ΑΠΑΤΕΣ ΣΕ ΣΧΕΣΗ ΜΕ ΚΡΥΠΤΟΣΤΟΙΧΕΙΑ

ΠΑΡΑΜΕΙΝΕΤΕ ΣΕ ΕΓΡΗΓΟΡΣΗ ΚΑΙ ΠΡΟΣΤΑΤΕΨΤΕ ΤΟΝ ΕΑΥΤΟ ΣΑΣ

Η ραγδαία ανάπτυξη των κρυπτοστοιχείων και τα ιδιαίτερα χαρακτηριστικά τους —παγκόσμια προσβασιμότητα, ταχύτητα, ανωνυμία και συχνά η μη αναστρέψιμη φύση των συναλλαγών— σας καθιστούν ελκυστικό στόχο για τους κυβερνοεγκληματίες. Απατεώνες χρησιμοποιούν προηγμένες τακτικές για να σας εξαπατήσουν, όπως τα «σχέδια Ponzi», ψευδείς επενδυτικές ευκαιρίες, δωρεάν προσφορές στα μέσα κοινωνικής δικτύωσης και παραπλανητικά μηνύματα. Προβαίνουν επίσης σε απάτη μέσω διαδικτυακών γνωριμιών ή χρησιμοποιούν διευθύνσεις που μοιάζουν με τις πραγματικές για να "μολύνουν" το ψηφιακό πορτοφόλι κρυπτοστοιχείων σας. Οι απατεώνες συχνά προσεγγίζουν τα θύματα από τα μέσα κοινωνικής δικτύωσης, εφαρμογές ανταλλαγής μηνυμάτων, μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου και απροσδόκητων τηλεφωνικών κλήσεων που ακούγονται αληθινές. Οι κίνδυνοι μπορεί να είναι σοβαροί και να περιλαμβάνουν οικονομική απώλεια, κλοπή ταυτότητας και σημαντική ψυχολογική επιβάρυνση.

Να είστε προσεκτικοί και να ακολουθείτε αυτές τις βασικές συμβουλές για να παραμείνετε ασφαλείς:

Παραμείνετε σε εγρήγορση για πιθανές απάτες και τεχνάσματα σε σχέση με κρυπτοστοιχεία:
μάθετε περισσότερα σχετικά με τα διάφορα είδη απάτης (δείτε σελίδες 5-8).

Αναγνωρίστε προειδοποιητικά σημάδια:
Μάθετε να αναγνωρίζετε ύποπτες συμπεριφορές, μηνύματα ή προσφορές (δείτε σελίδα 2).

Προστατέψτε τον εαυτό σας και τα περιουσιακά σας στοιχεία:
Φροντίστε για την ασφάλεια των προσωπικών σας δεδομένων και των κρυπτοστοιχείων σας (δείτε σελίδα 3).

Μάθετε τί πρέπει να κάνετε εάν πέσετε θύμα απάτης: Ακολουθήστε τα ενδεδειγμένα βήματα
(δείτε σελίδα 4).

Προειδοποιητικά σημάδια απάτης

Μια υπόσχεση που φαίνεται πολύ καλή για να είναι αληθινή.

Μια ανεπιθύμητη ή απρόσμενη προσφορά.

Μια εγγυημένη γρήγορη και υψηλή απόδοση.

Πίεση για άμεση δράση (π.χ. προσφορά που ισχύει για περιορισμένο χρόνο και σας πιέζει να ενεργήσετε άμεσα).

Αίτημα πληρωμής με τρόπο που δεν επιτρέπει την ανίχνευση της συναλλαγής (π.χ. κρυπτοστοιχεία, δωροκάρτες, εμβάσματα ή προπληρωμένες χρεωστικές κάρτες).

Μια πρόσκληση για να κάνετε κλικ σε έναν σύνδεσμο, να σαρώσετε έναν κωδικό QR ή να κατεβάσετε μια εφαρμογή.

Ένα αίτημα για να αποστείλετε ή να μοιραστείτε ιδιωτικά κλειδιά και φράσεις ανάκτησης (seed phrase - λίστα λέξεων για πρόσβαση και ανάκτηση του πορτοφολιού κρυπτοστοιχείων σας).

