

Κατευθυντήριες γραμμές και προτάσεις για την ασφάλεια των ηλεκτρονικών μεταφορών/συναλλαγών.

Το παρόν έγγραφο περιέχει βασικές πληροφορίες σχετικά με την ασφάλεια των μεταφορών / συναλλαγών μέσω του Διαδικτύου και προτάσεις για την ασφαλή και υπεύθυνη χρήση της Facto Προθεσμιακή, του λογαριασμού καταθέσεων της BFF Bank S.p.A.-Ελληνικό Υποκατάστημα (η "Τράπεζα"). Η Τράπεζα παραμένει διαθέσιμη για οποιεσδήποτε επιπλέον πληροφορίες σχετικά με αυτά τα θέματα.



1. Πρόσβαση στον ιστότοπο και εφαρμογή

Τεχνολογικές απαιτήσεις

Για να αποκτήσετε πρόσβαση στη Facto Προθεσμιακή, πρέπει να έχετε σύνδεση στο διαδίκτυο μέσω έναν ISP (Internet Service Provider / Πάροχο Υπηρεσιών Διαδικτύου) της επιλογής σας και να εξοπλιστείτε με μια συσκευή (π.χ. προσωπικό υπολογιστή, tablet) ικανή για να δημιουργήσει μια ασφαλή σύνδεση στο διαδίκτυο μέσω της χρήσης ενός ενημερωμένου antivirus και firewall.

Η υπηρεσία είναι προσβάσιμη με τη χρήση υποστηριζόμενων λειτουργικών συστημάτων και προγραμμάτων περιήγησης.

Τα διαπιστευτήριά σας

Για να αποκτήσετε πρόσβαση στο Facto Προθεσμιακή και να δώσετε εντολές / αιτήματα μέσω του δικτυακού τόπου της Τράπεζας, πρέπει να χρησιμοποιήσετε τους κωδικούς πρόσβασης που σας έχουν δοθεί από την ίδια την Τράπεζα. Το όνομα χρήστη και ο κωδικός πρόσβασής σας αποτελούν τα κλειδιά πρόσβασής σας στη Facto Προθεσμιακή: προστατέψτε τα σαν να είναι τα κλειδιά του σπιτιού σας! Μην τα καταγράφετε στο κινητό σας τηλέφωνο ή σε μέσα που μπορούν να κλαπούν.

Ένας αποτελεσματικός ισχυρός κωδικός πρόσβασης:

- δεν περιέχει προσωπικές πληροφορίες (ημερομηνία γέννησης, όνομα και επώνυμο),
- δεν περιέχει ακολουθίες γραμμάτων ή αριθμών (π.χ. 1234, abcd),
- δεν είναι το ίδιο για όλες τις προσβάσεις (λογαριασμός, email, ιστότοπος),
- πρέπει να αλλάζεται τουλάχιστον κάθε τρεις μήνες.

Μετά από 5 λανθασμένες προσπάθειες, ο κωδικός πρόσβασης θα μπλοκαριστεί για 1 ώρα, μετά την πάροδο αυτής της περιόδου, θα μπορείτε να τον χρησιμοποιήσετε ξανά. Για να αποφευχθεί η δόλια χρήση, σε περίπτωση που εάν ένας συνδεδεμένος χρήστης παραμείνει ανενεργός για ορισμένο χρονικό διάστημα, το σύστημα τον αποσυνδέει αυτόματα.

Να είστε ιδιαίτερα προσεκτικοί εάν παρατηρήσετε ξαφνικές αλλαγές στον τρόπο με τον οποίο σας ζητείται να εισάγετε τους κωδικούς πρόσβασης. Για παράδειγμα, εάν οι κωδικοί ζητούνται μέσω ενός αναδυόμενου παραθύρου αντί μέσω της σελίδας του ιστότοπου. Σε αυτή την περίπτωση, επικοινωνήστε άμεσα με την Τράπεζα μέσω της υπηρεσίας εξυπηρέτησης πελατών στο +30 2111994372 ή μέσω mail: info_factoprothesmiaki@bff.com.

