ΤΡΑΠΕΖΑ ΠΕΙΡΑΙΩΣ

Ασφάλεια συναλλαγών

Συμβουλές για την ασφάλεια των συναλλαγών

Απάτες με ψηφιακές συναλλαγές. Μπορείτε να τις διακρίνετε;

Στις μέρες μας χρησιμοποιούμε περισσότερο από κάθε άλλη φορά τα κανάλια ηλεκτρονικής τραπεζικής για την εξυπηρέτηση των καθημερινών μας συναλλαγών. Απαραίτητο είναι να είμαστε ακόμα πιο ενημερωμένοι για τη σωστή χρήση των υπηρεσιών και πιο προσεκτικοί με τη σωστή φύλαξη των προσωπικών μας δεδομένων (π.χ. κωδικοί πρόσβασης σε υπηρεσίες).

Το τελευταίο διάστημα παρατηρείται σημαντική έξαρση στις ηλεκτρονικές απάτες καθώς επιτήδειοι προσπαθούν με διάφορους τρόπους να αποκτήσουν πρόσβαση σε τραπεζικούς λογαριασμούς, κάρτες και δεδομένα πελατών επινοώντας διαρκώς νέους τρόπους εξαπάτησης.

Για αυτούς τους λόγους κύριο μέλημα και προτεραιότητα μας αποτελεί η σωστή και έγκυρη-έγκαιρη ενημέρωση μας.

Vishing – Φωνητικό ψάρεμα

Πρόκειται για απάτες που σχετίζονται με «φωνητικό ψάρεμα» (αλίευση προσωπικών στοιχείων μέσω τηλεφωνικής επικοινωνίας) και έχουν σχεδιαστεί για να μας παραπλανήσουν ώστε να κοινοποιήσουμε προσωπικές πληροφορίες.

Τηλεφωνική κλήση από τεχνικό

Τηλεφωνική κλήση από τεχνικό που υποστηρίζει ότι θα του διορθώσει / αναβαθμίσει τον υπολογιστή του. Ο επιτήδειος και με μεθοδικό τρόπο πιέζει τον πελάτη να τον αναγκάσει να παραχωρήσει απομακρυσμένη πρόσβαση στον υπολογιστή του, για να του λύσει ένα «υποτιθέμενο πρόβλημα» με σκοπό την πλήρη πρόσβαση στα προσωπικά του στοιχεία.

Αγοραπωλησίες αγαθών

Ο επιτήδειος καλεί τους πελάτες με πρόσχημα πως ενδιαφέρεται για μια αγορά ενός αγαθού, που έχει καταχωρήσει σε αγγελία ο χρήστης, και με μεθοδικό και πιεστικό τρόπο ζητά τους προσωπικούς τραπεζικούς κωδικούς του πελάτη, με πρόφαση να του μεταφέρει άμεσα τα χρήματα για την αγορά του αγαθού.

Εποχιακές απάτες

Οι επιτήδειοι έχοντας ως αφορμή διάφορα επιδόματα ή πληρωμές που αναμένουν οι πελάτες, τους τηλεφωνούν και παρουσιάζονται για παράδειγμα ως λογιστές, ως υπάλληλοι εταιρείας ηλεκτρικής ενέργειας, ως εφοριακοί υπάλληλοι, ως υπάλληλοι υγείας, ως ενδιαφερόμενοι για κράτηση καταλυμάτων, ως ιδιοκτήτες φορτηγών οχημάτων για μεταφορά καυσίμων κλπ. Και σε αυτή την περίπτωση οι απατεώνες με μεθοδικό τρόπο και λειτουργώντας πιεστικά προσπαθούν να αποσπάσουν τους προσωπικούς κωδικούς των πελατών ώστε να προβούν σε απατηλές συναλλαγές.

Vishing – Φωνητικό ψάρεμα

Επενδυτικές απάτες

Οι επιτήδειοι προσελκύουν τους πελάτες υποσχόμενοι εξαιρετικά υψηλές αποδόσεις σε σύντομο χρονικό διάστημα, διαβεβαιώνοντας τους πως οι επενδύσεις του θα είναι ασφαλείς και επικερδείς. Οι επιτήδειοι δελεάζοντας τα «θύματα» τους ώστε να τοποθετήσουν ένα μικρό αρχικά κεφάλαιο τους αναγκάζουν διαρκώς να τοποθετούν όλο και περισσότερα χρήματα ώστε η «επένδυση» να αποδώσει περισσότερα κέρδη. Πολλές φορές εγκαθιστούν και πρόγραμμα απομακρυσμένης πρόσβασης στον η/υ του «θύματος» και αποκτούν πλήρη πρόσβαση τόσο στο χαρτοφυλάκιο του όσο και στους τραπεζικούς του λογαριασμούς.

