Διαδικτυακά προβλήματα

Παρόλο που μέσω του διαδικτύου μπορείτε να έχετε πρόσβαση στους τραπεζικούς σας λογαριασμούς οποιαδήποτε στιγμή το επιθυμείτε, πρέπει να επιστήσουμε την προσοχή σας σε κινδύνους που υπάρχουν.

Λόγω της φύσης του διαδικτύου, συστήματα τα οποία παρέχουν πρόσβαση σε χρήστες μέσω του, υπόκεινται σε «επιθέσεις» από μη χρήστες των συστημάτων αυτών, που προσπαθούν να κερδίσουν πρόσβαση σε αυτά τα συστήματα.

Παρόλο που η τράπεζα εφαρμόζει τις υπάρχουσες λύσεις για την ασφάλεια των πελατών της έναντι τρίτων, δεν μπορεί να εγγυηθεί πλήρως την ασφάλεια σας. Ως χρήστης του διαδικτύου διαδραματίζετε ένα σημαντικό ρόλο στην ασφάλεια του λογαριασμού σας.

Μέτρα ασφαλείας που παρέχει η Alpha Bank Cyprus Ltd στους πελάτες της.

Η Alpha Bank Cyprus Ltd είναι δεσμευμένη στην παροχή μέγιστης ασφάλειας στους χρήστες της για ασφαλείς συναλλαγές μέσω του διαδικτύου.

Η Alpha Bank Cyprus Ltd εφαρμόζει διεθνώς αναγνωρισμένα πρότυπα, τα οποία χρησιμοποιούνται και από διεθνείς τράπεζες, για την ασφάλεια των προσωπικών σας δεδομένων καθώς και την ασφαλή διεκπεραίωση συναλλαγών σας μέσω διαδικτύου. Επίσης η Τράπεζα μας έχει συνεχή αναβάθμιση των συσκευών και προτύπων τα οποία διασφαλίζουν την ασφάλεια των πελατών μας.

Τα μέτρα ασφαλείας τα οποία λειτουργούν στην Τράπεζα μας είναι:

- ***Χρησιμοποίηση κωδικοποίησης 128-bit SSL***
    - Το Alpha Express Banking είναι επικυρωμένο από την VeriSign. Αυτό είναι μια πιστοποίηση για τους πελάτες της Τράπεζας μας ότι το περιεχόμενο των σελίδων του Alpha Express Banking αποστέλλεται κωδικοποιημένο μέσω Secure Socket Layer (SSL) session ούτως ώστε οι πληροφορίες αυτές να μην είναι αναγνώσιμες από άλλο χρήστη.
    - Στο παρόν στάδιο η 128-bit κωδικοποίηση δεδομένων είναι η ισχυρότερη που υπάρχει. Οποιαδήποτε πληροφορία αποστέλλεται από τον χρήστη στην Τράπεζα μας μέσω του Alpha Express Banking, κωδικοποιείται για να μην είναι αναγνώσιμη προτού αποσταλεί στον κεντρικό μας υπολογιστή. Με τη παραλαβή του κωδικοποιημένου μηνύματος η τράπεζα μας χρησιμοποιώντας ένα «κλειδί» μπορεί να αποκωδικοποιήσει το μήνυμα που έχει παραλάβει από τον πελάτη. Οποιαδήποτε πληροφορία αποστέλλεται από την Τράπεζα προς τον χρήστη τυχαίνει της ίδιας διαδικασίας για την μέγιστη προστασία των πληροφοριών του χρήστη.
      [128-bit κωδικοποιημένα μηνύματα είναι αρκετά τρισεκατομμύρια φορές (309,485,000,000,000,000,000,000,000,000) δυσκολότερο να αποκωδικοποιηθούν έναντι των 40-bit μηνυμάτων. Ο ισχυρότερος υπολογιστής σήμερα θα χρειαζόταν 1 τρισεκατομμύριο x 1 τρισεκατομμύριο χρόνια για να αποκωδικοποιήσει ένα μήνυμα].