Ύποπτη ή λανθασμένη διεύθυνση URL.

Λογότυπο με μικρές στρεβλώσεις, ιστότοπος που μιμείται την εμφάνιση του ιστότοπου μιας πραγματικής εταιρείας ή φαίνεται επαγγελματικός, αλλά δεν διαθέτει έγκυρα στοιχεία επικοινωνίας, στοιχεία από το μητρώο που είναι εγγεγραμμένη η εταιρεία, ιστορικό επιδόσεων ή επαληθεύσιμη παρουσία.

Άγνωστη πλατφόρμα διαπραγμάτευσης κρυπτοστοιχείων.

Ύποπτα συνημμένα αρχεία, ιδιαίτερα τύπου .exe, .scr, .zip ή αρχεία Office με δυνατότητα μακροεντολής (.docm, .xlsm).

Βήματα για να προστατεύσετε τον εαυτό σας:

1 **Σταματήστε και σκεφτείτε πριν ενεργήσετε:**

Μην βιαστείτε να επενδύσετε, να μοιραστείτε πληροφορίες ή να κάνετε κλικ σε συνδέσμους- οι απατεώνες δημιουργούν σκόπιμα την αίσθηση του επείγοντος. Αν έχετε την παραμικρή αμφιβολία, μην ενεργήσετε ή επενδύσετε πριν επαληθεύσετε προσεκτικά την πηγή.

2 **Ελέγξτε προσεκτικά την πηγή:**

- Πάντα να επαληθεύετε από πού προέρχονται τα μηνύματα, οι κλήσεις, τα μηνύματα ηλεκτρονικού ταχυδρομείου και οι σύνδεσμοι, ακόμη και αν φαίνονται επίσημα, φαίνονται να προέρχονται από έναν φίλο ή την οικογένειά σας ή ακόμα και από ένα δημόσιο πρόσωπο. Αναζητήστε ορθογραφικά λάθη, περίεργες διευθύνσεις URL ή ελλείποντες δείκτες ασφάλειας, π.χ. επαληθεύστε ότι ο σύνδεσμος ιστότοπου περιλαμβάνει ένα «s» στο «HTTPS» για να βεβαιωθείτε ότι ο ιστότοπος είναι ασφαλής και ελέγξτε για τυχόν πρόσθετα ή ελλείποντα γράμματα στην επωνυμία της εταιρείας.
- Μην ανοίγετε συνδέσμους από ανεπιθύμητα μηνύματα, να εγκαθιστάτε μόνο επίσημες εφαρμογές μέσω αξιόπιστων καταστημάτων εφαρμογών (app stores) και μην σαρώνετε άγνωστους κωδικούς QR.
- Ακόμη και αν μια προσφορά φαίνεται επίσημη και έγκυρη, διασταυρώστε την πάντα με τον επίσημο ιστότοπο της εταιρείας ή ελέγξτε αν ο λογαριασμός της στα μέσα κοινωνικής δικτύωσης είναι έγκυρος (π.χ. με επίσημα σημεία επαλήθευσης).
- Χρησιμοποιήστε μόνο επαληθευμένα στοιχεία επικοινωνίας για να επικοινωνήσετε απευθείας με την εταιρεία ή το άτομο και ποτέ μην βασίζεστε στα στοιχεία επικοινωνίας που παρέχονται από τον ύποπτο απατεώνα (π.χ. αναζητήστε την επωνυμία της εταιρείας ανεξάρτητα όπως μέσω επαληθευμένων καταλόγων επιχειρήσεων). Οι απατεώνες μπορεί να ισχυριστούν ότι είναι εξουσιοδοτημένοι ή να μιμούνται τον ιστότοπο μιας πραγματικής εταιρείας για να σας εξαπατήσουν. Μπορείτε να επαληθεύσετε αν ο πάροχος κρυπτοστοιχείων είναι αδειοδοτημένος στην ΕΕ ελέγχοντας το μητρώο της ESMA (↖). Μπορείτε επίσης να συμβουλευτείτε τον ιστότοπο της εθνικής αρμόδιας αρχής της χώρας σας- για την Κύπρο: Επιτροπή Κεφαλαιαγοράς Κύπρου (↖) και Κεντρική Τράπεζα της Κύπρου ([1])- για να δείτε αν έχουν εκδοθεί προειδοποιήσεις ή μαύρες λίστες ή να ελέγξετε τον κατάλογο IOSCO I-SCAN (iosco.org/i-scan/).

