

Σχετική ανακοίνωση της Αστυνομίας

Ποιες μορφές διαδικτυακής απάτης συναντώνται συχνότερα;

Οι συνηθέστερες μορφές διαδικτυακής απάτης είναι οι ακόλουθες:

α) Χρεώσεις της πιστωτικής κάρτας πολιτών μέσω του διαδικτύου για αγορές, οι οποίες δεν πραγματοποιήθηκαν από τους ίδιους.

Στις περιπτώσεις αυτές, κάποιος κακόβουλος χρήστης του διαδικτύου δημιουργεί μια πλασματική ιστοσελίδα και με αυτόν τον τρόπο καταφέρνει να συγκεντρώνει στοιχεία κι αριθμούς πιστωτικών καρτών χρηστών του διαδικτύου, οι οποίοι έχοντας εξαπατηθεί, νομίζουν ότι πρόκειται για κάποιο διαδικτυακό κατάστημα και κάνουν τις αγορές τους.

Επιπλέον, αρκετές είναι οι περιπτώσεις όπου επιτήδειοι καταφέρνουν να αποκτούν φυσική πρόσβαση στα στοιχεία πιστωτικών καρτών πολιτών τα οποία εν συνεχεία χρησιμοποιούν σε διαδικτυακές αγορές, καθώς για τις αγορές αυτές δεν είναι απαραίτητη η φυσική κατοχή της πιστωτικής κάρτας, παρά μόνο τα στοιχεία αυτής.

Επιπροσθέτως, σε αρκετές περιπτώσεις οι χρήστες του διαδικτύου δίνουν οι ίδιοι άθελά τους τα στοιχεία σε κακόβουλους χρήστες του διαδικτύου (phishing). Ειδικότερα, ο ανυποψίαστος πολίτης λαμβάνει μήνυμα ηλεκτρονικού ταχυδρομείου από Πιστωτικό Ίδρυμα, στο οποίο τηρεί λογαριασμό, με το οποίο του ζητείται να συμπληρώσει τα στοιχεία του (ονοματεπώνυμο, αριθμό λογαριασμού και πιστωτικής κάρτας κλπ.), για λόγους πχ. ενημέρωσης των αρχείων της τράπεζας. Το μήνυμα, μέσω υπερσυνδέσμου, τους οδηγεί σε μια πλασματική ιστοσελίδα της τράπεζας, με αποτέλεσμα ο πολίτης να πείθεται και να χορηγεί τα επίμαχα στοιχεία.

β) Διακίνηση μηνυμάτων με απατηλό περιεχόμενο, που επιδιώκουν την εξαπάτηση ανυποψίαστων πολιτών.

Ειδικότερα, ο τρόπος δράσης των κακόβουλων δραστών στην εν λόγω μορφή απάτης, που περιγράφεται υπό τον όρο «Ισπανικό Λόττο», είναι η μαζική αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας σε τυχαίους χρήστες του διαδικτύου, με τα οποία τους ενημερώνουν ότι έχουν κερδίσει ένα μεγάλο χρηματικό ποσό της τάξεως των εκατομμυρίων δολαρίων σε ηλεκτρονική κλήρωση του διαδικτύου.

Οι δημιουργοί των μηνυμάτων αυτών, για να γίνουν πιστευτοί, χρησιμοποιούν παραπλήσια ονόματα μεγάλων εταιρειών (πχ. Microsoft , Yahoo κλπ) και συνοδεύουν τα μηνύματα που αποστέλλουν με πλαστά πιστοποιητικά όσον αφορά στην υποτιθέμενη ηλεκτρονική κλήρωση.

Η απάτη έγκειται στο γεγονός ότι ζητούν από τους υποτιθέμενους νικητές την προπληρωμή κάποιων φόρων ή/και εξόδων εκταμίευσης των χρημάτων, ποσό που συνήθως είναι της τάξης των μερικών χιλιάδων δολαρίων.

γ) «Απάτες 419» ή «Νιγηριανές Απάτες»

Στις περιπτώσεις αυτές αποστέλλονται, μηνύματα σε τυχαίους χρήστες του διαδικτύου, με τα οποία τους πληροφορούν ότι κάποιος κάτοχος ιδιαίτερα μεγάλης περιουσίας έχει αποβιώσει και είτε δεν υφίσταται κανείς κληρονόμος και ο παραλήπτης του μηνύματος έχει επιλεγεί ούτως ώστε να κληρονομήσει αυτός την περιουσία, είτε για να καταστεί δυνατό να αποδεσμευτεί η περιουσία, χρειάζεται αυτή να μεταφερθεί σε τραπεζικό λογαριασμό του εξωτερικού και ο παραλήπτης του μηνύματος ενημερώνεται ότι εάν διαθέσει το λογαριασμό του, θα αποκτήσει κάποιο ποσοστό επί της περιουσίας αυτής.

Σε άλλες περιπτώσεις, άτομα από τη Νιγηρία αναζητούν τη βοήθεια επιχειρηματιών ή ελεύθερων επαγγελματιών με σκοπό να μεταφέρουν τα κεφάλαιά τους, τα οποία προέρχονται από εγκληματικές πράξεις (λαθρεμπόριο, απάτες, δωροδοκία κλπ.), υποσχόμενοι για τη συνεργασία αυτή υψηλό ποσοστό αμοιβής. Για το σκοπό αυτό, κάνουν χρήση τίτλων επίσημων φορέων της χώρας τους (Υπουργεία, Κεντρική Τράπεζα, Εθνική Εταιρεία Πετρελαίων Νιγηρίας κλπ.), χρησιμοποιούν τίτλους κυβερνητικών ή στρατιωτικών παραγόντων με υπαρκτά και ψεύτικα ονόματα ή προφασίζονται σχέση τους με «διάσημα» ή «σημαντικά» πρόσωπα.

Η απάτη έγκειται στο γεγονός ότι οι αποστολείς των μηνυμάτων ζητούν από τους παραλήπτες να τους αποστείλουν τα προσωπικά τους στοιχεία, τα στοιχεία των τραπεζικού λογαριασμού και πιστωτικής κάρτας κλπ. προκειμένου επιτευχθεί η συνεργασία τους και η αποκόμιση των χρηματικών ποσών.