Ενόψει του ότι το φαινόμενο της απάτης με διάφορες παραλλαγές και ιδίως της απάτης μέσω διαδικτύου, το τελευταίο διάστημα έχει λάβει τεράστιες διαστάσεις, παρατίθενται στη συνέχεια, <u>για ενημέρωση και προστασία του κοινού</u>, βασικές μορφές απάτης οι οποίες λαμβάνουν συχνά χώρα, καθώς και ορισμένα σημεία, στα οποία πρέπει να δίδεται ιδιαίτερη προσοχή προς αποφυγή της εξαπάτησης.

<u>ΑΠΑΤΕΣ ΣΕ ΑΓΟΡΕΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ /</u>

<u>απάτη των ψευδών αναγγελιών πώλησης διαφόρων αγαθών σε δημοφιλείς διαδικτυακούς ιστοτόπους αγγελιών αγοραπωλησίας (marketplace, car.gr κ.ά.) ή μέσων κοινωνικής δικτύωσης (Facebook)</u>

Οι δράστες της απάτης των ψευδών αναγγελιών πώλησης αγαθών άλλοτε μεν αξιώνουν την κατάθεση του τιμήματος πριν την παράδοση του πωλούμενου, το οποίο ουδέποτε παραδίδουν, άλλοτε δε αποστέλλουν πλαστογραφημένα αντίγραφα εμβάσματος και SWIFT, που φέρουν στοιχεία υπαρκτών εταιρειών με συναφή δραστηριότητα, ισχυριζόμενοι ότι εκ παραδρομής έχουν μεταφέρει χρηματικά ποσά στους τραπεζικούς λογαριασμούς των υποψήφιων αγοραστών. Εν συνεχεία, εκμεταλλευόμενοι την καθυστέρηση της πίστωσης του ποσού, λόγω του μηχανισμού των τοκοφόρων ημερομηνιών (valeur) μεταξύ διαφορετικών χρηματοπιστωτικών ιδρυμάτων, ζητούν την επιστροφή των χρημάτων σε υποδεικνυόμενους τραπεζικούς λογαριασμούς, τα οποία ιδιοποιούνται παράνομα.

<u>ΑΠΑΤΗΛΕΣ ΙΣΤΟΣΕΛΙΔΕΣ ΤΡΑΠΕΖΩΝ</u>

Τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου περιλαμβάνουν ηλεκτρονικούς συνδέσμους (links), που φέρουν αντίγραφα λογοτύπου επίσημων τραπεζών, οι οποίοι σύνδεσμοι τους ανακατευθύνουν σε μια ψεύτικη ιστοσελίδα, δήθεν της επίσημης τράπεζας συνεργασίας, όπου τους ζητείται να αποκαλύψουν τα οικονομικά και προσωπικά τους στοιχεία. Οι ψεύτικες ιστοσελίδες τραπεζών προσομοιάζουν αρκετά με τις νόμιμες ιστοσελίδες τραπεζών.

<u>ΑΠΑΤΕΣ ΜΕ ΤΟ ΠΡΟΣΧΗΜΑ ΕΞΕΙΔΙΚΕΥΜΕΝΩΝ ΤΕΧΝΙΚΩΝ</u>

Άτομα επιχειρούν να παραπλανήσουν χρήστες του διαδικτύου, προσποιούμενοι τους τεχνικούς που εργάζονται σε κέντρα υποστήριξης μεγάλων εταιρειών λογισμικού. Μέσω κλήσεων από τηλέφωνα τρίτων χωρών «προθυμοποιούνται» να βοηθήσουν στην επίλυση τεχνικών προβλημάτων του υπολογιστή. Από τα θύματα ζητούν να εγκαταστήσουν στον υπολογιστή τους λογισμικό απομακρυσμένης πρόσβασης. Με αυτόν τον τρόπο αποκτούν πλήρη έλεγχο και έχουν πρόσβαση σε αποθηκευμένους κωδικούς, τους οποίους στη συνέχεια έχουν τη δυνατότητα να χρησιμοποιήσουν για παράνομες ενέργειες.