3 **Ποτέ μην μοιράζεστε κωδικούς πρόσβασης, ιδιωτικά κλειδιά ή φράσεις ανάκτησης:**

Οποιοσδήποτε έχει πρόσβαση σε αυτά μπορεί να πάρει τον έλεγχο των περιουσιακών σας στοιχείων. Οι νόμιμες εταιρείες δεν θα ζητήσουν ποτέ τους κωδικούς πρόσβασης ή τους κωδικούς ασφαλείας σας μέσω ηλεκτρονικού ταχυδρομείου, γραπτού μηνύματος (text) ή τηλεφώνου.

4 **Διατηρείτε τις συσκευές και τα ιδιωτικά κλειδιά ασφαλή:**

Χρησιμοποιήστε ισχυρούς και μοναδικούς κωδικούς πρόσβασης για κάθε έναν από τους λογαριασμούς κρυπτοστοιχείων σας, διατηρήστε τον κωδικό πρόσβασής σας μυστικό και αποφύγετε την επαναχρησιμοποίηση των ίδιων διαπιστευτηρίων (username / password) σε διαφορετικές πλατφόρμες. Ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA), όπου είναι δυνατόν. Βλ. ορισμένες συμβουλές για κωδικούς πρόσβασης εδώ (shorturl.at/7ns3I). Διατηρήστε το λογισμικό σας και το σύστημα για προστασία από ιούς (anti virus/malware protection) επικαιροποιημένα και ενεργοποιημένα.

5 **Να είστε προσεκτικοί με απροσδόκητες επενδυτικές προσφορές:**

Να είστε επιφυλακτικοί και καχύποπτοι με τις επενδύσεις που υπόσχονται τεράστιες αποδόσεις. Αν ακούγεται πολύ καλό για να είναι αληθινό, μάλλον δεν είναι.

6 **Σκεφτείτε πριν αποκαλύψετε πληροφορίες στα μέσα κοινωνικής δικτύωσης:**

Οι ομάδες συνομιλίας, τα φόρουμ, οι αναρτήσεις στα μέσα κοινωνικής δικτύωσης και οι φωτογραφίες μπορούν να αποτελέσουν πολύτιμες πηγές πληροφοριών για τους απατεώνες. Αποκαλύπτοντας πάρα πολλά για τον εαυτό σας ή τις επενδύσεις σας μπορεί να σας κάνει έναν εύκολο και ελκυστικό στόχο.

([1]) Μέχρι την έκδοση του παρόντος δελτίου, δεν υπάρχουν αδειοδοτημένοι πάροχοι από την Κεντρική Τράπεζα της Κύπρου.

Τί να κάνετε όταν έχετε πέσει θύμα απάτης

Διακόψτε αμέσως τις συναλλαγές

για να αποτρέψετε περαιτέρω μεταφορές χρημάτων/ κρυπτοστοιχείων σε ύποπτους λογαριασμούς και να αποφύγετε πρόσθετες απώλειες. Τερματίστε κάθε επαφή με τους απατεώνες — αγνοήστε τις κλήσεις και τα μηνύματα ηλεκτρονικού ταχυδρομείου τους και αποκλείστε τον αποστολέα.

Αλλάξτε τους κωδικούς πρόσβασής σας σε όλες τις συσκευές και τις εφαρμογές/ ιστοσελίδες σας

οι απατεώνες συχνά αγοράζουν κωδικούς πρόσβασης που έχουν διαρρεύσει στο διαδίκτυο και τους δοκιμάζουν σε πολλαπλούς λογαριασμούς. Η αλλαγή μόνο ενός κωδικού πρόσβασης δεν αρκεί. Φροντίστε να αλλάξετε όλους τους κωδικούς πρόσβασης σας, ώστε οι απατεώνες να μην μπορούν να τους επαναχρησιμοποιήσουν.

