ΑΠΑΤΗ ΤΟΥ CEO / ΑΠΑΤΗ ΜΕ ΤΟ ΕΤΑΙΡΙΚΟ E-MAIL

Η απάτη του 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.

ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ;

Ο απατεώνας καλεί ή στέλνει μηνύματα ηλεκτρονικού ταχυδρομείου υποδυόμενος υψηλόβαθμο στέλεχος της επιχείρησης (π.χ. Γενικός Διευθυντής ή Οικονομικός Διευθυντής).

Γνωρίζουν επαρκώς την εσωτερική διάρθρωση και οργάνωση της επιχείρησης.

Απαιτούν τη διενέργεια μιας επείγουσας πληρωμής.

Χρησιμοποιούν όρους και εκφράσεις, όπως: "εχεμύθεια/εμπιστευτικότητα", "η επιχείρηση σε εμπιστεύεται", "δεν είμαι αυτή τη στιγμή διαθέσιμος".

Συχνά το αίτημα αφορά τη διενέργεια διασυνοριακών πληρωμών σε τράπεζες εγκατεστημένες εκτός Ευρώπης.

Ο υπάλληλος μεταφέρει τα χρήματα σε λογαριασμό που τηρεί ο απατεώνας.

Οδηγίες για την διαδικασία μπορεί να δοθούν αργότερα, μέσω τρίτου προσώπου ή μηνύματος ηλεκτρονικού ταχυδρομείου.

Αναφέρονται σε μια "ευαίσθητη" για την επιχείρηση κατάσταση (π.χ. φορολογικός έλεγχος, συγχώνευση, εξαγορά).

Απαιτούν από τον υπάλληλο της επιχείρησης να μην ακολουθήσει τις συνήθεις διαδικασίες λήψης έγκρισης για την πληρωμή.

ΠΟΙΕΣ ΕΙΝΑΙ ΟΙ ΕΝΔΕΙΞΕΙΣ;

- Αιφνιδιαστική / Απροειδοποίητη τηλεφωνική κλήση ή e-mail
- Απευθείας επικοινωνία με ανώτερο στέλεχος της επιχείρησης με το οποίο συνήθως δεν επικοινωνείς
- Αίτημα για απόλυτη εχεμύθεια
- Άσκηση πίεσης για το κατεπείγον του αιτήματος
- Ασύνηθες αίτημα αντίθετο με τις εσωτερικές διαδικασίες έγκρισης
- Απειλές ή ασυνήθιστη κολακεία / υποσχέσεις ανταμοιβής

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

Ως επιχείρηση

Να γνωρίζετε τους κινδύνους και να διασφαλίζετε ότι και οι υπάλληλοί σας είναι επίσης ενημερωμένοι.

Να ενθαρρύνετε το προσωπικό σας να προσεγγίζει τα αίτηματα για τη διενέργεια πληρωμών με προσοχή.

Εφαρμόστε εσωτερικές διαδικασίες σχετικά με τη διενέργεια πληρωμών.

Εφαρμόστε διαδικασία για την επαλήθευση της νομιμότητας αιτημάτων διενέργειας πληρωμών που λαμβάνονται μέσω e-mail.

Καθιερώστε διαδικασίες υποβολής αναφορών για τη διαχείριση περιστατικών απάτης.

Ελέγξτε τις πληροφορίες που αναρτώνται στην ιστοσελίδα της επιχείρησής σας, περιορίστε τις πληροφορίες και επιδείξτε ιδιαίτερη προσοχή σε σχέση με τα κοινωνικά μέσα δικτύωσης.

Να αναβαθμίζετε και να ενημερώνετε το λογισμικό τεχνικής ασφαλείας.

Να επικοινωνείτε πάντα με την αστυνομία σε περιπτώσεις απόπειρας απάτης, ακόμα και αν δεν είστε θύμα αυτής.

Ως εργαζόμενος

Να εφαρμόζετε αυστηρά τις υφιστάμενες διαδικασίες ασφαλείας σε σχέση με τη διενέργεια πληρωμών και καταβολής προμηθειών. Μην παραλείπετε κανένα βήμα και μην υποκύπτετε σε πιέσεις.

Να ελέγχετε πάντα με προσοχή τις διευθύνσεις ηλεκτρονικού ταχυδρομείου όταν διαχειρίζεστε ευαίσθητες πληροφορίες / πραγματοποιείτε μεταφορές χρημάτων.

Σε περίπτωση αμφιβολίας για εντολή πληρωμής, συμβουλευθείτε έναν αρμόδιο συνάδελφό σας.

Μην ανοίγετε ποτέ ύποπτους ηλεκτρονικούς συνδέσμους (links) ή ύποπτα επισυναπτόμενα αρχεία που λαμβάνετε μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου. Να είστε εξαιρετικά προσεκτικοί όταν ελέγχετε το προσωπικό σας e-mail στους υπολογιστές της επιχείρησης στην οποία εργάζεστε.

Περιορίστε τις πληροφορίες και επιδείξτε προσοχή σε σχέση με τα μέσα κοινωνικής δικτύωσης.

Αποφεύγετε την κοινοποίηση πληροφοριών σχετικά με την ιεραρχία, την ασφάλεια και τις ακολουθούμενες διαδικασίες της επιχείρησης στην οποία εργάζεστε.