ΑΠΑΤΗ ΤΟΥ CEO /

ΑΠΑΤΗ ΜΕ ΤΟ ΕΤΑΙΡΙΚΟ E-MAIL

Η απάτη τύπου CEO / απάτη με το εταιρικό e-mail, λαμβάνει χώρα όταν ένας εξουσιοδοτημένος να πραγματοποιεί πληρωμές υπάλληλος της εταιρείας εξαπατάται προκειμένου να πληρώσει ένα πλαστό τιμολόγιο ή να διενεργήσει μια μη εγκεκριμένη μεταφορά πίστωσης, από τον εταιρικό λογαριασμό της επιχείρησης.

Επίσης, έχουν παρατηρηθεί περιπτώσεις αποστολής απατηλών e-mails από λογαριασμούς ηλεκτρονικού ταχυδρομείου, οι οποίοι διαφέρουν ελάχιστα από λογαριασμούς ηλεκτρονικού ταχυδρομείου πραγματικών συνεργαζόμενων φορέων / εταιρειών / πελατών / προμηθευτών κλπ.

ΑΠΑΤΕΣ ΣΧΕΤΙΖΟΜΕΝΕΣ ΜΕ ΕΠΕΝΔΥΣΕΙΣ /

ΑΠΑΤΗ ΤΩΝ "ΜΗ ΡΕΑΛΙΣΤΙΚΩΝ ΑΠΟΔΟΣΕΩΝ"

Οι κοινές απάτες σχετιζόμενες με επενδύσεις υποσχόμενες εξαιρετικά υψηλές αποδόσεις, μπορεί να περιλαμβάνουν επικερδείς επενδυτικές ευκαιρίες, όπως μετοχές, ομόλογα, κρυπτονομίσματα, πολύτιμους λίθους, υπεράκτιες επενδύσεις σε ακίνητη περιουσία και εναλλακτικές πηγές ενέργειας.

ΑΠΑΤΗ ΤΗΣ ΜΟΡΦΗΣ "Phishing, Pharming & Cracking"
ΣΕ ΣΥΝΔΥΑΣΜΟ ΜΕ ΤΗ ΜΟΡΦΗ "Sim Swapping".

Οι δράστες σε αρκετές περιπτώσεις αποκτούν παράνομη πρόσβαση στους ηλεκτρονικούς υπολογιστές των θυμάτων και υποκλέπτουν τα ονόματα χρήστη και τους κωδικούς πρόσβασής τους στις διαδικτυακές τραπεζικές πλατφόρμες. Εν συνεχεία, με τη χρήση των στοιχείων αυτών εκδίδουν εξουσιοδοτήσεις, μέσω υπηρεσιών της ηλεκτρονικής διακυβέρνησης, δήθεν για λογαριασμό αυτών. Αφού εκδώσουν όλα τα απαραίτητα έγγραφα, οι δράστες χρησιμοποιούν «αχυράνθρωπους» για να εκδώσουν νέες κάρτες SIM για λογαριασμό των θυμάτων. Με τον τρόπο αυτό καταφέρνουν να παρακάμψουν τις διαδικασίες ασφαλείας του e-banking (αποστολή SMS ή VIBER κειμένου στους πελάτες με μοναδικό κωδικό για κάθε συναλλαγή) και να αφαιρέσουν μεγάλα χρηματικά ποσά από τα θύματα.

ΑΠΑΤΗΛΑ ΜΗΝΥΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ (PHISHING)

Ο όρος "phishing" αναφέρεται στα απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου, που σκοπό έχουν να εξαπατήσουν τους παραλήπτες τους και να γνωστοποιήσουν στους επιτήδειους δράστες προσωπικές και οικονομικές πληροφορίες ή κωδικούς ασφαλείας των θυμάτων.