Αποσύνδεση και ανάκληση της πρόσβασης

ανακαλέστε ύποπτα δικαιώματα στην ψηφιακή σας συμφωνία που εκτελούνται αυτόματα στο blockchain (έξυπνο συμβόλαιο ή smart contract) για να σταματήσετε τους απατεώνες να ξοδεύουν τις μάρκες (tokens) σας χωρίς τη συγκατάθεσή σας. Πολλά πορτοφόλια και εξερευνητές blockchain (blockchain explorers) προσφέρουν εργαλεία που σας επιτρέπουν να δείτε ποια έξυπνα συμβόλαια έχουν επί του παρόντος πρόσβαση για να ξοδέψουν τα token σας. Για να το κάνετε αυτό μπορείτε:

- να χρησιμοποιήσετε ένα αξιόπιστο «ελεγκτή εγκρίσεων» («permission checker»), ο οποίος επαληθεύει αν ένας χρήστης ή μια διεύθυνση blockchain είναι εξουσιοδοτημένος/-η να εκτελεί μια πράξη.
- να επανεξετάσετε τον κατάλογο των εγκρίσεων, και
- να χρησιμοποιήσετε το κουμπί «ανάκληση» («revoke») απευθείας από την πλατφόρμα.

Μετακινήστε τα κεφάλαιά σας

εάν το πορτοφόλι κρυπτοστοιχείων σας έχει παραβιαστεί, μεταφέρετε αμέσως τα υπόλοιπα περιουσιακά σας στοιχεία σε ένα νέο ασφαλές πορτοφόλι.

Επικοινωνήστε με τον πάροχο υπηρεσιών κρυπτοστοιχείων

ενημερώστε τον πάροχο υπηρεσιών κρυπτοστοιχείων το συντομότερο δυνατό χρησιμοποιώντας τα επίσημα κανάλια επικοινωνίας, για να διερευνήσετε πιθανές ενέργειες. Ακόμη και αν, στις περισσότερες περιπτώσεις, δεν είναι δυνατή η αντιστροφή της συναλλαγής blockchain, ο πάροχος ενδέχεται να παγώσει τον λογαριασμό του απατεώνα (εάν βρίσκεται στην πλατφόρμα του) και να συμπεριλάβει τη διεύθυνση του πορτοφολιού σε μαύρη λίστα.

Αναφορά και προειδοποίηση

αναφέρετε το περιστατικό στην αστυνομία ή στην εθνική αρμόδια αρχή της χώρας σας και ενημερώστε το οικείο περιβάλλον σας (π.χ. φίλους και οικογένεια) για ενίσχυση της ενημέρωσης τους σχετικά με τις απάτες. Αυτές οι ενέργειες είναι ο καλύτερος τρόπος για να προστατεύσετε τον εαυτό σας και τους γύρω σας.

Προσοχή στην απάτη «ανάκτησης χρημάτων / απωλειών» (recovery room fraud)

οι απατεώνες μπορεί να επικοινωνήσουν μαζί σας γνωρίζοντας ότι είστε θύμα προηγούμενης απάτης, ισχυριζόμενοι ότι επικοινωνούν εκ μέρους κάποιας δημόσιας αρχής (π.χ. αστυνομία, φορολογική ή χρηματοοικονομική αρχή κ.λπ.) και να προσφερθούν να σας βοηθήσουν να ανακτήσετε τα απολεσθέντα χρήματά σας, έναντι αμοιβής. Αυτό είναι συχνά μια άλλη προσπάθεια να σας εξαπατήσουν. Θυμηθείτε: το να σας εξαπατήσουν μία φορά δεν αποκλείει να εξαπατηθείτε ξανά.

Δείτε την κοινή προειδοποίηση των τριών Ευρωπαϊκών Εποπτικών Αρχών για να μάθετε περισσότερα σχετικά με τους κινδύνους που σχετίζονται με τα κρυπτοστοιχεία (↖) και το ενημερωτικό δελτίο «Κρυπτοστοιχεια: Τι Σημαινει Το Mica Για Εσας Ως Καταναλωτης» (↖).

