

ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΨΗΦΙΑΚΟ ΚΟΣΜΟ

Πρακτικές λύσεις για
ηλικιωμένους με ανάλυση
μελετών περιπτώσεων
εγκλήματος στον κυβερνοχώρο



ΠΕΡΙΕΧΟΜΕΝΑ:

ΚΕΦΑΛΑΙΟ 1.

ΕΠΙΘΕΣΕΙΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

- Επίθεση μέσω δικτύων Wi-Fi (ιδιωτικών και δημόσιων)
- Επιθέσεις μέσω ηλεκτρονικού ταχυδρομείου
- Επιθέσεις σε αδύναμο κωδικό πρόσβασης
- Phishing
- Κακόβουλο λογισμικό και ιοί υπολογιστών

ΚΕΦΑΛΑΙΟ 2

ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΕΠΕΝΔΥΤΙΚΗ ΑΠΑΤΗ

- Χρηματοοικονομικές και επενδυτικές χειραγωγήσεις
- Προφανής αλτρουισμός: φιланθρωπική απάτη
- Δελεαστικές ψευδαισθήσεις: πλασματικά βραβεία και κληρώσεις
- Απάτες με ψηφιακά νομίσματα
- Διεθνής οικονομική απάτη

ΚΕΦΑΛΑΙΟ 3

ΚΟΙΝΩΝΙΚΗ ΧΕΙΡΑΓΩΓΗΣΗ ΚΑΙ ΣΥΝΑΙΣΘΗΜΑΤΙΚΗ ΕΞΑΠΑΤΗΣΗ

- Εξαπάτηση στις σχέσεις ανδρών-γυναικών
- Smishing - απάτες SMS
- Τηλεφωνικές απάτες που αφορούν ηλικιωμένους
- Απάτες που εκμεταλλεύονται συναισθηματικούς οικογενειακούς δεσμούς
- Απάτες που αφορούν ιατρικά προϊόντα

ΚΕΦΑΛΑΙΟ 4

ΑΠΑΤΗ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

- Απάτες με ταξίδια και εισιτήρια
- Απάτη με συνδρομές
- Απάτη με τη δημιουργία ψεύτικων ηλεκτρονικών καταστημάτων
- Αθέμιτες αγορές μέσω διαδικτυακών διαφημίσεων (αγορά)
- Αθέμιτες αγορές μέσω ιστοσελίδων αγγελιών (πώληση)

ΚΕΦΑΛΑΙΟ 5

ΙΠΑΡΑΠΟΙΗΣΗ ΤΗΣ ΤΑΥΤΟΤΗΤΑΣ ΚΑΙ ΕΚΜΕΤΑΛΛΕΥΣΗ ΤΗΣ ΕΜΠΙΣΤΟΣΥΝΗΣ ΤΟΥ ΚΟΙΝΟΥ

- Ισχυρισμοί εμπλοκής σε εγκληματικές ενέργειες
- Χειραγωγήσεις με την προσποίηση κρατικών οργάνων
- Χειραγώγηση με χρήση τεχνολογίας deepfake
- Απάτη με υπηρεσίες που υποδύονται κρατικούς φορείς
- Απάτη μέσω πλαστών λογαριασμών



Η σύγχρονη τεχνολογία ενσωματώνεται ολοένα και περισσότερο στη ζωή μας, γεγονός που υπογραμμίζει τη ζωτική σημασία της ασφάλειας στον εικονικό κόσμο. Το ζήτημα αυτό είναι ιδιαίτερα σημαντικό για τους ηλικιωμένους, οι οποίοι συχνά δεν είναι τόσο ικανοί στις σύγχρονες τεχνολογίες και είναι περισσότερο εκτεθειμένοι σε απειλές στον κυβερνοχώρο. Το ηλεκτρονικό βιβλίο "Ασφάλεια στον ψηφιακό κόσμο. «Πρακτικές λύσεις για ηλικιωμένους με ανάλυση περιπτώσεων εγκλημάτων στον κυβερνοχώρο» προσφέρει τις απαραίτητες γνώσεις και τα εργαλεία που υποστηρίζουν τους ηλικιωμένους στην προστασία τους από τις απειλές στο Διαδίκτυο.

