



ΔΙΑΔΙΚΤΥΑΚΕΣ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΕΣ ΑΠΑΤΕΣ ΣΤΟΝ ΚΟΣΜΟ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

ΠΑΡΑΜΕΙΝΕΤΕ ΣΕ ΕΓΡΗΓΟΡΣΗ ΚΑΙ ΠΡΟΣΤΑΤΕΨΤΕ ΤΟΝ ΕΑΥΤΟ ΣΑΣ

Οι διαδικτυακές χρηματοοικονομικές απάτες δεν είναι κάτι καινούριο, εντούτοις η Τεχνητή Νοημοσύνη (TN) τις έχει κάνει πιο έξυπνες και πιο δύσκολο να εντοπιστούν. Οι απατεώνες χρησιμοποιούν πλέον ψεύτικα μηνύματα και ιστοσελίδες, ψεύτικα προφίλ διασημοτήτων, ακόμη και φωνές ή βίντεο που δημιουργούνται με TN και μοιάζουν με τον υπάλληλο της τράπεζάς σας, τους φίλους σας ή την οικογένειά σας για να σας παραπλανήσουν.

Συχνά σας προσεγγίζουν από τα μέσα κοινωνικής δικτύωσης, εφαρμογές ανταλλαγής μηνυμάτων, μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου και απροσδόκητων τηλεφωνικών κλήσεων που ακούγονται αληθινές.

Μπορεί να έρθετε αντιμέτωποι με σοβαρούς κινδύνους όπως οικονομική ζημιά, κλοπή ταυτότητας ή ακόμη και ψυχολογική επιβάρυνση. Γι' αυτό είναι σημαντικό να παραμείνετε προσεκτικοί και να ακολουθείτε τις παρακάτω βασικές συμβουλές για την προστασία σας:



Παραμείνετε σε εγρήγορση απέναντι στις διαδικτυακές χρηματοοικονομικές απάτες που δημιουργούνται με χρήση TN π.χ. πλαστοπροσωπία, ηλεκτρονικό ψάρεμα (phishing), επενδυτικές και ασφαλιστικές απάτες, καθώς και απάτες μέσω διαδικτυακών γνωριμιών. Για να μάθετε περισσότερα σχετικά με τα διάφορα είδη απάτης δείτε [σελίδες 5, 6 και 7](#).

Και για απάτες που σχετίζονται ειδικά με τα κρυπτοστοιχεία δείτε το αντίστοιχο ενημερωτικό δελτίο για τις απάτες με κρυπτοστοιχεία ([link](#)).



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



Προστατέψτε τον εαυτό σας:
Ακολουθήστε τα βασικά μέτρα ασφάλειας για την προστασία των προσωπικών σας στοιχείων (δείτε [σελίδα 3](#)).



**Μάθετε τί πρέπει να κάνετε
εάν πέσετε θύμα απάτης**
(δείτε [σελίδα 4](#)).



Προειδοποιητικά σημάδια



Μια υπόσχεση που φαίνεται πολύ καλή για να είναι αληθινή.



Μια αναπάντεχη κλήση από άγνωστο αριθμό.



Μια επείγουσα παράκληση για χρήματα ή προσωπικές πληροφορίες, μεταξύ άλλων από κάποιον που προσποιείται ότι είναι μέλος της οικογένειας, φίλος ή ακόμη και δημόσιο πρόσωπο.



Ένα αίτημα για να αποκτήσει κάποιος τον έλεγχο της συσκευής σας, για να κατεβάσετε μια εφαρμογή, για να σαρώσετε έναν κωδικό QR ή για να κάνετε κλικ σε έναν σύνδεσμο.



Ένα αίτημα για προσωπικές πληροφορίες ή τραπεζικά στοιχεία (π.χ. κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών, διαπιστευτήρια διαδικτυακής τραπεζικής (username/ password) ή κωδικοί ασφαλείας).