Απάτες δανείων

Οι επιτήδειοι προσεγγίζουν τα «θύματα» με πρόσχημα την εκταμίευση δανείων με εξωπραγματικούς όρους , π.χ. από τράπεζες του εξωτερικού με μηδενικό επιτόκιο κλπ., και τους ζητούν να καταβάλλουν ένα «μικρό» ποσό για την κάλυψη των εξόδων δανείων ώστε να τους εκταμιεύσουν το δάνειο.

Email με εξωπραγματικές προσφορές από αναξιόπιστα sites

Οι επιτήδειοι επικοινωνούν ευκαιρίες αγοράς καταναλωτικών αγαθών, υπηρεσιών κλπ. σε e-mail πελατών με εξωπραγματικές προσφορές επί αγαθών, ταξιδιών κλπ. ώστε να δελεάσουν τον πελάτη να επικοινωνήσει μαζί τους, με σκοπό να υποκλέψουν τους Τραπεζικούς κωδικούς τους.

Vishing – Φωνητικό ψάρεμα

Email με ψεύτικα προφίλ για διαδικτυακά ραντεβού

Οι επιτήδειοι μέσω ψεύτικων λογαριασμών κοινωνικών δικτύων και e-mail δελεάζουν τα «θύματα» τους με σκοπό αρχικά να αποκτήσουν οικειότητα μαζί τους και στη συνέχεια να τους πείσουν να προχωρήσουν σε μεταφορά χρημάτων με πρόφαση την κάλυψη κάποιας έκτακτης προσωπικής τους ανάγκης.

Email από CEO ή πληρωμής τιμολογίων

Οι επιτήδειοι έχοντας γνώση ποιος υπάλληλος εταιρείας έχει πρόσβαση σε εταιρικές πληρωμές τον ενημερώνουν με επείγον e-mail ως υποτιθέμενοι CEO να προβεί άμεσα σε εταιρική πληρωμή. Επίσης μία επιχείρηση μπορεί να λάβει e-mail/τηλέφωνο από έναν «συνεργάτη» της ώστε να αλλάξει τον τραπεζικό λογαριασμό στον οποίο πραγματοποιούσε πληρωμές με σκοπό οι μελλοντικές πληρωμές να πιστώνονται στου απατεώνα.

Email που αναζητούν κληρονόμους αμύθητης περιουσίας

Οι επιτήδειοι αποστέλλουν μηνύματα σε διευθύνσεις ηλεκτρονικής αλληλογραφίας πελατών αναφέροντας πως μπορούν να διεκδικήσουν σημαντικά κεφάλαια ως κληρονόμοι περιουσιών προτρέποντας τους να εκτελέσουν συγκεκριμένα βήματα ώστε να απολάβουν τα ποσά.

Vishing – Φωνητικό ψάρεμα

Τι μπορείτε να κάνετε για να αποφύγετε την απάτη μέσω vishing;

- ✓ Να είστε προσεκτικοί με αιφνιδιαστικές και απροειδοποίητες τηλεφωνικές κλήσεις.
- ✓ Αποφύγετε να απαντήσετε σε κλήσεις που προέρχονται από άγνωστους προς εσάς τηλεφωνικούς αριθμούς. Σε περίπτωση που επιλέξετε να απαντήσετε σε μία τέτοια κλήση μην κοινοποιήσετε ευαίσθητα προσωπικά δεδομένα ή/και τους τραπεζικούς σας κωδικούς.
- ✓ Μην δίνετε τον κωδικό "PIN" της πιστωτικής ή χρεωστικής σας κάρτας ή τον κωδικό πρόσβασης του τραπεζικού σας λογαριασμού.
- ✓ Αγνοείστε τυχόν οδηγίες για υποτιθέμενη πίστωση χρημάτων σε λογαριασμό σας σύμφωνα με τις οποίες πρέπει εσείς να κάνετε ενέργειες μέσω της πλατφόρμα ηλεκτρονικής τραπεζικής. Οι επιτήδειοι θα προσπαθήσουν να σας καθοδηγήσουν στον τρόπο που θα λάβετε χρήματα πραγματοποιώντας εσείς ενέργειες μέσω του internet banking. Το αποτέλεσμα θα είναι εσείς να αποστείλετε χρήματα και όχι να λάβετε από εκείνους.