Αυτό το ηλεκτρονικό βιβλίο δημιουργήθηκε στο πλαίσιο του έργου «Cyber Safe Senior» με αριθμό 2023-1-PL01-KA220-ADU-000160325 που χρηματοδοτείται από την Ευρωπαϊκή Ένωση. Το έργο αυτό αποσκοπεί στην ευαισθητοποίηση των ηλικιωμένων σε κανόνες ασφάλειας στο Διαδίκτυο και στην ανάπτυξη των ψηφιακών τους δεξιοτήτων. Ανταποκρινόμενο στην αυξανόμενη ζήτηση για εκπαίδευση στην ασφαλή χρήση του Διαδικτύου, το έργο παρέχει πρακτικές συμβουλές, μελέτες περιπτώσεων και αναλύσεις για να βοηθήσει τους ηλικιωμένους να αποφύγουν τους κινδύνους και να αντιδράσουν σε καταστάσεις έκτακτης ανάγκης.

Το ηλεκτρονικό βιβλίο περιέχει κεφάλαια για διάφορες πτυχές της ασφάλειας στον κυβερνοχώρο, όπως οι επιθέσεις στον κυβερνοχώρο, η οικονομική απάτη, η κοινωνική χειραγώγηση, η απάτη στις διαδικτυακές συναλλαγές και η κλοπή ταυτότητας. Κάθε κεφάλαιο περιέχει μελέτες περιπτώσεων που απεικονίζουν τις δραστηριότητες των κυβερνοεγκληματιών και δείχνουν πώς να αμυνθείτε αποτελεσματικά εναντίον τους. Χάρη στις πρακτικές συμβουλές του, αυτό το ηλεκτρονικό βιβλίο αποτελεί πολύτιμη πηγή γνώσεων για τους ηλικιωμένους που θέλουν να χρησιμοποιούν με ασφάλεια τις σύγχρονες τεχνολογίες.



Στο πλαίσιο του έργου, έχουμε ετοιμάσει μοναδικό υλικό που όχι μόνο παρέχει πολύτιμες γνώσεις, αλλά και εμπλέκει και ενδιαφέρει τους χρήστες. Ένα από τα βασικά στοιχεία είναι τα επαγγελματικά προετοιμασμένα βίντεο κλιπ - πέντε δυναμικές, οπτικά ελκυστικές ταινίες που απεικονίζουν πραγματικές καταστάσεις, πιθανές απειλές και κατάλληλες αντιδράσεις σε κινδύνους με προσιτό τρόπο. Οι ταινίες αυτές αποσκοπούν στην εκπαίδευση μέσω πρακτικών παραδειγμάτων, γεγονός που καθιστά τις παρεχόμενες πληροφορίες ευκολότερα κατανοητές και απομνημονεύσιμες.

Έχουμε επίσης ετοιμάσει ένα διαδραστικό πακέτο κουίζ. Αυτά τα κουίζ έχουν αναπτυχθεί με τρόπο που δεν είναι μόνο εκπαιδευτικός, αλλά και ενδιαφέρων και διασκεδαστικός, ώστε οι συμμετέχοντες να μπορούν να δοκιμάσουν τις γνώσεις τους διασκεδάζοντας. Αυτή η μορφή εμπλοκής των αποδεκτών όχι μόνο καθιστά το μήνυμα πιο ελκυστικό, αλλά αυξάνει και την αποτελεσματικότητά του, εξασφαλίζοντας ότι οι γνώσεις που θα αποκτηθούν θα παραμείνουν σε αυτούς για μεγαλύτερο χρονικό διάστημα.

Αυτά τα στοιχεία, που συνδυάζουν την εκπαίδευση και την ψυχαγωγία, καθιστούν το έργο όχι μόνο πολύτιμο, αλλά και ελκυστικό και ευχάριστο για κάθε παραλήπτη.



ΒΙΝΤΕΟ:

Συναισθηματική χειραγώγηση – φιλανθρωπική απάτη

Οικονομική χειραγώγηση

Σπάσιμο κωδικού πρόσβασης

Πλαστοπροσωπία και deepfake

Παγίδες ηλεκτρονικών αγορών

ΚΟΥΙΖ:

Απάτες μηνυμάτων SMS: Πόσο καλά μπορείτε να προστατευτείτε;

Επιθέσεις μέσω ηλεκτρονικού ταχυδρομείου, απάτες phishing, οι κίνδυνοι από τη χρήση αδύναμων κωδικών πρόσβασης, καθώς και κακόβουλο λογισμικό και ιοί υπολογιστών.