Ένα αίτημα για πληρωμή μέσω μη ανιχνεύσιμων τρόπων (π.χ. κρυπτοστοιχεία, δωροκάρτες, εμβάσματα ή προπληρωμένες χρεωστικές κάρτες).



Μια ύποπτη ή λανθασμένη διεύθυνση ηλεκτρονικού ταχυδρομείου ή σύνδεσμος (π.χ. με ορθογραφικά λάθη στη διεύθυνση ή ασυνήθιστες διευθύνσεις ιστοσελίδων).



Ένα συνημμένο αρχείο από άγνωστη πηγή, ειδικά σε μορφή .exe, .scr, .zip ή αρχείο Office με δυνατότητα μακροεντολής (.docm, .xlsm).



Γραμματικά λάθη ή λάθη στη μορφοποίηση εγγράφου που φαίνεται επίσημο, αν και η ΤΝ μπορεί να επιτρέψει στους απατεώνες να αποκρύψουν αυτά τα ελαττώματα πιο αποτελεσματικά.



Μια ιστοσελίδα που φαίνεται επαγγελματική αλλά δεν διαθέτει επαληθευμένα στοιχεία επικοινωνίας ή επίσημα στοιχεία εγγραφής της εταιρείας.



Τονισμός που ακούγεται αφύσικος, δεν έχει παύσεις και φαίνεται υπερβολικά ορθός ή ρομποτικός. Δώστε προσοχή στην «κλωνοποίηση φωνής», αν και η ομιλία που παράγεται από ΤΝ μπορεί επίσης να ακούγεται πολύ φυσική.



Βίντεο όπου η φωνή μπορεί να ακούγεται ρομποτική ή υπερβολικά ομαλή, οι κινήσεις των χειλιών και οι εκφράσεις του προσώπου μπορεί να μην ευθυγραμμίζονται με την ομιλία ή το φόντο, ο φωτισμός και οι σκιές μπορεί να είναι ασυνεπείς. Αυτά είναι συχνά βίντεο που παράγονται από ΤΝ (deepfakes).

Βήματα για να προστατεύσετε τον εαυτό σας

1

Ποτέ μην μοιράζεστε προσωπικές ή τραπεζικές πληροφορίες:

Οι νόμιμες εταιρείες δεν θα σας ζητήσουν ποτέ προσωπικούς αριθμούς αναγνώρισης (PIN), κωδικούς πρόσβασης, διαπιστευτήρια διαδικτυακής τραπεζικής (username/password) ή κωδικούς ασφαλείας μέσω ηλεκτρονικού ταχυδρομείου, μηνυμάτων (text), μέσων κοινωνικής δικτύωσης ή τηλεφώνου.

2

Σταματήστε και σκεφτείτε πριν ενεργήσετε:

Μην βιαστείτε να στείλετε χρήματα, να ανταλλάξετε πληροφορίες ή να κάνετε κλικ σε συνδέσμους- οι απατεώνες δημιουργούν σκόπιμα την αίσθηση του επείγοντος (π.χ. προβλήματα με την τράπεζά σας, κλήσεις έκτακτης ανάγκης που αφορούν φίλους και μέλη της οικογένειάς σας, απειλητική ή πιεστική γλώσσα κλπ.). Αν έχετε την παραμικρή αμφιβολία, μην προχωρήσετε: τερματίστε την κλήση και επαληθεύστε προσεκτικά την πηγή ή την ταυτότητα του προσώπου που επικοινωνεί.

