ΑΣΠΙS

ΟΛΟΙ ΜΑΖΙ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΤΟΥΜΕ ΑΠΟ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

ΕΚΣΤΡΑΤΕΙΑ ΕΝΗΜΕΡΩΣΗΣ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

ΑΣΠΙΣ

ΟΛΟΙ ΜΑΖΙ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΤΟΥΜΕ ΑΠΟ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

Ηλεκτρονικές απάτες κυρίως μέσω SMS, Κλήσεων και E-mail

Τα ηλεκτρονικά εγκλήματα ή απάτες αποτελούν ουσιαστικά τους τρόπους με τους οποίους κάποιοι κακόβουλα επιδιώκουν να αποκομίσουν χρήματα από ανυποψίαστους ιδιώτες ή επιχειρήσεις. Πολλοί πέφτουν σε αυτή την παγίδα, αφού η βασική τακτική που χρησιμοποιείται είναι η συλλογή πληροφοριών μέσω μηχανισμών που λειτουργούν από ξεχωριστά άτομα και όχι από αυτοματοποιημένα συστήματα.

Αυτού του είδους οι απάτες αποτελούν κλασικά παραδείγματα για το πως οι απατεώνες μπορούν εύκολα να παίξουν με την ψυχολογία αλλά και την προσέγγιση των ατόμων για διάφορα θέματα. Οι πιο κάτω συμβουλές στοχεύουν στο να βοηθήσουν το κοινό να προστατεύσει τον εαυτό του. Η γνώση αποτελεί την καλύτερη μορφή άμυνας από ψηφιακές απάτες και εγκλήματα.

ΑΣΠΙΣ

ΟΛΟΙ ΜΑΖΙ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΤΟΥΜΕ ΑΠΟ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

Γενικές Συμβουλές:

- Να ελέγχετε τακτικά τους ψηφιακούς λογαριασμούς σας.
- Να ελέγχετε τακτικά οποιοδήποτε λογαριασμό και να ειδοποιήσετε τον οργανισμό με τον οποίο συνεργάζεστε εάν παρατηρήσετε κάτι ασυνήθιστο.
- Να διεκπεραιώνετε τις διαδικτυακές πληρωμές σας μόνο μέσω ασφαλών ιστοσελίδων (π.χ. ελέγχετε ότι στο URL υπάρχει η σήμανση ασφαλείας με την κλειδαριά ή ότι υπάρχει το s μετά το γνωστό http) και παράλληλα να χρησιμοποιείτε ασφαλή σύνδεση στο διαδίκτυο, όπως για παράδειγμα η σύνδεσή σας με το δίκτυο του παρόχου σας όχι ανοικτά δίκτυα Wi-Fi.
- Η τράπεζά σας ή άλλος οργανισμός πχ Facebook, Google ή Microsoft ποτέ δεν θα ζητήσει ευαίσθητες πληροφορίες όπως οι κωδικοί του λογαριασμού σας μέσω τηλεφώνου, μηνύματος ή email. Οι κωδικοί σας είναι προσωπικοί και δεν πρέπει να του μοιράζεστε με κανένα.
- Όπου είναι εφικτό συνιστάται η χρήση διπλής ταυτοποίησης (π.χ. με επιβεβαιωτικό SMS, αποτύπωμα ή αποστολή email.
- Εάν μια προσφορά ακούγεται πολύ καλή για να είναι αληθινή, συνήθως αποτελεί απάτη.
- Να διατηρείτε τις προσωπικές σας πληροφορίες ασφαλισμένες.
- Να είστε ιδιαίτερα προσεκτικοί αναφορικά με τις προσωπικές πληροφορίες που μοιράζεστε στα μέσα κοινωνικής δικτύωσης (ΜΚΔ). Οι απατεώνες δυνατόν να χρησιμοποιήσουν τέτοιες πληροφορίες για δημιουργία πλαστών εγγράφων ή για να στήσουν μια απάτη με στόχο εσάς.
- Εάν θεωρήσετε ότι δώσατε λεπτομέρειες του λογαριασμού σας σε έναν απατεώνα επικοινωνήστε άμεσα με την τράπεζά σας.
- Πάντα να αναφέρετε οποιαδήποτε ύποπτη κίνηση ή απόπειρα απάτης στην Αστυνομία, ακόμη και εάν δεν πέσετε θύμα κάποιας διαδικτυακής απάτης ή εγκλήματος.

ΑΣΠΙΣ

ΟΛΟΙ ΜΑΖΙ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΤΟΥΜΕ ΑΠΟ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

Τι είναι Phishing, Smishing και Vishing

- **Phishing** (μέσω email)
- **Smishing** (μέσω sms στο τηλέφωνο)
- **Vishing** (μέσω τηλεφωνικής επικοινωνίας)

Είναι οι κύριες μέθοδοι που χρησιμοποιούνται για απάτες που στοχεύουν πελάτες τραπεζών.

