Η μεγάλη ανάπτυξη των ψηφιακών μέσων και η εντατικοποίηση της προσπάθε

Απάτη SIM Swapping (αντικατάσταση/αλλαγή SIM κάρτ

Μία μορφή ηλεκτρονικής εξαπάτησης η οποία την τελευταία χρονική περίοδο έχει εμφανισθεί διεθνώς, αλλά και στη χώρα μας είναι η απάτη της μορφής SIM Swapping (αντικατάσταση/ αλλαγή κάρτας SIM κινητού τηλεφώνου). Όπως αναφέρει στο ΑΠΕ/ ΜΠΕ ο Ιωάννης Τζάνος, group corporate security officer & chief information security officer της Eurobank, «οι εγκληματίες στη συγκεκριμένη μορφή απάτης στοχεύουν στην υποκλοπή και χρήση του αριθμού κινητού τηλεφώνου επειδή ολοένα και περισσότεροι οργανισμοί, τράπεζες, κυβερνήσεις χρησιμοποιούν τον αριθμό κινητού τηλεφώνου ως ένα από τα βασικά στοιχεία για την αξιόπιστη ταυτοποίηση του φυσικού προσώπου».

Το κύκλωμα αυτής της απάτης αποτελείται από δύο σκέλη. Ειδικότερα όπως εξηγεί ο κ.Τζάνος προκειμένου να γίνει απόλυτα κατανοητό στον μέσο καταναλωτή «στο πρώτο σκέλος οι δράστες έχουν καταφέρει να υποκλέψουν τους κωδικούς της ηλεκτρονικής υπηρεσίας του θύματος όπως, για παράδειγμα, τους κωδικούς e-Banking καθώς και τον αριθμό κινητού τηλεφώνου. Αυτό συνήθως γίνεται μέσω ενός ηλεκτρονικού μηνύματος «ψαρέματος», το γνωστό «
email
phishing
», ή μέσω κακόβουλου λογισμικού –
trojan
/
malware
– που έχουν εγκαταστήσει στον υπολογιστή του θύματος ή μέσω αγοράς από διάφορα παράνομα φόρουμ του διαδικτύου. Κατά το δεύτερο σκέλος της απάτης οι δράστες εκμεταλλεύονται τη δυνατότητα αλλαγής κάρτας
SIM
, η οποία είναι μία καθόλα νόμιμη υπηρεσία που προσφέρουν οι πάροχοι κινητής τηλεφωνίας στους συνδρομητές τους. Προσποιούνται, είτε τον νόμιμο συνδρομητή ή κάποιον εξουσιοδοτημένο από αυτόν, και προσπαθούν έτσι να εξαπατήσουν τους παρόχους κινητής τηλεφωνίας και να αποκτήσουν νέα κάρτα
SIM
προς αντικατάσταση αυτής που έχει ο νόμιμος κάτοχος».

«Με την ενεργοποίηση της νέας κάρτας SIM, η παλιά κάρτα, που βρίσκεται στην κατοχή του νόμιμου συνδρομητή, απενεργοποιείται και έτσι όλες οι υπηρεσίες κινητής τηλεφωνίας όπως κλήσεις, SMS, πρόσβαση στο Διαδίκτυο, λαμβάνονται στη συσκευή που βρίσκεται στην κατοχή των δραστών, δίνοντάς τους τη δυνατότητα να διεξάγουν παράνομες δραστηριότητες εν αγνοία των νόμιμων συνδρομητών. Για παράδειγμα, λαμβάνοντας κλήσεις και μηνύματα που προορίζονται γι' αυτούς, υποκλέπτοντας κωδικούς μιας χρήσης /
OTP
ή μηνυμάτων επαλήθευσης ασφάλειας κ.λ.π.».

