



ΔΙΑΔΙΚΤΥΑΚΕΣ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΕΣ ΑΠΑΤΕΣ ΣΤΟΝ ΚΟΣΜΟ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

ΜΕΙΝΕΤΕ ΣΕ ΕΓΡΗΓΟΡΣΗ ΚΑΙ ΠΡΟΣΤΑΤΕΨΤΕ ΤΟΝ ΕΑΥΤΟ ΣΑΣ

Οι διαδικτυακές χρηματοοικονομικές απάτες δεν είναι κάτι καινούργιο, όμως η Τεχνητή Νοημοσύνη (TN) τις έχει κάνει πιο έξυπνες και είναι πιο δύσκολο να εντοπιστούν. Οι απατεώνες χρησιμοποιούν πλέον ψευδή μηνύματα και διαδικτυακούς τόπους, πλαστά προφίλ διασημοτήτων, ακόμη και φωνές ή βίντεο που παράγονται από TN και μοιάζουν με την τράπεζά σας, τους φίλους σας ή την οικογένειά σας, για να σας ξεγελάσουν.

Συχνά σας προσεγγίζουν στα μέσα κοινωνικής δικτύωσης, με εφαρμογές ανταλλαγής μηνυμάτων, μηνύματα ηλεκτρονικού ταχυδρομείου και απροσδόκητες κλήσεις που φαίνονται πραγματικές.

Μπορεί να βρεθείτε αντιμέτωποι με κινδύνους όπως οικονομική ζημία, κλοπή ταυτότητας και συναισθηματική δυσφορία. Να είστε προσεκτικοί και να ακολουθείτε αυτές τις βασικές συμβουλές για να παραμένετε ασφαλείς:



Μένετε σε εγρήγορση για διαδικτυακές χρηματοοικονομικές απάτες που προκύπτουν από τη χρήση TN,

π.χ. πλαστοπροσωπία, ηλεκτρονικό ψάρεμα (phishing), επενδυτικές και ασφαλιστικές απάτες, ακόμη 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 ([📄](#)).



Εντοπίζετε προειδοποιητικά σημάδια:

Μάθετε να αναγνωρίζετε ύποπτες συμπεριφορές, μηνύματα ή προσφορές (δείτε [σελίδα 2](#))



Προστατεύετε τον εαυτό σας:

Φροντίζετε 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.



Μια απροσδόκητη κλήση από άγνωστο αριθμό.



Επείγον αίτημα με το οποίο σας ζητούνται χρήματα ή προσωπικές πληροφορίες, μεταξύ άλλων από κάποιον που προσποιείται ότι είναι μέλος της οικογένειας, φίλος ή ακόμη και δημόσιο πρόσωπο.



Αίτημα να αποκτήσει κάποιος τον έλεγχο της συσκευής σας, να «κατεβάσετε» μια εφαρμογή, να «σαρώσετε» έναν κωδικό QR ή να «κάνετε κλικ» σε έναν σύνδεσμο.



Αίτημα με το οποίο σας ζητούν προσωπικές πληροφορίες ή τραπεζικά στοιχεία (π.χ. κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών, κωδικοί e-banking ή κωδικοί ασφαλείας).



Αίτημα με το οποίο σας ζητούν να πληρώσετε με τρόπο που δεν επιτρέπει να ανιχνευτεί η συναλλαγή (π.χ. κρυπτοστοιχεία, δωροκάρτες, εμβάσματα ή προπληρωμένες χρεωτικές κάρτες).



Μια ύποπτη ή λανθασμένη διεύθυνση ηλεκτρονικού ταχυδρομείου ή συνδέσμου (π.χ. ορθογραφικά λάθη στη διεύθυνση URL ή «περιέργες» ιστοσελίδες).



Συνημμένο αρχείο σε μήνυμα που προέρχεται από άγνωστη πηγή, ειδικά σε μορφή .exe, .scr, .zip ή αρχείο Office με δυνατότητα μακροεντολής (.docm, .xlsm).



Γραμματικά λάθη ή λάθη στη μορφοποίηση δήθεν επίσημου εγγράφου, αν και η ΤΝ μπορεί να επιτρέψει στους απατεώνες να καλύψουν αυτά τα ελαττώματα αποτελεσματικά.



Ένας δικτυακός τόπος που φαίνεται επαγγελματικός αλλά δε διαθέτει επαληθευμένα στοιχεία επικοινωνίας ή στοιχεία από το μητρώο στο οποίο είναι εγγεγραμμένη μια εταιρεία.