Επαλήθευση πρωτοκόλλου

Βεβαιωθείτε ότι οι ιστοσελίδες στις οποίες εισάγετε τα διαπιστευτήρια σύνδεσης και τα προσωπικά σας δεδομένα είναι ασφαλείς, προστατευμένες και προσέξτε τα "αναδυόμενα παράθυρα". Για να επιβεβαιώσετε ότι η ιστοσελίδα είναι ασφαλής, ελέγξτε ότι στη διεύθυνση προηγείται η λέξη "https://" και ότι στο πρόγραμμα περιήγησης εμφανίζει το εικονίδιο που υποδηλώνει σύνδεσμο προς προστατευμένο ιστότοπο, το οποίο συνήθως απεικονίζει ένα κλειστό λουκέτο δίπλα στη διεύθυνση διαδικτύου.

Κατά την έξοδο από τον ιστότοπο, επιλέξτε "ΛΗΞΗ" πριν κλείσετε τη σελίδα, ανεξάρτητα από τον τύπο της συσκευής που χρησιμοποιείτε.

Ασφάλεια καναλιών επικοινωνίας

Για όλες τις ανταλλαγές δεδομένων πληρωμών-μεταφορών μέσω του Διαδικτύου, η ασφάλεια των διαύλων επικοινωνίας μεταξύ των εμπλεκόμενων μερών είναι εγγυημένη χάρη σε

- μέτρα κρυπτογράφησης και ασφάλειας καθ' όλη την διάρκεια της συνεδρίας,
- αποτελεσματικές και διεθνώς αποδεκτές τεχνολογίες κρυπτογράφησης.

Ο κωδικός OTP

Σε κάθε κρίσιμη επιλογή σας, όπως όταν πρέπει να ενεργοποιήσετε μια Προθεσμιακή κατάθεση, να αλλάξετε τον συνδεδεμένο λογαριασμό, να ζητήσετε κλείσιμο λογαριασμού κλπ, θα σας αποστέλλεται ένας κωδικός OTP (One-Time Password) για να επιβεβαιώσετε την αιτούμενη λειτουργία. Ο OTP είναι ένας κωδικός που ισχύει μόνο για μία (μοναδική εγγραφή) συνεδρία πρόσβασης ή συναλλαγής.

Οι κωδικοί OTP θα αποστέλλονται μέσω email ή SMS ανάλογα με το κανάλι που επιλέξατε για την αποστολή του κωδικού επιβεβαίωσης.

Επιπρόσθετα, για να διασφαλιστεί η συμμόρφωση με τις απαιτήσεις ασφαλείας, αποστέλλεται αυτόματα στον πελάτη ένα OTP μέσω SMS για την επιβεβαίωση κάθε εξερχόμενης μεταφοράς. Επιπλέον, για την πρόσβαση στο Home Banking απαιτείται εξουσιοδότηση πολλαπλών παραγόντων όπου εκτός από τη χρήση των προσωπικών κωδικών (username & password), οι πελάτες πρέπει να επιλέξουν ένα επιπλέον κανάλι επαλήθευσης: OTP μέσω SMS, OTP μέσω email ή εφαρμογή Authenticator.

Προσοχή:

Κανένας υπάλληλος της Τράπεζας δεν είναι εξουσιοδοτημένος να ζητήσει τους κωδικούς πρόσβασής σας. Η Τράπεζα δεν θα στείλει ποτέ αίτημα, είτε αυτό γίνεται αυτοπροσώπως είτε μέσω τηλεφώνου, ταχυδρομείου, ηλεκτρονικού ταχυδρομείου ή άλλων μέσων.



2. Κανόνες άμυνας

Οι προσωπικοί υπολογιστές, τα smartphones και όλες οι συσκευές που χρησιμοποιούνται την πρόσβαση στο Διαδίκτυο είναι εξελιγμένα εργαλεία. Είναι σημαντικό να γνωρίζετε τη σωστή συμπεριφορά ασφάλειας στο διαδίκτυο για να αποφύγετε την ανεύθυνη χρήση.

Τα μηνύματα ηλεκτρονικού ταχυδρομείου που προέρχονται από ύποπτες διευθύνσεις ή σας ζητούν να ακολουθήσετε ασυνήθιστους συνδέσμους, καθώς και τα προγράμματα που σας προσεγγίζουν να κατεβάσετε ύποπτα έγγραφα ή που προέρχονται από απροσδόκητες πηγές μπορεί να φέρουν κακόβουλο περιεχόμενο.