ΑΣΠΙΣ

ΟΛΟΙ ΜΑΖΙ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΤΟΥΜΕ ΑΠΟ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

Α. Απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου (Phishing)

Ο όρος "Phishing" αναφέρεται στα απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου, που σκοπό έχουν να εξαπατηθούν οι παραλήπτες τους και να γνωστοποιήσουν στους απατεώνες προσωπικές και οικονομικές τους πληροφορίες ή κωδικούς ασφαλείας τους.

Πως λειτουργεί;

Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου:

- Μπορεί να μοιάζουν πάρα πολύ με τα μηνύματα που στέλνουν στους πελάτες τους οι τράπεζες.
- Αντιγράφουν το λογότυπο, τα χαρακτηριστικά και το ύφος των πραγματικών μηνυμάτων ηλεκτρονικού ταχυδρομείου.
- Σας ζητούν να κατεβάσετε στη συσκευή σας ένα επισυναπτόμενο αρχείο ή να κάνετε κλικ σε έναν ηλεκτρονικό σύνδεσμο (link).
- Κάνουν χρήση ορολογίας που δίνει την αίσθηση του κατεπείγοντος.

ΑΣΠΙΣ

ΟΛΟΙ ΜΑΖΙ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΤΟΥΜΕ ΑΠΟ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

Απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου (Phishing)

Τι μπορείτε να κάνετε;

- Διατηρείτε το λογισμικό ενημερωμένο, περιλαμβανομένου του φυλλομετρητή ιστοσελίδων (browser), του αντιικού προγραμμάτος (antivirus) και του λειτουργικού συστήματος.
- Να είστε ιδιαίτερα προσεκτικοί εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου «τράπεζας» σας ζητά ευαίσθητες πληροφορίες (π.χ. τον κωδικό πρόσβασης του τραπεζικού σας λογαριασμού μέσω internet banking).
- Ελέγξτε προσεκτικά το μήνυμα ηλεκτρονικού ταχυδρομείου: συγκρίνετε τη διεύθυνση με τα προηγούμενα πραγματικά μηνύματα από την τράπεζα συνεργασίας σας.
- Ελέγξτε για ορθογραφικά λάθη και λάθη γραμματικής ή σύνταξης.
- Μην απαντάτε σε ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου, αντίθετα προωθήστε το στην τράπεζα συνεργασίας σας, πληκτρολογώντας την ηλεκτρονική της διεύθυνση μόνοι σας.
- Μην κάνετε απευθείας κλικ στον ηλεκτρονικό σύνδεσμο (link) και μην πραγματοποιείστε λήψη (download) του επισυναπτόμενου αρχείου, αντίθετα πληκτρολογήστε τη διεύθυνση του ηλεκτρονικού συνδέσμου στον φυλλομετρητή ιστοσελίδων (browser) που χρησιμοποιείτε.
- Σε περίπτωση οποιασδήποτε αμφιβολίας, ελέγξτε την ιστοσελίδα ή τηλεφωνήστε στην τράπεζα συνεργασίας σας.

Οι εγκληματίες στον κυβερνοχώρο βασίζονται στο γεγονός ότι οι άνθρωποι έχουν μεγάλο φόρτο εργασίας ή είναι βιαστικοί. Καταρχήν, αυτά τα απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου μοιάζουν να είναι νόμιμα.
Προσέξτε ιδιαίτερα όταν χρησιμοποιείτε μια φορητή συσκευή. Ενδεχομένως να είναι πιο δύσκολο να εντοπίσετε μια απόπειρα ηλεκτρονικού «ψαρέματος» από το κινητό τηλέφωνο ή το tablet σας.

ΑΣΠΙΣ

ΟΛΟΙ ΜΑΖΙ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΤΟΥΜΕ ΑΠΟ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

Β. Απατηλές τηλεφωνικές κλήσεις (vishing)

Ο όρος “Vishing” (συνδυασμός των λέξεων “Voice” και “Phishing”) είναι απάτη μέσω τηλεφώνου, που σκοπό έχει να εξαπατηθεί το θύμα προκειμένου να αποκαλύψει τις προσωπικές και οικονομικές του πληροφορίες ή κωδικούς ασφαλείας του ή και να μεταφέρει χρήματα στους απατεώνες.

ΑΣΠΙΣ

ΟΛΟΙ ΜΑΖΙ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΤΟΥΜΕ ΑΠΟ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

Απατηλές τηλεφωνικές κλήσεις (vishing)

Τι μπορείτε να κάνετε?

