ΑΠΑΤΕΣ ΣΕ ΚΡΥΠΤΟΣΤΟΙΧΕΙΑ

ΜΕΙΝΕΤΕ ΣΕ ΕΓΡΗΓΟΡΣΗ ΚΑΙ ΠΡΟΣΤΑΤΕΨΤΕ ΤΟΝ ΕΑΥΤΟ ΣΑΣ

Η ταχεία ανάπτυξη των κρυπτοστοιχείων και τα ειδικά χαρακτηριστικά τους- παγκόσμια προσβασιμότητα, ταχύτητα, ανωνυμία και συχνά μη αναστρεψιμότητα των συναλλαγών- σας καθιστούν πρωταρχικό στόχο για τους κυβερνοαπατεώνες. Οι απατεώνες χρησιμοποιούν εξελιγμένες τακτικές για να σας εξαπατήσουν, όπως «σχήματα Ponzi», ψευδείς επενδυτικές ευκαιρίες, δήθεν δωρεάν προσφορές στα μέσα κοινωνικής δικτύωσης και λοιπά ψευδή μηνύματα. Προβαίνουν επίσης σε απάτη μέσω διαδικτυακών γνωριμιών ή παρεμβάλλουν στο πορτοφόλι σας κακόβουλες διευθύνσεις που μοιάζουν με τις πραγματικές. Συχνά σας προσεγγίζουν από τα μέσα κοινωνικής δικτύωσης, με εφαρμογές ανταλλαγής μηνυμάτων, μηνύματα ηλεκτρονικού ταχυδρομείου και απροσδόκητες κλήσεις που φαίνονται πραγματικά. Μπορεί να αντιμετωπίσετε κινδύνους όπως οικονομική ζημία, κλοπή ταυτότητας και συναισθηματική δυσφορία.

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

Παραμείνετε σε εγρήγορση για πιθανές απάτες σε κρυπτοστοιχεία:
μάθετε περισσότερα σχετικά με τα διάφορα είδη απάτης (δείτε σελίδες 5, 6, 7 και 8)

Εντοπίστε 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 στοιχείων (δείτε σελίδα 3)

Μάθετε τι πρέπει να κάνετε εάν πέσετε θύμα απάτης
(δείτε σελίδα 4)

Προειδοποιητικά σημάδια

Μια υπόσχεση που φαίνεται πολύ καλή για να είναι αληθινή.

Ανεπιθύμητη προσφορά.

Εγγυημένη γρήγορη και υψηλή απόδοση.

Επείγουσα ανάγκη για ενέργεια (π.χ. προσφορά που ισχύει για περιορισμένο χρόνο και σας καλεί να ενεργήσετε άμεσα).

Σας ζητήθηκε να πληρώσετε με τρόπο που δεν επιτρέπει την ανίχνευση της πληρωμής (π.χ. κρυπτονομίσματα, 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.

Σας ζητήθηκε να στείλετε ή να μοιραστείτε ιδιωτικά κλειδιά και φράσεις ανάκτησης (seed phrase) (σύνολο λέξεων για πρόσβαση και ανάκτηση του πορτοφολιού κρυπτοστοιχείων).

Ύποπτη ή λανθασμένη διεύθυνση URL.

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

Άγνωστη πλατφόρμα ανταλλαγής κρυπτοστοιχείων.

Ύποπτο συνημμένο, ειδικά σε μορφή .exe, .scr, .zip ή αρχείο Office με δυνατότητα εκτέλεσης μακροεντολών (.docm, .xlsm).

Βήματα για να προστατεύσετε τον εαυτό σας:

1 **Σταματήστε και σκεφτείτε πριν ενεργήσετε:**

Μην βιαστείτε να επενδύσετε, να ανταλλάξετε πληροφορίες ή να κάνετε κλικ σε συνδέσμους- οι απατεώνες δημιουργούν σκόπιμα την αίσθηση του επείγοντος. Σε περίπτωση αμφιβολιών, ακόμη και ήσσονος σημασίας, μην ενεργήσετε ή μην 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, αν φαίνεται να προέρχονται από έναν φίλο ή την οικογένειά σας ή ακόμα και από ένα δημόσιο πρόσωπο. Αναζητήστε ορθογραφικά λάθη, ύποπτες 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 αξιόπιστες εφαρμογές μέσω επίσημων app stores και να μην «σαρώνετε» άγνωστους κωδικούς QR.
- Ακόμη και αν μια προσφορά φαίνεται αξιόπιστη, διασταυρώστε την πάντα με τον ιστότοπο της εταιρείας ή ελέγξτε αν έχει επαληθευτεί ο λογαριασμός στα μέσα κοινωνικής δικτύωσης (π.χ. με επίσημα σημεία ελέγχου).
- Να χρησιμοποιείτε επαληθευμένα στοιχεία επικοινωνίας για να επικοινωνήσετε απευθείας με μια εταιρεία ή ένα φυσικό πρόσωπο και ποτέ να μην βασίζεστε στα στοιχεία επικοινωνίας που προέρχονται από τον ύποπτο απατεώνα (π.χ. επιβεβαιώστε την επωνυμία της εταιρείας ανεξάρτητα, μόνοι σας, ανατρέξτε σε επίσημα μητρώα/καταλόγους επιχειρήσεων). Οι απατεώνες μπορεί να ισχυριστούν ότι είναι αδειοδοτημένοι ή να μιμούνται τον ιστότοπο μιας αδειοδοτημένης εταιρείας. Μπορείτε να επαληθεύσετε αν ο πάροχος κρυπτοστοιχείων είναι αδειοδοτημένος στην ΕΕ ελέγχοντας το μητρώο της ESMA (). Μπορείτε επίσης να συμβουλευτείτε τον δικτυακό τόπο των εθνικών αρμόδιων αρχών της χώρας σας (Επιτροπή Κεφαλαιαγοράς Κατάλογος παρόχων υπηρεσιών κρυπτοστοιχείων στην Ελλάδα (http://www.hcmc.gr/el_GR/web/portal/agores-kryptostoicheion#), Τράπεζα της Ελλάδος ()) για να δείτε αν έχουν εκδοθεί προειδοποιήσεις ή η εταιρεία περιλαμβάνεται σε μαύρες λίστες ή να ανατρέξετε στον κατάλογο IOSCO I-SCAN (iosco.org/i-scan/).

3 **Ποτέ μην δίνετε πληροφορίες για κωδικούς πρόσβασης, ιδιωτικά κλειδιά ή φράσεις ανάκτησης (seed phrases):**

Οποιοσδήποτε έχει πρόσβαση σε αυτά μπορεί να αποκτήσει τον έλεγχο των περιουσιακών σας στοιχείων. Οι νόμιμες εταιρείες δεν θα ζητήσουν ποτέ τους κωδικούς πρόσβασης ή τους κωδικούς ασφαλείας σας μέσω ηλεκτρονικού ταχυδρομείου, μηνυμάτων ή τηλεφώνου.

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

Να χρησιμοποιείτε ισχυρούς και μοναδικούς κωδικούς πρόσβασης για κάθε έναν από τους λογαριασμούς κρυπτοστοιχείων, να τηρείτε τον κωδικό πρόσβασής σας μυστικό και να αποφεύγετε την επαναχρησιμοποίηση των ίδιων διαπιστευτηρίων σε διαφορετικές πλατφόρμες. Ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων, όπου είναι δυνατόν. Βλ. συμβουλές για κωδικούς πρόσβασης εδώ (). Εξασφαλίστε ότι οι εφαρμογές που χρησιμοποιείτε είναι επικαιροποιημένες και το λογισμικό προστασίας από ιούς είναι ενεργοποιημένο και επικαιροποιημένο.

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

Να είστε επιφυλακτικοί με τις επενδύσεις που υπόσχονται υπέρμετρες αποδόσεις. Αν ακούγεται πολύ καλό για να είναι αληθινό, μάλλον έτσι είναι.

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

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

Τι να κάνετε όταν έχετε πέσει θύμα απάτης

Σταματήστε αμέσως τις συναλλαγές

Για να αποτρέψετε τυχόν περαιτέρω μεταφορές χρηματικών ποσών σε ύποπτους λογαριασμούς και να αποφύγετε πρόσθετες απώλειες. Σταματήστε 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 προμηθεύονται κωδικούς πρόσβασης που έχουν διαρρεύσει στο διαδίκτυο και τους δοκιμάζουν σε διάφορους λογαριασμούς. Η αλλαγή μόνο ενός κωδικού πρόσβασης δεν αρκεί. Φροντίστε να τους αλλάξετε όλους, ώστε οι απατεώνες να μην μπορούν να τους επαναχρησιμοποιήσουν.

