Συνεχίζεται η εκστρατεία ενημέρωσης και ευαισθητοποί-ησης του κοινού για τις ηλεκτρονικές απάτες που ξεκίνη-σε το 2021 με τη συνεργασία των δυνάμεων του...

υπουργείου Προστασίας του Πολίτη, της Τράπεζας της Ελλάδος, της Ελληνικής Αστυνομίας και της Ελληνικής Ένωσης Τραπεζώ ν (ΕΕΤ) και έχει συμβάλει καθοριστικά στο περιορισμό των περιστατικώ ν σε ένα εξαιρετικά μικρό ποσοστό στο σύνολο των συναλλαγώ ν.
Σε αναρτήσεις τους στις ιστοσελίδες, τόσο η ΕΕΤ όσο και ο Ελληνικός Χρηματοοικονομικός Μεσολαβητής, επανέρχονται δίνοντας απαντήσεις σε επίκαιρα ερωτήματα στο πλαίσιο της ενημερωτικής εκστρατείας.
Συχνές Ερωτήσεις και Απαντήσεις
Ερώ τηση: Τις τελευταίες ημέρες έχω λάβει αρκετά e-mails και SMS. Στα μηνύματα αυτά η "τράπεζα" μου αναφέρει ότι «έχει παρατηρηθεί ύποπτη δραστηριότητα» στον λογαριασμό ή την κάρτα μου ή ότι «έχει κλειδωθεί ή απενεργοποιηθεί» ο λογαριασμός ή η κάρτα μου. Τα μηνύματα περιέχουν κάποιον σύνδεσμο (link) και με προτρέπουν να ακολουθήσω αμέσως τις οδηγίες που υπάρχουν σε αυτόν για να λυθεί το πρόβλημά και για να ξεμπλοκάρω την πρόσβασή μου.
Απάντηση: Τα μηνύματα αυτά ΔΕΝ ΠΡΟΕΡΧΟΝΤΑΙ από την τράπεζά σας (μάλιστα κάποιες φορές φαίνεται να τα στέλνει τράπεζα με την οποία δεν διατηρείτε καν συνεργασία). Είναι μηνύματα απατηλά (phishing) και αποσκοπούν στο να σας