Αν λάβετε ένα ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου ή μια ύποπτη τηλεφωνική κλήση, να ενημερώνετε πάντοτε τη διεύθυνση μηχανογραφικής υποστήριξης.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ · 90 YEARS 1928-2018 HELLENIC BANK ASSOCIATION

#CyberScams

ΑΠΑΤΕΣ ΣΧΕΤΙΖΟΜΕΝΕΣ ΜΕ ΕΠΕΝΔΥΣΕΙΣ

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

ΠΟΙΕΣ ΕΙΝΑΙ ΟΙ ΕΝΔΕΙΞΕΙΣ;

- Σας υπόσχονται γρήγορες αποδόσεις και σας διαβεβαιώνουν ότι οι επενδύσεις είναι ασφαλείς.
- Η προσφορά είναι διαθέσιμη για περιορισμένο χρονικό διάστημα.
- Λαμβάνετε επανειλλημένα αιφνιδιαστικές / απροειδοποίητες τηλεφωνικές κλήσεις.
- Η προσφορά είναι προσωπική και σας ζητείται να μην τη μοιραστείτε με άλλους.

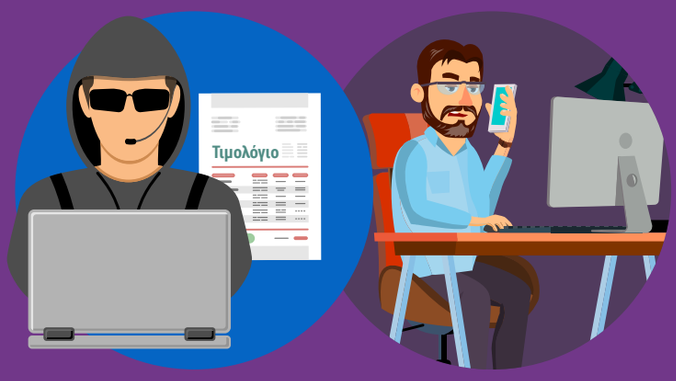
ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

- Σε κάθε περίπτωση, να λαμβάνετε αμερόληπτες χρηματοπιστωτικές συμβουλές, προτού δώσετε χρήματα ή πραγματοποιήσετε μια επένδυση.
- Να απορρίπτετε τις τηλεφωνικές κλήσεις που σχετίζονται με επενδυτικές ευκαιρίες.
- Να είστε επιφυλακτικοί με προσφορές που υπόσχονται ασφαλείς επενδύσεις, εγγυημένες αποδόσεις και υψηλά κέρδη.
- Προσοχή σε μελλοντικά περιστατικά απάτης. Αν έχετε ήδη πραγματοποιήσει επένδυση σε προϊόν που αποτελεί αντικείμενο απάτης, είναι εξαιρετικά πιθανό οι απατεώνες να σας στοχοποιήσουν εκ νέου ή να πουλήσουν τα προσωπικά σας στοιχεία σε άλλους εγκληματίες.
- Επικοινωνήστε με την αστυνομία αν έχετε υπόνοιες για περιστατικό απάτης

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ | 90 YEARS | HELLENIC BANK ASSOCIATION

#CyberScams

ΑΠΑΤΗ ΜΕΣΩ ΤΙΜΟΛΟΓΙΩΝ ΚΑΙ ΛΟΙΠΩΝ ΠΑΡΑΣΤΑΤΙΚΩΝ



ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ;

- Μια επιχείρηση προσεγγίζεται από κάποιον τρίτο που ισχυρίζεται ότι εκπροσωπεί έναν προμηθευτή/πάροχο υπηρεσιών/δικαιούχο μιας πληρωμής.
- Μπορεί να γίνει χρήση συνδυασμού πρακτικών προσέγγισης: τηλέφωνο, επιστολή, e-mail, κ.λπ
- Ο απατεώνας ζηταεί να τροποποιηθούν οι πληροφορίες για τις μελλοντικές πληρωμές τιμολογιών (δηλαδή τα στοιχεία του τραπεζικού λογαριασμού του δικαιούχου πληρωμής). Ο νέος προτεινόμενος λογαριασμός ανήκει στον απατεώνα.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

ΩΣ ΕΠΙΧΕΙΡΗΣΗ

Διασφαλίστε ότι οι υπάλληλοι είναι ενημερωμένοι και γνωρίζουν τη συγκεκριμένη μορφή απάτης και τον τρόπο αποφυγής της.

Εφαρμόστε διαδικασία για την επαλήθευση της νομιμότητας των αιτημάτων πληρωμής που λαμβάνετε.

Δώστε εντολή στο προσωπικό που είναι αρμόδιο για την πληρωμή τιμολογίων να προβαίνει πάντα στη διενέργεια ελέγχων για τον εντοπισμό τυχόν παρατυπιών.

Ελέγξτε τις πληροφορίες που αναρτώνται στην ιστοσελίδα της επιχείρησής σας και συγκεκριμένα τα συμβόλαια και τους προμηθευτές σας. Διασφαλίστε ότι το προσωπικό περιορίζει τη γνωστοποίηση πληροφοριών της επιχείρησης στα μέσα κοινωνικής δικτύωσης.