Για να διασφαλιστεί η πλοήγηση στο υψηλότερο επίπεδο, είναι απαραίτητο:

- Να προστατέψετε τα προσωπικά σας δεδομένα και να φυλάξετε με προσοχή τα στοιχεία πρόσβασής σας στον ιστότοπο (όνομα χρήστη και κωδικός πρόσβασης). Αποφύγετε την αποθήκευσή τους στον υπολογιστή σας, διατηρώντας το όνομα χρήστη και τον κωδικό πρόσβασης ξεχωριστά και αλλάζοντας τον κωδικό πρόσβασης περιοδικά.),
- ΠΟΤΕ μην δίνετε τους κωδικούς σας σε τρίτους,
- Να έχετε πάντοτε πρόσβαση στις ηλεκτρονικές υπηρεσίες πληκτρολογώντας www.factoprothesmiaki.bff.com & www.factoprothesmiaki.gr, αποφεύγοντας να κάνετε κλικ σε συνδέσμους που περιέχονται στα μηνύματα ηλεκτρονικού ταχυδρομείου και ακολουθώντας τα αιτήματα που περιέχονται σε αυτά,
- Να δίνετε ιδιαίτερη προσοχή στην παρουσία "παραποιημένων" σελίδων, δηλαδή σελίδων με διαφορετική γραφική εμφάνιση από εκείνη της εφαρμογής διαδικτυακής τραπεζικής ή με ύποπτο περιεχόμενο (π.χ. μηνύματα που δεν είναι στα Ελληνικά),
- Να ελέγχετε τακτικά τις καταστάσεις των καταθέσεών σας για να διασφαλίζετε ότι οι συναλλαγές που αναφέρονται είναι αυτές που πράγματι πραγματοποιήθηκαν.

Για να προστατευτείτε από απειλές που θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια των δεδομένων και των συσκευών σας, συνιστούμε τα εξής:

- μην κατεβάζετε ποτέ προγράμματα από ύποπτες ή αμφίβολες τοποθεσίες/ιστότοπους,
- μην μοιράζεστε αρχεία στο διαδίκτυο. Ο διαμοιρασμός αρχείων στο Διαδίκτυο σημαίνει ότι αφήνετε μια "ανοιχτή πόρτα" με κίνδυνο ιών ή/και εισβολών από το εξωτερικές επιθέσεις. Συγκεκριμένο λογισμικό, γνωστό ως spyware (είδη λογισμικού που συλλέγουν πληροφορίες τη διαδικτυακή δραστηριότητα ενός χρήστη, όπως ιστοσελίδες που επισκέπτεται, αγορές που πραγματοποιεί στο διαδίκτυο κ.λπ. χωρίς τη συγκατάθεσή του), μπορεί εύκολα να αποκτήσει πρόσβαση στον υπολογιστή σας και να "συλλάβει" προσωπικές πληροφορίες στο διαδίκτυο χωρίς να το γνωρίζετε,
- μην ανοίγετε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου που έχουν συνημμένο αρχείο, ακόμη και αν γνωρίζετε τον αποστολέα (μπορεί να είναι πλαστό),
- να είστε επιφυλακτικοί με οποιοδήποτε μήνυμα ηλεκτρονικού ταχυδρομείου που σας ζητά να εισάγετε εμπιστευτικά δεδομένα σχετικά με κωδικούς πρόσβασης σε τραπεζικές υπηρεσίες ή άλλες προσωπικές πληροφορίες. Η Τράπεζα δεν ζητά τέτοιες πληροφορίες μέσω ηλεκτρονικού ταχυδρομείου,
- Ποτέ μην κατεβάζετε προγράμματα με τη μορφή ActiveX. Το ActiveX είναι μια τεχνολογία που, όταν ενσωματώνεται σε μια εφαρμογή, καθιστά δυνατή την προσθήκη νέων δυνατοτήτων, εντολών και ενδεχομένως την απλούστευση ορισμένων διαδικασιών, ιδίως στον τομέα της ανάπτυξης λογισμικού. Εάν επισκέπτεστε ιστοσελίδες που απαιτούν τη χρήση ActiveX, προσθέστε τις στη λίστα περιορισμένων ιστότοπων του προγράμματος περιήγησής σας.
- Διατηρείτε το λειτουργικό σας σύστημα και το πρόγραμμα περιήγησης ενημερωμένα, κατεβάζοντας τις κατάλληλες ενημερώσεις (διορθώσεις λογισμικού που έχουν σχεδιαστεί για να ενημερώνουν ή να βελτιώνουν ένα πρόγραμμα). Αυτό περιλαμβάνει τη διόρθωση ευπαθειών ασφαλείας και άλλων γενικών σφαλμάτων. Οι εν λόγω ενημερώσεις, γνωστές και ως patches ή διορθώσεις σφαλμάτων, βελτιώνουν επίσης τη χρηστικότητα και την απόδοση της εφαρμογής. Κατεβάστε τις ενημερώσεις από τον επίσημο ιστότοπο του προμηθευτή του συστήματός.