Τεχνολογίες πλαστοπροσωπίας και deepfake.

Αγορές και πωλήσεις μέσω διαδικτύου: Μπορείτε να εντοπίσετε τις απειλές;

Οικονομική χειραγώγηση και εκμετάλλευση των συναισθημάτων των ηλικιωμένων.

ΚΕΦΑΛΑΙΟ 1

ΕΠΙΘΕΣΕΙΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Στον σημερινό ψηφιακό κόσμο, οι ηλικιωμένοι είναι όλο και πιο ευάλωτοι σε κυβερνοεπιθέσεις που απειλούν την ηλεκτρονική τους ασφάλεια. Σε αυτό το κεφάλαιο, θα συζητήσουμε τις μεθόδους επίθεσης και τα μέτρα ασφαλείας που μπορούν να βοηθήσουν τους ηλικιωμένους να προστατευτούν από τις απειλές.

Οι επιθέσεις Wi-Fi περιλαμβάνουν τόσο ιδιωτικά όσο και δημόσια δίκτυα, τα οποία μπορούν να χρησιμοποιηθούν από εγκληματίες για την υποκλοπή δεδομένων. Είναι σημαντικό να κατανοήσετε τους κινδύνους που εγκυμονεί η χρήση δημόσιων hotspots και να είστε σε θέση να αναγνωρίζετε ασφαλή δίκτυα Wi-Fi.

Οι επιθέσεις μέσω ηλεκτρονικού ταχυδρομείου, όπως το phishing, στέλνουν ψεύτικα μηνύματα που φαίνεται να προέρχονται από αξιόπιστα ιδρύματα, προκειμένου να αποκτήσουν προσωπικές πληροφορίες. Οι αδύναμοι κωδικοί πρόσβασης είναι ένα άλλο πρόβλημα που μπορεί να διευκολύνει την πρόσβαση σε ιδιωτικούς λογαριασμούς.

Το κακόβουλο λογισμικό και οι ιοί αποτελούν σοβαρό κίνδυνο που μπορούν να διεισδύσουν σε συσκευές και να υποκλέψουν δεδομένα. Θα συζητήσουμε μεθόδους προστασίας, όπως οι τακτικές ενημερώσεις, το λογισμικό προστασίας από ιούς και η αποφυγή ύποπτων συνδέσμων.

Θα επικεντρωθούμε σε πρακτικές συμβουλές και στρατηγικές που θα βοηθήσουν τους ηλικιωμένους να κατανοήσουν και να αποφύγουν αυτούς τους κινδύνους και να προστατεύσουν τα δεδομένα και την ιδιωτική τους ζωή στο διαδίκτυο.

Επίθεση μέσω δικτύων Wi-Fi (ιδιωτικών και δημόσιων)

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Τα δημόσια δίκτυα Wi-Fi επιτρέπουν δωρεάν πρόσβαση στο Διαδίκτυο και θεωρούνται μεγάλη ευκολία. Είναι διαθέσιμα σε πολλούς δημόσιους χώρους, όπως βιβλιοθήκες, καφετέριες, αεροδρόμια, εστιατόρια και ξενοδοχεία. Ωστόσο, το ανοιχτό Wi-Fi θεωρείται εδώ και καιρό ένα επικίνδυνο διαδικτυακό περιβάλλον για τις πληροφορίες σας. Ενώ κανένα δίκτυο Wi-Fi δεν είναι εντελώς ακίνδυνο, η ασφάλεια των προσωπικών σας δεδομένων εξαρτάται σε μεγάλο βαθμό από τον τύπο του δικτύου Wi-Fi. Οι επιθέσεις σε δίκτυα Wi-Fi, τόσο ιδιωτικά όσο και δημόσια, μπορούν να λάβουν πολλές μορφές.

Ακολουθούν πέντε τύποι τέτοιων επιθέσεων:

Σε μια επίθεση MitM, ο επιτιθέμενος υποκλέπτει την επικοινωνία μεταξύ δύο συσκευών σε ένα δίκτυο Wi-Fi προσποιούμενος ένα από τα μέρη. Χάρη σε αυτό, μπορεί να συλλάβει δεδομένα όπως συνδέσεις, κωδικούς πρόσβασης ή τραπεζικές πληροφορίες χωρίς να το γνωρίζουν οι χρήστες.