Οι οδηγίες που δίνονται στους πολίτες – Τι πρέπει να προσέξουν

– Αν το κινητό τους σταματήσει να λειτουργεί για ασυνήθιστους λόγους, πρέπει να επικοινωνήσουν αμέσως με τον πάροχο κινητής τηλεφωνίας τους. Μερικές φορές μπορεί να χάσουν το σήμα λόγω ευρύτερων προβλημάτων που επηρεάζουν την υπηρεσία κινητής τηλεφωνίας. Ωστόσο, εάν χαθεί η υπηρεσία σε μια θέση που συνήθως έχει καλή κάλυψη, είναι ασφαλέστερο να επικοινωνήσουν με τον πάροχο του δικτύου τους και να επιβεβαιώσουν ότι δεν έχει αντικατασταθεί η SIM.

– Να μην κοινοποιούν σε κανέναν και μην εισάγουν σε άγνωστες ιστοσελίδες τους κωδικούς e
-
banking
, δηλαδή
username
και
password
, ή αριθμούς καρτών. Οι τράπεζες ποτέ και με κανένα τρόπο δεν ζητούν τους κωδικούς των πελατών.

– Να ελέγχουν συχνά τις κινήσεις των λογαριασμών τους.

Μια ακόμη μορφή απάτης- Υποτιθέμενη βλάβη υπολογιστή

Μια άλλη μορφή απάτης που έχει κάνει την εμφάνιση της γίνεται με τη μέθοδο της παροχής υπηρεσιών τεχνικής υποστήριξης ή επισκευής υποτιθέμενης βλάβης υπολογιστή (technical s
upport
scams
). Οι δράστες τηλεφωνούν σε ανυποψίαστους πολίτες και υποδύονται τεχνικούς από μεγάλη πχ πολυεθνική εταιρία πληροφορικής. Η τηλεφωνική συνομιλία είναι μάλιστα αρκετές φορές στα αγγλικά. Με πρόφαση ότι ο υπολογιστής τους ή / και η φορητή συσκευή τους είναι «μολυσμένα» από κακόβουλο λογισμικό ζητούν να εγκαταστήσουν λογισμικό απομακρυσμένης πρόσβασης, για τη δήθεν επιδιόρθωση – αποκατάσταση του προβλήματος.

Όπως αναφέρει ο κ.Τζάνος «οι εφαρμογές αυτές, αφότου εγκατασταθούν, επιτρέπουν στους δράστες να έχουν πλήρη έλεγχο στις ηλεκτρονικές συσκευές των θυμάτων τους, τους οποίους στη συνέχεια εξαπατούν για να τους «δώσουν» και τους προσωπικούς κωδικούς τους για το e-banking. Οι δράστες προβαίνουν στη συνέχεια σε μεταφορές χρημάτων από τους λογαριασμούς (e-banking) των θυμάτων τους σε τραπεζικούς λογαριασμούς που ελέγχουν οι ίδιοι ή συνεργοί τους».

Συστάσεις στους πολίτες

-Εάν κάποιος καλεί από άγνωστο αριθμό και ισχυρίζεται ότι είναι από μεγάλη πολυεθνική

εταιρία πληροφορικής, χωρίς να έχουν δηλώσει κάποια βλάβη, να διακόπτουν την κλήση.

– Να μην εγκαθιστούν το προτεινόμενο από αγνώστους λογισμικό απομακρυσμένης διαχείρισης.

