



Μέτρα Ασφαλείας

Κατά τη χρήση της Εφαρμογής Κινητού My Fibank

Αγαπητοί μας Πελάτες,

Η First Investment Bank (Fibank, η Τράπεζα) σας παρέχει υψηλό επίπεδο προστασίας και ασφάλειας κατά την πρόσβαση και χρήση της Εφαρμογής Κινητού Fibank. Σε αυτό το πλαίσιο, παρακαλείστε να διαβάσετε και να συμμορφωθείτε με τα ακόλουθα Μέτρα Ασφαλείας.

Περιεχόμενα

Βασικές αρχές και συστάσεις.....	3
Μέτρα κατά απειλών από ηλεκτρονικό «ψαρεμα» (phishing).....	3
Προσθετά μέτρα για την εφαρμογή κινητού my fibank:.....	4
Μέτρα κατά τη χρήση της κινητής σας συσκευής	6
Απειλές στην εποχή της τεχνητής νοημοσύνης	6

ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΚΑΙ ΣΥΣΤΑΣΕΙΣ

1. Αλλάξτε τον κωδικό πρόσβασής σας μετά την αρχική σύνδεση στην Εφαρμογή Κινητού.
2. Χρησιμοποιήστε έναν «ισχυρό» κωδικό πρόσβασης που περιέχει συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμών, ειδικών χαρακτήρων, και περιλαμβάνει τουλάχιστον 8 χαρακτήρες. Μη χρησιμοποιείτε ως κωδικό πρόσβασης τίποτα από τα ακόλουθα: ονόματα, ημερομηνίες γέννησης, διαδοχικούς αριθμούς/γράμματα (12345, ΑΒΓΔ, κ.λ.π.), επαναλαμβανόμενους χαρακτήρες (ααα, 111, κ.λ.π.). Αλλάζετε τον κωδικό πρόσβασής σας ανά τακτά χρονικά διαστήματα.
3. Μη χρησιμοποιείτε τον ίδιο κωδικό για πρόσβαση σε διαφορετικές πλατφόρμες και προφίλ στις ψηφιακές τραπεζικές σας υπηρεσίες, στη διεύθυνση ηλεκτρονικού ταχυδρομείου, στα κοινωνικά δίκτυα κ.α.
4. Το όνομα χρήστη πρέπει να περιέχει μόνο λατινικά γράμματα και αριθμούς, και να είναι μεταξύ 6 και 24 χαρακτήρων. Χρησιμοποιήστε ένα όνομα χρήστη με περισσότερους χαρακτήρες που δεν σχετίζεται με το όνομα ή το επώνυμό σας.
5. Μη μοιράζετε το όνομα χρήστη, τον κωδικό ή την Κινητή Συσκευή σας με τρίτους.
6. Μη αποθηκεύετε το όνομα χρήστη, τον κωδικό ή το PINt σας εγγράφως ή σε οποιοδήποτε άλλο ανθεκτικό μέσο, συμπεριλαμβανομένης της ηλεκτρονικής μορφής.
7. Εάν λάβετε μήνυμα ή ειδοποιηθείτε με άλλο τρόπο για έκτακτη αλλαγή στον τρόπο σύνδεσης και ταυτοποίησης στο My Fibank, ή λάβετε αίτημα για παροχή των στοιχείων της κάρτας σας, μην ανταποκριθείτε και ειδοποιήστε αμέσως την Τράπεζα.
8. Όταν ολοκληρώνετε την εργασία σας στο My Fibank, χρησιμοποιήστε την ένδειξη «Έξοδος» για να τερματίσετε τη συνεδρία.
9. Χρησιμοποιείτε τα πιο ενημερωμένα λειτουργικά συστήματα και προϊόντα λογισμικού. Μη χρησιμοποιείτε δοκιμαστικές εκδόσεις λειτουργικών συστημάτων ή/και προϊόντων λογισμικού.
10. Εξετάζετε τακτικά και προσεκτικά τις ειδοποιήσεις που λαμβάνετε. Εάν λάβετε μήνυμα ή ειδοποιηθείτε με άλλο τρόπο για έκτακτη αλλαγή στον τρόπο σύνδεσης και ταυτοποίησης στο My Fibank, ή λάβετε αίτημα ή λάβετε αίτημα για παροχή των στοιχείων της κάρτας σας, μην ανταποκριθείτε και ειδοποιήστε αμέσως την Τράπεζα στους ακόλουθους αριθμούς τηλεφώνου:

+302103006303**+ 359 2 4861001****ΜΕΤΡΑ ΚΑΤΑ ΑΠΕΙΛΩΝ ΑΠΟ ΗΛΕΚΤΡΟΝΙΚΟ «ΨΑΡΕΜΑ» (PHISHING)**

11. Να είστε προσεκτικοί όταν λαμβάνετε ύποπτα μηνύματα στη διεύθυνση ηλεκτρονικού ταχυδρομείου σας (τα λεγόμενα μηνύματα ηλεκτρονικού «ψαρέματος» (phishing)). Το ηλεκτρονικό «ψάρεμα» (phishing) είναι μια απόπειρα απάτης, στο πλαίσιο της οποίας κακόβουλοι τρίτοι παραπλανούν εσκεμμένα τους χρήστες προκειμένου αυτοί να αποκαλύψουν

προσωπικά στοιχεία, στοιχεία σύνδεσης και ταυτοποίησης, ή άλλες εμπιστευτικές πληροφορίες, να πατήσουν «κλικ» σε συνδέσμους, να εισάγουν κωδικούς, ονόματα χρηστών ή κωδικούς μίας χρήσης που αποστέλλονται στο τηλέφωνο ως μήνυμα, κ.λ.π. Εάν επιτύχουν το σκοπό τους, μπορούν να διεισδύσουν στον ψηφιακό τραπεζικό λογαριασμό σας, το οποίο μπορεί να οδηγήσει σε ανάληψη κεφαλαίων ή άλλες αρνητικές συνέπειες.

α. Χαρακτηριστικά των μηνυμάτων ηλεκτρονικού ταχυδρομείου που αποτελούν phishing

- συχνά ζητούν προσωπικά στοιχεία για διάφορους λόγους (π.χ. τεχνική υποστήριξη, αναστολή λογαριασμού, ανενεργός λογαριασμός, ενημέρωση τραπεζικών στοιχείων, ανανέωση υπηρεσιών, επιβεβαίωση τραπεζικού λογαριασμού, ενημέρωση στοιχείων, προσθήκη ασφάλειας, κ.λ.π.). **Η Fibank δεν ζητά ποτέ τέτοιες πληροφορίες.**
- ακόμη και αν το πεδίο αποστολέα («Από:») αναφέρει τη Fibank, αυτό δεν αποτελεί εγγύηση ότι το ληφθέν μήνυμα ηλεκτρονικού ταχυδρομείου προέρχεται από την Τράπεζα.
- Συνήθως υπάρχει αναντιστοιχία μεταξύ του ονόματος τομέα (domain) του αποστολέα και του domain που περιλαμβάνουν στους συνδέσμους που περιέχουν.
- περιέχουν «επείγουσες» προειδοποιήσεις για να σας επιστήσουν την προσοχή αναφορικά με ενδεχόμενη απάτη, όπως: «Ο λογαριασμός είναι φραγμένος», «Ο λογαριασμός σας έχει πρόβλημα», «Εάν δεν ολοκληρώσετε τη διαδικασία εντός 24 ωρών, ο λογαριασμός σας θα φραγεί επ' αόριστον», «Σημαντικό μήνυμα», «Επιβεβαιώστε τα στοιχεία του λογαριασμού σας», «Σημαντική προϋπόθεση για να συνεχίσετε να χρησιμοποιείτε τις υπηρεσίες My Fibank», κ.λ.π.
- περιέχουν συνδέσμους για εισαγωγή και επιβεβαίωση προσωπικών και τραπεζικών στοιχείων. Μην πατάτε «κλικ» σε αυτούς τους συνδέσμους, η Fibank δεν θα σας ζητήσει ποτέ να εισάγετε στοιχεία σε σύνδεσμο που αποστέλλεται μέσω μηνύματος. Οι ειδοποιήσεις από την Τράπεζα μπορεί να περιέχουν μόνο έγγραφα που ανοίγουν χωρίς εισαγωγή προσωπικών στοιχείων, για παράδειγμα σε περίπτωση αλλαγών στον Τιμοκατάλογο ή τους Γενικούς Όρους και Προϋποθέσεις.

β. Συνημμένα αρχεία

- Μην ανοίγετε ή αποθηκεύετε συνημμένα αρχεία από ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου.