3

Ελέγξτε προσεκτικά την πηγή / ταυτότητα:

- Πάντα να επαληθεύετε από πού προέρχονται τα μηνύματα, οι κλήσεις, τα μηνύματα ηλεκτρονικού ταχυδρομείου και οι σύνδεσμοι- ακόμη και αν φαίνονται επίσημα, ή ότι μοιάζουν να προέρχονται από ένα φίλο ή μέλος της οικογένειάς σας ή ακόμα και από ένα δημόσιο πρόσωπο. Για παράδειγμα, καλέστε ή στείλτε μήνυμα στην οικογένεια και στους φίλους σας χρησιμοποιώντας έναν γνωστό αριθμό μέσω ενός αξιόπιστου καναλιού, για να βεβαιωθείτε ότι όντως σας κάλεσε. Αναζητήστε ορθογραφικά λάθη, παράξενες ηλεκτρονικές διευθύνσεις (URL) ή ελλειπείς δείκτες ασφαλείας (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 μη σαρώνετε άγνωστους κωδικούς QR.
- Συμφωνήστε με την οικογένειά σας σε μια «λέξη ασφαλείας»- μια μυστική φράση που μπορείτε να χρησιμοποιήσετε για να επαληθεύετε την ταυτότητα σας, σε περίπτωση που κάποιος με οικεία φωνή σας καλεί με επείγον αίτημα για χρήματα και ισχυρίζεται ότι είναι μέλος της οικογένειας (π.χ. γονείς, αδελφή / αδελφός, παιδί).
- Χρησιμοποιήστε μόνο επαληθευμένα στοιχεία επικοινωνίας για να επικοινωνήσετε απευθείας με την εταιρεία ή το άτομο και μην βασίζεστε ποτέ στα στοιχεία επικοινωνίας που παρέχονται από τον ύποπτο απατεώνα (π.χ. αναζήτηση του ονόματος της εταιρείας ανεξάρτητα, χρήση επαληθευμένων καταλόγων επιχειρήσεων, χρήση μεθόδων επικοινωνίας που είχατε χρησιμοποιήσει και επιβεβαιώσει στο παρελθόν). Οι απατεώνες μπορεί να ισχυριστούν ότι είναι εξουσιοδοτημένοι ή να μιμούνται την ιστοσελίδα μιας νόμιμης εταιρείας. Επαληθεύστε επίσης αν έχουν εκδοθεί προειδοποιήσεις από την εθνική αρμόδια αρχή της χώρας σας όπως την Επιτροπή Κεφαλαιαγοράς Κύπρου (🔗) ή αν τέτοιες προειδοποιήσεις περιλαμβάνονται στον κατάλογο IOSCO I-SCAN (iosco.org/i-scan/). Για τους παρόχους κρυπτοστοιχείων, ελέγξτε αν έχουν λάβει άδεια λειτουργίας στην Ευρωπαϊκή Ένωση (π.χ. ελέγξτε το μητρώο της ESMA (🔗)).

4

Δώστε προσοχή σε πιθανά τεχνάσματα ΤΝ:

Καθώς η τεχνολογία ΤΝ εξελίσσεται, οι απάτες γίνονται πιο πειστικές από ποτέ- ακόμη και με τις καλύτερες πρακτικές ασφαλείας. Αν κάτι σας φανεί ασυνήθιστο ή εντοπίσετε κάποιο από τα προειδοποιητικά σημάδια που περιγράφονται πιο πάνω, σταματήστε και επανεκτιμήστε την κατάσταση.

5

Μην εγκαταστήσετε ποτέ λογισμικό απομακρυσμένης πρόσβασης και μην επιτρέπετε ποτέ κοινή χρήση της οθόνης σας:

Οι τράπεζες και τα χρηματοπιστωτικά ιδρύματα δεν θα το ζητήσουν ποτέ από εσάς.

6

Κρατήστε τις συσκευές και τους λογαριασμούς ασφαλείς:

Χρησιμοποιήστε ισχυρούς και μοναδικούς κωδικούς πρόσβασης, κρατήστε τους μυστικούς και αποφύγετε την επαναχρησιμοποίηση των ίδιων κωδικών πρόσβασης σε διαφορετικές πλατφόρμες. Ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων, όπου είναι δυνατόν. Για συμβουλές δημιουργίας κωδικών πρόσβασης δείτε εδώ (🔗). Διατηρήστε το λογισμικό και το σύστημα προστασίας από ιούς (antivirus protection) επικαιροποιημένα και ενεργοποιημένα.