Σε μια επίθεση Evil Twin, ο επιτιθέμενος δημιουργεί ένα ψεύτικο δίκτυο Wi-Fi που, με την πρώτη ματιά, μοιάζει πανομοιότυπο με ένα νόμιμο δίκτυο. Οι χρήστες, νομίζοντας ότι συνδέονται σε ένα πραγματικό δίκτυο, συνδέονται σε ένα ψεύτικο δίκτυο, επιτρέποντας στον επιτιθέμενο να υποκλέψει οποιαδήποτε δεδομένα μεταδίδονται.

**Επίθεση Man
in the middle
(MitM)**

**Επίθεση Evil
Twin type**

Επίθεση μέσω δικτύων Wi-Fi (ιδιωτικών και δημόσιων)

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Επίθεση Brute Force σε κωδικό πρόσβασης Wi-Fi

Ο επιτιθέμενος προσπαθεί να μαντέψει τον κωδικό πρόσβασης Wi-Fi χρησιμοποιώντας προγράμματα που δοκιμάζουν συστηματικά διαφορετικούς συνδυασμούς χαρακτήρων. Όταν ο κωδικός πρόσβασης είναι αδύναμος ή πολύ απλός, αυτή η επίθεση μπορεί να είναι αποτελεσματική, επιτρέποντας μη εξουσιοδοτημένη πρόσβαση στο δίκτυο.

Επίθεση τύπου Packet Sniffing

Σε αυτή την επίθεση, ο επιτιθέμενος χρησιμοποιεί ειδικό λογισμικό για να καταγράφει και να αναλύει τα πακέτα δεδομένων που αποστέλλονται μέσω ενός δικτύου Wi-Fi. Ακόμη και σε ένα ασφαλές δίκτυο, εάν τα δεδομένα δεν είναι σωστά κρυπτογραφημένα, μπορούν να διαβαστούν και να χρησιμοποιηθούν.

Επίθεση άρνησης παροχής υπηρεσιών (DoS)

Σε μια επίθεση DoS, ο επιτιθέμενος στέλνει μεγάλο αριθμό άκυρων αιτήσεων ή ψευδών σημάτων απενεργοποίησης εξουσιοδότησης σε ένα σημείο πρόσβασης Wi-Fi, προκαλώντας συμφόρηση του δικτύου. Αυτό μπορεί να απενεργοποιήσει προσωρινά ή να διακόψει το δίκτυο, εμποδίζοντας τους χρήστες να χρησιμοποιήσουν τη σύνδεση.

Επίθεση μέσω δικτύων Wi-Fi (ιδιωτικών και δημόσιων)



ΣΥΝΕΠΕΙΕΣ:

Η χρήση της δημόσιας και δωρεάν πρόσβασης στο Διαδίκτυο ενέχει διάφορους κινδύνους που μπορούν να θέσουν σε κίνδυνο ευαίσθητα δεδομένα και την ασφάλεια στο διαδίκτυο. Είναι σημαντικό να γνωρίζετε ποιοι είναι οι κίνδυνοι κατά τη χρήση δημόσιων δικτύων Wi-Fi.

Συνέπειες που προκύπτουν από διάφορους τύπους επιθέσεων στο δίκτυο Wi-Fi:

01 Man-in-the-Middle (MitM)

Οι ηλίκιωμένοι μπορεί να πέσουν θύματα κλοπής ταυτότητας ή να χάσουν τις αποταμιεύσεις τους εάν κάποιος εγκληματίας υποκλέψει τα στοιχεία σύνδεσης σε τραπεζικούς λογαριασμούς ή ιστότοπους κοινωνικής δικτύωσης.

02 Evil Twin

Οι χρήστες μπορεί να παρέχουν εν αγνοία τους τα στοιχεία σύνδεσής τους, αριθμούς πιστωτικών καρτών ή άλλες ευαίσθητες πληροφορίες, νομίζοντας ότι χρησιμοποιούν ένα ασφαλές δίκτυο.

Επίθεση μέσω δικτύων Wi-Fi (ιδιωτικών και δημόσιων)



ΣΥΝΕΠΕΙΕΣ:

03 Brute Force

Εάν οι ηλικιωμένοι χρησιμοποιούν απλούς ή επαναλαμβανόμενους κωδικούς πρόσβασης, οι εγκληματίες μπορούν να αποκτήσουν πρόσβαση στα δίκτυά τους, γεγονός που μπορεί να οδηγήσει σε παραβιάσεις της ιδιωτικής ζωής καθώς και σε αυξημένους λογαριασμούς διαδικτύου.