- ***Προσωπικός Αριθμός Ασφαλείας (PIN) και αριθμός Χρήστη (User ID)***
    - Σαν πρώτο μέτρο ασφάλειας, παρέχουμε σε κάθε νέο χρήστη δυο κωδικούς πρόσβασης στο Alpha Express Banking. Με αυτό τον τρόπο ο χρήστης πρέπει να καταχωρήσει τον αριθμό του χρήστη καθώς και τον προσωπικό αριθμό ασφάλειας του για να μπορεί να έχει πρόσβαση στο διαδίκτυο της Τράπεζας μας.
    - Η χρήση του Alpha Express Banking βασίζεται στον αριθμό του χρήστη καθώς και τον προσωπικό αριθμό ασφαλείας οι οποίοι είναι μοναδικοί για τον κάθε χρήστη. Ο συνδυασμός των δυο αυτών κωδικών εξασφαλίζει την μοναδικότητα του χρήστη.
- ***Προσθετός Κωδικός Ασφαλείας (ΠΚΑ):***
    - Η συσκευή και η λειτουργία του Πρόσθετου Κωδικού Ασφαλείας συνδυάζει την αυξημένη ασφάλεια και την ευκολία στην εκτέλεση των ηλεκτρονικών συναλλαγών. Μέσω μιας ειδικής ηλεκτρονικής συσκευής γνωστής και ως Token, ο χρήστης είναι σε θέση να παράγει μοναδικούς κωδικούς αυθεντικότητας οι οποίοι συνδέονται μοναδικά με τους κωδικούς χρήστη (User Id). Για την εκτέλεση μιας νέας συναλλαγής στο Alpha Express Banking θα καλείστε να καταχωρείτε στην σχετική οθόνη ένα νέο αυθεντικό ''κωδικό'' που θα σας παράγει η συσκευή αυτή. Πιέζοντας το πλήκτρο της συσκευής παράγεται ένας κωδικός αριθμός μιας χρήσεως (''Πρόσθετος Κωδικός Ασφαλείας'' ή ''Π.Κ.Α''). Τα συστήματα της Τραπέζης θα επιβεβαιώνουν κάθε φορά τον εισαχθέντα Πρόσθετο Κωδικό Ασφαλείας και με τον τρόπο αυτό πιστοποιείται ότι η συναλλαγή προέρχεται πράγματι από το νόμιμο κάτοχο της συγκεκριμένης συσκευής.
- ***Αυτόματη αποσύνδεση από το σύστημα***
    - Αν μετά την πρόσβαση σας στην ιστοσελίδα του Alpha Express Banking αφήσετε ανενεργή την συγκεκριμένη σελίδα για ορισμένο χρονικό διάστημα, το σύστημα για λόγους ασφαλείας θα σας αποσυνδέσει. Αν επιθυμείτε επανασύνδεση στην ιστοσελίδα θα πρέπει να καταχωρήσετε και πάλι τους κωδικούς σας (*Προσωπικός Αριθμός Ασφαλείας (PIN) και αριθμός Χρήστη (User ID)*).

Ο ρόλος του πελάτη στην ασφάλεια των προσωπικών του δεδομένων

Εκτός από τα μέτρα ασφαλείας τα οποία παρέχει η Alpha Bank Cyprus Ltd, ο χρήστης συμβάλλει σημαντικά στην ασφάλεια των προσωπικών του δεδομένων.

Θα **ΠΡΕΠΕΙ** να τηρείτε τις ακόλουθες συμβουλές ασφαλείας που παρέχουμε για την προστασία των προσωπικών σας δεδομένων:

- Μόνο εσείς πρέπει να γνωρίζετε τον προσωπικό αριθμό ασφαλείας (PIN)
- Πάντοτε να χρησιμοποιείτε το μενού «Έξοδος» προτού κλείσετε την ιστοσελίδα του Alpha Express Banking
- Να **ΜΗΝ** φυλάσσονται οι κωδικοί πρόσβασης στον υπολογιστή σας
- Να **ΜΗΝ** δίνετε τα προσωπικά σας δεδομένα σε ύποπτες ιστοσελίδες
- Χρησιμοποιείτε υπολογιστή τον οποίο εμπιστεύεστε
- Χρησιμοποιήστε ασφαλή σύνδεση στο διαδίκτυο (ειδικά εάν συνδέεστε μέσω wireless internet το οποίο δεν ζητά κωδικούς για πρόσβαση)
- Καθάρισμα ιστορικού και προσωρινών αρχείων του Internet Explorer.
- Προστατεύετε τον υπολογιστή σας από ιούς και επιβλαβή προγράμματα
- Προστασία σημαντικών δεδομένων
- Αποσυνδέστε την "File and Printer Sharing" λειτουργία από το λογισμικό σας
- Ελέγχετε συχνά το ιστορικό συναλλαγών του λογαριασμού σας