γ. Αιτήματα για παροχή εμπιστευτικών πληροφοριών

- Η First Investment Bank AD **δεν ζητά** την αποστολή PINs, κωδικών πρόσβασης ή άλλων εμπιστευτικών πληροφοριών μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου.
- **Μην ακολουθείτε οδηγίες** από μηνύματα που σας ζητούν να καλέσετε έναν συγκεκριμένο αριθμό τηλεφώνου και να μοιραστείτε διαπιστευτήρια.

- 12.** Να είστε ιδιαίτερα προσεκτικοί όταν εισάγετε οικονομικά ή άλλα προσωπικά στοιχεία σε ιστοσελίδες, ιδίως ιστολόγια (blogs) και κοινωνικά δίκτυα όπως το Facebook. Ελέγχετε την αυθεντικότητα της ιστοσελίδας και την ασφάλεια του πρωτοκόλλου επικοινωνίας.

ΠΡΟΣΘΕΤΑ ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΕΦΑΡΜΟΓΗ ΚΙΝΗΤΟΥ MY FIBANK:

- 13.** Για να αποκτήσετε πρόσβαση στον λογαριασμό σας στην Εφαρμογή Κινητού My Fibank, πρέπει να ενεργοποιήσετε την Εφαρμογή Κινητού στη Κινητή σας Συσκευή ακολουθώντας μια βήμα προς βήμα διαδικασία που καθορίζεται από την Τράπεζα, η οποία εφαρμόζει ισχυρή ταυτοποίηση πελατών.

- 14.** Η Εφαρμογή Κινητού My Fibank μπορεί να εντοπιστεί και να κατέβει στη Κινητή σας Συσκευή (τηλέφωνο, tablet, κ.λ.π.) από τα επίσημα καταστήματα εφαρμογών κινητού: Google Play (Android), AppStore (iOS/iPad OS), και AppGallery (HarmonyOS). Οι ελάχιστες απαιτήσεις λειτουργικού συστήματος είναι Android OS v.8.0, ή iOS 16.0.
- 15.** Να θυμάστε τον κωδικό PINt σας. Μην τον γράφετε σε χαρτί, ή τον αποθηκεύετε στη μνήμη της Κινητής σας Συσκευής. Remember your PINt code.
- 16.** Για μεγαλύτερη ασφάλεια, συνιστούμε τη χρήση βιομετρικών στοιχείων όπως δακτυλικό αποτύπωμα ή αναγνώριση προσώπου (Face ID) για σύνδεση και ταυτοποίηση, καθώς και για επιβεβαίωση ηλεκτρονικών συναλλαγών στην Εφαρμογή Κινητού.
- 17.** Μην εισάγετε ή αποθηκεύετε βιομετρικά στοιχεία άλλων ατόμων στη Κινητή σας Συσκευή.
- 18.** Αλλάζετε τον κωδικό PINt σας ανά τακτά χρονικά διαστήματα.
- 19.** Μην ορίζετε κωδικό PINt που είναι πολύ απλός. Αποφύγετε απλούς συνδυασμούς ψηφίων, ή συνδυασμούς που σχετίζονται με την ημερομηνία ή το έτος γέννησής σας.
- 20.** Διαβάζετε προσεκτικά τα κείμενα των μηνυμάτων SMS ή των ειδοποιήσεων τύπου “Push Notification” (Άμεση Ειδοποίηση) που σας αποστέλλει η Τράπεζα. Πριν εισάγετε έναν κωδικό που λάβατε από την Τράπεζα, ελέγξτε την ενέργεια στην οποία αναφέρεται αυτός ο κωδικός. Μην εισάγετε τον κωδικό εάν δεν αναγνωρίζετε την ενέργεια ως δική σας. Πριν επιβεβαιώσετε μια συναλλαγή πληρωμής, ελέγξτε προσεκτικά τα μηνύματα που περιέχουν πληροφορίες για το ποσό της συναλλαγής και το νόμισμα, καθώς και τους λογαριασμούς του εντολέα και του παραλήπτη. Εάν έχετε αμφιβολίες ή λάβετε μήνυμα που περιέχει ενέργεια που δεν αναγνωρίζετε, μην εκτελέσετε περαιτέρω βήματα για επιβεβαίωση, όπως παροχή κωδικών. Επικοινωνήστε αμέσως με την Fibank.
- 21.** Για λόγους ασφαλείας, η Τράπεζα ενημερώνει τους πελάτες της, μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου ή ειδοποιήσεων SMS, κάθε φορά που η Εφαρμογή Κινητού ενεργοποιείται σε νέα συσκευή. Να είστε προσεκτικοί! Σε περίπτωση που λάβετε μήνυμα για ενεργοποίηση της Εφαρμογής Κινητού σας σε συσκευή που δεν αναγνωρίζετε, επικοινωνήστε αμέσως με την Τράπεζα στους αριθμούς τηλεφώνου που αναφέρονται ανωτέρω, καθώς και στους Γενικούς Όρους και Προϋποθέσεις για την Ψηφιακή Τραπεζική Υπηρεσία My Fibank.
- 22.** Μπορείτε να αλλάζετε τη διάρκεια των συνεδριών σας στην Εφαρμογή Κινητού από το μενού «Προφίλ», «Τερματισμός συνεδρίας» (Session timeout), ανάλογα με το είδος των συναλλαγών που επιθυμείτε να εκτελέσετε. Μην ορίζετε υπερβολικά μεγάλη διάρκεια.
- 23.** Μπορείτε να αλλάζετε τον τρόπο σύνδεσης και έγκρισης για χρήση της Εφαρμογής Κινητού και εκτέλεση όλων των ειδών συναλλαγών από το μενού «Προφίλ», «Πολιτική σύνδεσης και έγκρισης» (Login and authorization policy).
- 24.** Χρησιμοποιήστε το μενού «Προφίλ», «Ειδοποιήσεις» (notifications) για να ορίσετε τα είδη ειδοποιήσεων τύπου “Push Notification” (Άμεση Ειδοποίηση) που επιθυμείτε να λαμβάνετε σχετικά με τις συναλλαγές πληρωμών σας ή/και άλλες πληροφορίες αναφοράς, ώστε να είστε πάντα ενημερωμένοι και να μπορείτε να αντιδράσετε άμεσα σε περίπτωση ύποπτης δραστηριότητας σε σχέση με τον λογαριασμό σας.