Αφύσικος φωνητικός τονισμός, χωρίς παύσεις, που φαίνεται υπερβολικά ορθός ή μηχανικός. 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 μηχανική 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 μην «ταιριάζουν». Αυτά, είναι συχνά βίντεο που παράγονται από ΤΝ (deepfakes).

Βήματα για να προστατεύσετε τον εαυτό σας

1

Ποτέ μην αποκαλύπτετε προσωπικές ή τραπεζικές πληροφορίες:

Οι νόμιμες εταιρείες δε θα σας ζητήσουν ποτέ PINs, διαπιστευτήρια ηλεκτρονικής τραπεζικής (username/password) ή κωδικούς ασφαλείας μέσω ηλεκτρονικού ταχυδρομείου, μηνυμάτων, μέσων κοινωνικής δικτύωσης ή τηλεφώνου.

2

Να σκέφτεστε πριν ενεργήσετε:

Μην βιάζεστε να στείλετε χρήματα, να αποκαλύψετε πληροφορίες ή να «κάνετε κλικ» σε συνδέσμους- οι απατεώνες δημιουργούν σκόπιμα την αίσθηση του επείγοντος (π.χ. προβλήματα τεχνικής υποστήριξης από την τράπεζά σας, κλήσεις έκτακτης ανάγκης με τη συμμετοχή φίλων και μελών της οικογένειάς σας, απειλητική γλώσσα κ.λπ.). Σε περίπτωση αμφιβολιών, ακόμη και ήσσονος σημασίας, μην ενεργείτε. Να τερματίζετε την κλήση και να επαληθεύετε προσεκτικά την πηγή της πληροφορίας ή την ταυτότητα του καλούντος.

3

Ελέγχετε 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, αν φαίνεται να προέρχονται από έναν φίλο ή την οικογένειά 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. Να αναζητείτε ορθογραφικά λάθη, ύποπτες διευθύνσεις URL ή ελλείποντες δείκτες ασφαλείας (π.χ. να επαληθεύετε ότι ο σύνδεσμος δικτυακού τόπου περιλαμβάνει ένα «s» στο «HTTPS» για να βεβαιωθείτε ότι ο δικτυακός τόπος είναι ασφαλής και να ελέγχετε αν στην επωνυμία της εταιρείας λείπουν κάποια γράμματα ή υπάρχουν κάποια παραπάνω).
- Μην ανοίγετε συνδέσμους από ανεπιθύμητα μηνύματα, να εγκαθιστάτε μόνο αξιόπιστες εφαρμογές μέσω επίσημων app stores και μη «σαρώνετε» άγνωστους κωδικούς QR.
- Συμφωνήστε με την οικογένειά σας μια «λέξη-κλειδί»- μια μυστική φράση που να μπορείτε να χρησιμοποιείτε για να επιβεβαιώνετε την ταυτότητα κάποιου που με οικεία φωνή σας ζητά επείγοντως χρήματα και ισχυρίζεται ότι είναι μέλος της οικογένειας (π.χ. γονείς, αδελφή / αδελφός, παιδί).
- Χρησιμοποιείτε επαληθευμένα στοιχεία επικοινωνίας για να επικοινωνείτε απευθείας με μια εταιρεία ή ένα φυσικό πρόσωπο και ποτέ να μην βασίζεστε στα στοιχεία επικοινωνίας που παρέχονται από τον ύποπτο (π.χ. δική σας, ανεξάρτητη αναζήτηση και επιβεβαίωση της επωνυμίας της εταιρείας, χρήση αξιόπιστων μητρώων/καταλόγων με στοιχεία επιχειρήσεων, μέθοδοι επικοινωνίας που είχατε χρησιμοποιήσει και επιβεβαιώσει στο παρελθόν). Οι απατεώνες μπορεί να ισχυριστούν ότι είναι αδειοδοτημένοι ή να μιμούνται τον δικτυακό τόπο μιας αδειοδοτημένης εταιρείας. Να επαληθεύετε αν έχουν εκδοθεί προειδοποιήσεις από την αρμόδια εθνική αρχή της χώρας σας 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 ΕΕ (π.χ. να ανατρέχετε στο μητρώο της ESMA (www.esma.europa.eu/)).

4

Δίνετε προσοχή σε πιθανά τεχνάσματα με χρήση ΤΝ:

Καθώς η τεχνολογία ΤΝ εξελίσσεται, οι απάτες γίνονται πιο πειστικές από ποτέ- ακόμη και με τις καλύτερες δικλίδες ασφαλείας. Εάν έχετε την αίσθηση ότι πρόκειται για κάτι ασυνήθιστο ή εντοπίζετε κάποιο από τα προειδοποιητικά σημάδια που περιγράφονται παραπάνω, να διακόπτετε και να επανεκτιμάτε την κατάσταση.