- Ενημερώστε μας για αλλαγή προσωπικών στοιχείων (διεύθυνσης, τηλεφώνου, e-mail κτλ.)
- Ενημερώστε μας για τυχόν προβλήματα που θα συναντήσετε

- ***Ασφάλεια του προσωπικού σας κωδικού PIN***
  - Ο προσωπικός σας κωδικός αριθμός (PIN) είναι το «κλειδί» για την ασφαλή σύνδεση σας στην διαδικτυακή υπηρεσία του Alpha Express Banking. Η αναγνώριση του χρήστη για πρόσβαση στην υπηρεσία μας γίνεται με εισαγωγή του προσωπικού σας αριθμού καθώς και του προσωπικού σας κωδικού (User ID και PIN). Για αυτό τον λόγο θα πρέπει μόνο εσείς να γνωρίζετε αυτό τον κωδικό.
  - **Συμβουλές για την προστασία του προσωπικού σας κωδικού:**
    - **ΠΟΤΕ** μην χρησιμοποιείτε τον ίδιο κωδικό αριθμό με άλλες διαδικτυακές υπηρεσίες όπως τραπεζικές υπηρεσίες, ηλεκτρονικό ταχυδρομείο και άλλες διαδικτυακές υπηρεσίες.
    - **ΜΗΝ** χρησιμοποιείτε προσωπικό κωδικό αριθμό ο οποίος μαντεύεται εύκολα, για παράδειγμα αριθμός τηλεφώνου, αριθμός ταυτότητας, ημερομηνία γέννησης κ.α. Θα πρέπει να επιλέξετε ένα προσωπικό κωδικό ο οποίος είναι δύσκολος να μαντευθεί.
    - **ΜΗΝ** χρησιμοποιείτε συνεχόμενους αριθμούς (π.χ. 123456) ή τον ίδιο αριθμό περισσότερο από μια φορά (π.χ. 121145).
    - **ΜΗΝ** δίνετε τον κωδικό σας σε κανένα.
    - Αποστηθίστε τον προσωπικό σας κωδικό και μην τον φυλάσσετε στον υπολογιστή σας ή σε άλλα μη ασφαλή μέσα.
    - **ΜΗΝ** καταχωρείτε τον προσωπικό σας κωδικό όταν κάποιος σας βλέπει.
    - Προτού καταχωρήσετε τον προσωπικό αριθμό και κωδικό, όταν επισκέπτεστε το Alpha Express Banking, βεβαιωθείτε ότι η σελίδα η οποία επισκέπτεστε ξεκινά με την διεύθυνση https://online.alphabank.com.cy/
    - Όταν κάνετε πληρωμές μέσω της ιστοσελίδας μας βεβαιωθείτε ότι η διεύθυνση ξεκινά με https://online.alphabank.com.cy/.
    - Για χρήστες του Netscape, ένα εικονίδιο κλειδαριάς πρέπει να υπάρχει στην ιστοσελίδα.
    - Για χρήστες του Internet Explorer, μπορείτε να ελέγχετε την ασφάλεια της σελίδας κάνοντας δεξί κλικ στην σελίδα και μετά επιλέξτε "Properties" («Ιδιότητες»).
    - Πάντα χρησιμοποιείτε τα τελευταία λογισμικά τα οποία χρησιμοποιούν 128-bit κωδικοποίηση η οποία διασφαλίζει την μέγιστη σας ασφάλεια στο διαδίκτυο.
    - Αλλάζετε τον κωδικό ασφαλείας σας τακτικά μέσω της επιλογής «Συντήρηση» και μετά «Αλλαγή κωδικών πρόσβασης» (μεταξύ 6 και 9 ψηφίων).
    - Αλλάξετε τον προσωπικό σας κωδικό μόλις παρατηρήσετε κάτι ύποπτο στον λογαριασμό σας ή όταν κάποιος μάθει τον προσωπικό σας κωδικό.
    - Κλειδώστε τον λογαριασμό σας μόλις παρατηρήσετε κάτι ύποπτο. Μπορείτε να κλειδώσετε τον λογαριασμό σας καταχωρώντας 3 φορές λανθασμένο κωδικό πρόσβασης.

