-virus και anti-spyware είναι επικαιροποιημένα.

3.3. Επιβεβαιώστε ότι τα λειτουργικά συστήματα και προγράμματα του υπολογιστή σας είναι επικαιροποιημένα με τις τελευταίες προσθήκες ασφαλείας.

3.4. Χρησιμοποιείτε firewall (ή προσωπικό firewall) για να αποτρέπετε εξωτερικούς χρήστες να εισβάλουν στον υπολογιστή σας, ειδικά αν έχετε γρήγορη (high-speed) ή συνεχή σύνδεση στο Διαδίκτυο όπως DSL ή cable modem.

3.5. Αναφερθείτε στους Όρους και Προϋποθέσεις της 1bank για τις υποχρεώσεις και ευθύνες των διαφόρων μερών.

4. ΠΡΟΣΤΑΣΙΑ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ

4.1. Ποτέ μην αποκαλύψετε τον Κωδικό Ασφαλείας σας της 1bank σε οποιονδήποτε.

4.2. Μην γράφετε τον Κωδικό Ασφαλείας σας κάπου που μπορεί να εντοπιστεί από τρίτους.

4.3. Τα μέλη του προσωπικού της Τράπεζας Κύπρου δεν θα σας ζητήσουν ποτέ να αποκαλύψετε τον Κωδικό Ασφαλείας σας, είτε από το τηλέφωνο ή μέσω του ηλεκτρονικού ταχυδρομείου.

4.4. Μην αφήσετε κανένα να σας παρακολουθεί ενώ πληκτρολογείτε το User ID σας και τον Κωδικό Ασφαλείας σας κατά την πρόσβασή σας στην 1bank.

4.5. Αποφεύγετε τη χρήση αυτόματης σύνδεσης η οποία φυλάει τον Κωδικό Ασφαλείας σας.

4.6. Πάντοτε να αποσυνδέεστε από την 1bank όταν έχετε τελειώσει. Μην κλείνετε απλά τον περιηγητή σας ή την εφαρμογή στο τηλέφωνο σας.

4.7. Ενεργοποιήστε τη δυνατότητα “time out” για να κλειδώνετε τον υπολογιστή σας όταν απομακρύνεστε.

4.8. Μην καθορίζετε προβλέψιμους Κωδικούς Ασφαλείας, όπως την ημερομηνία γεννήσεως σας, τον αριθμό ταυτότητας ή διαβατηρίου σας, κλπ.

4.9. Για μεγαλύτερη ασφάλεια, εισηγούμαστε όπως αλλάζετε τον Κωδικό Ασφαλείας σας τακτικά.

4.10. Αναφερθείτε στους Όρους και Προϋποθέσεις της 1bank για τις υποχρεώσεις και ευθύνες των διαφόρων μερών.

5. ΠΡΟΣΤΑΣΙΑ ΣΥΣΚΕΥΩΝ ΠΑΡΑΓΩΓΗΣ ΚΩΔΙΚΩΝ ΜΙΑΣ ΧΡΗΣΗΣ (DIGIPASS)

5.1. Μεταφέρετε τη συσκευή παραγωγής κωδικών (digipass) μαζί σας.

5.2. Μην αποκαλύπτετε το PIN της συσκευής σας σε κανένα.

5.3. Μην αποκαλύπτετε σε κανένα τους Κωδικούς Μιας Χρήσης (OTP) που δίνονται από τη συσκευή σας.

5.4. Αναφορικά με τη χρήση των hardware digipass, αναφερθείτε στους Όρους και Προϋποθέσεις της 1bank για τις υποχρεώσεις και ευθύνες των συμβαλλόμενων μερών, μέχρι την πλήρη απόσυρση αυτών κατόπιν απόφασης της Τράπεζας.

5.5. Αναφερθείτε στους Όρους και Προϋποθέσεις Απόκτησης και Λειτουργίας του Digipass APP για τις υποχρεώσεις και ευθύνες των συμβαλλόμενων μερών.

5.6. Αναφερθείτε στους Όρους και Προϋποθέσεις Απόκτησης και Λειτουργίας του SMS Digipass για τις υποχρεώσεις και ευθύνες των συμβαλλόμενων μερών.

6. ΥΠΟΚΛΟΠΗ ΚΩΔΙΚΟΥ ΑΣΦΑΛΕΙΑΣ ΤΗΣ 1BANK / ΚΑΤΑΧΩΡΗΣΗ ΚΩΔΙΚΟΥ ΑΣΦΑΛΕΙΑΣ Η OTP ΣΕ ΙΣΤΟΣΕΛΙΔΑ ΠΟΥ ΔΕΝ ΑΝΗΚΕΙ ΣΤΗΝ ΤΡΑΠΕΖΑ

6.1. Σε περίπτωση που υποψιάζεστε ότι ο Κωδικός Ασφαλείας σας έχει κλαπεί ή αποκαλυφθεί σε τρίτους, αλλάξτε τον αμέσως είτε μέσω του internet ή mobile banking.