ΩΣ ΥΠΑΛΛΗΛΟΣ

Επαληθεύστε ότι όλα τα αιτήματα πληρωμών προέρχονται από τους πραγματικούς προμηθευτές της επιχείρησης, ειδικά εάν σας ζητούν να τροποποιήσετε τα στοιχεία των τραπεζικών τους λογαριασμών για τις μελλοντικές πληρωμές των τιμολογίων ή λοιπών παραστατικών.

Μην κάνετε χρήση των στοιχείων επικοινωνίας που περιλαμβάνονται στην επιστολή/fax/e-mail στο οποίο ζητείται η αλλαγή στοιχείων. Αντίθετα, χρησιμοποιείστε τα στοιχεία επικοινωνίας από την προηγούμενη αλληλογραφία σας με τον προμηθευτή.

Καθορίστε μοναδικά σημεία επικοινωνίας με επιχειρήσεις, στις οποίες πραγματοποιείτε πληρωμές ανά τακτά χρονικά διαστήματα.

Περιορίστε τις πληροφορίες που γνωστοποιείτε για τον εργοδότη σας στα μέσα κοινωνικής δικτύωσης.

Για πληρωμές που υπερβαίνουν ένα συγκεκριμένο όριο ποσού, καθορίστε μια διαδικασία για την επιβεβαίωση του ορθού τραπεζικού λογαριασμού και του αποδέκτη (π.χ. επικοινωνία με την επιχείρηση).

Όταν πληρώνετε ένα τιμολόγιο, να στέλνετε e-mail ενημέρωσης του αποδέκτη της πληρωμής. Σε αυτό να γράφετε την επωνυμία της τράπεζάς του και τα τέσσερα τελευταία ψηφία του τραπεζικού του λογαριασμού για τη διασφάλιση της συναλλαγής.

Να αναφέρετε πάντοτε τυχόν ύποπτη απόπειρα απάτης στην αστυνομία, ακόμα και αν δεν είστε θύμα αυτής.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ | 90 YEARS HELLENIC BANK ASSOCIATION

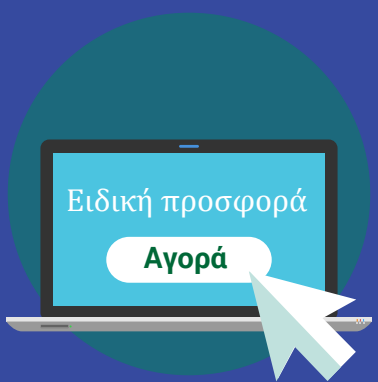
#CyberScams

ΑΠΑΤΕΣ ΣΕ ΑΓΟΡΕΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

Οι προσφορές μέσω διαδικτύου συνιστούν συχνά επικερδείς αγορές, αλλά χρειάζεται ιδιαίτερη προσοχή στα περιστατικά απάτης.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

- Να κάνετε χρήση εγχώριων ιστοσελίδων λιανικών πωλήσεων, όταν είναι δυνατόν - είναι πιθανότερο να λύσετε τυχόν προβλήματα που θα ανακύψουν.
- Πραγματοποιήστε την έρευνα σας - ελέγξτε τις κριτικές προτού προβείτε σε κάποια αγορά.
- Χρησιμοποιήστε πιστωτικές κάρτες - έχετε περισσότερες πιθανότητες να σας επιστραφούν τα χρηματικά ποσά σε περίπτωση απάτης.



- Πληρώστε μόνο μέσω μιας ασφαλούς υπηρεσίας πληρωμών - Σας ζητούν μεταφορά χρημάτων; Σκεφτείτε το διπλά!
- Πληρώστε μόνο εφόσον είστε συνδεδεμένοι στο διαδίκτυο μέσω ασφαλών συνδέσεων - αποφεύγετε τη χρήση δωρεάν ή ανοικτών δημόσιων δικτύων WiFi.
- Πληρώστε μόνο μέσω ασφαλούς συσκευής - Διατηρείτε το λειτουργικό σας σύστημα και λογισμικό ασφαλείας ενημερωμένο.
- Προσοχή στις διαφημίσεις που προσφέρουν εξωφρενικές προσφορές ή θαυματουργά προϊόντα - Εάν ακούγεται πολύ καλό για να είναι αληθινό, τότε κατά πάσα πιθανότητα είναι ψεύτικο!
- Αναδυόμενο παράθυρο που ισχυρίζεται ότι έχετε κερδίσει βραβείο; Σκεφτείτε το ξανά. Ενδεχομένως να κερδίσατε κακόβουλο λογισμικό.
- Εάν δεν παραλάβετε το προϊόν σας, επικοινωνήστε με τον έμπορο/πωλητή. Εάν δεν λάβετε απάντηση, επικοινωνήστε με την τράπεζα συνεργασίας σας.