ξεγελάσουν ώ στε να καταχωρήσετε σε απατηλή ιστοσελίδα πανομοιότυπη με αυτήν της τράπεζας σας τους κωδικούς σας πρόσβασης στο ebanking ή τα στοιχεία της κάρτας σας αλλά και τους Κωδικούς μιας Χρήσης (OTP) που λαμβάνετε εκείνη τη στιγμή και απαιτούνται για την έγκριση συναλλαγώ ν.
Η απάντηση σε όλες αυτές τις κακόβουλες προσπάθειες είναι μια και απλή. Ποτέ δεν δίνουμε προσωπικά μας στοιχεία σε κανέναν που μας τα ζητάει. Η Τράπεζά σας ποτέ δεν θα σας ζητήσει κάτι τέτοιο.
Ερώ τηση: Πρόσφατα ανάρτησα μία αγγελία στο διαδίκτυο για να πουλήσω κάποιο προσωπικό μου αντικείμενο. Δέχτηκα τηλεφώ νημα από κάποιον άγνωστο ο οποίος μου είπε ότι ενδιαφέρεται να το αγοράσει, μάλιστα χωρίς καν να το δει ή να το ελέγξει. Μου ζήτησε όμως να του δώ σω τα στοιχεία της κάρτας μου ή τους κωδικούς του e-Banking μου ώ στε να μπορέσει να μου καταθέσει τα χρήματα. Να τα δώ σω τα στοιχεία μου; να τον εμπιστευτώ ;
Απάντηση: Όχι, δεν πρέπει. Για κατάθεση χρημάτων, αρκεί μόνο να δώ σετε τον IBAN του λογαριασμού σας. Μην αποκαλύψετε ποτέ τους κωδικούς σας στο ebanking ή τα στοιχεία της κάρτας σας ή τυχόν κωδικούς μίας χρήσης (OTP) που θα λάβετε εκείνη τη στιγμή.
Επίσης, σε περίπτωση που ο αγοραστής ισχυρίζεται ότι έχει καταθέσει τα χρήματα σε λογαριασμό σας, ελέγξτε εσείς ο ίδιος το ακριβές ποσό μόνο μέσα από το eBanking σας. Μην βασιστείτε σε τυχόν αποδείξεις κατάθεσης που μπορεί να σας προσκομίσει ή σας αποστείλει. Μπορεί να είναι πλαστές.
Ερώ τηση: Πρόσφατα δέχτηκα τηλεφωνική κλήση από το εξωτερικό, και αυτός που με κάλεσε μου είπε (στα Αγγλικά) ότι είναι τεχνικός από μεγάλη εταιρεία πληροφορικής και ότι ο υπολογιστής μου έχει μολυνθεί από κακόβουλο λογισμικό και μπορούσε να επιδιορθώ σει το πρόβλημα. Δεν τον πίστεψα όμως και έκλεισα το τηλέφωνο. Καλά έκανα?
Απάντηση: Ναι. Πρόκειται για προσπάθεια εξαπάτησης. Αν συνέχιζες θα σου ζητούσε να εγκαταστήσεις λογισμικό απομακρυσμένης πρόσβασης και έτσι θα αποκτούσε πλήρη έλεγχο στον υπολογιστή σου. Μετά, ο απατεώ νας, με πρόφαση την επιδιόρθωση του προβλήματος θα σου ζητούσε τους κωδικούς σου σύνδεσης στο e-Banking σου και θα προσπαθούσε ο ίδιος να κάνει μεταφορές χρημάτων από τους λογαριασμούς σου. Μην εμπιστεύεστε τον υπολογιστή σας σε αγνώ στους. Εάν κάποιος σας καλεί από άγνωστο αριθμό, ειδικά από το εξωτερικό, και ισχυρίζεται ότι είναι από οποιαδήποτε εταιρεία πληροφορικής, χωρίς εσείς να έχετε δηλώ σει βλάβη σε συσκευή σας, διακόψτε την κλήση. Μην προχωράτε σε εγκατάσταση λογισμικού απομακρυσμένης διαχείρισης που σας προτείνει κάποιος άγνωστος.
Ερώ τηση: Μου ζητήθηκε να μεσολαβήσω στη μεταφορά χρημάτων προσφέροντας μου αμοιβή για να γίνει κατάθεση χρημάτων σε λογαριασμό μου. Υπάρχει κάποιο πρόβλημα; Είναι παράνομο;
Απάντηση: Ναι είναι παράνομο. Εάν σας προσεγγίσουν μέσω e-mail ή μέσω κοινωνικώ ν δικτύων ή μέσω αγγελιώ ν και σας ζητήσουν να μεταφέρετε χρήματα (τα οποία θα έχουν μπει προηγουμένως στον λογαριασμό σας) σε λογαριασμούς τρίτων συνήθως σε άλλες χώ ρες ή να τους τα δώ σετε κάνοντας ανάληψη από κάποιο ATM ή κατάστημα, κρατώ ντας ένα ποσοστό ως προμήθεια, πρέπει να γνωρίζετε ότι προσπαθούν να σας εξαπατήσουν για να διαμεσολαβήσετε στη