Ευρωπαϊκή Αρχή Τραπεζών, Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων, Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών, 2025

Λουξεμβούργο: Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης, 2025

PDF ISBN 978-92-9407-265-8 doi:10.2853/0100408 DZ-01-25-153-EL-N

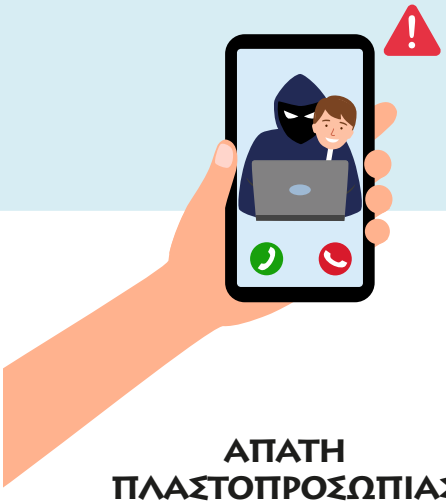
ΕΙΔΗ ΑΠΑΤΗΣ ΜΕ ΧΡΗΣΗ ΚΡΥΠΤΟΣΤΟΙΧΕΙΩΝ

ΜΕΘΟΔΟΙ «ΤΕΧΝΗΤΗΣ ΔΙΟΓΚΩΣΗΣ (PUMP AND DUMP SCHEMES)» Η «ΑΙΦΝΙΔΙΑΣ ΑΠΟΣΥΡΣΗΣ ΡΕΥΣΤΟΤΗΤΑΣ (RUG PULL)»

Βλέπετε μια διαφήμιση (ad) στα μέσα κοινωνικής δικτύωσης ή έναν ιστότοπο που προωθεί μια «επενδυτική ευκαιρία περιορισμένου χρόνου» σε κρυπτοστοιχεία, συστήνοντας την επένδυση σε μια νέα ψηφιακή μάρκα (token) ή σχετικό έργο (project). Αφού εκδηλώσετε ενδιαφέρον, επικοινωνούν μαζί σας και ανακατευθύνεστε σε μια πλατφόρμα διαπραγμάτευσης κρυπτοστοιχείων ή σε ένα κανάλι ανταλλαγής μηνυμάτων (π.χ. Telegram, Viber ή WhatsApp). Μια φαινομενικά αξιόπιστη επαφή υπόσχεται γρήγορα κέρδη ή υψηλές αποδόσεις εάν επενδύσετε γρήγορα. Σας ενθαρρύνουν να επενδύσετε ένα μικρό ποσό και στη συνέχεια σας πιέζουν να επενδύσετε περισσότερο.

Τί μπορεί να συμβεί:

Συνειδητοποιείτε ότι η ψηφιακή μάρκα στην οποία υποτίθεται ότι επενδύσατε δεν έχει καμία αξία και η επαφή με την οποία επικοινωνήσατε σταματά να ανταποκρίνεται. Όταν προσπαθήσετε να αποσύρετε τα χρήματά σας, ο ιστότοπος έχει εξαφανιστεί και η εταιρεία δεν είναι πλέον προσβάσιμη. Οι απατεώνες διογκώνουν τεχνητά ή υπερεκτιμούν ένα κρυπτοστοιχείο χαμηλής αξίας για να αυξήσουν την αξία του («pump»), στη συνέχεια πωλούν τις δικές τους μάρκες («dump»), προκαλώντας κατάρρευση της αξίας και αφήνοντας τους επενδυτές με ζημιές. Εναλλακτικά, θα μπορούσαν να διακόψουν το έργο και να εξαφανιστούν με τα κεφάλαια («rug pull»).