Να αναφέρετε πάντοτε τυχόν ύποπτη απόπειρα απάτης στην αστυνομία, ακόμα και αν δεν είστε θύμα αυτής.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ | HELLENIC BANK ASSOCIATION

#CyberScams

ΑΠΑΤΗΛΑ ΜΗΝΥΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ (PHISHING)

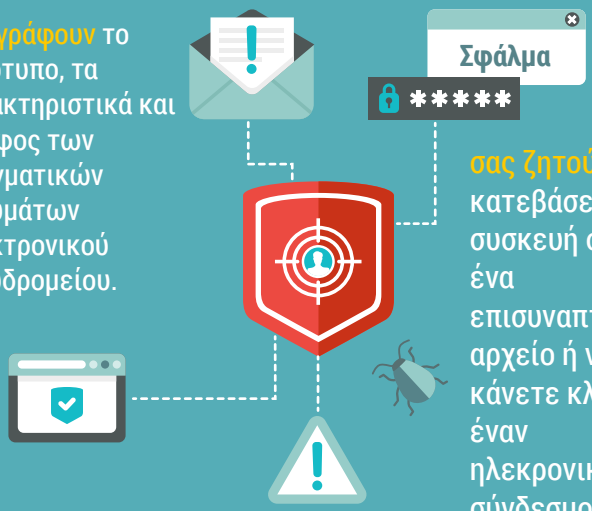
Ο όρος "phishing" αναφέρεται στα απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου, που σκοπό έχουν να εξαπατηθούν οι παραλήπτες τους και να γνωστοποιήσουν στους απατεώνες προσωπικές και οικονομικές τους ροφορίες ή κωδικούς ασφαλείας τους.

ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ;

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 ηλεκρονικό σύνδεσμο (link).

κάνουν χρήση ορολογίας που δίνει την αίσθηση του κατεπείγοντος.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

- 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 είναι απασχολημένοι και 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.

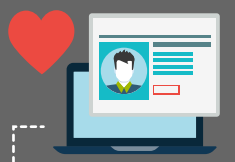
#CyberScams

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ | 90 YEARS 1928-2018 | HELLENIC BANK ASSOCIATION

ΑΠΑΤΗ ΜΕΣΩ ΔΙΑΔΙΚΤΥΑΚΩΝ ΡΑΝΤΕΒΟΥ

Οι απατεώνες στοχεύουν σε υποψήφια θύματα μέσω ιστοσελίδων διοργάνωσης διαδικτυακών ραντεβού, αλλά μπορούν, επίσης, να κάνουν χρήση των μέσων κοινωνικής δικτύωσης ή μηνυμάτων ηλεκτρονικού ταχυδρομείου για να έρθουν σε επαφή με τα υποψήφια θύματά τους.

ΠΟΙΕΣ ΕΙΝΑΙ ΟΙ ΕΝΔΕΙΞΕΙΣ;



Κάποιος που γνωρίσατε πρόσφατα μέσω διαδικτύου δηλώνει ότι τρέφει έντονα συναισθήματα για εσάς, ζητώντας σας να επικοινωνήσετε κατ' ιδίαν.

Τα μηνύματά τους είναι συχνά κακώς διατυπωμένα και ασαφή.

Το διαδικτυακό τους προφίλ δεν συνάδει με αυτά που σας λένε.

Μπορεί να σας ζητήσουν να στείλετε προσωπικές σας φωτογραφίες ή βίντεο.

€€€

Πρωτίστως κερδίζουν την εμπιστοσύνη σας. Εν συνεχεία σας ζητούν χρήματα, δώρα ή στοιχεία του τραπεζικού σας λογαριασμού/της πιστωτικής σας κάρτας.

Εάν δεν στείλετε τα χρήματα, ενδέχεται να αποπειραθούν να σας εκβιάσουν. Εάν τα στείλετε, θα σας ζητήσουν περισσότερα.

ΕΙΣΤΕ ΘΥΜΑ;

Μην αισθάνεστε ντροπιασμένοι!

Σταματήστε κάθε μορφή επικοινωνίας.

Εάν είναι δυνατόν, διατηρείστε όλο το ιστορικό επικοινωνίας, όπως τα μηνύματα συνομιλιών.

Υποβάλλετε καταγγελία στην αστυνομία.

Αναφέρετε το συμβάν στην ιστοσελίδα στην οποία ο απατεώνας σας προσέγγισε για πρώτη φορά Εάν έχετε παράσχει στοιχεία του τραπεζικού σας λογαριασμού, επικοινωνήστε με την τράπεζα συνεργασίας σας.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

- Να είστε πολύ προσεκτικοί με τις προσωπικές πληροφορίες που διαμοιράζετε στα μέσα κοινωνικής δικτύωσης και στις ιστοσελίδες διοργάνωσης διαδικτυακών ραντεβού.
- Να λαμβάνετε πάντα υπ' όψιν σας τους κινδύνους. Οι απατεώνες είναι παρόντες στις πιο αξιόπιστες ιστοσελίδες.
- Να μη βιάζεστε να απαντήσετε και να κάνετε ερωτήσεις.
- Να ψάξετε τη φωτογραφία και το προφίλ του ατόμου που σας έχει προσεγγίσει για να δείτε εάν το υλικό αυτό έχει χρησιμοποιηθεί και αλλού.
- Να είστε ιδιαίτερα προσεκτικοί στα ορθρογραφικά λάθη και στα λάθη γραμματικής και σύνταξης, στις ασυνέπειες στις ιστορίες τους, καθώς και σε δικαιολογίες, όπως το γεγονός ότι η κάμερα τους είναι εκτός λειτουργίας.
- Μην μοιράζεστε οποιοδήποτε υλικό, το οποίο θα μπορούσε να χρησιμοποιηθεί για να σας εκβιάσουν.
- Εάν συμφωνήσετε να συναντηθείτε κατ' ιδίαν από κοντά, ενημερώστε την οικογένειά σας και τους φίλους σας για τον προορισμό σας.
- Επιδείξτε τεράστια προσοχή σε αιτήματα μεταφοράς χρημάτων. Να μην στέλνετε ποτέ χρήματα, να μη δίνετε στοιχεία της πιστωτικής σας κάρτας, του τραπεζικού σας λογαριασμού, των κωδικών σας στο e-banking ή αντίγραφα προσωπικών σας εγγράφων.
- Να αποφεύγετε την αποστολή χρηματικών προκαταβολών.
- Μην μεταφέρετε χρήματα για κάποιον άλλο: το ξέπλυμα βρώμικου χρήματος είναι ποινικό αδίκημα.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

