Χρήσιμες συμβουλές για να προστατέψετε την κάρτα σας και το PIN σας!

Προτεραιότητά μας είναι η ασφάλεια των συναλλαγών. Ενημερωθείτε για τους τρόπους προστασίας της κάρτας και του PIN σας. Πραγματοποιήστε τις συναλλαγές σας στο εξωτερικό, εσωτερικό και στο διαδίκτυο με ασφάλεια. Αποφύγετε τις απάτες μέσω κακόβουλων e-mail/ SMS.

Προστατέψτε τις συναλλαγές σας στο ATM:

- Πριν ξεκινήσετε τη συναλλαγή ελέγξτε προσεκτικά το χώρο γύρω σας για τυχόν ύποπτες κινήσεις.
- Βεβαιωθείτε ότι στο χώρο που βρίσκεται το ATM δεν υπάρχει κάποιο πρόσθετο εξάρτημα, του οποίου η παρουσία δεν δικαιολογείται.
- Εάν εντοπίσετε οποιοδήποτε ύποπτο αντικείμενο, αλλοιώσεις ή σημάδια στη σχισμή υποδοχής της κάρτας, όπως στρεβλωμένο πλαίσιο, εκδορές, επιπλέον εξαρτήματα, τρύπες κ.λ.π. αποφύγετε να χρησιμοποιήσετε το συγκεκριμένο ATM. Ειδοποιήστε αμέσως την Τράπεζα (800 11 800 ή +357 22575555 από εξωτερικό).
- Σε περίπτωση που το ATM κρατήσει την κάρτα ή αντιμετωπίσετε οποιοδήποτε πρόβλημα κατά τη συναλλαγή, επικοινωνήστε μόνο με την **AstroBank** (800 11 800 ή +357 22575555 από εξωτερικό).
- Μην εμπιστεύεστε αγνώστους που προθυμοποιούνται να σας βοηθήσουν στο χειρισμό του ATM ή ζητούν το PIN της κάρτας σας.
- Σε περίπτωση που το μηχάνημα παρουσιάσει οποιαδήποτε βλάβη, επικοινωνήσετε μόνο με τα τηλέφωνα της Τράπεζας (800 11 800 ή +357 22575555 από εξωτερικό).
- Όταν πληκτρολογείτε τον κωδικό σας PIN «καλύψτε» το πληκτρολόγιο με το χέρι σας, ώστε κανείς γύρω σας να μην αντιληφθεί τον τετραψήφιο αριθμό.
- Μετά την ολοκλήρωση της ανάληψης χρημάτων μετρήστε τα χρήματα με διακριτικότητα και όσο πιο σύντομα μπορείτε.
- Φροντίστε να μην είστε μόνοι σας, αν χρειαστεί να χρησιμοποιήστε ATM κατά τη διάρκεια της νύχτας και ιδιαίτερα σε ερημικές τοποθεσίες.
- Εάν χρησιμοποιείτε ATM που βρίσκεται σε ειδικό θάλαμο, μην επιτρέπετε σε άτομα που δεν γνωρίζετε να εισέλθουν στο χώρο, κατά τη διάρκεια της συναλλαγής.
- Μην αφήνετε τα κλειδιά σας ή πολύτιμα αντικείμενα στο αυτοκίνητό σας, ενώ χρησιμοποιείτε ATM και μην αφήνετε τη μηχανή του αυτοκινήτου σας αναμμένη.
- Βεβαιωθείτε ότι παραλάβατε την κάρτα σας μετά το τέλος της συναλλαγής.
- Μην αφήνετε ποτέ την απόδειξη συναλλαγής που έχει εκδώσει το ATM.