ΑΠΑΤΗΛΑ ΜΗΝΥΜΑΤΑ SMS (SMISHING)

Ο όρος "smishing" (ένας συνδυασμός των λέξεων "SMS" και "Phishing") αναφέρεται στην προσπάθεια των επιτήδειων δραστών να αποκτήσουν προσωπικές και οικονομικές πληροφορίες ή κωδικούς ασφαλείας μέσω μηνυμάτων SMS.

Το μήνυμα κειμένου συνήθως ζητά από το θύμα να κάνει κλικ σε έναν ηλεκτρονικό σύνδεσμο (link) ή να καλέσει έναν αριθμό τηλεφώνου, προκειμένου να επαληθεύσει, ενημερώσει ή επανανεργοποιήσει τον λογαριασμό του.

ΑΠΑΤΗ ΜΕΣΩ ΤΗΣ ΧΡΗΣΗΣ ΤΡΑΠΕΖΙΚΗΣ ΥΠΗΡΕΣΙΑΣ ΤΑΧΕΙΑΣ ΑΝΑΛΗΨΗΣ ΜΕΤΡΗΤΩΝ

Η τραπεζική υπηρεσία παρέχει τη δυνατότητα άμεσης ανάληψης μετρητών από τα ΑΤΜ Τράπεζας, χωρίς τη χρήση κάρτας. Στην προκειμένη περίπτωση, ανάληψη των μετρητών μπορεί να κάνει ακόμη και παραλήπτης που δεν είναι πελάτης της Τράπεζας από οποιοδήποτε ΑΤΜ, αρκεί να διαθέτει τον Κωδικό Ανάληψης Μετρητών που για λόγους ασφαλείας η Τράπεζα κοινοποιεί μόνο στον αποστολέα των χρημάτων.

Ειδικότερα, οι δράστες των εν λόγω απατών χρησιμοποιούν εύσχημες δικαιολογίες και βασίζονται κυρίως στην άγνοια των υποψήφιων θυμάτων για το πώς λειτουργεί η ως άνω τραπεζική υπηρεσία. Παραπλανούν τα θύματα και αυτά ενώ πιστεύουν ότι πληκτρολογούν το ποσό που θα λάβουν για συγκεκριμένη συναλλαγή/αγοραπωλησία/συμφωνία, στην πραγματικότητα δίνουν εντολή χρέωσης του δικού τους λογαριασμού (δηλαδή γίνεται ανάληψη από το λογαριασμό τους). Στη συνέχεια, οι δράστες ζητούν από τα θύματα να τους γνωρίσουν τον Κωδικό Ανάληψης Μετρητών μίας χρήσης που τα θύματα λαμβάνουν από την Τράπεζα. Τέλος, οι δράστες, μέσω του εν λόγω κωδικού, εισπράττουν άμεσα με ανάληψη από ΑΤΜ τα χρήματα που υποτίθεται ότι έπρεπε να καταβάλουν στα θύματα για τη συγκεριμένη συναλλαγή / αγοραπωλησία / συμφωνία.

ΠΡΟΣΟΧΗ:

- ✓ **Μην κάνετε κλικ ποτέ σε ηλεκτρονικούς συνδέσμους (links) που περιλαμβάνονται σε μηνύματα ηλεκτρονικού ταχυδρομείου, τα οποία δήθεν ανακατευθύνουν στην ιστοσελίδα της τράπεζας συνεργασίας.**

- ✓ **Μην δίνετε τον κωδικό "PIN" / "EXTPA PIN" της πιστωτικής ή χρεωστικής κάρτας ή τον κωδικό πρόσβασης του τραπεζικού λογαριασμού μέσω e-banking. Η τράπεζα συνεργασίας δεν θα ζητήσει ποτέ τέτοιου είδους πληροφορίες.**

- ✓ **Συνιστάται ιδιαίτερη προσοχή για συναλλαγές ή επικοινωνίες κατά τις μεταμεσημβρινές / απογευματινές / βραδινές ώρες καθώς και κατά τις ημέρες**

εορτών και αργιών και θεωρείται αναγκαία η άμεση τηλεφωνική επικοινωνία με την τράπεζα συνεργασίας.