90 YEARS 1928-2018 HELLENIC BANK ASSOCIATION

#CyberScams

ΑΠΑΤΗΛΑ ΜΗΝΥΜΑΤΑ 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 ΛΕΙΤΟΥΡΓΕΙ;

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.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

- 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.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ | 90 YEARS 1928-2018 HELLENIC BANK ASSOCIATION

#CyberScams

ΑΠΑΤΗΛΕΣ ΙΣΤΟΣΕΛΙΔΕΣ ΤΡΑΠΕΖΩΝ

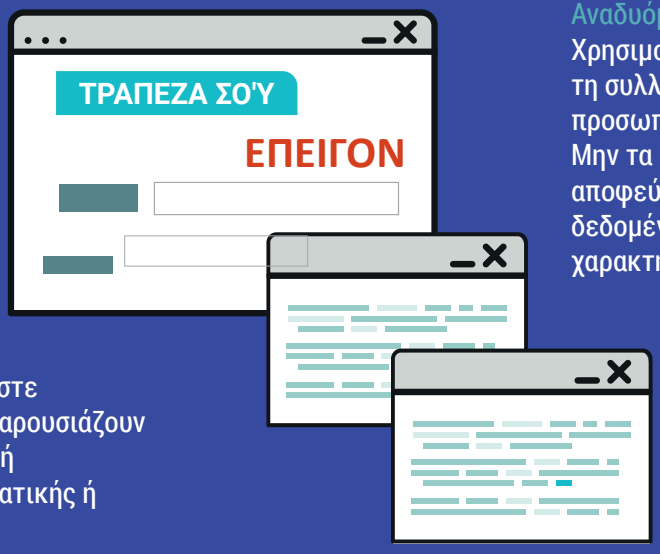
Τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου περιλαμβάνουν ηλεκτρονικούς συνδέσμους (links), οι οποίοι θα σας ανακατευθύνουν σε μια ψεύτικη ιστοσελίδα, δήθεν της τράπεζας συνεργασίας σας, όπου θα σας ζητηθεί να αποκαλύψετε τα οικονομικά και προσωπικά σας στοιχεία.

ΠΟΙΕΣ ΕΙΝΑΙ ΟΙ ΕΝΔΕΙΞΕΙΣ;

Οι ψεύτικες ιστοσελίδες τραπεζών προσομοιάζουν αρκετά με τις νόμιμες ιστοσελίδες της τράπεζάς σας. Οι ψεύτικες ιστοσελίδες θα διαθέτουν συχνά ένα αναδυόμενο παράθυρο, με το οποίο θα σας ζητείται η εισαγωγή των εξατομικευμένων διαπιστευτηρίων ασφαλείας σας. Οι τράπεζες δεν κάνουν χρήση τέτοιων αναδυόμενων παραθύρων.

Αυτές οι ιστοσελίδες συχνά εμφανίζουν:

Επείγον: δεν θα συναντήσετε ποτέ τέτοιους είδους μηνύματα σε νόμιμες ιστοσελίδες.



Αναδυόμενα παράθυρα: Χρησιμοποιούνται συνήθως για τη συλλογή ευαίσθητων προσωπικών σας πληροφοριών. Μην τα επιλέγετε και αποφεύγετε την υποβολή δεδομένων προσωπικού χαρακτήρα σε αυτά.

Ελαττωματικός σχεδιασμός: Να είστε προσεκτικοί σε ιστοσελίδες που παρουσιάζουν ελαττώματα στον σχεδιασμό τους ή ορθογραφικά λάθη και λάθη γραμματικής ή σύνταξης.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

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

Πάντοτε να πληκτρολογείτε εσείς τον ηλεκτρονικό σύνδεσμο της τράπεζάς σας ή να χρησιμοποιείτε υφιστάμενο ηλεκτρονικό σύνδεσμο από τον κατάλογο των αγαπημένων σας σελιδοδεικτών.

Χρησιμοποιείτε φυλλομετρητή ιστοσελίδων (browser) που σας επιτρέπει την επιλογή αποκλεισμού αναδυόμενων παραθύρων.

Εάν κάτι σημαντικό πραγματικά χρειάζεται την προσοχή σας θα ενημερωθείτε για αυτό από την τράπεζά σας όταν θα συνδεθείτε ηλεκτρονικά στον τραπεζικό σας λογαριασμό (π.χ. μέσω e-banking).

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ | 90 YEARS | HELLENIC BANK ASSOCIATION

#CyberScams

ΑΠΑΤΗΛΕΣ ΤΗΛΕΦΩΝΙΚΕΣ ΚΛΗΣΕΙΣ

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.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

- 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 αριθμό 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.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ | 90 YEARS 1928-2018 HELLENIC BANK ASSOCIATION

#CyberScams

Πώς να αναγνωρίσεις τις διαδικτυακές απάτες

EUROPEAN CYBER SECURITY MONTH

Λαμβάνεις ένα SMS από το δράστη Γιώργο, ο οποίος υποδύεται ότι εργάζεται στην τράπεζα συνεργασίας σου. Κάνεις κλικ στον ηλεκτρονικό σύνδεσμο του SMS.