ΠΡΟΣΟΧΗ: ***Κανείς υπάλληλος της Alpha Bank Cyprus Ltd δεν θα σας ζητήσει τον προσωπικό σας κωδικό πρόσβασης (PIN number).***

- ***Πάντοτε να αποσυνδέεστε από την υπηρεσία μας***
  - Αποσυνδεθείτε από την διαδικτυακή υπηρεσία και κλείστε το παράθυρο της ιστοσελίδας όταν απομακρύνεστε από τον υπολογιστή σας, έστω και για ελάχιστο χρονικό διάστημα. Με αυτό τον τρόπο αποσυνδέεστε από την υπηρεσία μας και δεν μπορεί κάποιος να έχει πρόσβαση στον λογαριασμό σας χωρίς καταχώρηση προσωπικού αριθμού και κωδικού πρόσβασης. Θα πρέπει να αποσυνδέετε και τον ηλεκτρονικό σας υπολογιστή όταν δεν τον χρησιμοποιείτε για μεγάλο χρονικό διάστημα για να μην έχει πρόσβαση άλλος χρήστης στα δεδομένα σας.
  - Για ακόμα περισσότερη ασφάλεια μπορείτε να καταχωρήσετε κωδικό πρόσβασης και για τον screen saver ο οποίος αποτρέπει άλλους χρήστες στην χρήση του υπολογιστή σας. Για ενεργοποίηση της δικλίδας ασφαλείας:
    - Κάντε δεξί κλικ στο desktop («Επιφάνεια εργασίας»)
    - Επιλέξτε το "Properties" («Ιδιότητες»)
    - Κάντε κλικ στην επιλογή "Screen Saver" («Προστασία οθόνης»)
    - Επιλέξτε μια από τις επιλογές
    - Κάντε κλικ στην επιλογή "Password protected" («Έλεγχος κωδικού πρόσβασης»)
    - Κάντε κλικ στο "Change..." («Αλλαγή») για να κάνετε αλλαγή του "Screen Saver" («Προστασία οθόνης»)
    - Κάτω από το πλήκτρο "Wait:" («Αναμονή»), επιλέξτε την περίοδο που θα μένει ανενεργός ο υπολογιστής σας για ενεργοποίηση του κωδικού ασφαλείας.
    - Πατώντας το "OK" θα φυλάξετε τις καταχωρημένες αλλαγές.

- ***Μην φυλάσσετε κωδικούς πρόσβασης στον υπολογιστή σας***
  - Μερικά λογισμικά επιτρέπουν στον χρήστη την φύλαξη κωδικών πρόσβασης όταν επισκέπτεται ιστοσελίδες. Για απενεργοποίηση αυτής της επιλογής:
    - Ανοίξτε το παραθυράκι του Internet Explorer
      - Κάντε κλικ στο "Tools" >> "Internet Options" >> "Content".
      - Κάτω από το "Personal Information", επιλέξτε το "AutoComplete".
      - Απενεργοποιήστε το "User names and passwords on forms" και κάντε κλικ στο "Clear Passwords".
      - Κάντε κλικ στο "OK" για φύλαξη των αλλαγών.
    - Ανοίξτε το παραθυράκι του Netscape
      - Κάντε κλικ στο "Netscape" ή "Edit"
      - Επιλέξτε "Preferences"
      - Κάντε διπλό κλικ στο "Privacy & Security"
      - Κάντε κλικ στο "Passwords"
      - Σιγουρευτείτε ότι το "Remember passwords" κάτω από το "Password Manager" είναι ανενεργό
      - Πατώντας το "OK" θα φυλάξετε τις καταχωρημένες αλλαγές.