ΑΠΑΤΗ ΠΛΑΣΤΟΠΡΟΣΩΠΙΑΣ (IMPERSONATION SCAM)

Αφού δημοσιεύσετε μια ερώτηση σε μια πλατφόρμα μέσων κοινωνικής δικτύωσης ή σε έναν ιστότοπο σχετικά με ένα ζήτημα που αφορά το πορτοφόλι σας, λαμβάνετε ένα απροσδόκητο απ' ευθείας μήνυμα (DM) ή ένα μήνυμα ηλεκτρονικού ταχυδρομείου από κάποιον που προσποιείται ότι είναι αξιόπιστη επαφή (π.χ. πλατφόρμα διαπραγμάτευσης κρυπτοστοιχείων, πάροχος πορτοφολιού, τεχνική υποστήριξη ή ακόμη και φίλος). Το άτομο ζητά τη φράση ανάκτησης (seed phrase), (δηλ. ακολουθία λέξεων που χρησιμεύει ως κεντρικό εφεδρικό αντίγραφο για την πρόσβαση στο ψηφιακό πορτοφόλι σας), κωδικούς πρόσβασης ή ιδιωτικά κλειδιά (αυτόματος κρυπτογραφικός κώδικας που αποδεικνύει την κυριότητα ψηφιακών περιουσιακών στοιχείων και εξασφαλίζει πλήρη πρόσβαση στο πορτοφόλι και στα ψηφιακά σας περιουσιακά στοιχεία).

Τί μπορεί να συμβεί:

Μόλις μοιραστείτε τη φράση ανάκτησης, τους κωδικούς πρόσβασης ή τα ιδιωτικά κλειδιά σας, ο απατεώνας αποκτά πρόσβαση και τα χρησιμοποιεί για να κλέψει τα κρυπτοστοιχεία ή τα χρήματά σας. Λάβετε υπόψη ότι η απώλεια ιδιωτικών κλειδιών έχει ως αποτέλεσμα τη μόνιμη και μη αναστρέψιμη απώλεια πρόσβασης και ιδιοκτησίας στα κρυπτοστοιχεία σας. Σε αντίθεση με τις τραπεζικές συναλλαγές, οι μεταφορές κρυπτοστοιχείων δεν μπορούν να αναιρεθούν. Η ανάκτηση κεφαλαίων μετά τη μεταφορά τους είναι σχεδόν αδύνατη.

ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ (PHISHING)

Λαμβάνετε ένα απροσδόκητο μήνυμα μέσω ηλεκτρονικού ταχυδρομείου, τηλεφώνου, pop-up μηνύματος ή μέσων κοινωνικής δικτύωσης, το οποίο υποτίθεται ότι προέρχεται από γνωστό πάροχο υπηρεσιών κρυπτοστοιχείων. Το μήνυμα σας προτρέπει να συνδεθείτε σε ένα σύνδεσμο ή να κατεβάσετε μια νέα εφαρμογή. Ενδέχεται επίσης να λάβετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχεται από την εφαρμογή πορτοφολιού κρυπτοστοιχείων σας, προτρέποντάς σας να επιλύσετε ένα ζήτημα ασφάλειας κάνοντας κλικ σε έναν σύνδεσμο που παρέχεται από ανεπίσημη πηγή ή ενημερώνοντας την εφαρμογή (app).

Τί μπορεί να συμβεί:

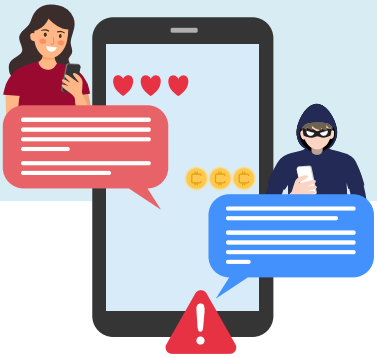
Κάνοντας κλικ στον σύνδεσμο, κατεβάζοντας το επισυναπτόμενο αρχείο ή την εφαρμογή ή σαρώνοντας έναν κωδικό QR, εγκαθιστάτε ένα κακόβουλο λογισμικό που επιτρέπει στον απατεώνα να αποκτήσει πρόσβαση στα δεδομένα σας και να κλέψει τα κρυπτοστοιχεία σας ή τα χρήματά σας.