6.2. Αν έχετε παραλάβει μήνυμα τύπου «phishing» με σύνδεσμο που οδηγεί σε μη αυθεντική ιστοσελίδα, μην ανταποκριθείτε σε αυτό. Στείλτε το αμέσως στην ηλεκτρονική διεύθυνση abuse@bankofcyprus.com. Η Τράπεζα θα φροντίσει να αφαιρέσει την ιστοσελίδα αυτή το συντομότερο.

6.3. Αν έχετε απαντήσει σε οποιοδήποτε μήνυμα τύπου «Phishing» και έχετε καταχωρήσει προσωπικές πληροφορίες και άλλα στοιχεία, επικοινωνήστε μαζί μας το συντομότερο:

- Για Κωδικό Ασφαλείας της 1bank - Θα ακυρώσουμε τον υφιστάμενο κωδικό σας και θα σας αποστείλουμε νέο
- Για κάρτα - Θα ακυρώσουμε την κάρτα και θα σας εκδώσουμε νέα.

6.4. Σε περίπτωση που η υποκλοπή έγινε εκτός ωρών εργασίας του Τηλεφωνικού Κέντρου, ανάλογα με την περίπτωση εισηγούμαστε:

- Για Κωδικό Ασφαλείας της 1bank - Αλλάξτε τον αμέσως, αν μπορείτε. Αν δεν μπορείτε να συνδεθείτε (αν το τρίτο άτομο έχει ήδη αλλάξει τον Κωδικό Πρόσβασης σας), να κάνετε τουλάχιστον 6 προσπάθειες σύνδεσης με την υπηρεσία χρησιμοποιώντας το User ID σας και οποιοδήποτε Κωδικό Πρόσβασης για να κλειδωθεί ο νέος αριθμός που έχει καθοριστεί. Επικοινωνήστε μαζί μας την επόμενη εργάσιμη μέρα.
- Για κάρτα - Επικοινωνήστε με τη JCC στο τηλ +357 22868100 για να σας ακυρώσουν την κάρτα. Επικοινωνήστε μαζί μας την επόμενη εργάσιμη μέρα.

6.5. Αναφερθείτε στους Όρους και Προϋποθέσεις της 1bank για τις υποχρεώσεις και ευθύνες των διαφόρων μερών.

7. ΟΔΗΓΙΕΣ ΓΙΑ ΧΡΗΜΑΤΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

7.1. Οι χρηματικές συναλλαγές για πίστωση λογαριασμού τρίτου προσώπου, απαιτούν τη χρήση Μέσων Παραγωγής Κωδικών Μιας Χρήσης (SMS Digipass & Digipass APP).

7.2. Μπορείτε να καθορίσετε να απαιτείται η έγκριση συναλλαγών από ένα ή περισσότερα άτομα.

7.3. Η ακύρωση μιας συναλλαγής, είναι δυνατή μόνο εφόσον αυτή είναι με μελλοντική ημερομηνία εκτέλεσης ή από το άτομο στο οποίο εκκρεμεί η έγκριση.

7.4. Με την υποβολή της συναλλαγής στην Τράπεζα, η οδηγία θα εκτελεστεί αυτόματα και ο λογαριασμός θα χρεωθεί (με το ποσό και πιθανά έξοδα), νοουμένου ότι η οδηγία πληροί τα καθορισμένα από την Τράπεζα κριτήρια. Συναλλαγές που δεν πληρούν τα κριτήρια για αυτόματη εκτέλεση, παραλαμβάνονται από Μονάδες της Τράπεζας και εκτελούνται. Η επικοινωνία μαζί με τον Κάτοχο Λογαριασμού ή με το Συνδρομητή δεν είναι προϋπόθεση για την εκτέλεση μιας οδηγίας.

7.5. Καταχωρήστε προειδοποιητικά μηνύματα Alerts και λαμβάνετε πληροφορίες για τα υπόλοιπα ή/και συναλλαγές στους λογαριασμούς σας. Τα μηνύματα αποστέλλονται στο ηλεκτρονικό ταχυδρομείο σας (email) ή κινητό τηλέφωνο σας (sms). Η υπηρεσία προσφέρεται δωρεάν

7.6. Η Υπηρεσία QuickPay της 1bank είναι διαθέσιμη σε όλους τους Χρήστες και μπορεί να ενεργοποιηθεί μέσω του ειδικού App της Τράπεζας Κύπρου στο κινητό σας. Η QuickPay επιτρέπει σε Χρήστες να συνδέσουν ένα λογαριασμό τους με τον αριθμό κινητού τους για να διενεργούν και να λαμβάνουν πληρωμές. Η QuickPay επιτρέπει σε Χρήστες της 1bank να πληρώσουν άλλους ενεργοποιημένους χρήστες της QuickPay με τη χρήση του αριθμού κινητού τους και επιτρέπει πληρωμές σε όλους τους κατόχους λογαριασμού της τράπεζας Κύπρου με την εισαγωγή του αριθμού λογαριασμού τους. Αναφερθείτε στους 'Ορους και Προϋποθέσεις και Συχνές Ερωτήσεις της QuickPay για περισσότερες πληροφορίες

7.7. Αναφερθείτε στους Όρους και Προϋποθέσεις της 1bank για τις υποχρεώσεις και ευθύνες των διαφόρων μερών.