μεταφορά παράνομου χρήματος (money muling) και ότι η πράξη αυτή διώ κεται ποινικά.
Συνεπώ ς:
μη δεχτείς να μεσολαβήσεις ως ενδιάμεσος σε διακίνηση χρημάτων από άλλα άτομα, συνήθως άγνωστα σε σένα. Μπορεί να υποστείς σημαντικές επιπτώ σεις, καθώ ς με αυτόν τον τρόπο εμπλέκεσαι σε παράνομες ενέργειες, είτε το γνωρίζεις είτε όχι εάν λάβεις ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου (email), μην απαντήσεις και μην ακολουθήσεις τυχόν υποδεικνυόμενο σύνδεσμο (link), διασταύρωσε τα στοιχεία της εταιρείας που προσφέρει τη θέση εργασίας και τα στοιχεία επικοινωνίας της (ειδικά αν εδρεύει στο εξωτερικό),
μην παραχωρείς ποτέ στοιχεία του τραπεζικού σου λογαριασμού σε κανέναν, εκτός εάν έχεις μαζί του μονιμότερη συνεργασία, ή είναι άτομο του στενού οικογενειακού σου περιβάλλοντος εάν πιστεύεις ότι έχεις εμπλακεί σε μεταφορά παράνομου χρήματος, μην προβείς σε οποιαδήποτε άλλη μεταφορά χρημάτων που τυχόν σου ζητηθεί. Ειδοποίησε αμέσως την τράπεζα σου, την υπηρεσία στην οποία πραγματοποίησες την συναλλαγή και την αστυνομία.
Ερώ τηση: Σε γενικές γραμμές, τι θα πρέπει να κάνω για να μην πέσω θύμα ηλεκτρονικής απάτης;
Απάντηση: Η τράπεζα ή οι τράπεζες συνεργασίας σας έχουν αναρτήσει στις ιστοσελίδες τους χρήσιμες συμβουλές, προκειμένου να μην πέσετε θύμα απάτης. Σε κάθε περίπτωση, παρατίθενται παρακάτω ορισμένες βασικές οδηγίες, για να διενεργείτε με τη μεγαλύτερη δυνατή ασφάλεια τις ηλεκτρονικές σας συναλλαγές:
Πληκτρολογείτε οι ίδιοι την ηλεκτρονική διεύθυνση της Τράπεζάς σας για την πρόσβασή σας στις υπηρεσίες ηλεκτρονικής τραπεζικής. Μην ακολουθείτε αποτελέσματα από μηχανές αναζήτησης.
Βεβαιωθείτε ότι πλοηγείστε στο ασφαλές περιβάλλον της Τράπεζας. Ελέγξτε αν ο σύνδεσμος στον οποίο εισέρχεστε (https://www.....gr) αντιστοιχεί στην ηλεκτρονική διεύθυνση της Τράπεζας σας. Κάνετε κλικ στο εικονίδιο του λουκέτου, για να ελέγξτε ότι η σύνδεση αναφέρεται ως ασφαλής.
Ελέγξετε προσεκτικά την συναλλαγή που περιγράφεται στο μήνυμα της Τράπεζας (π.χ. μέσω sms, viber ή εφαρμογής του mobile app) με τον κωδικό μιας χρήσης OTP, πριν την επιβεβαίωσή της.
Αποφύγετε τη χρήση δημόσιων ή κοινόχρηστων δικτύων.
Μην αποθηκεύετε ποτέ τους κωδικούς σας σε οποιαδήποτε συσκευή σας.
Αλλάζετε τουλάχιστον ανά εξάμηνο τους κωδικούς ασφαλείας σας (passwords).
Ενισχύστε την ασφάλεια των συσκευώ ν σας διατηρώ ντας ενημερωμένο πρόγραμμα προστασίας από κακόβουλο λογισμικό και ενημερώ νετε τακτικά το λειτουργικό τους.
Ελέγχετε ότι τα στοιχεία των ηλεκτρονικώ ν διευθύνσεων των e-mails που λαμβάνετε αντιστοιχούν στο όνομα του προσώ που που εμφανίζεται ως αποστολέας τους, ιδίως όταν α) το πρόσωπο αυτό ανήκει στη λίστα των επαφώ ν σας, β) φέρεται ότι είναι η Τράπεζα σας ή γ) άλλη γνωστή εταιρεία παροχής προϊόντων και υπηρεσιώ ν.
Αγνοείστε και διαγράψτε μηνύματα αμφίβολης προέλευσης που λαμβάνετε στις ηλεκτρονικές σας συσκευές και τις εφαρμογές σας και μην ακολουθείτε συνδέσμους (links) που περιλαμβάνουν και παραπέμπουν σε ιστοσελίδες.