ΑΠΑΤΗ ΜΕΣΩ «ΠΡΟΣΦΟΡΑΣ ΔΩΡΩΝ» (GIVEAWAY FRAUD)

Συναντάτε μια ανακοίνωση στα μέσα κοινωνικής δικτύωσης που ισχυρίζεται ότι εταιρείες δωρίζουν κρυπτοστοιχεία μετά από μια μικρή επένδυση σε κρυπτονομίσματα. Συνοδεύεται από ένα βίντεο ή μια ανάρτηση με φωτογραφίες διασημοτήτων ή ενός εμπορικού σήματος —συνήθως πλαστά ή αποκτηθέντα χωρίς άδεια— που υπόσχεται να «διπλασιάσει τα κρυπτοστοιχεία σας» εάν στείλετε πρώτα χρήματα. Το λογότυπο, η εμφάνιση, οι μαρτυρίες και η γλώσσα που χρησιμοποιείται φαίνονται επαγγελματικά και έγκυρα, όπως και η ιστοσελίδα στην οποία ανακατευθύνεστε.

Τί μπορεί να συμβεί:

Μετά την αποστολή των κρυπτοστοιχείων σας, δεν λαμβάνετε τίποτα σε αντάλλαγμα και έχετε χάσει τα χρήματα που αποστείλατε. Η «προσφορά δώρων» ήταν ψεύτικη και η ανάρτηση ή η ζωντανή μετάδοση που εμφανίζει διασημότητες ή εταιρείες, δημιουργήθηκε αποκλειστικά για να σας εξαπατήσει.



ΑΠΑΤΗ ΜΕΣΩ ΔΙΑΔΙΚΤΥΑΚΩΝ ΓΝΩΡΙΜΙΩΝ (ROMANCE INVESTMENT SCAM)

Έχει έρθει σε επαφή μαζί σας, χρησιμοποιώντας τα μέσα κοινωνικής δικτύωσης, εφαρμογές γνωριμιών ή τηλεφωνικά/γραπτά μηνύματα, κάποιο άτομο που δεν έχετε συναντήσει στην πραγματική ζωή. Αυτό το άτομο μπορεί να συμμετέχει σε συχνές, προσωπικές και ρομαντικές συνομιλίες, χτίζοντας εμπιστοσύνη και χρησιμοποιώντας ψεύτικα προφίλ. Σταδιακά, μετατοπίζει τη συζήτηση προς επενδυτικές ευκαιρίες, ισχυριζόμενο τεράστια κέρδη από επενδύσεις σε κρυπτοστοιχεία και ενθαρρύνοντάς σας να επενδύσετε υποσχόμενο υψηλές αποδόσεις και χαμηλό κίνδυνο. Σας καθοδηγεί να δημιουργήσετε έναν λογαριασμό και να καταθέσετε ένα μικρό αρχικό ποσό, ώστε να φαίνεται ότι το σύστημα λειτουργεί νόμιμα.

Οι απατεώνες συνήθως δημιουργούν ψεύτικα διαδικτυακά προφίλ και χρησιμοποιούν κλεμμένες ή δημιουργημένες από Τεχνητή Νοημοσύνη (ΤΝ) εικόνες, για να σας προσεγγίσουν.

Τί μπορεί να συμβεί:

Ο απατεώνας αποσπά όσο το δυνατόν περισσότερα χρήματα, στη συνέχεια διακόπτει κάθε επικοινωνία και εξαφανίζεται. Η κακόβουλη επενδυτική ιστοσελίδα ή εφαρμογή αποσυνδέεται/τίθεται εκτός λειτουργίας, αφήνοντάς σας χωρίς πρόσβαση στις υποτιθέμενες επενδύσεις. Σε ορισμένες περιπτώσεις, οι απατεώνες μπορούν να χρησιμοποιήσουν τις πληροφορίες που αποκτήθηκαν κατά τη διάρκεια της απάτης για να στοχεύσουν τους φίλους και την οικογένειά σας και να διαπράξουν κλοπή ταυτότητας που μπορεί να έχει οικονομικές ή νομικές συνέπειες για εσάς (π.χ. ο απατεώνας μπορεί να επαληθεύσει κλεμμένα πορτοφόλια στο όνομά σας και μπορεί να θεωρηθείτε υπεύθυνος για χρέη ή εγκλήματα που διαπράχθηκαν με το όνομά σας έως ότου αποδειχθεί το αντίθετο).