8. ΕΥΘΥΝΗ ΤΡΑΠΕΖΑΣ, ΣΥΝΔΡΟΜΗΤΗ ΚΑΙ ΚΑΤΟΧΟΥ ΛΟΓΑΡΙΑΣΜΟΥ

8.1. Ελέγχετε σε τακτά χρονικά διαστήματα τις καταστάσεις λογαριασμών που είναι συνδεδεμένοι με τη συνδρομή σας (είτε αυτοί σας ανήκουν ή ανήκουν σε τρίτα άτομα – φυσικά ή νομικά πρόσωπα). Αν εντοπίσετε ύποπτες συναλλαγές, επικοινωνήστε μαζί μας.

8.2. Ελέγχετε σε τακτά χρονικά διαστήματα τις εντολές πληρωμής των λογαριασμών που είναι συνδεδεμένοι με τη συνδρομή σας (είτε αυτοί σας ανήκουν ή ανήκουν σε τρίτα άτομα – φυσικά ή νομικά πρόσωπα) για τυχόν εντολές που μπορεί να μην ανοίξατε εσείς ή ο Κάτοχος Λογαριασμού και επικοινωνήστε μαζί μας.

8.3. Ελέγχετε τις Μη Εκτελεσθείσες Οδηγίες στην Κατάσταση Συναλλαγών για οδηγίες που μπορεί να μην δώσατε εσείς. Ακυρώστε τις αν μπορείτε και επικοινωνήστε μαζί μας.

8.4. Αναφερθείτε στους Όρους και Προϋποθέσεις της 1bank για τις υποχρεώσεις και ευθύνες των διαφόρων μερών.

9. ΆΛΛΕΣ ΧΡΗΣΙΜΕΣ ΣΥΜΒΟΥΛΕΣ ΑΣΦΑΛΕΙΑΣ

9.1. Η 1bank έχει προκαθορισμένα όρια μεταφορών, όπως αυτά εμφανίζονται στις αιτήσεις. Μπορείτε όμως να καθορίστε χαμηλότερα όρια για μεταφορές χρημάτων μέσω 1bank.

9.2. Μπορείτε να χρησιμοποιείστε τη δυνατότητα των πολλαπλών υπογραφών. Η δυνατότητα αυτή σας επιτρέπει να καθορίζετε διάφορα επίπεδα ετοιμασίας και έγκρισης για συναλλαγές. Έτσι συναλλαγές που γίνονται από ένα άτομο να χρειάζονται έγκριση από δεύτερο πριν αυτές αποσταλούν στην Τράπεζα για εκτέλεση.

9.3. Σε περίπτωση που κάποιος συνδρομητής τερματίσει τη σχέση του μαζί σας:

- Ειδοποιήστε μας για να τερματιστεί η πρόσβαση του.
- Μη δώσετε τους κωδικούς πρόσβασης σε άλλο άτομο χωρίς να υποβληθούν οι σχετικές αιτήσεις σε εμάς.
- Σε περίπτωση που έχετε δώσει εξουσιοδότηση σε τρίτο άτομο για πρόσβαση στους λογαριασμούς σας και επιθυμείτε να την αναιρέσετε, επικοινωνήστε μαζί μας.

9.4. Αναφερθείτε στους Όρους και Προϋποθέσεις της 1bank για τις υποχρεώσεις και ευθύνες των διαφόρων μερών.

10. ΧΡΟΝΙΚΑ ΠΕΡΙΘΩΡΙΑ ΓΙΑ ΤΗ ΔΙΕΞΑΓΩΓΗ ΕΞΕΡΧΟΜΕΝΩΝ ΕΜΒΑΣΜΑΤΩΝ

Η Τράπεζα διεκπεραιώνει εξερχόμενα εμβάσματα με αξία ίδια με την ημερομηνία εκτέλεσης (same day value date), εντός εργάσιμων ημερών και πριν τα πιο κάτω χρονικά περιθώρια:

Νόμισμα	Ώρα
EUR	Μέχρι τις 13:30
USD	Μέχρι τις 13:30
GBP	Μέχρι τις 13:00
CAD, RUB	Μέχρι τις 13:00
CHF, RON	Μέχρι τις 13:00
NOK, PLN, SEK, CZK, DKK, HUF	Μέχρι τις 12:00

11. ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

- Τηλεφωνικό Κέντρο 1bank 800 00 800 ή +357 22 128000 αν καλείτε από το εξωτερικό, Δευτέρα με Παρασκευή, 07:45 - 20:00.
- Φόρμα Επικοινωνίας
- email: info@bankofcyprus.com