

ΤΡΑΠΕΖΑ ΠΕΙΡΑΙΩΣ



Ασφάλεια συναλλαγών

Συμβουλές για την ασφάλεια των συναλλαγών



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 επιτήδριοι προσελκύουν τους πελάτες υποσχόμενοι εξαιρετικά υψηλές αποδόσεις σε σύντομο χρονικό διάστημα, διαβεβαιώνοντας τους πως οι επενδύσεις του θα είναι ασφαλείς και επικερδείς. Οι επιτήδριοι 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 επιτήδριοι 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 επιτήδριοι 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



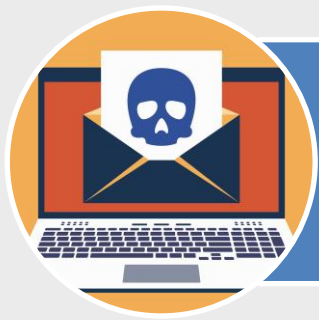
Email με ψεύτικα προφίλ για διαδικτυακά ραντεβού

Οι επιτήδριοι 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 πληρωμές τιμολογίων

Οι επιτήδριοι 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 επιτήδριοι 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.
- ✓ Αγνοείτε τυχόν οδηγίες για υποτιθέμενη πίστωση χρημάτων σε λογαριασμό σας σύμφωνα με τις οποίες πρέπει εσείς να κάνετε ενέργειες μέσω της πλατφόρμα ηλεκτρονικής τραπεζικής. Οι επιτήδριοι 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 καταγγείτε το περιστατικό σε αρμόδια αστυνομική αρχή, είτε με τη φυσική σας παρουσία είτε μέσω του gov.gr.

