Χρήσιμες Πληροφορίες Ασφαλείας

Η πρόσβαση στην υπηρεσία e-banking επιτυγχάνεται χρησιμοποιώντας διεθνώς αναγνωρισμένες πρακτικές, τόσο σε τεχνικό όσο και σε επίπεδο χρήστη.

- Η πρόσβασή σας στην υπηρεσία e-banking γίνεται με συνδυασμένη χρήση των προσωπικών κωδικών ασφαλείας User ID και Password. Το Password θα πρέπει να πληροί συγκεκριμένους κανόνες ασφαλείας που εκάστοτε ορίζει η Optima bank. Για επιπλέον ασφάλεια, εφόσον υποψιάζεστε απώλεια ή υποκλοπή των κωδικών ασφαλείας, παρέχεται η δυνατότητα κλειδώματος αυτών μετά από 3 συνεχόμενες αποτυχημένες προσπάθειες σύνδεσης (η επαναφορά των κωδικών ασφαλείας μπορεί να γίνει online). Το σύστημα απαιτεί την υποχρεωτική αλλαγή του password τουλάχιστον ανά εξάμηνο, ενώ είναι δυνατή η αλλαγή του οποτεδήποτε με δική σας πρωτοβουλία.
- Λαμβάνετε δωρεάν άμεση ενημέρωση στοemail σας στις εξής περιπτώσεις:
    - Αποτυχημένη προσπάθεια σύνδεσης στο e-banking
    - Κλείδωμα κωδικών ασφαλείας μετά από 3 συνεχόμενες αποτυχίες σύνδεσης
    - Αλλαγή password

Σε τεχνικό επίπεδο, χρησιμοποιούμε τις πιο σύγχρονες τεχνολογίες προκειμένου να σας προσφέρουμε τη μέγιστη δυνατή ασφάλεια. Το e-banking μας διαθέτει ψηφιακό πιστοποιητικό κρυπτογράφησης το οποίο έχει εκδοθεί από τον διεθνώς αναγνωρισμένο πάροχο πιστοποιητικών κρυπτογράφησης *ESET SSL Filter CA (όπως φαίνεται στην εικόνα με το λουκέτο πριν την ηλεκτρονική διεύθυνση):*

Παράλληλα με τα μέτρα που λαμβάνουμε εμείς για την ασφάλειά σας, συστήνεται και η εκ μέρους σας τήρηση των παρακάτω βασικών κανόνων ασφαλείας:

- **Βεβαιωθείτε ότι πλοηγήστε στην ιστοσελίδα της Optima bank**, πριν από κάθε σύνδεση, για την ασφάλειά σας από κακόβουλες ενέργειες.
- **Ελέγξτε ότι χρησιμοποιείτε προγράμματα προστασίας**, antivirus και antimalware, για ασφάλεια από κακόβουλα λογισμικά.
- **Κρατήστε τους μυστικούς σας κωδικούς… μυστικούς.** Μην κοινοποιείτε τους κωδικούς σας σε οποιονδήποτε. Το ίδιο επικίνδυνη είναι και η συνήθεια να τους κρατάτε γραμμένους σε χαρτί, σημειωματάριο ή ακόμη και στο κινητό σας.
- **Μη χρησιμοποιείτε τους ίδιους κωδικούς στο e-banking και σε άλλα sites.**
- **Μην αποθηκεύετε τους κωδικούς σας στον browser ή σε τρίτες εφαρμογές (π.χ. Password Managers), ειδικά μάλιστα αν χρησιμοποιείτε δημόσια ή κοινόχρηστα δίκτυα.**
- **Διαγράφετε συχνά τα προσωρινά αρχεία Internet (Temporary Files) του υπολογιστή σας.** Μεταβείτε στις «Ρυθμίσεις» του browser που χρησιμοποιείτε για την είσοδό σας στο e-banking και επιλέξτε το "Ιστορικό" για να διαγράψετε τα σχετικά αρχεία. Εναλλακτικά, χρησιμοποιήστε τη συντόμευση CTRL+SHIFT+DEL στο πληκτρολόγιό σας (ισχύει για όλους τους browsers).
- **Προσοχή στις απόπειρες κλοπής κωδικών (phishing).** Συνήθως αυτές οι απόπειρες γίνονται με αποστολή κάποιου παραπλανητικού μηνύματος (email/SMS) το οποίο με αφορμή κάποια δήθεν επείγουσα κατάσταση (π.χ. θα κλειδωθεί ο λογαριασμός σας) σας οδηγεί σε κάποιο "ψεύτικο" web site το οποίο οπτικά μοιάζει με το e-banking σας. Επισκεπτόμενοι αυτό το web site και καταχωρώντας τους κωδικούς σας, πρακτικά τους δημοσιοποιείτε σε κακόβουλους τρίτους. Παρακαλούμε μην απαντήσετε στο email και διαγράψτε ή τερματίστε αμέσως την επικοινωνία. Η σύνδεση στο e-banking σας θα πρέπει να γίνεται αφού ελέγξετε ότι η διεύθυνση που εμφανίζει ο browser σας είναι η σωστή για την οποία μάλιστα εμφανίζεται εικονίδιο με σχετικό λουκέτο, δείγμα ότι έχει εκδοθεί επίσημο ψηφιακό πιστοποιητικό κρυπτογράφησης.
- Η Τράπεζα δε θα σας ζητήσει ποτέ και με κανέναν τρόπο (τηλεφωνικά ή μέσω email) πρόσβαση στους λογαριασμούς ή κωδικούς ασφαλείας σας. Είναι προσωπικοί και δεν πρέπει να τους αποκαλύπτετε σε κανέναν.
- **Πρόσβαση μέσω WiFi.** Βεβαιωθείτε ότι η σύνδεση WiFi που χρησιμοποιείτε είναι ασφαλής και κρυπτογραφημένη βάσει και των πιο πρόσφατων προδιαγραφών όπως WPA2 ή WPA2-Enterprise εάν συνδέεστε μέσω εταιρικού δικτύου. Σε διαφορετική περίπτωση είναι δυνατό κάποιος κακόβουλος χρήστης να υποκλέψει την επικοινωνία αποκτώντας πρόσβαση σε ευαίσθητες πληροφορίες, όπως οι μυστικοί σας κωδικοί. Εάν δεν είστε σίγουροι για τις προδιαγραφές ασφαλείας ενός WiFi δικτύου, είναι καλύτερα να χρησιμοποιήσετε τη 4G/5G σύνδεσή σας για να πραγματοποιήσετε τραπεζικές συναλλαγές από τη συσκευή σας.
- **Ελέγχετε το λογαριασμό σας.** Καλό είναι να συνδέεστε τακτικά στο λογαριασμό σας μέσω e-banking και να ελέγχετε το ιστορικό των συναλλαγών σας. Σε περίπτωση που εντοπίσετε κάποια ύποπτη συναλλαγή θα πρέπει να μας ειδοποιήσετε άμεσα.
- **Προσέχετε πάντα τις συσκευές σας.** Επειδή το email και το κινητό σας αποτελούν αποδεικτικά της ταυτότητάς σας, θα πρέπει να προσέχετε ώστε να μην είναι δυνατόν να αποκτήσει κάποιος τρίτος πρόσβαση σε αυτά. Σε περίπτωση απώλειας του κινητού σας θα πρέπει να ακολουθήσετε τα εξής βήματα:

- Επικοινωνήστε με τον τηλεπικοινωνιακό σας πάροχο προκειμένου να απενεργοποιηθεί η συσκευή σας
- Αλλάξτε άμεσα το password του email σας (ειδικά εάν έχετε επιτρέψει την πρόσβαση στο email μέσω του κινητού σας)

Συνδεθείτε στο e-banking και αλλάξτε τόσο το User ID σας όσο και το password σας. Εναλλακτικά, μπορείτε να κλειδώσετε προσωρινά τους κωδικούς ασφαλείας σας, καταχωρώντας 3 συνεχόμενες φορές λάθος password (μπορείτε αργότερα να τους επαναφέρετε εύκολα online μέσω της επιλογής "Ξεχάσατε τους κωδικούς σας").