Αν έχετε δεχτεί προσέγγιση της μορφής vishing και παρείχατε τα προσωπικά σας στοιχεία σε τρίτους θα πρέπει να επικοινωνήσετε αμέσως με την τράπεζα συνεργασίας σας.

- ✓ Μπορείτε να καλέσετε στο 210-3288000 (24/7/365) για να μας αναφέρετε οποιοδήποτε σχετική προσπάθεια απάτης μέσω vishing. Εξειδικευμένο προσωπικό θα είναι στη διάθεση σας για να σας καθοδηγήσει και να σας συμβουλεύσει.
- ✓ Για την πιο άμεση εξυπηρέτηση σας μπορείτε να μας αναφέρετε περιεκτικά το λόγο κλήσης σας, ώστε να σας δοθεί προτεραιότητα μέσω της αυτοματοποιημένης πύλης φωνητικής αναγνώρισης και να επικοινωνήσετε άμεσα με εκπρόσωπο μας.
- ✓ Π.χ. κακόβουλο e-mail/sms, απάτη e-banking, εξαπάτηση καρτών, phishing απάτη, κλοπή χρημάτων , αμφισβήτηση συναλλαγής κλπ.

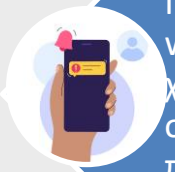
Επίσης θα πρέπει να καταγγείλετε το περιστατικό σε αρμόδια αστυνομική αρχή , είτε με τη φυσική σας παρουσία είτε μέσω του gov.gr.

Phishing – Ηλεκτρονικό ψάρεμα

Phishing (ή ηλεκτρονικό ψάρεμα) είναι η κακόβουλη προσπάθεια επίδοξων απατεώνων να υποκλέψουν προσωπικά στοιχεία όπως, κωδικούς πρόσβασης web banking, αριθμούς ή PIN πιστωτικών / χρεωστικών καρτών, αριθμούς διαβατηρίων, αστυνομικών ταυτοτήτων, ΑΦΜ κλπ.

Phishing email

Πρόκειται για απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου (e-mails) που στέλνονται μαζικά σε τυχαίους λογαριασμούς ανυποψίαστων παραληπτών, όπου είτε δελεάζοντάς τους, είτε προσπαθώντας να τους πείσουν ότι είναι αναγκαίο, τους καλούν να πατήσουν σε έναν σύνδεσμο (link) που υπάρχει μέσα στο email. Ο σύνδεσμος αυτός οδηγεί σε ιστοσελίδες που έχουν φτιάξει επιτήδειοι, οι οποίες προσομοιάζουν με τις αυθεντικές ιστοσελίδες των Τραπεζών. Στόχος τους είναι να παραπλανήσουν τους χρήστες να πληκτρολογήσουν εκεί τα προσωπικά τους στοιχεία, τα οποία στη συνέχεια θα χρησιμοποιήσουν για να εισέλθουν στο περιβάλλον της ηλεκτρονικής τραπεζικής και να ενεργούν ως πραγματικοί πελάτες.



Phishing sms

Πρόκειται για απατηλά μηνύματα sms που μέσω ενός link που περιέχουν ζητούν να συνδεθείτε στη winbank επιλέγοντας αυτόν τον σύνδεσμο. Προσπαθούν να δελεάσουν τον πελάτη να επιλέξει τον σύνδεσμο χρησιμοποιώντας λεκτικό της μορφής π.χ. καλέστε έναν αριθμό για να ακυρώσετε/επαληθεύσετε μία συναλλαγή, να ξεκλειδώσετε/ενεργοποιήσετε το λογαριασμό σας, επικαιροποιήστε τα στοιχεία σας πατώντας εδώ, κλπ. Αν επιλέξετε τον κακόβουλο σύνδεσμο θα οδηγηθείτε σε περιβάλλον όμοιο με αυτό της Τράπεζας και θα σας ζητηθεί να καταχωρήσετε τους προσωπικούς σας κωδικούς και εν συνεχεία τους κωδικούς μιας χρήσης που λαμβάνετε.