5

Μην εγκαθιστάτε 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

Κρατάτε τις συσκευές και τους λογαριασμούς σας ασφαλείς:

Χρησιμοποιείτε ισχυρούς και μοναδικούς κωδικούς πρόσβασης, τηρείτε τους μυστικούς και αποφύγετε την επαναχρησιμοποίησή τους σε διαφορετικές πλατφόρμες. Ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων, όπου είναι δυνατόν. Δείτε μερικές συμβουλές για κωδικούς πρόσβασης εδώ (<https://www.esma.europa.eu/press-material/press-conferences-and-other-events/esma-press-conference-2022-03-23>). Εξασφαλίστε ότι οι εφαρμογές που χρησιμοποιείτε είναι επικαιροποιημένες και το λογισμικό προστασίας από ιούς είναι ενεργοποιημένο και επικαιροποιημένο.

7

Να είστε προσεκτικοί με επενδυτικές ευκαιρίες που είτε δεν τις περιμένετε είτε πρέπει να πραγματοποιηθούν μέσα σε στενά χρονικά περιθώρια:

Αν ακούγεται πολύ καλό για να είναι αληθινό, μάλλον έτσι είναι.

8

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 αν πέσετε 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.



Επικοινωνήστε με την τράπεζά σας ή τον πάροχο χρηματοπιστωτικών υπηρεσιών σας:

Ενημερώστε αμέσως την τράπεζά σας ή τον πάροχο χρηματοπιστωτικών υπηρεσιών σας μέσω επίσημων διαύλων επικοινωνίας, για να δείτε πώς μπορείτε να «παγώσετε» ή και να ανακαλέσετε τις συναλλαγές.



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.



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 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 άλλη μια προσπάθεια εξαπάτησης. Θυμηθείτε: το να σας εξαπατήσουν μια φορά δεν αποκλείει να εξαπατηθείτε ξανά.

ΕΙΔΗ ΔΙΑΔΙΚΤΥΑΚΩΝ ΑΠΑΤΩΝ ΠΟΥ ΥΠΟΣΤΗΡΙΖΟΝΤΑΙ ΑΠΟ ΤΗΝ ΤΝ



ΑΠΑΤΗ ΠΛΑΣΤΟΠΡΟΣΩΠΙΑΣ ΚΑΙ ΧΡΗΣΗ DEERFAKE

Λαμβάνετε μια απροσδόκητη κλήση από κάποιον που ισχυρίζεται ότι είναι η τράπεζά σας, δημόσια αρχή (π.χ. αστυνομία, φορολογική ή οικονομική αρχή κ.λπ.), διανομέας ασφαλιστικών προϊόντων, εταιρεία τεχνολογίας πληροφορικής ή ακόμη και μέλος της οικογένειάς σας. Ο καλών μπορεί να σας προτρέψει να μεταφέρετε χρήματα για να τα κρατήσετε ασφαλή, επικαλούμενος ύποπτη δραστηριότητα στο λογαριασμό σας ή το ασφαλιστήριο συμβόλαιό σας. Μπορεί επίσης να σας ζητηθεί να αποκαλύψετε τα τραπεζικά σας στοιχεία (π.χ. αριθμό κάρτας πληρωμής, διαπιστευτήρια ή κωδικούς πρόσβασης), να κάνετε κλικ σε έναν σύνδεσμο ή να εγκαταστήσετε ένα λογισμικό, με την πρόφαση άμεσης επίλυσης κάποιου δήθεν ζητήματος. Ο καλών μπορεί να χρησιμοποιήσει παραποιημένο αριθμό, ο οποίος συχνά αντιστοιχεί στον αριθμό τηλεφώνου της τράπεζάς σας ώστε να φαίνεται νόμιμος (πλαστογράφηση ταυτότητας- spoofing).

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

Τι μπορεί να συμβεί:

Με την αναφορά προσωπικών στοιχείων και τη δημιουργία αίσθησης επείγοντος, ο απατεώνας σας παρασύρει 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. 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 ο καλών γνωρίζει προσωπικές σας πληροφορίες δεν σημαίνει ότι είναι αξιόπιστος.