7

Να είστε επιφυλακτικοί με απροσδόκητες και περιορισμένου χρόνου επενδυτικές ευκαιρίες:

Αν ακούγεται πολύ καλό για να είναι αληθινό, πιθανότατα είναι.

8

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 γνώσης για τους απατεώνες. Αποκαλύπτοντας πάρα πολλά για τον εαυτό σας ή τις επενδύσεις σας μπορεί να σας κάνει έναν εύκολο στόχο.

Τί να κάνετε όταν έχετε πέσει θύμα απάτης



Σταματήστε αμέσως τις συναλλαγές

για να εμποδίσετε τυχόν περαιτέρω μεταφορές χρημάτων σε ύποπτους λογαριασμούς και να αποφύγετε πρόσθετες απώλειες. Σταματήστε κάθε επικοινωνία με τους απατεώνες — αγνοήστε τις κλήσεις και τα μηνύματα ηλεκτρονικού ταχυδρομείου τους και αποκλείστε τον αποστολέα.



Επικοινωνήστε με την τράπεζά σας ή τον πάροχο χρηματοπιστωτικών υπηρεσιών σας

ενημερώστε αμέσως την τράπεζά σας ή τον πάροχο χρηματοπιστωτικών υπηρεσιών σας μέσω των επίσημων διαύλων επικοινωνίας, για να διερευνήσετε επιλογές για το πάγωμα ή την αντιστροφή των συναλλαγών.



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, ώστε οι απατεώνες να μην μπορούν να τους επαναχρησιμοποιήσουν.



Αναφορά και προειδοποίηση

αναφέρετε το περιστατικό στην αστυνομία ή στην εθνική αρμόδια αρχή και ενημερώστε το περιβάλλον σας (π.χ. φίλους και οικογένεια) για να αυξήσετε την ευαισθητοποίηση. Αυτές οι ενέργειες μπορούν να σας βοηθήσουν να προστατεύσετε τον εαυτό σας και τους άλλους.



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 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 μια φορά δεν αποκλείει να εξαπατηθείτε ξανά.

ΕΙΔΗ ΔΙΑΔΙΚΤΥΑΚΗΣ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ ΑΠΑΤΗΣ ΠΟΥ ΥΠΟΣΤΗΡΙΖΟΝΤΑΙ ΑΠΟ ΤΗΝ ΤΝ



ΑΠΑΤΗ ΠΛΑΣΤΟΠΡΟΣΩΠΙΑΣ ΚΑΙ ΧΡΗΣΗ DEEP FAKE

Μπορεί να λάβετε μια αναπάντεχη κλήση από κάποιον που ισχυρίζεται ότι εκπροσωπεί την τράπεζά σας, δημόσια αρχή (π.χ. αστυνομία, φορολογική ή χρηματοοικονομική αρχή κ.λπ.), διανομέα ασφαλιστικών προϊόντων, εταιρεία πληροφορικής ή ακόμη ότι είναι μέλος της οικογένειάς σας. Αυτός που σας κάλεσε μπορεί να σας προτρέψει να μεταφέρετε χρήματα για να τα «κρατήσετε ασφαλή», επικαλούμενος ύποπτη δραστηριότητα στο λογαριασμό σας ή το ασφαλιστήριο συμβόλαιο σας. Μπορεί επίσης να σας ζητήσει να αποκαλύψετε τα τραπεζικά σας στοιχεία (π.χ. αριθμό κάρτας πληρωμής, διαπιστευτήρια διαδικτυακής τραπεζικής ή κωδικούς πρόσβασης), να κάνετε κλικ σε έναν σύνδεσμο ή να εγκαταστήσετε ένα λογισμικό, προσποιούμενος ότι μπορεί να λύσει γρήγορα το ζήτημα. Επίσης, μπορεί να χρησιμοποιήσει παραποιημένο αριθμό, ο οποίος συχνά αντιστοιχεί στον αριθμό τηλεφώνου της τράπεζάς σας ώστε να φαίνεται νόμιμος (πλαστογράφηση ταυτότητας/ caller ID spoofing).

