

ΤΡΑΠΕΖΑ ΠΕΙΡΑΙΩΣ



Ασφάλεια συναλλαγών

Συμβουλές για την ασφάλεια των συναλλαγών



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 Europortal και της Ελληνικής Ένωσης Τραπεζών.