Αποσύνδεση και αποκλεισμός της πρόσβασης:

Ανακαλέστε ύποπτα δικαιώματα στις ψηφιακές σας συμφωνίες 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 προσφέρουν εργαλεία που σας επιτρέπουν να δείτε ποια έξυπνα συμβόλαια έχουν επί του παρόντος πρόσβαση για να ξοδέψουν τα tokens σας. Για να το κάνετε αυτό μπορείτε:

- Να χρησιμοποιήσετε έναν αξιόπιστο «ελεγκτή εγκρίσεων», ο οποίος επαληθεύει αν ένας χρήστης ή μια διεύθυνση blockchain έχει εξουσιοδοτηθεί να εκτελεί μια λειτουργία.
- να επανεξετάσετε τον κατάλογο των εγκρίσεων, και
- να χρησιμοποιήσετε το κουμπί «ανάκληση» απευθείας μέσα από την πλατφόρμα.

Μετακινήστε τα κεφάλαιά σας:

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

Επικοινωνήστε με τον πάροχο υπηρεσιών κρυπτοστοιχείων σας:

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

Αναφορά και προειδοποίηση:

Αναφέρετε το περιστατικό στην αστυνομία ή στην εθνική αρμόδια αρχή της χώρας σας (Επιτροπή Κεφαλαιαγοράς (http://www.hcmc.gr/el_GR/web/portal/katagellies), Τράπεζα της Ελλάδος (↖) και ενημερώστε το περιβάλλον σας (π.χ. φίλους και οικογένεια) για την αύξηση της ευαισθητοποίησης. Αυτές οι ενέργειες είναι ο καλύτερος τρόπος για να προστατεύσετε τον εαυτό σας και τους άλλους.

Προσοχή στην απάτη υποτιθέμενης ανάκτησης χρημάτων ('recovery room' fraud):

Ο απατεώνας μπορεί να επικοινωνήσει μαζί σας γνωρίζοντας ότι είστε θύμα προηγούμενης απάτης, ισχυριζόμενος ότι επικοινωνεί εκ μέρους κάποιας δημόσιας αρχής (π.χ. αστυνομία, φορολογική ή οικονομική αρχή κ.λπ.) προσφερόμενος να σας βοηθήσει να ανακτήσετε τα απολεσθέντα χρήματά σας έναντι αμοιβής. Αυτό είναι συχνά μια άλλη προσπάθεια εξαπάτησης. Θυμηθείτε: το να σας εξαπατήσουν μία φορά δεν αποκλείει να εξαπατηθείτε ξανά.

Βλ. την προειδοποίηση της Κοινής Επιτροπής (Joint Committee) των τριών Ευρωπαϊκών Εποπτικών Αρχών για να μάθετε περισσότερα σχετικά με τους κινδύνους που σχετίζονται με τα κρυπτοστοιχεία (↖) και το ενημερωτικό δελτίο «Crypto-assets explained: What MiCA means for you as a consumer» (*Κατανοωντας Τα Κρυπτοστοιχεια: Τι Σημαινει Ο Κανονισμος Για Τις Αγορες Κρυπτοστοιχειων (Mica) Για Εσας Ως Καταναλωτη* (↖).

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 ΑΠΑΤΩΝ ΜΕ ΧΡΗΣΗ ΚΡΥΠΤΟΣΤΟΙΧΕΙΩΝ

ΜΈΘΟΔΟΙ «ΤΕΧΝΗΤΉΣ ΔΙΌΓΚΩΣΗΣ (PUMP AND DUMP SCHEMES)» Ή «ΑΙΦΝΊΔΙΑΣ ΑΠΌΣΥΡΣΗΣ ΡΕΥΣΤΌΤΗΤΑΣ (RUG PULL)»

Βλέπετε μια διαφήμιση (ad) στα μέσα κοινωνικής δικτύωσης ή έναν ιστότοπο που προωθεί μια «επενδυτική ευκαιρία περιορισμένου χρόνου», συνιστώντας την επένδυση σε ένα νέο κρυπτοστοιχείο ή κάποιο σχετικό έργο. Αφού εκδηλώσετε ενδιαφέρον, επικοινωνούν μαζί σας και σας ανακατευθύνουν σε μια πλατφόρμα ανταλλαγής κρυπτοστοιχείων ή σε ένα κανάλι ανταλλαγής μηνυμάτων (π.χ. Telegram, Viber ή WhatsApp). Μια φαινομενικά αξιόπιστη επαφή υπόσχεται γρήγορα κέρδη ή υψηλές αποδόσεις αν επενδύσετε γρήγορα. Ενθαρρύνεστε να επενδύσετε ένα μικρό ποσό και στη συνέχεια πιέζεστε να επενδύσετε περισσότερο.