ΜΕΤΡΑ ΚΑΤΑ ΤΗ ΧΡΗΣΗ ΤΗΣ ΚΙΝΗΤΗΣ ΣΑΣ ΣΥΣΚΕΥΗΣ

- 25.** Ενεργοποιείτε πρόσθετη ασφάλεια στην Κινητή σας Συσκευή, όπως κωδικό ξεκλειδώματος, αναγνώριση προσώπου, δακτυλικό αποτύπωμα, χειρονομίες, κ.λ.π., ανάλογα με το μοντέλο και τον τύπο της συσκευής. Με αυτόν τον τρόπο θα αυξήσετε την ασφάλειά σας σε περίπτωση απώλειας ή κλοπής της συσκευής.
- 26.** Μην επιτρέπετε τη χρήση της Κινητής σας Συσκευής από τρίτους, συμπεριλαμβανομένων παιδιών, γονέων και συζύγων. Μην αποθηκεύετε βιομετρικά στοιχεία τρίτων σε αυτήν.
- 27.** Σε περίπτωση απώλειας/κλοπής της Κινητής Συσκευής, επικοινωνήστε με την Τράπεζα για να φράξετε τον λογαριασμό σας στην Εφαρμογή Κινητού My Fibank.
- 28.** Εάν υποπτεύεστε επίθεση hacker ή κλοπή δεδομένων, συμπεριλαμβανομένων κωδικών/PINs ή ονομάτων χρηστών, ειδοποιήστε αμέσως την Τράπεζα.
- 29.** Μην εγκαθιστάτε ή χρησιμοποιείτε λογισμικό/εφαρμογές αμφίβολης προέλευσης.
- 30.** Ενημερώνετε πάντα το λειτουργικό σύστημα της Κινητής σας Συσκευής στην τελευταία δυνατή έκδοση. Μέσω αυτών των ενημερώσεων οι κατασκευαστές εξαλείφουν τρωτά σημεία που εντοπίστηκαν σε προηγούμενες εκδόσεις του συστήματος. Ακολουθείτε προσεκτικά τις οδηγίες του κατασκευαστή.
- 31.** Μη χρησιμοποιείτε, στο πλαίσιο ψηφιακής τραπεζικής υπηρεσίας, κινητές συσκευές στις οποίες έχουν αποκτηθεί «δικαιώματα διαχειριστή» (rooting ή jailbreaking) προκειμένου να παρέχουν αυξημένα ή εκτεταμένα δικαιώματα χρήση. Τέτοιες συσκευές μπορεί να επιτρέψουν σε κακόβουλους τρίτους να αποκτήσουν πλήρη και μη εξουσιοδοτημένη πρόσβαση στα δεδομένα που αποθηκεύονται σε αυτές τις συσκευές.