Προστατέψτε την κάρτα και το PIN σας:

- Αποφεύγετε να χρησιμοποιείτε ως κωδικό (PIN) την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά σας στοιχεία που μπορεί να γίνουν εύκολα αντιληπτά από επιτήδειους.
- Αποφεύγετε να γράφετε το PIN οπουδήποτε, όπως για παράδειγμα στην μνήμη του κινητού σας τηλεφώνου.
- Αποφεύγετε να χρησιμοποιείτε το ίδιο PIN σε περισσότερες από μια κάρτες.
- Επιλέξτε και απομνημονεύστε τον κωδικό PIN που μόνο εσείς θα γνωρίζετε και που δεν θα μπορεί να προσδιορισθεί από προσωπικά σας αντικείμενα που υπάρχουν στο πορτοφόλι ή στη τσάντα σας.
- Σε καμία περίπτωση μην δίνετε τον κωδικό σας PIN σε τρίτους. Εάν κάποιος, για παράδειγμα επικαλεσθεί ότι τηλεφωνεί από την **AstroBank** και ζητήσει τον αριθμό του PIN για επαλήθευση, μην τον δώσετε. Καμία τράπεζα δεν ακολουθεί αυτή την πρακτική. Εάν έχετε αναγνώριση κλήσης, καταγράψτε τον αριθμό που εμφανίστηκε στην τηλεφωνική σας συσκευή και ενημερώστε αμέσως την Αστυνομία.
- Συγκρίνετε τις αποδείξεις συναλλαγών σας με το μηνιαίο ενημερωτικό δελτίο κίνησης του λογαριασμού σας. Εάν παρατηρήσετε οποιαδήποτε συναλλαγή που δεν έχετε πραγματοποιήσει ενημερώστε αμέσως την **AstroBank**.

- Μη δίνετε και μη δανείζετε ποτέ και σε κανέναν την κάρτα σας.
- Όταν κυκλοφορείτε έχετε μαζί σας μόνο τις κάρτες που προτίθεστε να χρησιμοποιήσετε.
- Αναφέρατε αμέσως την κλοπή ή την απώλεια κάρτας στην **AstroBank** (800 11 800 ή +357 22575555 από εξωτερικό).
- Ποτέ μην φυλάσσετε το PIN μαζί με την κάρτα σας.
- Πάντα να καταστρέφετε οποιοδήποτε έγγραφο (απόδειξη, αλληλογραφία κ.λ.π.) που μπορεί να περιέχει οποιαδήποτε προσωπική σας πληροφορία (όνομα, δ/νση κ.α.).
- Να ελέγχετε πάντα την ημερομηνία λήξης της κάρτας σας. Αν δεν έχετε λάβει την ανανεωμένη σας κάρτα επικοινωνήστε μαζί μας στο 800 11 800 ή +357 22575555 από εξωτερικό.

Ταξίδι στο εξωτερικό:

- Βεβαιωθείτε ότι έχουμε ενημερωμένα στοιχεία επαφής , ιδιαίτερα τον αριθμό του κινητού σας τηλεφώνου καθώς και την διεύθυνση του ηλεκτρονικού σας ταχυδρομείου.
- Έχετε υπόψιν σας το τηλεφωνικό μας κέντρο σε περίπτωση κλοπής ή απώλειας (800 11 800 ή +357 22575555 από εξωτερικό).
- Να προτιμάτε να έχετε μαζί σας τη κάρτα ή τις κάρτες που πρόκειται να χρησιμοποιήσετε.

Προστασία στο διαδίκτυο:

- Αλλάζετε συχνά τους κωδικούς σας και χρησιμοποιείτε συνδυασμούς από γράμματα, αριθμούς και ειδικούς χαρακτήρες όπως # και @. Μην χρησιμοποιείτε τους κωδικούς της **AstroBank** σας σε άλλους λογαριασμούς ή δραστηριότητες.
- Έχετε την ευθύνη διαφύλαξης των προσωπικών κωδικών ασφαλείας. Σε περίπτωση δε διαρροής αυτών, οφείλετε να ειδοποιήσετε αμέσως την **AstroBank** (800 11 800 ή +357 22575555 από εξωτερικό).
- Μην μοιράζεστε τα προσωπικά σας στοιχεία/δεδομένα.
- Μη δίνετε τα στοιχεία της κάρτας σας στις επιχειρήσεις τηλεφωνικά ,καθώς αυτό εγκυμονεί κινδύνους διαρροής των στοιχείων σας προς τρίτα πρόσωπα.
- Να πλοηγείστε και να δίνετε τα στοιχεία των καρτών σας σε πιστοποιημένους ιστοτόπους /επιχειρήσεις. Αν δεν είστε σίγουροι για την ασφάλεια τους αποφύγετε να συναλλάσσεστε μαζί τους.
- Πριν από κάθε χρήση των ηλεκτρονικών υπηρεσιών της **AstroBank** , βεβαιωθείτε ότι βρίσκεστε στο ασφαλές περιβάλλον συναλλαγών της Τράπεζας. Μπορείτε να αναγνωρίσετε τον επίσημο ιστότοπο της τράπεζας από το λουκέτο (security lock) στη γραμμής αναζήτησης.
- Τα μέσα κοινωνικής δικτύωσης είναι όλο και πιο δημοφιλή, αλλά είναι φρονιμότερο να κρατήσει κανείς ορισμένα προσωπικά στοιχεία ιδιωτικά. Αποφύγετε την κοινή χρήση των προσωπικών σας στοιχείων που χρησιμοποιείτε για να συναλλάσσεστε με τα χρηματοπιστωτικά ιδρύματα για την αναγνώρισή σας, όπως η ημερομηνία γέννησής σας, η διεύθυνση κατοικίας, το πατρικό όνομα της μητέρας, σχολεία φοίτησης και το όνομα του κατοικίδιου ζώου. Οι απατεώνες μπορούν να χρησιμοποιήσουν αυτό το είδος των πληροφοριών για να αποκτήσουν πρόσβαση σε οποιονδήποτε λογαριασμό, δεδομένου ότι οι απαντήσεις στις ερωτήσεις ασφαλείας είναι κοινές.
- Χρησιμοποιείτε τις ηλεκτρονικές υπηρεσίες της **AstroBank** μόνο μέσω της ιστοσελίδας της www.astrobank.com και όχι μέσω συνδέσμων (links) από άλλους ιστοτόπους.
- Πάντα να εξετάζετε προσεκτικά τις επιλογές απορρήτου των μέσων κοινωνικής δικτύωσης που εγγράφεστε. Οι επιλογές απόρρητου και τα εργαλεία των μέσων κοινωνικής δικτύωσης μπορεί να είναι περίπλοκα, γι΄ αυτό πρέπει να εξετάζονται προσεκτικά, διότι μπορεί να περικλείουν πληροφορίες που θα θέλατε να παραμείνουν απόρρητες.
- Η **AstroBank** δεν θα σας ζητήσει ποτέ και με κανένα τρόπο (είτε μέσω τηλεφωνικής κλήσης ή λήψης γραπτού μηνύματος (SMS/MMS) ή μέσω ηλεκτρονικού ταχυδρομείου) στοιχεία λογαριασμών, στοιχεία καρτών, κωδικούς πρόσβασης. Είναι στοιχεία προσωπικά και δεν πρέπει να τα αποκαλύπτετε σε κανέναν.
- Μετά την ολοκλήρωση των συναλλαγών σας, αποσυνδεθείτε από τις ηλεκτρονικές υπηρεσίες της **AstroBank** επιλέγοντας "Έξοδος".

Απάτη μέσω κακόβουλου mail/sms:

Κακόβουλο mail (phish email)

Πρόκειται για απάτη που αποτελείται από δύο μέρη, τα μηνύματα του ηλεκτρονικού ταχυδρομείου και μία «ψεύτικη» ιστοσελίδα. Οι απατεώνες, γνωστοί ως phishers, στέλνουν e-mail στο ευρύ κοινό που μοιάζει να είναι από αξιόπιστη εταιρία. Γνωστό ως phishing mail.
Το e-mail αυτό εμπεριέχει συνδέσμους για τις «ψεύτικες» ιστοσελίδες με σκοπό να πείσουν τα θύματα να μοιραστούν τις προσωπικές τους πληροφορίες με τη χρήση της έξυπνης γλώσσας, όπως π.χ. «Είναι επιτακτική ανάγκη να ενημερώσετε τα στοιχεία σας αμέσως για τη δική σας ασφάλεια». Μόλις πάρουν τα προσωπικά σας στοιχεία μπορεί να τα χρησιμοποιήσουν για κακόβουλες συναλλαγές.