Αν δηλώσετε τα στοιχεία σας όπως αναφέρεται παραπάνω οι επιτήδειοι θα εισέλθουν άμεσα στην εφαρμογή και θα έχουν τη δυνατότητα διαχείρισης των χρημάτων σας.

Phishing – Ηλεκτρονικό ψάρεμα

Τι μπορείτε να κάνετε αν δεχτείτε e-mail ή sms το οποίο περιέχει σύνδεσμο που σας προτρέπει να τον επιλέξετε για να καταχωρήσετε τα προσωπικά σας δεδομένα;

- ✓ Αποφύγετε να ανοίξετε e-mails/sms από αγνώστους σε εσάς αποστολείς.
- ✓ Σε καμία περίπτωση μη δηλώνετε τους κωδικούς σας και τα προσωπικά σας στοιχεία σε sites χωρίς πρώτα να επιβεβαιώσετε ότι ο οργανισμός που σας στέλνει το μήνυμα είναι όντως ο πραγματικός. Επίσης τα συγκεκριμένα μηνύματα συνήθως εμπεριέχουν λεκτικό με ορθογραφικά-γραμματικά ή και συντακτικά λάθη και ενδέχεται να απευθύνονται στον πελάτη με τρόπο που δεν είθισται στην επικοινωνία με την τράπεζα του (π.χ. προσφώνηση μικρού ή υποκοριστικού ονόματος κ.α.)
- ✓ Μπορείτε εύκολα επίσης να διαπιστώσετε ότι δεν προέρχονται από την Τράπεζα καθώς η διεύθυνση του αποστολέα αλλά και ο σύνδεσμος που σας ζητούν να επιλέξετε είναι διαφορετικά από αυτά της Τράπεζας μας.
- ✓ Αποφύγετε να κάνετε κλικ σε ηλεκτρονικούς συνδέσμους (links), συνημμένα αρχεία ή εικόνες που λαμβάνετε με μηνύματα κειμένου (sms) δίχως και πάλι να έχετε επαληθεύσει τον αποστολέα.
- ✓ Ποτέ μην απαντάτε σε μήνυμα κειμένου (sms) που σας ζητά τον κωδικό "PIN" ή τον κωδικό πρόσβασης ("password") στον τραπεζικό σας λογαριασμό ή οποιαδήποτε άλλα εξατομικευμένα διαπιστευτήρια ασφαλείας (π.χ. e-banking user name).

Phishing – Ηλεκτρονικό ψάρεμα

Συμβουλή

- Μην βιάζεστε. Πάρτε τον χρόνο σας και πραγματοποιήστε τους απαραίτητους ελέγχους προτού απαντήσετε.
- Εάν νομίζετε ότι ενδέχεται να έχετε απαντήσει σε ένα ύποπτο e-mail ή μήνυμα κειμένου (sms) και παρείχατε τα στοιχεία των τραπεζικών σας λογαριασμών, επικοινωνήστε αμέσως με την τράπεζα συνεργασίας σας.
- Μπορείτε να καλέσετε στο 2103288000 (24/7/365) για να μας αναφέρετε οποιοδήποτε «ύποπτο» e-mail ή sms που σας έχει σταλεί με υποτιθέμενο αποστολέα την Τράπεζα μας. Εξειδικευμένο προσωπικό θα είναι στη διάθεση σας για να σας καθοδηγήσει και να σας συμβουλεύσει.