Μην αποκαλύπτετε σε τρίτους (π.χ. ενδιαφερόμενους αγοραστές, υποψήφιους πελάτες), μέσω τηλεφώ νου, κινητού τηλεφώ νου, email, φόρμας στο Internet, μέσων κοινωνικής δικτύωσης και άλλων μέσων, εμπιστευτικά στοιχεία σας όπως το όνομα χρήστη (username), τον κωδικό πρόσβασης (password), τα στοιχεία της κάρτας σας (αριθμό, κωδικό επαλήθευσης CVV και PIN), OTP (One Time Password - κωδικούς μίας χρήσης) και άλλους αριθμητικούς κωδικούς.
Χρησιμοποιείτε πάντα τις πιο ενημερωμένες εκδόσεις Internet browsers (π.χ. Chrome, Microsoft Edge, κ.λπ), οι οποίες εξασφαλίζουν προηγμένο σχεδιασμό ασφαλείας.
Επικοινωνήστε αμέσως με την Τράπεζά σας, σε κάθε περίπτωση υπόνοιας διαρροής των κωδικώ ν ασφαλείας σας.
Ερώ τηση. Το τελευταίο διάστημα λαμβάνω συχνά τηλεφωνικές κλήσεις από άγνωστους αριθμούς, στη διάρκεια των οποίων υποτιθέμενος εκπρόσωπος επενδυτικής εταιρείας μου προτείνει επενδυτικές ευκαιρίες «στα μέτρα μου», με γρήγορη και εγγυημένη απόδοση. Αναρωτιέμαι αν πρέπει να του εμπιστευτώ τα χρήματά μου.
Απάντηση: Προσοχή υπάρχει σοβαρός κίνδυνος εξαπάτησής σας.
Μην εμπιστεύεστε όσους σας υπόσχονται ασφαλείς επενδύσεις με υψηλά, γρήγορα και εγγυημένα κέρδη.
Εάν επιθυμείτε να κάνετε μια επένδυση, βεβαιωθείτε πρώ τα ότι η εταιρία έχει άδεια λειτουργίας από την Επιτροπή Κεφαλαιαγοράς ή από άλλη ευρωπαϊκή Αρχή. Βεβαιωθείτε ότι, είτε καλύπτεται από το Ταμείο Εγγύησης Καταθέσεων και Επενδύσεων (ΤΕΚΕ), είτε συμμετέχει στο Συνεγγυητικό Κεφάλαιο ή άλλο ξένο Φορέα που διασφαλίζει την επένδυση σας. Επισκεφτείτε τα ακόλουθα sites: www.cmc.gov.gr www.ethe.org.gr www.smexa.gr https://www.syneggiitiko.gr/
Ερώ τηση: Σε περίπτωση που πέσω θύμα ηλεκτρονικής απάτης και το δηλώ σω στην Τράπεζα συνεργασίας μου, υπάρχει κάποιος άλλος φορέας στον οποίο μπορώ να απευθυνθώ άμεσα; Επίσης αν πέσω θύμα απάτης σχετικά με επενδύσεις υπάρχει φορέας στον οποίο μπορώ να απευθυνθώ ;
Απάντηση: Ναι, και στις δυο περιπτώ σεις θα πρέπει να καταγγείλετε το περιστατικό απάτης:
στο πλησιέστερο σε εσάς αστυνομικό τμήμα ή στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙΔΗΕ) της Ελληνικής Αστυνομίας
Τηλέφωνο : 11188
Fax: 213-1527471
Email: ccu@cybercrimeunit.gov.gr
μέσω του portal στη διεύθυνση: https://goo.gl/vOHdVb
Ταχυδρομική διεύθυνση: Λ. Αλεξάνδρας 173, Τ.Κ. 11522, Αθήνα
Ερώ τηση: Το τελευταίο διάστημα είδα στην τηλεόραση και άκουσα στο ραδιόφωνο για μια εκστρατεία ενημέρωσης και ευαισθητοποίησης του κοινού για τις ηλεκτρονικές απάτες με το σύνθημα «Μια Παύση Αρκεί για να Αποφύγουμε την Ηλεκτρονική Απάτη». Που μπορώ να ανατρέξω για να βρω περισσότερες πληροφορίες για τη συγκεκριμένη εκστρατεία;
Απάντηση: Μπορείτε να ανατρέξετε στην ιστοσελίδα της Ελληνικής Ένωσης Τραπεζώ ν (ΕΕΤ) (https://www.hba.gr/info/PhishingCamp) για να αντλήσετε περισσότερες πληροφορίες για τη συγκεκριμένη εκστρατεία, προϊόν συνεργασίας

μεταξύ του Υπουργείου Προστασίας του Πολίτη, της Τράπεζας της Ελλάδος, της Ελληνικής Αστυνομίας και της Ελληνικής Ένωσης Τραπεζών. Ξεκίνησε στο τέλος του 2021 και συνεχίζεται το 2022.

Ερώτηση: Που μπορώ να ανατρέξω για περισσότερες πληροφορίες σχετικά με τις διάφορες τυπολογίες ηλεκτρονικής απάτης και απάτης σχετικά με επενδύσεις που υφίστανται;

Απάντηση: Στην ιστοσελίδα της Ελληνικής Ένωσης Τραπεζών (ΕΕΤ) υπάρχει αναρτημένο όλο το υλικό των διαφόρων εκστρατειών ενημέρωσης και ευαισθητοποίησης του κοινού για τις ηλεκτρονικές απάτες, όπως:

εκείνης που αφορά τις απάτες στον «κυβερνοχώρο» (CyberScams), https://old.hba.gr/News/Details/1509 και

εκείνης που αφορά τους μεταφορείς παράνομου χρήματος (European Money Mule Action - EMMA). https://old.hba.gr/News/Details/36

Περαιτέρω, στην ιστοσελίδα της ΕΕΤ υπάρχουν χρήσιμες ανακοινώσεις επί διαφόρων τυπολογιών απάτης (π.χ. απάτη μέσω αλλαγής κάρτας SIM, απάτη «υποτιθέμενης τεχνικής υποστήριξης», τηλεφωνικές απάτες, κ.ά.) στο πλαίσιο της διαχρονικής ενημέρωσης και ευαισθητοποίησης του συναλλακτικού κοινού.

Περισσότερες συμβουλές για την αποφυγή εξαπάτησης πολιτών είναι διαθέσιμες σε ειδικό banner στην ιστοσελίδα της Ελληνικής Αστυνομίας (www.hellenicpolice.gr). Επιπλέον, πληροφορίες και συμβουλές για περιστατικά ηλεκτρονικών απατών υπάρχουν στην ιστοσελίδα της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος www.cyberalert.gr.

Πηγή: ΑΠΕ-ΜΠΕ