Κακόβουλο γραπτό μήνυμα (sms)

Μια απόπειρα phishing μέσω SMS (Υπηρεσία σύντομων μηνυμάτων) ή γραπτού μηνύματος στο κινητό τηλέφωνο ή συσκευή. Η τακτική αυτή είναι επίσης γνωστή και ως smishing, η οποία είναι ένας συνδυασμός των SMS και phishing. Ο σκοπός του μηνύματος κειμένου phishing είναι ο ίδιος με το παραδοσιακό phishing e-mail, δηλαδή να πείσει τους παραλήπτες να μοιραστούν τις απόρρητες πληροφορίες τους.

Μην απαντάτε στις παραπάνω κατηγορίες που σας ζητούν στοιχεία των λογαριασμών, των καρτών ή των κωδικών σας και μην ακολουθείτε συνδέσμους (links) που περιέχονται σε phishing mails ή γραπτά μηνύματα και σας προτρέπουν να κάνετε είσοδο (log in) στην ηλεκτρονική τραπεζική της **AstroBank**.

Προωθήστε οποιοδήποτε παρόμοιο «ύποπτο» e-mail ή SMS στην Τράπεζα (στο κατάστημα που σας εξυπηρετεί ή τηλεφωνήστε στο 800 11 800 ή +357 22575555 από εξωτερικό) και στη συνέχεια διαγράψτε το από το ηλεκτρονικό σας ταχυδρομείο ή την συσκευή σας.

<u>Απάτη μέσω κινητού τηλεφώνου</u>:

Όταν χρησιμοποιείται το κινητό σας τηλέφωνο για τους λογαριασμούς σας, έχετε υπ' όψιν σας τα παρακάτω:

- Χρησιμοποιήστε τις λειτουργίες ασφαλείας που εμπεριέχονται στην συσκευή σας, όπως το κλείδωμα του πληκτρολογίου ή λειτουργία κλειδώματος του τηλεφώνου όταν δεν είναι σε χρήση, ή "βρείτε το τηλέφωνό μου" ή "διαγραφή μνήμης" σε περίπτωση απώλειας.
- Διαγράφετε συχνά τα γραπτά μηνύματα που λαμβάνετε από τα χρηματοπιστωτικά ιδρύματα, ιδιαίτερα σε περίπτωση που έχετε σκοπό να δανείσετε ή πουλήσετε την συσκευή σας.
- Κρατήστε αριθμούς λογαριασμών, κωδικούς πρόσβασης και την ημερομηνία γέννησης σας απόρρητα. Ποτέ μη μοιράζεστε με τρίτους τις προσωπικές ή οικονομικές πληροφορίες σας σε μήνυμα κειμένου, τηλεφώνημα ή e-mail.
- Αν χάσετε το κινητό σας τηλέφωνο ή αν αλλάξετε τον αριθμό του κινητού σας τηλεφώνου, μεταβείτε άμεσα στο πλησιέστερο κατάστημα της **AstroBank** για να το αφαιρέσετε/αλλάξετε.
- Αποφύγετε την αποθήκευση του τραπεζικού σας κωδικού πρόσβασής ή άλλες ευαίσθητες πληροφορίες στο smartphone σας ή σε μια εφαρμογή αυτού ,απ' όπου θα μπορούσαν να αποκαλυφθούν εάν το τηλέφωνό σας κλαπεί.
- Όταν ολοκληρώσετε τις τραπεζικές σας συναλλαγές διαμέσου κινητού τηλεφώνου ή διαμέσου Winbank Mobile, πάντα να αποσυνδέεστε και όχι απλά να κλείσετε το πρόγραμμα περιήγησης ή την εφαρμογή. Για την ασφάλειά σας η **AstroBank** θα σας αποσυνδέσει μετά από 10 λεπτά αδράνειας.
- Για να εξασφαλίσετε υψηλότερο επίπεδο προστασίας, ενημερώνετε το λογισμικό του κινητού σας τηλεφώνου, ακολουθώντας τις οδηγίες του κατασκευαστή.
- Να είστε προσεκτικοί όταν χρησιμοποιείτε δημόσια δίκτυα. Εξετάστε προσεκτικά τις ρυθμίσεις σύνδεσης Wi-Fi και Bluetooth, ακόμη και σε έναν αξιόπιστο λιανοπωλητή, καθώς οι απατεώνες μπορεί να έχουν πλαστογραφήσει το όνομα του αξιόπιστου δικτύου.
- Κατεβάστε την εφαρμογή **AstroBank** Mobile ή, από αξιόπιστες σελίδες για να διασφαλίσετε την ασφάλεια των προσωπικών σας δεδομένων.
- Αντιμετωπίστε τους κώδικες QR (Δισδιάστατα Barcodes που μπορούν να αποκωδικοποιηθούν εύκολα, με υψηλή ταχύτητα και να διαβαστούν γρήγορα με ηλεκτρονικό τρόπο. Η συντομογραφία QR προέρχεται από τις αγγλικές λέξεις Quick Response) με την ίδια καχυποψία, όπως θα κάνατε με οποιαδήποτε διεύθυνση URL ή mail. Οι κωδικοί QR μπορούν να χρησιμοποιηθούν από απατεώνες για να σας κάνουν να μεταβείτε σε ιστοσελίδες που ζητούν προσωπικές και οικονομικές πληροφορίες ή θα μπορούσαν να εισβάλλουν στην συσκευή σας.
- Να είστε προσεκτικοί με τους κωδικούς QR που σαρώνετε, γιατί μπορεί να έχουν παραποιηθεί