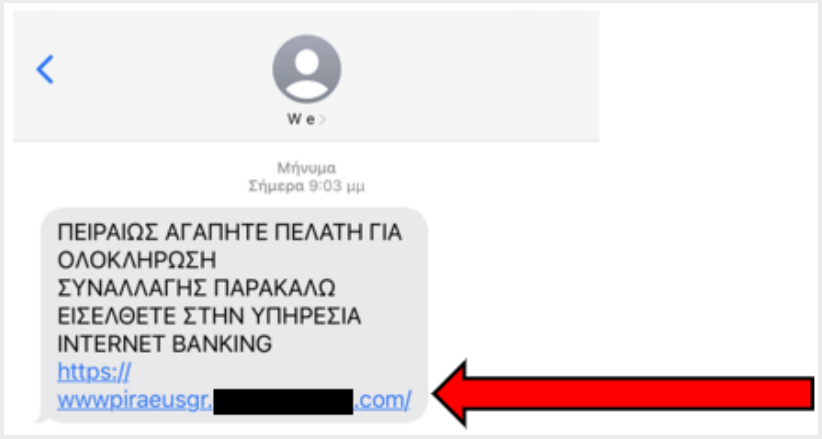
Για την πιο άμεση εξυπηρέτηση σας μπορείτε να μας αναφέρετε περιεκτικά το λόγο κλήσης σας, ώστε να σας δοθεί προτεραιότητα μέσω της αυτοματοποιημένης πύλης φωνητικής αναγνώρισης και να επικοινωνήσετε άμεσα με εκπρόσωπο μας. (Π.χ. κακόβουλο e-mail/sms, απάτη e-banking, εξαπάτηση καρτών, phishing απάτη, κλοπή χρημάτων , αμφισβήτηση συναλλαγής κλπ.)

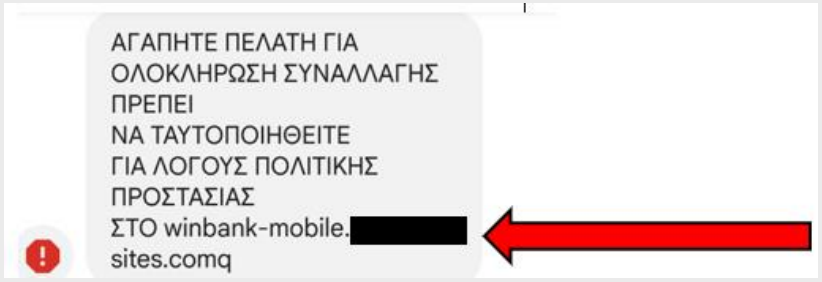
Μη ξεχνάτε!

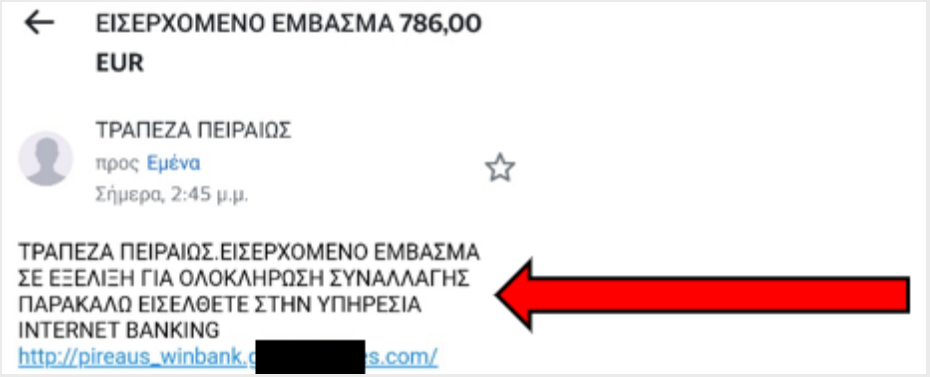
Η Τράπεζα Πειραιώς δεν θα σας ζητήσει ποτέ και με κανένα τρόπο (τηλεφωνικώς ή μέσω e-mail) στοιχεία λογαριασμών, στοιχεία καρτών, κωδικούς πρόσβασης.