ΑΠΕΙΛΕΣ ΣΤΗΝ ΕΠΟΧΗ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

- 32.** Καθώς η τεχνολογία προοδεύει, κακόβουλοι τρίτοι χρησιμοποιούν νέες μεθόδους κοινωνικής μηχανικής, συμπεριλαμβανομένων χειραγωγημένων κλήσεων και οπτικοακουστικών μηνυμάτων.
- 33.** Να είστε προσεκτικοί όταν λαμβάνετε κλήσεις που ακούγονται παράξενες ή χρησιμοποιούν ρομποτικές ή αφύσικες φωνές. Οι σύγχρονες τεχνολογίες όπως το «deepfake» επιτρέπουν μίμηση φωνής υψηλής πιστότητας. Εάν λάβετε κλήση που απαιτεί εμπιστευτικές πληροφορίες ή πρόσβαση στους λογαριασμούς σας, τερματίστε την κλήση και επικοινωνήστε απευθείας με την Τράπεζα.
- 34.** Όπως αναφέρθηκε ανωτέρω, η Fibank δεν ζητά από τους πελάτες της να παρέχουν κωδικούς, αναγνωριστικά χρηστών, κωδικούς πρόσβασης υπηρεσιών (π.χ. στο My Fibank), κωδικούς PIN, αριθμούς τραπεζικών καρτών ή άλλες εμπιστευτικές πληροφορίες. Ωστόσο, κακόβουλοι τρίτοι χρησιμοποιούν όλο και περισσότερο προηγμένες τεχνολογίες και εργαλεία τεχνητής νοημοσύνης για να εξαπατήσουν πιθανά θύματα. Οπτικοακουστικό υλικό από το Διαδίκτυο, όπως φωτογραφίες και βίντεο από επίσημες εκδηλώσεις, τους επιτρέπουν να αναδημιουργήσουν ένα αληθοφανές βίντεο ενός στενού συγγενή, ή ενός εργαζόμενου στην

τράπεζα όπως του CEO, στο οποίο ζητούν από τους χρήστες να παρέχουν πληροφορίες. Η πίεση ασκείται συνήθως δημιουργώντας μία αίσθηση επείγοντος. Παρότι η τεχνητή νοημοσύνη παράγει σχεδόν όμοια πρόσωπα, δεν είναι τέλεια και υπάρχουν τρόποι να αναγνωρίσετε ένα βίντεο που έχει δημιουργηθεί με τεχνητή νοημοσύνη.

- 35.** Οι εικόνες που δημιουργούνται με τεχνητή νοημοσύνη έχουν στοιχεία που αποκαλύπτουν την προέλευσή τους, όπως αφύσικες κινήσεις ή εκφράσεις του πρόσωπο του ατόμου του οποίου η ταυτότητα έχει παραποιηθεί, ή λάθος αριθμό δακτύλων στα χέρια. Τα μοντέλα τεχνητής νοημοσύνης που χρησιμοποιούνται για τη δημιουργία συνθετικών μέσων συχνά έχουν δυσκολία με αυτές τις λεπτομέρειες και μπορεί να παραμορφώσουν χαμόγελα ή να τοποθετήσουν περισσότερα ή λιγότερα δάκτυλα στα χέρια, στο βαθμό που το οπτικό υλικό περιέχει τέτοια καρέ.

Αυτά τα **Μέτρα Ασφαλείας** έχουν δημοσιευτεί στην εταιρική ιστοσελίδα της Τράπεζας στη διεύθυνση www.fibank.gr. Ενδέχεται να ανανεώνονται όποτε είναι απαραίτητο, επομένως συνιστάται οι πελάτες να τα εξετάζουν ανά τακτά χρονικά διαστήματα.

Μείνετε Ενημερωμένοι.