- εγκαταστήστε ένα πρόγραμμα προστασίας από ιούς και ενημερώστε το συχνά,
- ενδεχομένως να εγκαταστήσετε ένα προσωπικό τείχος προστασίας (ένα στοιχείο ασφάλειας υπολογιστών με σκοπό τον έλεγχο της πρόσβασης στους πόρους ενός συστήματος φιλτράροντας όλη την κυκλοφορία που ανταλλάσσει το σύστημα αυτό με εξωτερικές πηγές),
- να μην επιτρέπετε, κατά την πλοήγησή σας στο Διαδίκτυο, την εκτέλεση απομακρυσμένων δραστηριοτήτων χωρίς την άδειά σας και να επιτρέπετε την εγκατάσταση από το διαδίκτυο μόνο προγραμμάτων των οποίων η προέλευση και η αξιοπιστία μπορούν να επαληθευτούν.



3. Τι να κάνετε σε περίπτωση που...;

Έχετε αμφιβολίες ότι έχετε υποστεί απάτη ή απόπειρα απάτης;

Εάν πιστεύετε ότι έχετε υποστεί απάτη ή απόπειρα απάτης, επικοινωνήστε αμέσως με την Τράπεζα καλώντας την Υπηρεσία Εξυπηρέτησης Πελατών (αριθμός επικοινωνίας +302111994372 ή μέσω mail: info_factoprothesmiaki@bff.com)

Έμαθε κανείς ή υποψιάζεστε ότι έμαθε κανείς για τα διαπιστευτήριά σας;

Σε περίπτωση απώλειας, κλοπής, υπεξαίρεσης ή μη εξουσιοδοτημένης χρήσης (ή υποψίας χρήσης) των διαπιστευτηρίων πρόσβασής σας, πρέπει να ενημερώσετε αμέσως την Τράπεζα καλώντας την Υπηρεσία Εξυπηρέτησης Πελατών, αριθμός επικοινωνίας +30 2111994372 ή μέσω mail: info_factoprothesmiaki@bff.com.

Η Τράπεζα θα μπλοκάρει τους κωδικούς πρόσβασης εντός του απαραίτητου τεχνικού χρονικού πλαισίου και θα αρχίσει αμέσως τους δικούς της ελέγχους:

σε περίπτωση που δεν προκύψουν ανωμαλίες, η Τράπεζα θα σας ενημερώσει αμέσως για το γεγονός αυτό.

Εάν προκύψουν ανωμαλίες, η Τράπεζα θα σας ενημερώσει άμεσα για τις ανωμαλίες που εντοπίστηκαν και την πιθανή απάτη ή παραβίαση της ασφάλειας, ενώ παράλληλα θα δρομολογήσει τις απαραίτητες ενέργειες για την αντιμετώπιση του συμβάντος. Σε κάθε περίπτωση και εφόσον απαιτηθεί (πχ κλιμάκωση του συμβάντος) θα ζητηθεί η παρέμβαση των αρμοδίων Αρχών, οι οποίες θα ξεκινήσουν τη δική τους έρευνα. Ο πελάτης θα πρέπει να αποστείλει γραπτή επιβεβαίωση του συμβάντος είτε μέσω HomeBanking (με επισύναψη αναλυτικής περιγραφής), είτε μέσω email είτε με συστημένη επιστολή. Η Τράπεζα θα σας ενημερώνει συνεχώς για την πρόοδο της έρευνας και θα σας κρατά ενήμερους για την έκβαση του περιστατικού.