PHISHING ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ

Λαμβάνετε μήνυμα ηλεκτρονικού ταχυδρομείου ή μήνυμα που φαίνεται να προέρχεται από την τράπεζά σας ή από χρηματοπιστωτική 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 μοιάζει πανομοιότυπη με αυτή της ηλεκτρονικής σας τραπεζικής. Χωρίς να το συνειδητοποιείτε, εισάγετε τα στοιχεία σας σε έναν δικτυακό τόπο που έχει σχεδιαστεί για να κλέψει τα προσωπικά σας στοιχεία.

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

Τι 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 απάτη.



ΕΠΕΝΔΥΤΙΚΗ Ή ΑΣΦΑΛΙΣΤΙΚΗ ΑΠΑΤΗ

Βλέπετε μια διαφήμιση στα μέσα κοινωνικής δικτύωσης ή έναν δικτυακό τόπο που προωθεί μια «επενδυτική ευκαιρία περιορισμένου χρόνου με χαμηλού κινδύνους» ή μια «έκπτωση περιορισμένου χρόνου» σε ασφάλιση από 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, επικοινωνούν μαζί σας και ανακατευθύνετε σε μια πλατφόρμα ή ένα κανάλι ανταλλαγής μηνυμάτων όπου λαμβάνετε συμβουλές και έγγραφα με επαγγελματική όψη. Σας ενθαρρύνουν να επενδύσετε ένα μικρό ποσό, ακολουθούμενο από μεγαλύτερα ποσά, ή να πληρώσετε το ασφάλιστρο σε έναν λογαριασμό που φαίνεται να είναι ασφαλής.

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

Τι μπορεί να συμβεί:

Αφού προσπαθήσετε να αποσύρετε τα χρήματά σας ή να τα διεκδικήσετε, η επαφή σταματά να ανταποκρίνεται. Ανακαλύπτετε ότι η εταιρεία δεν υπάρχει ή ότι ο ασφαλιστικός κίνδυνος δεν καλύπτεται. Στη συνέχεια, συνειδητοποιείτε ότι έχετε στείλει χρήματα απευθείας σε έναν απατεώνα ως μέρος ενός δόλιου σχεδίου. Δυστυχώς, δεν μπορείτε να πάρετε πίσω τα χρήματά σας και τα προσωπικά και οικονομικά 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

Έχετε έρθει σε επαφή στα μέσα κοινωνικής δικτύωσης, εφαρμογές γνωριμιών ή μέσω τηλεφώνου/μηνύματος με κάποιο άτομο που δεν έχετε συναντήσει στην πραγματική ζωή. Το εν λόγω άτομο 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 σας ζητά 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.

Τι μπορεί να συμβεί:

Ο απατεώνας εξαγει όσο το δυνατόν περισσότερα χρήματα, στη συνέχεια διακόπτει κάθε επικοινωνία και εξαφανίζεται. Ο πλαστός επενδυτικός δικτυακός τόπος ή η εφαρμογή παύει να λειτουργεί, με αποτέλεσμα να μην μπορείτε να έχετε πρόσβαση στις 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 να σας ενοχοποιήσει για χρέη ή εγκλήματα που διαπράχθηκαν στο όνομά σας έως ότου αποδειχθεί το αντίθετο).



ΑΠΑΤΗ ΑΓΟΡΑΣ

Συναντάτε μια ελκυστική προσφορά για μια αγορά σε διαδικτυακή πλατφόρμα ηλεκτρονικού εμπορίου. Η εταιρεία πίσω από την εν λόγω προσφορά ζητά πληρωμή εκτός της επίσημης πλατφόρμας, ισχυριζόμενη ότι χρησιμοποιεί «ασφαλές σύστημα πληρωμών» και σας αποστέλλει σύνδεσμο για την ολοκλήρωση της αγοράς. Ο σύνδεσμος σας ανακατευθύνει σε μια πλαστή σελίδα ταυτοποίησης της τράπεζας που μιμείται τον επίσημο δικτυακό τόπο της τράπεζας 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 μιμηθούν το ύφος, το branding και το στυλ των πραγματικών εταιρειών. Σε ορισμένες περιπτώσεις, χρησιμοποιούν AI chatbots για να απαντήσουν σε ερωτήσεις και να κάνουν τη συμφωνία να φαίνεται πιο πιστευτή.

Τι μπορεί να συμβεί:

Η πληρωμή μέσω συνδέσμου τρίτου παρακάμπτει την προστασία της πλατφόρμας ηλεκτρονικού εμπορίου. Ο απατεώνας λαμβάνει τα στοιχεία σας για σύνδεση στον τραπεζικό σας λογαριασμό και κλέβει τα χρήματά σας.