- ***ΜΗΝ δίνετε τα προσωπικά σας δεδομένα σε ύποπτες ιστοσελίδες.***
  - Για την ασφάλεια των προσωπικών σας δεδομένων, δεν πρέπει να καταχωρείτε τα προσωπικά σας δεδομένα σε ιστοσελίδες που δεν εμπιστεύεστε.

- ***Χρησιμοποίηση συσκευής ή ηλεκτρονικού υπολογιστή που εμπιστεύεστε***

- Δεν θα πρέπει να εκτελείτε τραπεζικές συναλλαγές μέσω συσκευών ή ηλεκτρονικών υπολογιστών τους οποίους δεν εμπιστεύεστε, όπως για παράδειγμα υπολογιστές που χρησιμοποιούνται από διάφορους χρήστες. Εάν είναι αναγκαία η χρήση τέτοιου υπολογιστή θα πρέπει να βεβαιωθείτε για την απάλειψη των προσωπικών σας δεδομένων μετά την χρήση του. Για χρήστες του λογισμικού "Internet Explorer 5.x" θα πρέπει να βεβαιωθούν ότι η επιλογή για «Αυτόματη συμπλήρωση» ("Auto Complete") των σελίδων είναι απενεργοποιημένη.

- ***Μέγιστη ασφάλεια για ασύρματο διαδίκτυο***
  - Ασύρματος εξοπλισμός που δεν έχει διαμορφωθεί σωστά μπορεί να αφήσει διάφορους χρήστες να έχουν πρόσβαση στον υπολογιστή σας. Εάν χρησιμοποιείτε ασύρματη συσκευή / διαδίκτυο σας συμβουλεύουμε να διαβάσετε τις οδηγίες του κατασκευαστή ή συμβουλευτείτε τον προμηθευτή σας για οδηγίες για την διαμόρφωση του ασύρματου σας διαδικτύου με τα απαραίτητα μέτρα ασφαλείας.

- ***Καθαρισμός των προσωρινών αρχείων και σελίδων που φυλάσσονται στον υπολογιστή***
  - Τα προσωρινά αρχεία του υπολογιστή σας μπορεί να περιέχουν προσωπικά δεδομένα και για αυτό σας συμβουλεύουμε να καθαρίζετε τα προσωρινά αρχεία μετά την χρήση του υπολογιστή. Η διαδικασία θεωρείται αναγκαία εάν χρησιμοποιείται υπολογιστής ο οποίος χρησιμοποιείται από πολλούς χρήστες.

- ***Προφυλάξτε τον υπολογιστή σας από ιούς και κακόβουλα προγράμματα***
  - Εκτός από την καταστροφή σημαντικών δεδομένων στον υπολογιστή σας, οι ιοί και τα κακόβουλα προγράμματα μπορεί να αποθηκεύσουν τους προσωπικούς σας κωδικούς χωρίς να το γνωρίζετε. Η συνεχής σύνδεση του υπολογιστή σας με το διαδίκτυο αυξάνει τις πιθανότητες να επηρεασθεί ο υπολογιστής σας από τέτοιου είδους προγράμματα. Για αποτροπή προσβολής του υπολογιστή σας θα πρέπει:
    - Να μην κατεβάζετε αρχεία από το διαδίκτυο (π.χ. προγράμματα, παιχνίδια, εικόνες, τραγούδια) ή από άλλους χρήστες (π.χ. επισυναπτόμενα αρχεία μέσω ηλεκτρονικού ταχυδρομείου) για τα οποία δεν είστε σίγουροι.
    - Διαγράφετε από το ηλεκτρονικό σας ταχυδρομείο μηνύματα τα οποία δεν γνωρίζετε τον παραλήπτη ή μαζικά μηνύματα και μηνύματα «αλυσίδας».
    - Μην χρησιμοποιείτε επιλογές στα προγράμματα σας οι οποίες αφήνουν την αυτόματη παραλαβή αρχείων ή αυτόματη προεπισκόπηση αρχείων. Για παράδειγμα, δεν θα πρέπει να έχετε ενεργοποιημένη την επιλογή «Αυτόματη παραλαβή DCC» στο λογισμικό mIRC και μην έχετε ενεργοποιημένο το «Προεπισκόπηση» (Preview Mode) στο Outlook ή άλλα λογισμικά για έλεγχο του ηλεκτρονικού σας ταχυδρομείου.
    - Εγκαταστήστε λογισμικά τα οποία έχουν την δυνατότητα απενεργοποίησης και αφαίρεσης ιών από τον ηλεκτρονικό σας υπολογιστή. Θα πρέπει επίσης να κάνετε συχνή αναβάθμιση του λογισμικού για αφαίρεση ιών από τον υπολογιστή σας.
    - Μερικά λογισμικά τα οποία μπορείτε να χρησιμοποιήσετε για προστασία του υπολογιστή σας είναι*:
      - Trend Micro
      - McAfee