Έχετε χάσει ή σας έχουν κλέψει το πιστοποιημένο κινητό σας τηλέφωνο;

Αλλάξτε τον μόνιμο κωδικό πρόσβασής σας στον ιστότοπο απευθείας από το HomeBanking, αποκτώντας πρόσβαση στην ενότητα "Προφίλ- Όνομα Χρήστη & Κωδικός Πρόσβασης" και επικοινωνήστε με την Εξυπηρέτηση Πελατών στο +30 2111994372 για να ενημερώσετε την Τράπεζα για το περιστατικό.

Δεν θυμάστε πλέον το όνομα χρήστη σας ή έχετε ξεχάσει τον κωδικό πρόσβασης για τον ιστότοπο;

Μπαίνοντας στην επίσημη σελίδα της Τράπεζας, Home Banking για να συνδεθείτε, θα χρειαστεί να εισέλθετε στην ενότητα 'Ξεχάσατε το όνομα χρήστη ή τον κωδικό πρόσβασής σας;'. Εκεί θα συμπληρώσετε το ΑΦΜ σας και στην συνέχεια θα σας ζητηθεί να επιλέξετε το κανάλι λήψης (κινητό τηλέφωνο ή email) κωδικού OTP για την επιβεβαίωση των στοιχείων. Με την λήψη και στην συνέχεια συμπλήρωση του συγκεκριμένου κωδικού λαμβάνετε το όνομα χρήστη στο email σας. Ως επόμενο βήμα θα σας ζητηθεί να συμπληρώσετε το νέο κωδικό πρόσβασης σύμφωνα με το ζητούμενο μοτίβο ασφάλειας. Αν συνεχίζετε να αντιμετωπίζετε προβλήματα μπορείτε να μας αποστείλετε email με τα στοιχεία σας στο info_factoprothesmiaki@bff.com και ένας εκπρόσωπος της Facto Προθεσμιακή θα επικοινωνήσει μαζί σας το συντομότερο δυνατόν.

Χρειάζεστε περαιτέρω βοήθεια με την ασφάλεια on-line συναλλαγών;

Εάν έχετε περαιτέρω ερωτήσεις ή αιτήματα για βοήθεια σχετικά με την ασφάλεια των on-line συναλλαγών, επικοινωνήστε με την Εξυπηρέτηση Πελατών καλώντας στο +30 2111994372 από Δευτέρα έως Παρασκευή από τις 09:00 έως τις 16.00.

Θέλετε να υποβάλετε καταγγελία σχετικά με την ασφάλεια των πληρωμών-μεταφορών;

Για παράπονα σχετικά με την ασφάλεια των μεταφορών/συναλλαγών, ο Πελάτης μπορεί να υποβάλει καταγγελία / παράπονο στην Τράπεζα με τους εξής τρόπους γραπτώς:

- με επιστολή που αποστέλλεται ταχυδρομικά στην ακόλουθη διεύθυνση: Λεωφ. Πεντέλης 72, 15234 Χαλάνδρι, Αττική, Ελλάδα, ή
- με μήνυμα ηλεκτρονικού ταχυδρομείου (e-mail), στην ακόλουθη διεύθυνση: BFGcomplaints@bff.com.



4. Κύριοι τύποι απάτης και επιθέσεων στον κυβερνοχώρο

Το ηλεκτρονικό ταχυδρομείο είναι το κύριο εργαλείο που χρησιμοποιείται για την ηλεκτρονική απάτη. Παριστάνοντας την Τράπεζα, οι απατεώνες μπορούν να ζητήσουν προσωπικά δεδομένα εκμεταλλευόμενοι την καλή πίστη του πελάτη. Ακολουθούν μερικές απλές συμβουλές για να αποφύγετε αυτές τις απάτες: μία από αυτές είναι το λεγόμενο phishing.