- Να είστε προσεκτικοί με αιφνιδιαστικές και απροειδοποίητες τηλεφωνικές κλήσεις.
- Κρατήστε τον αριθμό τηλεφώνου από τον οποίο σας έχουν καλέσει και ενημερώστε ότι θα τους επιστρέψετε εσείς την τηλεφωνική κλήση.
- Για να επαληθεύσετε την ταυτότητά τους, αναζητήστε τον αριθμός τηλεφώνου της επιχείρησης και επικοινωνήστε απευθείας μαζί τους.
- Μην επαληθεύετε το άτομο που σας καλεί με τον αριθμό τηλεφώνου που σας έδωσε (μπορεί να είναι ψεύτικος ή πλαστογραφημένος αριθμός).
- Οι απατεώνες μπορούν να βρουν τα βασικά στοιχεία επικοινωνίας σας μέσω διαδικτύου (π.χ. από τα μέσα κοινωνικής δικτύωσης). Μην υποθέσετε ότι το άτομο που σας καλεί δηλώνει την αληθινή του ιδιότητα επειδή έχει στη διάθεσή του τέτοιες πληροφορίες.
- Μην δίνετε τον κωδικό “PIN” της πιστωτικής ή χρεωστικής σας κάρτας ή τον κωδικό πρόσβασης του τραπεζικού σας λογαριασμού μέσω e-banking. Η τράπεζα συνεργασίας σας δεν θα ζητήσει ποτέ τέτοιου είδους πληροφορίες.
- Μην μεταφέρετε χρήματα σε άλλο τραπεζικό λογαριασμό κατόπιν αιτήματός τους. Η τράπεζα συνεργασίας σας δεν θα σας ζητήσει ποτέ να προβείτε σε τέτοια ενέργεια.
- Αν νομίζετε ότι πρόκειται για απατηλή τηλεφωνική κλήση, αναφέρετέ το στην τράπεζα συνεργασίας σας.

ΑΣΠΙΣ

ΟΛΟΙ ΜΑΖΙ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΤΟΥΜΕ ΑΠΟ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

Γ. Απατηλά μηνύματα SMS (Smishing)

Ο όρος “smishing” (ένας συνδυασμός των λέξεων “sms” και “Phishing”) αναφέρεται στην προσπάθεια των απατεώνων να αποκτήσουν προσωπικές και οικονομικές πληροφορίες ή κωδικούς ασφαλείας μέσω μηνυμάτων SMS.

Πως λειτουργεί;

Το μήνυμα κειμένου συνήθως θα σας ζητά να κάνετε κλικ σε έναν ηλεκτρονικό σύνδεσμο (link) ή να καλέσετε έναν αριθμό τηλεφώνου, προκειμένου να επαληθεύσετε, ενημερώσετε ή επανανεργοποιήσετε τον λογαριασμό σας. Αλλά…ο ηλεκτρονικός σύνδεσμος οδηγεί σε ψεύτικη ιστοσελίδα και ο αριθμός τηλεφώνου οδηγεί στον απατεώνα που ισχυρίζεται ότι εκπροσωπεί τη νόμιμη επιχείρηση.

ΑΣΠΙΣ

ΟΛΟΙ ΜΑΖΙ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΤΟΥΜΕ ΑΠΟ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

Απατηλά μηνύματα SMS (Smishing)

Τι μπορείτε να κάνετε?

- Μην κάνετε κλικ σε ηλεκτρονικούς συνδέσμους (links), συνημμένα αρχεία ή εικόνες που λαμβάνετε με μηνύματα κειμένου (sms) δίχως να έχετε επαληθεύσει τον αποστολέα.
- Μην βιάζεστε. Πάρτε τον χρόνο σας και πραγματοποιήστε τους απαραίτητους ελέγχους προτού απαντήσετε.
- Ποτέ μην απαντάτε σε μήνυμα κειμένου (sms) που σας ζητά τον κωδικό “PIN” ή τον κωδικό πρόσβασης (password) στον τραπεζικό σας λογαριασμό ή οποιαδήποτε άλλα εξατομικευμένα διαπιστευτήρια ασφαλείας (π.χ. e-banking user name).
- Εάν νομίζετε ότι ενδέχεται να έχετε απαντήσει σε ένα απατηλό μήνυμα κειμένου (sms) και παρείχατε τα στοιχεία των τραπεζικών σας λογαριασμών, επικοινωνήστε αμέσως με την τράπεζα συνεργασίας σας.

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

NATIONAL CSIRT-CY

ΑΣΤΥΝΟΜΙΑ ΚΥΠΡΟΥ

ΚΕΝΤΡΙΚΗ ΤΡΑΠΕΖΑ ΤΗΣ ΚΥΠΡΟΥ

ΣΤΚ
ΣΥΝΔΕΣΜΟΣ ΤΡΑΠΕΖΩΝ ΚΥΠΡΟΥ