Ανακατευθύνεσαι σε ιστοσελίδα που μοιάζει με εκείνη της τράπεζας συνεργασίας σου. Εισάγεις τα διαπιστευτήρια ασφαλείας σου (user name & password).

Ο δράστης Γιώργος πλέον έχει πρόσβαση στα οικονομικά σου στοιχεία και στο ιστορικό των πρόσφατων ηλεκτρονικών σου συναλλαγών.

Σου τηλεφωνεί υποδυόμενος τον τραπεζικό υπάλληλο και παραθέτει τα στοιχεία σου.

Ο δράστης Γιώργος σε πείθει να προχωρήσεις στη μεταφορά χρημάτων σε άλλο τραπεζικό λογαριασμό τον οποίο ελέγχει ο ίδιος.

Προστατεύσου από τις διαδικτυακές απάτες!

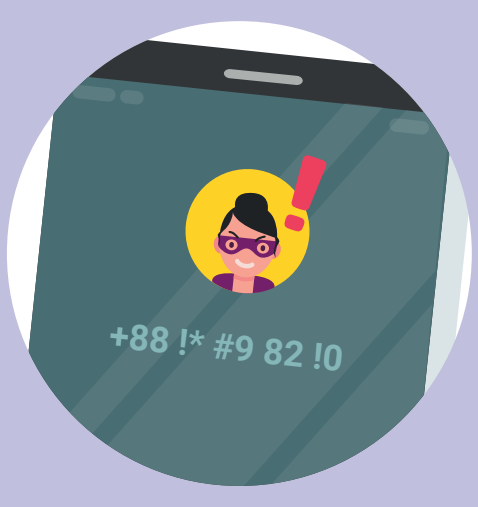
1. Προσοχή σε ανεπιθύμητα μηνύματα κειμένου ή μηνύματα ηλεκτρονικού ταχυδρομείου που ισχυρίζονται ότι προέρχονται από την τράπεζα συνεργασίας σου.
2. Εάν περιέχουν ηλεκτρονικούς συνδέσμους (links) και συνημμένα αρχεία, μην τα ανοίξεις.
3. Εάν λάβεις μια ύποπτη κλήση από την τράπεζα με την οποία συνεργάζεσαι, κλείσε το τηλέφωνο και επαλήθευσέ την κλήση καλώντας το τμήμα εξυπηρέτησης πελατών της τράπεζας.
4. Ποτέ μην κοινοποιείς τα διαπιστευτήρια ασφαλείας σου (user name & password) ή τους κωδικούς για την εκτέλεση συναλλαγής πληρωμής (π.χ. SMS OTP).
5. Εάν νομίζεις ότι έχεις πέσει θύμα απάτης, επικοινώνησε αμέσως με την τράπεζα συνεργασίας σου και ανέφερε το σχετικό περιστατικό στην αστυνομία.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ · ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Πώς να αναγνωρίσεις τις απάτες υποτιθέμενης τεχνικής υποστήριξης

EUROPEAN CYBER SECURITY MONTH

Η δράστης Χριστίνα σε καλεί υποδυόμενη τον πάροχο τεχνικής υποστήριξης, ισχυριζόμενη ότι υπάρχει πρόβλημα με το λογισμικό του υπολογιστή σου.



Η υπηρεσία αναγνώρισης του τηλεφώνου σου εμφανίζει έναν τηλεφωνικό αριθμό από μια αξιόπιστη εταιρεία τηλεπικοινωνιών.

Η δράστης Χριστίνα σε παροτρύνει να δράσεις γρήγορα, ειδάλλως θα χάσεις όλα σου τα δεδομένα.

Σου συνιστά να κάνεις λήψη ενός προγράμματος, το οποίο θα λύσει το πρόβλημα.

Το πρόγραμμα που κατέβασες της δίνει πρόσβαση στον υπολογιστή σου και σε όλα σου τα δεδομένα.

Σου ζητάει μια μικρή αμοιβή για την παρεχόμενη υπηρεσία, προκειμένου να σε αναγκάσει να συνδεθείς στο περιβάλλον ηλεκτρονικής τραπεζικής της τράπεζας συνεργασίας σου.

Η δράστης Χριστίνα πλέον έχει πρόσβαση στον τραπεζικό σου λογαριασμό και μπορεί να προχωρήσει στην εκτέλεση συναλλαγών.

Προστατεύσου από απάτες υποτιθέμενης τεχνικής υποστήριξης!

1. Μην απαντάς σε τηλεφωνικές κλήσεις από οποιονδήποτε ισχυρίζεται ότι υπάρχει πρόβλημα με τον υπολογιστή σου.
2. Κάνε λήψη/αναβάθμιση λογισμικού μόνο από επίσημες ιστοσελίδες.
3. Ανέφερε το συμβάν στην αστυνομία και στον πραγματικό πάροχο υπηρεσιών.
4. Προχώρα σε αποκλεισμό των τηλεφωνικών αριθμών των απατεώνων, προκειμένου να μην μπορούν να σε ξανακαλέσουν.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Πώς να αναγνωρίσεις την ηλεκτρονική απάτη μέσω τηλεφωνικής επικοινωνίας?