Phishing

Το Phishing ("ψάρεμα") είναι μια από τις πιο διαδεδομένες τεχνικές απάτης μέσω υπολογιστή που αποσκοπεί στη κλοπή ψηφιακής ταυτότητας. Οι ηλεκτρονικές απάτες αυτού του είδους, γνωστές ως "phishing", συνίστανται στη δημιουργία και χρήση ηλεκτρονικών μηνυμάτων ή ιστότοπων που συνδέονται φαινομενικά με χρηματοπιστωτικά ιδρύματα και

έχουν πιθανότητες επιτυχίας μόνο εάν οι απατεώνες καταφέρουν να οικειοποιηθούν τα προσωπικά διαπιστευτήρια πρόσβασης, καθώς και τα διαπιστευτήρια πρόσβασης των κατόχων Τραπεζικών υπηρεσιών.

Τα ηλεκτρονικά μηνύματα phishing περιέχουν συνήθως έναν σύνδεσμο που οδηγεί σε ιστοσελίδες παρόμοιες με αυτής της Τράπεζας, όπου ο χρήστης καλείται να εισάγει στοιχεία λογαριασμού. Είναι δυνατόν να αναγνωρίσετε τις απάτες ηλεκτρονικού ταχυδρομείου με λίγη προσοχή.

Σε γενικές γραμμές, αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου:

- δεν είναι εξατομικευμένα και περιέχουν ένα γενικό μήνυμα που ζητά προσωπικές πληροφορίες για απροσδιόριστους λόγους (π.χ. λήξη, απώλεια, τεχνικά προβλήματα),
- χρησιμοποιούν "εκφοβιστικούς" τόνους, π.χ. απειλώντας ότι θα αναστείλουν τον λογαριασμό αν ο χρήστης δεν ανταποκριθεί,
- υπόσχονται άμεση αμοιβή μετά την επαλήθευση των διαπιστευτηρίων της ταυτότητάς τους.

Κοινωνική μηχανική

Η "κοινωνική μηχανική" αποτελείται συνίσταται σε τεχνικές που χρησιμοποιούνται για τη χειραγώγηση ανθρώπων προκειμένου να αποκτηθούν πληροφορίες (π.χ. μέσω ηλεκτρονικού ταχυδρομείου ή τηλεφωνικών κλήσεων) ή να ανακτήσουν πληροφορίες από κοινωνικά δίκτυα, για δόλιους σκοπούς ή για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή ή δίκτυο.

Κακόβουλο λογισμικό

Το "κακόβουλο λογισμικό" αποτελείται από ένα πρόγραμμα υπολογιστή που χρησιμοποιείται για να διαταράξει τις λειτουργίες μιας συσκευής, να υποκλέψει ευαίσθητες πληροφορίες, να αποκτήσει πρόσβαση σε ιδιωτικά συστήματα υπολογιστών ή να εμφανίσει ανεπιθύμητη διαφήμιση.



5. Ασφαλές κανάλι και ενημερώσεις ασφαλείας

Η Τράπεζα αποστέλλει τις τακτικές ανακοινώσεις της σχετικά με την ορθή και ασφαλή χρήση υπηρεσιών μεταφορών & on line συναλλαγών, μέσω του Διαδικτύου αποκλειστικά μέσω του δικτυακού της τόπου. Συνεπώς, θα πρέπει να είναι κανείς προσεκτικός απέναντι σε οποιαδήποτε επικοινωνία εκ μέρους της Τράπεζας που λαμβάνεται μέσω άλλων καναλιών, π.χ. μέσω ηλεκτρονικού ταχυδρομείου.

Η Τράπεζα επανεξετάζει και επικαιροποιεί το παρόν έγγραφο σε τακτά χρονικά διαστήματα, καθώς και με την ευκαιρία τυχόν αλλαγών στις διαδικασίες ασφαλείας της και όταν εντοπίζονται κατά καιρούς νέοι σημαντικοί αναδυόμενοι κίνδυνοι. Τυχόν αλλαγές ή/και προσθήκες στην παρούσα ειδοποίηση θα κοινοποιούνται στον πελάτη μέσω του προαναφερθέντος ασφαλούς καναλιού.