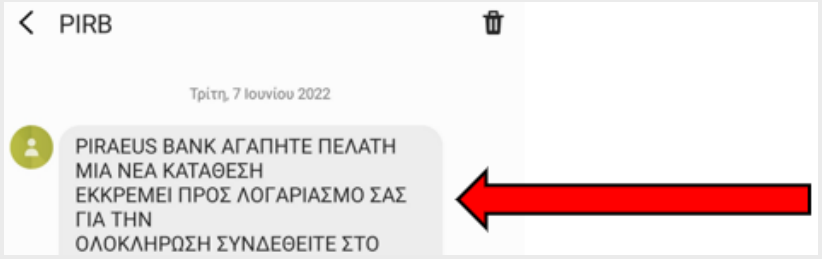
Phishing – Ηλεκτρονικό ψάρεμα

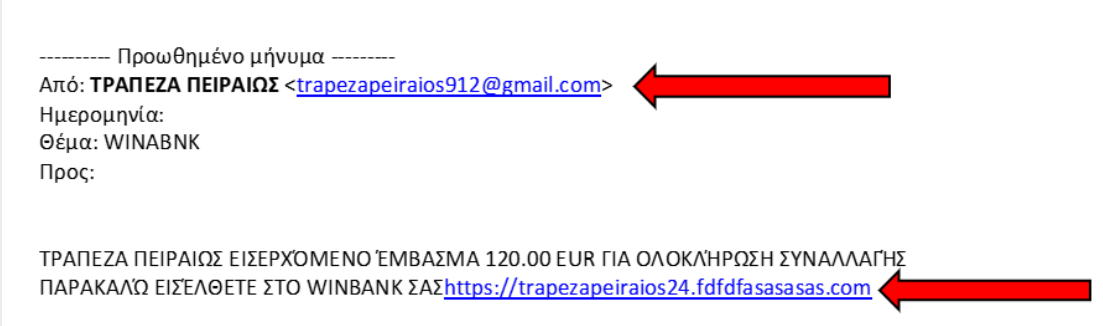
Παραδείγματα











Phishing – Ηλεκτρονικό ψάρεμα

Παραδείγματα

-------- Αρχικό μήνυμα --------
Θέμα: Νέα επιστολή από Winbank
Ημερομηνία:
Αποστολέας: Winbank <winbank@camepotsblstripmaster.org>
Παραλήπτης:

Αγαπητέ πελάτη,

Η εισερχόμενη διαδικτυακή μεταφορά
Winbank τέθηκε σε αναμονή εν αναμονή της διόρθωσης προφίλ λογαριασμού.

Κάντε κλικ εδώ [1] για να δείτε τις
λεπτομέρειες του εμβάσματος.

Σας ευχαριστούμε για την τραπεζική
συνεργασία μαζί μας.

Υποστήριξη εξυπηρέτησης πελατών.

Piraeus Winbank

Links:
---
[1] http://.3.137.201.73

Από: WinBank Επαλήθευση <postmaster@vivirropartmasterdando.com>
Εστάλη:
Προς:
Θέμα: Απαιτείται επαλήθευση SMS

PIRAEUS BANK

Χαίρετε,
Αυτή είναι η δεύτερη ειδοποίηση.
Καθώς αλλάζει το πιο πρόσφατο σύστημά μας, ο αριθμός τηλεφώνου που είναι συνδεδεμένος στον λογαριασμό σας πρέπει να επιβεβαιωθεί μέσω επαλήθευσης μέσω SMS
Μεταβείτε στη διεύθυνση:

web banking login
και ακολουθήστε τις οδηγίες για να ολοκληρώσετε τη διαδικασία επαλήθευσης.
Έχετε υπόψη σας, εάν δεν ολοκληρώσετε αυτήν την επαλήθευση τις επόμενες 24 ώρες, ο λογαριασμός σας θα κλειδωθεί για λόγους ασφαλείας.

τις καλύτερες ευχές,
Εξυπηρέτηση πελατών

Σημαντική σημείωση:
Αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου στάλθηκε σε εσάς επειδή είστε πελάτης της Τράπεζα Πειραιώς. Για να βεβαιωθείτε ότι λαμβάνετε όλες τις επικοινωνίες μας, σας συνιστούμε να προσθέσετε τη διεύθυνση customer-service Αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου δημιουργήθηκε αυτόματα από μια διεύθυνση email μόνο αποστολή. Παρακαλώ μην απαντήσετε σε αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου

SIM swapping – Αντικατάσταση / αλλαγή κάρτας SIM

- Η αντικατάσταση/αλλαγή της κάρτας SIM (SIM Replace) είναι μια καθόλα νόμιμη υπηρεσία που προσφέρουν οι πάροχοι κινητής τηλεφωνίας στους συνδρομητές τους, ώστε οι τελευταίοι να διατηρήσουν τον αριθμό τηλεφώνου τους σε περίπτωση απώλειας ή κλοπής της συσκευής τους ή λόγω ανάγκης χρήσης διαφορετικού μεγέθους κάρτας SIM. Με την ενεργοποίηση της νέας κάρτας SIM, η παλαιά κάρτα αυτόματα απενεργοποιείται και οι υπηρεσίες κινητής τηλεφωνίας (κλήσεις, SMS, πρόσβαση στο διαδίκτυο) πραγματοποιούνται εφεξής από την καινούργια κάρτα που λειτουργεί με τον ίδιο αριθμό.
- Στις περιπτώσεις απάτης τύπου SIM Swapping, οι δράστες εκμεταλλεύονται τη δυνατότητα αλλαγής κάρτας SIM και προσποιούνται είτε τον κάτοχο της κάρτας SIM ή κάποιον εξουσιοδοτημένο από τον νόμιμο συνδρομητή, προσπαθώντας έτσι να εξαπατήσουν τους παρόχους κινητής τηλεφωνίας και να αποκτήσουν νέα κάρτα προς αντικατάσταση αυτής που έχει ο νόμιμος κάτοχος.
- Μόλις ενεργοποιήσουν τη νέα κάρτα, η παλιά, που βρίσκεται στην κατοχή του νόμιμου συνδρομητή απενεργοποιείται και έτσι όλες οι υπηρεσίες (κλήσεις, SMS, πρόσβαση στο διαδίκτυο) λαμβάνονται στη συσκευή που βρίσκεται στην κατοχή του εξαπατήσαντος δράστη, δίνοντάς τους τη δυνατότητα να διεξάγουν παράνομες δραστηριότητες εν αγνοία των νόμιμων συνδρομητών. (π.χ. λαμβάνοντας κλήσεις και μηνύματα που προορίζονται για αυτούς, υποκλέπτοντας κωδικούς μιας χρήσης ή μηνυμάτων επαλήθευσης ασφάλειας κ.λπ).

SIM swapping – Αντικατάσταση / αλλαγή κάρτας SIM

Πως μπορούν όμως οι δράστες με την αντικατάσταση/ανταλλαγή της κάρτας SIM να μπουν στο e-Banking μου;

- Η μη εξουσιοδοτημένη αντικατάσταση/ανταλλαγή της κάρτας SIM αποτελεί συνήθως το δεύτερο σκέλος του παραπάνω παράνομου τρόπου δράσης. Κατά το πρώτο σκέλος, οι δράστες έχουν καταφέρει να υποκλέψουν τους κωδικούς e-Banking συνήθως μέσω ενός ηλεκτρονικού μηνύματος "ψαρέματος" (phishing) ή μέσω κακόβουλου λογισμικού (trojan/malware) που έχουν εγκαταστήσει στον υπολογιστή του θύματος.
- Τι μπορείτε να κάνετε αν δεχτείτε απάτη sim swap;
- Αν το κινητό σας σταματήσει να λειτουργεί για ασυνήθιστους λόγους, επικοινωνήστε αμέσως με τον πάροχο κινητής τηλεφωνίας σας. Μερικές φορές μπορεί να χάσετε σήμα λόγω ευρύτερων προβλημάτων που επηρεάζουν την υπηρεσία κινητής τηλεφωνίας. Ωστόσο, εάν χάσετε την υπηρεσία σε μια θέση που συνήθως έχει καλή κάλυψη, είναι ασφαλέστερο να επικοινωνήσετε με τον πάροχο του δικτύου σας και να επιβεβαιώσετε ότι δεν έχει απενεργοποιηθεί η SIM σας.
- Μην αποκαλύπτετε τον αριθμό του κινητού σας τηλεφώνου στα μέσα κοινωνικής δικτύωσης.
- Εγγραφείτε στις υπηρεσίες των οργανισμών που παρέχουν ειδοποιήσεις SMS και ηλεκτρονικού ταχυδρομείου όταν εκτελούνται συναλλαγές σας.
- Μην απαντάτε ποτέ σε άγνωστα μηνύματα ή κλήσεις που σας ζητούν τα στοιχεία λογαριασμών σας και τον καταχωρημένο αριθμό του κινητού σας τηλεφώνου.