EUROPEAN CYBER SECURITY MONTH

Λαμβάνεις ένα τηλεφώνημα από την απατεώνα Χριστίνα, η οποία προσποιείται ότι είναι από την εταιρεία ηλεκτρικής σου ενέργειας. Σου προτείνει μια διαφημιστική προσφορά.

Αποδέχεσαι την προσφορά και η απατεώνας Χριστίνα ζητά προσωπικά και οικονομικά σου στοιχεία για να επιβεβαιώσει την παραγγελία σου.

Η απατεώνας Χριστίνα έχει πλέον πρόσβαση στον τραπεζικό σου λογαριασμό και προσπαθεί να πραγματοποιήσει μια απατηλή συναλλαγή.

Σου ζητάει να επιβεβαιώσεις τα στοιχεία μέσω SMS που αποστέλλεται στο τηλέφωνό σου, ενώ εκτελείται η απατηλή συναλλαγή.

Προστάτευσε τον εαυτό σου από διαδικτυακές απάτες!

1. Προσοχή στις ανεπιθύμητες κλήσεις που ισχυρίζονται ότι προέρχονται από παρόχους υπηρεσιών κοινής ωφέλειας (τηλεφωνία, ενέργεια, ύδρευση, κ.λπ).
2. Εάν ζητήσουν προσωπικά ή οικονομικά σου στοιχεία μέσω τηλεφώνου, κλείσε το τηλέφωνο και κάλεσε την εξυπηρέτηση πελατών της εταιρείας.
3. Ανέφερε το συμβάν στην αστυνομία και στον πραγματικό πάροχο υπηρεσιών.
4. Απέκλεισε τους απατηλούς τηλεφωνικούς αριθμούς, προκειμένου να μην μπορούν να σε ξανακαλέσουν.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Πώς να αναγνωρίσεις την κλοπή στοιχείων ταυτότητας

EUROPEAN CYBER SECURITY MONTH

Τι είναι η κλοπή στοιχείων ταυτότητας?

Η κλοπή στοιχείων ταυτότητας συμβαίνει όταν κάποιος κλέβει τα προσωπικά σου στοιχεία (π.χ. ονοματεπώνυμο, αριθμός πιστωτικής κάρτας, αριθμός κοινωνικής ασφάλισης, αριθμός άδειας οδήγησης, αριθμός αστυνομικής ταυτότητας ή διαβατηρίου, ΑΦΜ, κ.λπ.) με σκοπό την πραγματοποίηση απάτης.

Ο σκοπός της κλοπής των στοιχείων ταυτότητας ενδέχεται να είναι:

Το άνοιγμα ενός τραπεζικού λογαριασμού (π.χ. για την έκδοση πλαστών επιταγών ή λήψη δανείων)

Η παραβίαση email λογαριασμών

Η λήψη ασφαλιστηρίων συμβολαίων

Η πώληση πληροφοριών σε άλλους δράστες στο διαδίκτυο

Συνηθισμένες μέθοδοι κλοπής που χρησιμοποιούν οι επιτήδειοι:

1

Ηλεκτρονικό «ψάρεμα» μέσω μηνύματος ηλεκτρονικού ταχυδρομείου, μέσω τηλεφωνικής επικοινωνίας και μέσω μηνύματος SMS

2

Πληροφορίες διαθέσιμες στο διαδίκτυο

3

Μη ασφαλή ασύρματα δίκτυα

Προστατεύσου από την κλοπή στοιχείων ταυτότητας!

1. **Επαλήθευσε όλα τα αιτήματα για τα προσωπικά σου δεδομένα.**
2. **Περιόρισε τον αριθμό των προσωπικών σου δεδομένων που μοιράζεσαι μέσω διαδικτύου (π.χ. στα μέσα κοινωνικής δικτύωσης).**
3. **Να παρακολουθείς τακτικά τις διαδικτυακές σου τραπεζικές δραστηριότητες και τις κινήσεις της πιστωτικής σου κάρτας.**
4. **Για να διατηρήσεις ασφαλές το email σου, άδειασε τα εισερχόμενά σου το συντομότερο δυνατό.**
5. **Εάν πιστεύεις ότι είσαι θύμα κλοπής στοιχείων ταυτότητας, επικοινώνησε αμέσως με την τράπεζα συνεργασίας σου, συγκέντρωσε όλα τα πιθανά στοιχεία και ανέφερε το συμβάν στην αστυνομία.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

CYBER CRIME DIVISION ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Πώς να αναγνωρίσεις την κλοπή στοιχείων ταυτότητας

EUROPEAN CYBER SECURITY MONTH

Ο απατεώνας Γιώργος δημοσιεύει μια αγγελία εργασίας στα μέσα κοινωνικής δικτύωσης.

Υποβάλεις την αίτησή σου (βιογραφικό, συνοδευτική επιστολή κ.λπ.) και τα προσωπικά σου στοιχεία (διαβατήριο ή ταυτότητα).

Ο απατεώνας Γιώργος κάνει χρήση των προσωπικών σου στοιχείων μαζί με τη φωτογραφία του για να δημιουργήσει μια νέα ταυτότητα.