ΣΧΕΔΙΑ PONZI

Προσκαλείστε να συμμετάσχετε σε ένα επενδυτικό πρόγραμμα που υπόσχεται σταθερά υψηλές αποδόσεις από επενδύσεις σε κρυπτοστοιχεία, οι οποίες συχνά συνοδεύονται από ψεύτικες μαρτυρίες ή ιστορίες ‘επιτυχημένων επενδυτών’. Το πρόγραμμα μπορεί να παρουσιαστεί ως μια ευκαιρία μάρκετινγκ πολλαπλών επιπέδων, όπου κερδίζετε όχι μόνο από τη δική σας επένδυση, αλλά και από την ένταξη νέων συμμετεχόντων. Οι πρώτοι επενδυτές φαίνεται να λαμβάνουν πραγματικές πληρωμές, γεγονός που ενθαρρύνει περισσότερους ανθρώπους να ενταχθούν και να προωθήσουν το πρόγραμμα.

Στην πραγματικότητα, δεν υπάρχει καμία πραγματική επιχείρηση ή κέρδος που παράγεται. Αντ’ αυτού, τα χρήματα προέρχονται αποκλειστικά από τη συνεισφορά νεότερων επενδυτών, η οποία χρησιμοποιείται για την καταβολή αποδόσεων στους διοργανωτές και τους πρώτους συμμετέχοντες του προγράμματος.

Τί μπορεί να συμβεί:

Μόλις οι νέες επενδύσεις επιβραδυνθούν, το πρόγραμμα καταρρέει και εσείς, όπως και οι περισσότεροι συμμετέχοντες, χάνετε τα χρήματά σας. Οι διοργανωτές εξαφανίζονται, χωρίς δυνατότητα ανάκτησης των κεφαλαίων. Η πολυεπίπεδη δομή επιτρέπει στην απάτη να εξαπλωθεί γρήγορα, καθώς τα θύματα γίνονται εν αγνοία τους υποστηρικτές της.

ΜΙΑ ΠΑΡΟΜΟΙΑ ΔΙΕΥΘΥΝΣΗ ΠΟΥ «ΜΟΛΥΝΕΙ» ΤΟ ΠΟΡΤΟΦΟΛΙ ΣΑΣ

Μετά από μια συναλλαγή κρυπτοστοιχείων, παρατηρείτε μια νέα, άγνωστη διεύθυνση που εμφανίζεται στο ιστορικό του πορτοφολιού σας. Αυτή η διεύθυνση μοιάζει πολύ με αυτή με την οποία είχατε αλληλεπιδράσει στο παρελθόν. Οι απατεώνες μπορούν να κάνουν ψεύτικες διευθύνσεις πορτοφολιού να εμφανιστούν στο ιστορικό συναλλαγών σας στέλνοντας μια μικρή ποσότητα κρυπτοστοιχείων από μια παρόμοια διεύθυνση στο πορτοφόλι σας. Καταλήγετε να αποθηκεύετε στην πρόσφατη δραστηριότητα ή στις αυτόματες προτάσεις του πορτοφολιού σας την ψεύτικη διεύθυνση που δημιουργήθηκε από τον απατεώνα. Οι απατεώνες δημιουργούν σκόπιμα παρόμοιες διευθύνσεις αλλάζοντας μόνο λίγους χαρακτήρες, συχνά στη μέση της διεύθυνσης, ώστε η διαφοροποίηση να είναι δύσκολο να εντοπιστεί.

Τί μπορεί να συμβεί:

Την επόμενη φορά που θα στείλετε κρυπτοστοιχεία και θα επιλέξετε ή θα αντιγράψετε μια διεύθυνση από το ιστορικό του πορτοφολιού σας, μπορεί άθελά σας να χρησιμοποιήσετε τη διεύθυνση του απατεώνα, στέλνοντας εν αγνοία σας κεφάλαια στο πορτοφόλι του. Επειδή οι συναλλαγές κρυπτοστοιχείων είναι συχνά μη αναστρέψιμες, τα κεφάλαιά σας χάνονται στις περισσότερες περιπτώσεις, μόνιμα. Αυτή η απάτη βασίζεται σε οπτική εξαπάτηση και σφάλμα εκ μέρους του χρήστη, εκμεταλλευόμενη τη συνήθεια της αντιγραφής και επικόλλησης διευθύνσεων πορτοφολιού χωρίς στενή επιθεώρηση.