Οι απατεώνες μπορούν να χρησιμοποιούν ΤΝ για τη δημιουργία ψεύτικων βίντεο, εικόνων ή ήχου που μιμούνται τη φωνή, την εμφάνιση ή τις κινήσεις κάποιου (π.χ. του υπαλλήλου της τράπεζάς σας ή μέλους της οικογένειάς σας ή διασημότητας). **Αυτό είναι γνωστό ως «Deepfake».**

Τί μπορεί να συμβεί:

Με την αναφορά προσωπικών στοιχείων και τη δημιουργία αίσθησης του επείγοντος, ο απατεώνας σας ξεγελά σε ενέργειες που δεν σκοπεύατε να κάνετε - όπως αποστολή χρημάτων στον λογαριασμό τους, κλικ σε κακόβουλο σύνδεσμο ή εγκατάσταση κακόβουλου λογισμικού στη συσκευή σας. Αυτό μπορεί να δώσει στον απατεώνα άμεση πρόσβαση στα τραπεζικά διαπιστευτήριά σας (username/ password). Με αυτές τις πληροφορίες, μπορούν να αλλάξουν τον κωδικό πρόσβασής σας, να αποκτήσουν πρόσβαση στον τραπεζικό σας λογαριασμό και να κλέψουν τα χρήματά σας. Θυμηθείτε: μόνο και μόνο επειδή αυτός που σας καλεί γνωρίζει τα προσωπικά σας στοιχεία δεν σημαίνει ότι είναι αξιόπιστος.



ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ (PHISHING) ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ (SOCIAL ENGINEERING)

Μπορεί να λάβετε μήνυμα ηλεκτρονικού ταχυδρομείου ή άλλο μήνυμα που φαίνεται να προέρχεται από την τράπεζά σας ή από χρηματοοικονομική εταιρεία, το οποίο σας προειδοποιεί για «ύποπτη δραστηριότητα» στον λογαριασμό σας. Το λογότυπο, η διάταξη και η γλώσσα φαίνονται επαγγελματικά και το μήνυμα μπορεί να εμφανιστεί στο ίδιο νήμα με άλλες συνομιλίες από την τράπεζά σας. Το μήνυμα σας προτρέπει να κάνετε κλικ σε έναν σύνδεσμο για να επαληθεύσετε τον λογαριασμό σας ή να επαναφέρετε τον κωδικό πρόσβασής σας. Ο σύνδεσμος οδηγεί σε μια πλαστή ιστοσελίδα που είναι πανομοιότυπη με αυτή της τράπεζάς σας. Χωρίς να το συνειδητοποιείτε, εισάγετε τα προσωπικά σας στοιχεία σε μια ιστοσελίδα που έχει σχεδιαστεί για να τα κλέψει.

Οι απατεώνες χρησιμοποιούν την ΤΝ για να δημιουργήσουν πειστικά μηνύματα ηλεκτρονικού ψαρέματος, αναλύοντας τα δεδομένα των μέσων κοινωνικής δικτύωσης για να εντοπίσουν τα θύματά τους και προσαρμόζοντας το περιεχόμενο για κάθε στόχο.

Τί μπορεί να συμβεί:

Ο απατεώνας αποκτά πρόσβαση στον τραπεζικό σας λογαριασμό και κλέβει τα χρήματά σας ή δημιουργεί ένα ψεύτικο προφίλ με τα προσωπικά σας στοιχεία για να διαπράξει περαιτέρω απάτες.