- Symantec

**Τα παραπάνω λογισμικά είναι εισήγηση και δεν αποτελούν την επίσημη προτίμηση στα λογισμικά.*

- ***Προστασία σημαντικών δεδομένων***
  - Δημιουργείστε σημείο επαναφοράς σημαντικών δεδομένων και διασφαλίστε την προστασία τους στον ηλεκτρονικό σας υπολογιστή.

- ***Απενεργοποιήστε την επιλογή "File and Printer Sharing" στο λειτουργικό σας σύστημα***
  - Με απενεργοποίηση της επιλογής αυτής δεν αφήνετε άλλους χρήστες να έχουν πρόσβαση στον ηλεκτρονικό σας υπολογιστή. Για περισσότερες πληροφορίες επικοινωνήστε με τον προμηθευτή σας.

- ***Ελέγχετε συχνά το ιστορικό συναλλαγών***
  - Πάντοτε να ελέγχετε το ιστορικό συναλλαγών και την κατάσταση κίνησης κάθε λογαριασμού για επιβεβαίωση ότι δεν υπάρχουν μεταφορές από / προς τον λογαριασμό σας που δεν εξουσιοδοτήσατε.

- ***Κρατήστε μας ενήμερους για αλλαγή στοιχείων επικοινωνίας***
  - Πάντοτε να μας κρατάτε ενήμερους σε περίπτωση που αλλάξετε διεύθυνση και διεύθυνση στο ηλεκτρονικό ταχυδρομείο γιατί σε περίπτωση που παρατηρήσουμε κάτι ασυνήθιστο στον λογαριασμό σας θα θέλαμε να επικοινωνήσουμε μαζί σας.

- ***Ειδοποιείστε μας αμέσως εάν υπάρχει πρόβλημα!***
  - Εάν παρατηρήσετε κάτι το ασυνήθιστο ή μεταφορές που δεν εξουσιοδοτήσατε, παρακαλούμε όπως αλλάξετε αμέσως τον κωδικό πρόσβασης σας (PIN) ή κλειδώστε τον λογαριασμό σας (καταχωρώντας 3 φορές λάθος κωδικό PIN) και ειδοποιήστε μας αμέσως. Όταν κρίνετε απαραίτητο μπορείτε να ζητήσετε διαγραφή του λογαριασμού σας από την υπηρεσία μας για την δική σας προστασία. Μπορείτε να επικοινωνείτε μαζί μας στο:
    Τηλ1: 8000-3333 (για κλήσεις από Κύπρο)
    Τηλ2: +357 22888610 (Διεθνείς κλήσεις)
    Email: esupport@alphabank.com.cy

- ***Οι Υποχρεώσεις, Ευθύνες και Δικαιώματα σας***
  - Η χρήση του Alpha Express Banking υπόκειται στους Όρους χρήσης που διέπουν τις «Ηλεκτρονικές Υπηρεσίες» καθώς και στους Όρους χρήσης που υπόκειται κάθε προϊόν ή υπηρεσία που παρέχεται μέσω ηλεκτρονικής υπηρεσίας. Θα θέλαμε, για την δική σας ασφάλεια, να ακολουθείτε τις οδηγίες ασφαλείας που αναγράφονται.