• Χρησιμοποιήστε ένα σαρωτή κωδικού QR από αξιόπιστη πηγή που θα ελέγξει τις συνδέσεις για κακόβουλο περιεχόμενο. Αυτή η ικανότητα μπορεί να βρεθεί πριν από τη λήψη, στην περιγραφή της εφαρμογής.

Προστασία απάτης μέσω ηλεκτρονικού υπολογιστή:

• Να αποφεύγετε τη λήψη προγραμμάτων από άγνωστες πηγές.

• Πριν από τη λήψη μιας ενημέρωσης για το πρόγραμμα του υπολογιστή σας, πηγαίνετε πρώτα στην ιστοσελίδα της εταιρείας για να επιβεβαιώσετε ότι πρόκειται για νόμιμη αναβάθμιση/ ενημέρωση.

• Θωρακίστε τον υπολογιστή σας με προγράμματα προστασίας (firewalls, antivirus, antispyware).

• Να είστε επιφυλακτικοί με τη διεξαγωγή online τραπεζικών δραστηριοτήτων σε υπολογιστές που μοιράζονται άλλοι. Δημόσιοι υπολογιστές θα πρέπει να χρησιμοποιούνται με προσοχή. Online τραπεζικές δραστηριότητες και προβολή ή λήψη εγγράφων (αντίγραφα λογαριασμών, κ.λπ.) θα πρέπει να διεξάγονται, κατά κύριο λόγο, σε έναν υπολογιστή που ξέρετε ότι είναι ασφαλής.

• Ρυθμίστε τις προσωπικές σας συσκευές έτσι ώστε να αποτρέψετε μη εξουσιοδοτημένους χρήστες από απομακρυσμένη πρόσβαση να εισέλθουν σε αυτές. Για παράδειγμα, εάν χρησιμοποιείτε ένα ασύρματο δρομολογητή(router) για σύνδεση internet στο σπίτι σας, ακολουθήστε τις συστάσεις του κατασκευαστή για να ρυθμίσετε το router με τις κατάλληλες ρυθμίσεις ασφαλείας.

Αναφέρετε ύποπτα περιστατικά που σχετίζονται με την ασφάλεια των συναλλαγών σας:

Παρακαλούμε επικοινωνήστε με το Κέντρο Εξυπηρέτησης Πελατών της AstroBank Limited στο 800-11-800 (εάν καλείτε από Κύπρο) ή +357-22575555 (εάν καλείτε από εξωτερικό), 24 ώρες, 7 ημέρες την εβδομάδα.