Τι μπορεί να συμβεί:

Ανακαλύπτετε ότι το κρυπτοστοιχείο στο οποίο υποτίθεται ότι επενδύσατε δεν έχει καμία αξία και η επαφή με την οποία επικοινωνήσατε σταματά να ανταποκρίνεται. Όταν προσπαθείτε να αποσύρετε τα χρήματά σας, ο ιστότοπος δεν υπάρχει πλέον και η εταιρεία δεν είναι προσβάσιμη. Οι απατεώνες διογκώνουν τεχνητά ή υπερεκτιμούν την τιμή ενός κρυπτοστοιχείου για να αυξήσουν την αξία του («pump»), στη συνέχεια πωλούν τις δικές τους μάρκες («dump»), προκαλώντας μείωση της αξίας και αφήνοντας τους επενδυτές με ζημίες. Εναλλακτικά, μπορούν να αποσύρουν αιφνιδίως τη ρευστότητα του κρυπτοστοιχείου και να εξαφανιστούν με τα κεφάλαια («rug pull»).

ΑΠΆΤΗ ΠΛΑΣΤΟΠΡΟΣΩΠΊΑΣ

Αφού δημοσιεύσετε μια ερώτηση σε μια πλατφόρμα μέσων κοινωνικής δικτύωσης ή σε έναν ιστότοπο σχετικά με ένα ζήτημα πορτοφολιού κρυπτοστοιχείων, λαμβάνετε ένα απροσδόκητο άμεσο μήνυμα (DM - direct message) ή ένα μήνυμα ηλεκτρονικού ταχυδρομείου από κάποιον που προσποιείται ότι είναι αξιόπιστη επαφή (π.χ. πλατφόρμα ανταλλαγής 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 (αποδεικτικό κυριότητας ψηφιακών περιουσιακών στοιχείων).

Τι μπορεί να συμβεί:

Μόλις μοιραστείτε τη φράση ανάκτησης, τους κωδικούς πρόσβασης ή τα ιδιωτικά κλειδιά σας, ο απατεώνας τα χρησιμοποιεί για να κλέψει τα κρυπτοστοιχεία ή άλλα 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, σε περίπτωση μεταφοράς κρυπτοστοιχείων, μόλις χαθεί η κυριότητά τους, η ανάκτησή τους είναι σχεδόν αδύνατη.

Phishing

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

Τι μπορεί να συμβεί:

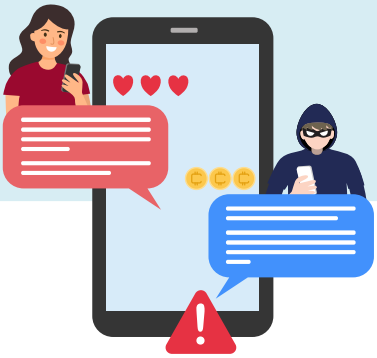
Κάνοντας κλικ στον σύνδεσμο, κατεβάζοντας την εφαρμογή ή σαρώνοντας έναν κωδικό QR, εγκαθιστάτε ένα κακόβουλο λογισμικό που επιτρέπει στον απατεώνα να έχει πρόσβαση και να χρησιμοποιεί τις πληροφορίες για να κλέψει τα κρυπτοστοιχεία σας ή τα χρήματά σας.

Απάτη του Giveaway

Συναντάτε μια ανακοίνωση στα μέσα κοινωνικής δικτύωσης που ισχυρίζεται ότι εταιρείες δωρίζουν κρυπτοστοιχεία μετά από μια μικρή επένδυση. Περιλαμβάνει ένα βίντεο ή μια ανάρτηση με φωτογραφίες ενός διάσημου προσώπου ή ενός εμπορικού σήματος- συνήθως πλαστού ή άνευ άδειας χρήσης- που υπόσχεται να «διπλασιάσει τα κρυπτοστοιχεία σας» εάν στείλετε πρώτα χρήματα. Το λογότυπο, η διάταξη, οι μαρτυρίες και η γλώσσα που χρησιμοποιείται φαίνονται επαγγελματικά και επίσημα, όπως και η ιστοσελίδα στην οποία ανακατευθύνεστε.

Τι μπορεί να συμβεί:

Μετά την αποστολή των χρημάτων σας, δεν λαμβάνετε τίποτα σε αντάλλαγμα και έχετε χάσει τα χρήματα που αποστείλατε. Ο διαγωνισμός ήταν ψεύτικος και η ανάρτηση ή η ζωντανή μετάδοση που προβάλλει δημόσια πρόσωπα ή εταιρείες σχεδιάστηκε για να σας εξαπατήσει.