‘Αλλοι τρόποι απάτης που πρέπει να γνωρίζει ο καταναλωτής

Εκτός από αυτές τις δύο μορφές απάτης υπάρχουν και άλλες περιπτώσεις απάτης που έχουν κάνει την εμφάνιση τους με χαρακτηριστική αυτή των απατηλών εντολών πληρωμής μέσω e-mail (BEC-Business Email Compromise, CEO Fraud & Man in the middle attacks). Στην περίπτωση αυτή οι δράστες αποκτούν μη εξουσιοδοτημένη πρόσβαση και παρεμβαίνουν σε τμήματα της ηλεκτρονικής αλληλογραφίας μεταξύ συναλλασσόμενων επαγγελματιών και εμπόρων με επιχειρήσεις – προμηθευτές ή πελάτες – κυρίως του εξωτερικού. Μόλις εντοπίσουν
e
-
mail
μηνύματα που αφορούν επικείμενη πληρωμή σε τραπεζικό λογαριασμό, παρεμβαίνουν αποστέλλοντας απατηλά μηνύματα, είτε από τις παραβιασμένες διευθύνσεις ηλεκτρονικού ταχυδρομείου είτε από άλλες που προσομοιάζουν με τις πραγματικές. Στη συνέχεια, προτρέπουν τους συναλλασσόμενους να μεταφέρουν χρήματα σε απατηλούς τραπεζικούς λογαριασμούς, διαφορετικούς από αυτούς που είχαν συμφωνηθεί αρχικά.

Χρήσιμες συμβουλές στους επαγγελματίες

– Να επαληθεύουν τηλεφωνικά, με τον προμηθευτή ή τον πελάτη τους, ότι το αίτημα πληρωμής είναι έγκυρο. Να διασταυρώνουν επίσης τηλεφωνικά τον αριθμό λογαριασμού στον οποίο θα πιστωθούν τα χρήματα.

– Να διασφαλίζουν ότι οι υπάλληλοί τους είναι ενημερωμένοι και προσεγγίζουν τα αιτήματα για τη διενέργεια πληρωμών με προσοχή.

Money mules – Τι είναι και τι πρέπει να προσέχουμε

Πρόκειται για άτομα (πολλές φορές ανυποψίαστα θύματα) τα οποία ενεργούν ως μεταφορείς παράνομου χρήματος. Τους συναντάμε συνήθως σε όλες τις μορφές απάτης. Όπως μας αναφέρει ο κ.Τζάνος «οι δράστες στρατολογούν τα υποψήφια θύματά τους με διάφορες μεθόδους, όπως με διαδικτυακές αγγελίες, με διαφημίσεις σε μέσα κοινωνικής δικτύωσης ή με απευθείας αποστολή προσωπικών μηνυμάτων, με σκοπό να τα εξαπατήσουν και να τα χρησιμοποιήσουν ως ενδιάμεσους για να μεταφέρουν σε λογαριασμούς τρίτων, χρήματα που έχουν αποκτηθεί παράνομα, κρατώντας ένα ποσοστό ως προμήθεια. Η μεταφορά χρημάτων που προέρχονται από εγκληματική δραστηριότητα είναι παράνομη καθώς επιτρέπει σε ομάδες οργανωμένου εγκλήματος να νομιμοποιήσουν τα κεφάλαιά τους και να τα μετακινήσουν εύκολα σε όλον τον κόσμο.

Οι καταναλωτές θα πρέπει να είναι ιδιαίτερα προσεκτικοί για προσφορές που υπόσχονται εύκολα χρήματα.

Είναι σημαντικό οι πολίτες αν θεωρούν ότι έχουν πέσει θύματα σχετικής εξαπάτησης, οποιαδήποτε μορφής, να επικοινωνούν άμεσα με την τράπεζά τους και να το καταγγείλουν στις αρμόδιες Αστυνομικές Αρχές.

Τα μέτρα που λαμβάνουν οι τράπεζες

«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 και των πληρωμών καθώς και τους ισχύοντες νόμους και κανονισμούς», αναφέρει ο κ.Τζανός.

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 οι συναλλασσόμενοι μπορούν να επισκεφθούν τις επίσημες ιστοσελίδες τους, τον ιστότοπο της Δίωξης Ηλεκτρονικού Εγκλήματος, της Europol καθώς και της Ελληνικής Ένωσης Τραπεζών.

ΟΔΥΣΣΕΙΑ, 26/7/2020 #ODUSSEIA #ODYSSEIA