ΕΠΕΝΔΥΤΙΚΗ Η ΑΣΦΑΛΙΣΤΙΚΗ ΑΠΑΤΗ

Μπορεί να δείτε μια διαφήμιση στα μέσα κοινωνικής δικτύωσης ή μια ιστοσελίδα που προωθεί μια «επενδυτική ευκαιρία περιορισμένου χρόνου με χαμηλούς κινδύνους» ή μια «έκπτωση περιορισμένου χρόνου» σε ασφάλιση από φαινομενικά γνωστή εταιρεία. Η διαφήμιση περιλαμβάνει φωτογραφία διασημότητας και συστάσεις που συχνά είναι ψεύτικες. Αφού εκδηλώσετε ενδιαφέρον κάνοντας κλικ σε έναν σύνδεσμο ή συμπληρώνοντας μια φόρμα, οι απατεώνες επικοινωνούν μαζί σας και σας κατευθύνουν σε μια πλατφόρμα ή ένα κανάλι ανταλλαγής μηνυμάτων όπου παρέχονται συμβουλές και δίδουν επίσημα έγγραφα. Σας ενθαρρύνουν να επενδύσετε ένα μικρό ποσό, ακολουθούμενο από μεγαλύτερα ποσά, ή να πληρώσετε ασφάλιστρο σε ένα λογαριασμό που φαίνεται ασφαλής, αλλά ελέγχουν οι ίδιοι.

Οι απατεώνες χρησιμοποιούν εργαλεία ΤΝ για να κάνουν αυτές τις ψεύτικες προτάσεις ή μηνύματα ηλεκτρονικού ταχυδρομείου εξαιρετικά πειστικά και δύσκολο να εντοπιστούν. Χρησιμοποιούν επίσης ρομπότ κοινωνικών μέσων (bot) που λειτουργούν με ΤΝ δημιουργώντας πλαστούς λογαριασμούς που αλληλεπιδρούν μαζί σας, διαδίδουν παραπληροφόρηση και προσομοιώνουν πραγματικές συμπεριφορές για να κερδίσουν εμπιστοσύνη και να επηρεάσουν τις αποφάσεις σας.

Τί μπορεί να συμβεί:

Όταν προσπαθήσετε να αποσύρετε τα χρήματά σας ή να τα διεκδικήσετε πίσω, η επαφή σταματά να ανταποκρίνεται. Ανακαλύπτετε ότι η εταιρεία δεν υπάρχει ή ότι ο κίνδυνος που ασφαλίσατε δεν καλύπτεται. Στη συνέχεια, συνειδητοποιείτε ότι έχετε στείλει χρήματα απευθείας σε έναν απατεώνα ως μέρος ενός δόλιου σχεδίου. Δυστυχώς, δεν μπορείτε να ανακτήσετε τα χρήματά σας και τα προσωπικά και χρηματοοικονομικά σας στοιχεία μπορούν να χρησιμοποιηθούν για τη διάπραξη περαιτέρω απάτης (π.χ. υπογραφή συμβάσεων για λογαριασμό σας, η οποία μπορεί να σας οδηγήσει να χάσετε ακόμη περισσότερα χρήματα).



ΑΠΑΤΗ ΜΕΣΩ ΔΙΑΔΙΚΤΥΑΚΩΝ ΓΝΩΡΙΜΙΩΝ

Μπορεί να έρθει σε επαφή μαζί σας, χρησιμοποιώντας τα μέσα κοινωνικής δικτύωσης, εφαρμογές γνωριμιών ή μέσω τηλεφώνου / μηνύματος, κάποιος που δεν έχετε συναντήσει στην πραγματική ζωή. Το άτομο αυτό, συμμετέχει σε συχνές, προσωπικές και ρομαντικές συνομιλίες, χτίζοντας εμπιστοσύνη χρησιμοποιώντας ψεύτικα προφίλ. Με την πάροδο του χρόνου, η συζήτηση μετατοπίζεται προς τα χρήματα ή τις οικονομικές ευκαιρίες, όπως οι επενδύσεις σε κρυπτοστοιχεία με υποσχέσεις υψηλών αποδόσεων και χαμηλού κινδύνου. Το άτομο μπορεί να σας ζητήσει να μεταφέρετε χρήματα σε έναν λογαριασμό ή σας καθοδηγεί μέσω της δημιουργίας ενός λογαριασμού και κάνοντας μια μικρή αρχική κατάθεση για να κάνει το σύστημα να φαίνεται νόμιμο, πριν σας ενθαρρύνει να επενδύσετε περισσότερο.