Απάτη μέσω διαδικτυακών γνωριμιών

Έχετε έρθει σε επαφή με μέσα κοινωνικής δικτύωσης, εφαρμογές γνωριμιών ή μέσω τηλεφώνου /μηνύματος με κάποιον που δεν έχετε συναντήσει στην πραγματική ζωή. Το εν λόγω άτομο συμμετέχει σε συχνές, προσωπικές και ρομαντικές συνομιλίες, χτίζοντας εμπιστοσύνη και χρησιμοποιώντας ψεύτικα προφίλ. Σταδιακά, κατευθύνει τη συζήτηση προς οικονομικές ευκαιρίες, ισχυριζόμενο ότι έχει αποκομίσει τεράστια κέρδη από επενδύσεις σε κρυπτοστοιχεία και ενθαρρύνοντάς σας να συμμετέχετε με υποσχέσεις υψηλών αποδόσεων και χαμηλού κινδύνου. Σας καθοδηγούν να δημιουργήσετε έναν λογαριασμό και να κάνετε μια μικρή αρχική κατάθεση ώστε να θεωρήσετε ότι πρόκειται για μια νόμιμη δραστηριότητα.

Οι απατεώνες δημιουργούν πλαστά διαδικτυακά προφίλ και χρησιμοποιούν εικόνες είτε κλεμμένες είτε παραγόμενες με χρήση Τεχνητής Νοημοσύνης ώστε να σας προσεγγίσουν.

Τι μπορεί να συμβεί:

Ο απατεώνας εξάγει όσο το δυνατόν περισσότερα χρήματα, στη συνέχεια κόβει κάθε επικοινωνία και εξαφανίζεται. Η κακόβουλη επενδυτική ιστοσελίδα ή εφαρμογή τίθεται εκτός σύνδεσης, 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 θεωρηθεί υπεύθυνος για χρέη ή εγκλήματα που διαπράχθηκαν με το όνομά σας έως ότου αποδειχθεί το αντίθετο).

Σχήμα Ponzi

Έχετε προσκληθεί να συμμετάσχετε σε ένα πρόγραμμα που υπόσχεται σταθερά υψηλές αποδόσεις από επενδύσεις σε κρυπτοστοιχεία, οι οποίες συχνά υποστηρίζονται από μαρτυρίες ή ψευδείς ιστορίες επιτυχίας. Το πρόγραμμα μπορεί να παρουσιαστεί ως μια ευκαιρία μάρκετινγκ πολλαπλών επιπέδων, όπου κερδίζετε ανταμοιβές όχι μόνο από τη δική σας επένδυση, αλλά συμβάλλοντας στο να γίνουν και άλλες επενδύσεις. Οι πρώτοι επενδυτές φαίνεται να λαμβάνουν πληρωμές, ενθαρρύνοντας περισσότερους ανθρώπους να συμμετάσχουν και να προωθήσουν το πρόγραμμα.

Στην πραγματικότητα, δεν υπάρχει 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 συστήματος.

Τι μπορεί να συμβεί:

Μόλις οι νέες επενδύσεις αρχίσουν να αραιώνουν, το πρόγραμμα καταρρέει και εσείς, όπως και οι περισσότεροι συμμετέχοντες, χάνετε τα χρήματά σας. Οι διοργανωτές εξαφανίζονται, χωρίς να υπάρχει τρόπος ανάκτησης κεφαλαίων. Η πολυεπίπεδη δομή βοηθά την απάτη να εξαπλωθεί γρήγορα, καθώς τα θύματα γίνονται εν αγνοία τους υποστηρικτές.

Παρεμβολή κακόβουλης διεύθυνσης στο πορτοφόλι σας (wallet poisoning)

Αφού πραγματοποιήσετε μια συναλλαγή κρυπτοστοιχείου, παρατηρείτε μια νέα διεύθυνση που εμφανίζεται στο ιστορικό του πορτοφολιού σας. Αυτή η διεύθυνση μοιάζει με αυτή με την οποία έχετε αλληλεπιδράσει στο παρελθόν. Οι απατεώνες μπορούν να κάνουν ψευδείς 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 τις 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, για να αποφύγουν τον εντοπισμό.

Τι μπορεί να συμβεί:

Όταν προσπαθείτε να στείλετε κρυπτοστοιχεία, αντιγράφοντας την απατηλή διεύθυνση από το ιστορικό του πορτοφολιού σας, στέλνετε εν αγνοία σας κεφάλαια στο πορτοφόλι του απατεώνα. 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 επαρκή προσοχή.