Ο απατεώνας Γιώργος πηγαίνει σε μια τράπεζα και χρησιμοποιεί την πλαστή ταυτότητα για να ανοίξει τραπεζικό λογαριασμό.

Χρησιμοποιεί τον τραπεζικό λογαριασμό για να πραγματοποιεί παράνομες συναλλαγές.

Προστατεύσου από την κλοπή στοιχείων ταυτότητας!

1. Επαλήθευσε όλα τα αιτήματα για τα προσωπικά σου δεδομένα.
2. Περιόρισε τον αριθμό των προσωπικών σου δεδομένων που μοιράζεσαι μέσω διαδικτύου (π.χ. στα μέσα κοινωνικής δικτύωσης).
3. Να παρακολουθείς τακτικά τις διαδικτυακές τραπεζικές σου δραστηριότητες και τις κινήσεις της πιστωτικής σου κάρτας.
4. Για να διατηρήσεις ασφαλές το email σου, άδειασε τα εισερχόμενά σου το συντομότερο δυνατό.
5. Εάν πιστεύεις ότι είσαι θύμα κλοπής ταυτότητας, επικοινώνησε αμέσως με την τράπεζα συνεργασίας σου, συγκέντρωσε όλα τα πιθανά στοιχεία και ανέφερε το συμβάν στην αστυνομία.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

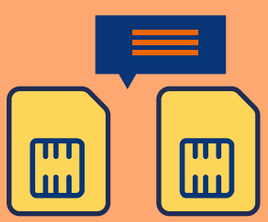
ΑΠΑΤΗ ΑΛΛΑΓΗΣ ΚΑΡΤΑΣ SIM – ΜΙΑ ΑΠΑΤΗ ΜΕΣΩ ΚΙΝΗΤΟΥ ΤΗΛΕΦΩΝΟΥ

Η απάτη αλλαγής κάρτας SIM πραγματοποιείται όταν ένας απατεώνας, κάνοντας χρήση τεχνικών κοινωνικής μηχανικής, αναλαμβάνει τον έλεγχο της κάρτας SIM του κινητού σου τηλεφώνου χρησιμοποιώντας τα κλεμμένα προσωπικά σου δεδομένα.

ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ;

Ένας δράστης αποκτά τα προσωπικά στοιχεία του θύματος μέσω π.χ. παραβιάσεων δεδομένων, ηλεκτρονικού «ψαρέματος», αναζητήσεων στα μέσα κοινωνικής δικτύωσης, κακόβουλων εφαρμογών, αγορών μέσω διαδικτύου, κακόβουλου λογισμικού κ.λπ.

Με αυτές τις πληροφορίες, ο απατεώνας εξαπατά τον πάροχο υπηρεσιών κινητής τηλεφωνίας για τη μεταφορά του αριθμού κινητού τηλεφώνου του θύματος σε μια κάρτα SIM που έχει στην κατοχή του.



Ο δράστης μπορεί τώρα να λαμβάνει εισερχόμενες κλήσεις και μηνύματα SMS, συμπεριλαμβανομένης της πρόσβασης σε περιβάλλον ηλεκτρονικής τραπεζικής του θύματος.

Το θύμα θα παρατηρήσει την απώλεια σήματος στο κινητό του τηλέφωνο και τελικά θα διαπιστώσει ότι δεν έχει πρόσβαση στον τραπεζικό του λογαριασμό μέσω διαδικτύου.

ΤΙ ΜΠΟΡΕΙΣ ΝΑ ΚΑΝΕΙΣ;

- Διατήρησε το λογισμικό σου ενημερωμένο, συμπεριλαμβανομένου του περιηγητή, του αντιικού λογισμικού και του λειτουργικού σου συστήματος.
- Περιόρισε το διαμοιρασμό πληροφοριών και δώσε ιδιαίτερη προσοχή όσον αφορά τα κοινωνικά μέσα δικτύωσης.
- Μην ανοίγεις ποτέ ύποπτους ηλεκτρονικούς συνδέσμους ή συνημμένα αρχεία που λαμβάνεις μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου ή μηνυμάτων SMS.
- Μην απαντάς σε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου ή μην επικοινωνείς τηλεφωνικά με άτομα που ζητούν τα προσωπικά σου στοιχεία.
- Κατέβαζε εφαρμογές μόνο από επίσημους παρόχους και διάβαζε πάντα τα δικαιώματα των εφαρμογών.
- Εάν είναι δυνατόν, μην συσχετίζεις τον αριθμό τηλεφώνου σου με ευαίσθητους διαδικτυακούς λογαριασμούς.
- Καθόρισε τον δικό σου κωδικό PIN για να περιορίσεις την πρόσβαση στην κάρτα SIM σου. Μην διαμοιράζεσαι τον κωδικό PIN με κανέναν.
- Έλεγχε συχνά τις οικονομικές σου κινήσεις.
- Ενημέρωνε τακτικά τους κωδικούς πρόσβασής σου.

ΕΙΣΑΙ ΘΥΜΑ;

- Εάν το κινητό σου τηλέφωνο χάσει το σήμα χωρίς λόγο, ανέφερε το συμβάν αμέσως στον τηλεπικοινωνιακό σου πάροχο.
- Εάν ο τηλεπικοινωνιακός σου πάροχος επιβεβαιώσει ότι έχει γίνει αλλαγή της κάρτας SIM, ανέφερε το συμβάν στην αστυνομία.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

#CyberScams