Οι απατεώνες χρησιμοποιούν την ΤΝ για να δημιουργήσουν ψεύτικα προφίλ, να εντοπίσουν τα θύματά τους στα μέσα κοινωνικής δικτύωσης/εφαρμογές γνωριμιών χρησιμοποιώντας δεδομένα που έχετε καταστήσει διαθέσιμα ή να χρησιμοποιήσουν chatbots για τη δημιουργία μηνυμάτων.

Τί μπορεί να συμβεί:

Ο απατεώνας εξαγεί όσο το δυνατόν περισσότερα χρήματα, στη συνέχεια διακόπτει κάθε επικοινωνία και εξαφανίζεται. Η υποτιθέμενη επενδυτική ιστοσελίδα ή η εφαρμογή εξαφανίζεται ή γίνεται μη προσβάσιμη, με αποτέλεσμα να μην μπορείτε να ανακτήσετε τις υποτιθέμενες επενδύσεις. Εκτός από την οικονομική απώλεια, οι προσωπικές πληροφορίες που κοινοποιήσατε ενδέχεται να χρησιμοποιηθούν για τη στόχευση των φίλων και της οικογένειάς σας ή για κλοπή ταυτότητας που μπορεί να έχει οικονομικές ή νομικές συνέπειες για εσάς (π.χ. ο απατεώνας θα μπορούσε να πραγματοποιήσει αγορές, να λάβει δάνεια στο όνομά σας ή μπορεί να θεωρηθείτε υπεύθυνος για χρέη ή εγκλήματα που διαπράχθηκαν στο όνομά σας έως ότου αποδειχθεί το αντίθετο).



ΑΠΑΤΗ ΑΓΟΡΑΣ

Μπορεί να εντοπίσετε μια ελκυστική προσφορά για κάποιο προϊόν σε μια διαδικτυακή πλατφόρμα ηλεκτρονικού εμπορίου. Η εταιρεία που προσφέρει το προϊόν, ζητά να πραγματοποιήσετε την πληρωμή εκτός της επίσημης πλατφόρμας, ισχυριζόμενη ότι χρησιμοποιεί «ασφαλές σύστημα πληρωμών» και σας αποστέλλει ένα σύνδεσμο για την ολοκλήρωση της συναλλαγής. Ο σύνδεσμος σας ανακατευθύνει σε μια πλαστή σελίδα ελέγχου ταυτότητας που μιμείται την επίσημη ιστοσελίδα της τράπεζας σας και χρησιμοποιεί το λογότυπο και τον σχεδιασμό της, ώστε να εισαγάγετε τα στοιχεία ηλεκτρονικής τραπεζικής σας για να πραγματοποιήσετε την πληρωμή.

Οι απατεώνες χρησιμοποιούν ΤΝ για να δημιουργήσουν εξαιρετικά πειστικές πλαστές ιστοσελίδες τραπεζών, επιβεβαιώσεις παραγγελιών και τιμολόγια. Η ΤΝ τους βοηθά να μιμούνται τον ύφος, την επωνυμία και το στυλ των πραγματικών εταιρειών. Σε ορισμένες περιπτώσεις, χρησιμοποιούν chatbots ΤΝ για να απαντούν σε ερωτήσεις και να κάνουν τη συμφωνία να φαίνεται πιο πειστική.

Τί μπορεί να συμβεί:

Η πληρωμή μέσω συνδέσμου τρίτου μέρους παρακάμπτει τις δικλίδες προστασίας της πλατφόρμας ηλεκτρονικού εμπορίου. Ο απατεώνας αποκτά τα στοιχεία σύνδεσής σας στον τραπεζικό σας λογαριασμό και κλέβει τα χρήματά σας.