SIM swapping – Αντικατάσταση / αλλαγή κάρτας SIM

Πως μπορούν όμως οι δράστες με την αντικατάσταση/ανταλλαγή της κάρτας SIM να μπουν στο e-Banking μου;

- Μην ακολουθείτε συνδέσμους (links) ιστοσελίδων και μην ανοίγετε συνημμένα αρχεία που μπορεί να λάβετε από άγνωστους αποστολείς ηλεκτρονικού ταχυδρομείου. Ελέγξτε προσεκτικά τον αποστολέα καθώς οι δράστες συχνά προσποιούνται νόμιμες επιχειρήσεις και οργανισμούς.
- Μην κοινοποιείτε σε κανέναν και μην εισάγετε σε άγνωστες ιστοσελίδες, τους κωδικούς e-banking σας (username και password) ή αριθμούς καρτών. Επιβεβαιώνετε ότι έχετε επισκεφθεί το επίσημο site της Τράπεζάς σας και θυμηθείτε ότι οι τράπεζες ποτέ και με κανένα τρόπο δεν θα σας ζητήσουν τους κωδικούς σας.
- Ο υπολογιστής και οι συσκευές σας (tablet, έξυπνα κινητά) να έχουν πάντα τις τελευταίες ενημερώσεις λειτουργικού και εφαρμογών. Εγκαταστήστε και έχετε πάντα ενημερωμένο ένα αξιόπιστο πρόγραμμα προστασίας από κακόβουλο λογισμικό.
- Να ελέγχετε συχνά τις κινήσεις των λογαριασμών σας.
- Εάν έχετε πέσει θύμα απάτης τύπου SIM Swapping ή έχετε διαπιστώσει συναλλαγές οι οποίες δεν έχουν την έγκρισή σας ενημερώστε άμεσα την Τράπεζά σας.

SIM swapping – Αντικατάσταση / αλλαγή κάρτας SIM

Τι μέτρα λαμβάνουν οι τράπεζες;

- Οι τράπεζες δεν μπορούν να γνωρίζουν εάν ένας συνδρομητής έχει πέσει θύμα απάτης τύπου SIM Swapping, phishing ή εάν έχει μολυνθεί με κακόβουλο λογισμικό ο υπολογιστής του και έχουν υποκλαπεί οι κωδικοί του.
- Οι τράπεζες πάντοτε στοχεύουν στη διασφάλιση των ηλεκτρονικών συναλλαγών σύμφωνα με τις τρέχουσες τεχνικές και τεχνολογικές εξελίξεις, τις παγκόσμιες βέλτιστες πρακτικές στο χώρο της ασφάλειας πληροφοριών καθώς και τους ισχύοντες νόμους και κανονισμούς. Επιπλέον, δίνεται μεγάλη έμφαση στην εμπειρία χρήσης και την ταχύτητα των υπηρεσιών που παρέχουν στους Πελάτες τους.
- Οι ηλεκτρονικές απάτες είναι ένα ευρύτερο πρόβλημα και για την αντιμετώπισή τους απαιτείται η συνεργασία πολλών εμπλεκόμενων μερών ώστε να αποτρέπονται ή να προλαμβάνονται. Ειδικά αυτή την περίοδο, όπου η χρήση ηλεκτρονικών υπηρεσιών έχει αυξηθεί σημαντικά σε παγκόσμιο επίπεδο λόγω του κορωνοϊού, οι δράστες προσπαθούν να εκμεταλλευτούν τις ιδιαίτερες συνθήκες με αυξημένες απόπειρες υποκλοπής στοιχείων. Στην Ελληνική Ένωση Τραπεζών έχει συσταθεί ειδική Επιτροπή Πρόληψης και Αντιμετώπισης της Απάτης στα Μέσα και Συστήματα Πληρωμών με σκοπό την παρακολούθηση, επεξεργασία και καθοδήγηση στον τομέα αυτό. Η Επιτροπή συντονίζει τη συνεργασία με την Δίωξη Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, την Τράπεζα της Ελλάδος και συνεργάζεται συστηματικά με λοιπούς αρμόδιους φορείς στην Ελλάδα και το εξωτερικό.
- Για περισσότερες συμβουλές ασφαλείας καθώς και για τα μέτρα προστασίας των συναλλαγών σε κάθε τράπεζα μπορείτε να επισκεφθείτε τις επίσημες ιστοσελίδες τους, τον ιστότοπο της Europol και της Ελληνικής Ένωσης Τραπεζών.