04 Ανίχνευση πακέτων (Packet Sniffing)

Οι ηλικιωμένοι μπορεί να κινδυνεύουν να διαρρεύσουν ιδιωτικές πληροφορίες, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, κωδικούς πρόσβασης και προσωπικές πληροφορίες, εάν οι επιτιθέμενοι υποκλέψουν μη κρυπτογραφημένα δεδομένα.

05 Άρνηση παροχής υπηρεσιών (DoS)

Μια επίθεση DoS μπορεί να εμποδίσει τους ηλικιωμένους να χρησιμοποιούν το Διαδίκτυο, κάτι που είναι ιδιαίτερα προβληματικό για τους ανθρώπους που βασίζονται στην τεχνολογία για να επικοινωνούν με τους αγαπημένους τους ή να διεκπεραιώνουν καθημερινά ζητήματα.

Επίθεση μέσω δικτύων Wi-Fi (ιδιωτικών και δημόσιων)



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Ο Φίλιππος αποφάσισε να δειπνήσει σε ένα κοντινό εστιατόριο. Χρησιμοποιώντας το δημόσιο Wi-Fi του εστιατορίου, άνοιξε το email του για να ελέγξει τα τελευταία νέα. Δυστυχώς, αγνοώντας τους κινδύνους που σχετίζονται με τα δημόσια δίκτυα Wi-Fi, δεν ασφάλισε τη σύνδεσή του. Ως αποτέλεσμα μιας επίθεσης Man-in-the-Middle, ο εγκληματίας υπέκλεψε τα στοιχεία σύνδεσης στο email του, με αποτέλεσμα τη μη εξουσιοδοτημένη πρόσβαση στο λογαριασμό του και την πιθανή διαρροή εμπιστευτικών πληροφοριών.



Η ιστορία του Φίλιππου δεν είναι ασυνήθιστη και δεν συμβαίνει μόνο σε ηλικιωμένους. Ωστόσο, αυτό μπορεί να διορθωθεί. Δείτε τις συμβουλές μου παρακάτω.

Συνέπειες από την μη αναγνώριση της απειλής:

ΒΗΜΑ 1: Επίθεση στο δίκτυο Wi-Fi ενός εστιατορίου σε δημόσιο χώρο

Ο Φίλιππος χρησιμοποιεί το δημόσιο δίκτυο Wi-Fi στο εστιατόριο για να ελέγξει το ηλεκτρονικό του ταχυδρομείο. Η έλλειψη κατάλληλων μέτρων ασφαλείας, όπως η έλλειψη ελέγχου ταυτότητας δύο παραγόντων, επέτρεψε στον εγκληματία να υποκλέψει τα στοιχεία σύνδεσης.

ΒΗΜΑ 2: Μη εξουσιοδοτημένη πρόσβαση στο email

Ως αποτέλεσμα της επίθεσης, ο εγκληματίας απέκτησε μη εξουσιοδοτημένη πρόσβαση στο λογαριασμό ηλεκτρονικού ταχυδρομείου του Φίλιππου, αποκτώντας ευαίσθητες πληροφορίες, όπως ιδιωτική αλληλογραφία, επαφές και άλλα εμπιστευτικά δεδομένα.

ΒΗΜΑ 3: Διαρροή εμπιστευτικών πληροφοριών

Η κατάληψη ενός λογαριασμού ηλεκτρονικού ταχυδρομείου μπορεί να οδηγήσει σε πιθανή διαρροή εμπιστευτικών πληροφοριών του Φίλιππου, γεγονός που μπορεί να απειλήσει την ιδιωτική ζωή και την ασφάλειά του. Ένας εγκληματίας θα μπορούσε να χρησιμοποιήσει αυτά τα δεδομένα για απάτη, κλοπή ταυτότητας ή άλλες παράνομες δραστηριότητες.

ΒΗΜΑ 4: Συναισθηματικές συνέπειες

Ο Φίλιππος βίωσε άγχος, ανησυχία και απώλεια εμπιστοσύνης στη χρήση δημόσιων δικτύων Wi-Fi. Επιπλέον, η ανάγκη αλλαγής των κωδικών πρόσβασης, παρακολούθησης των λογαριασμών και λήψης μέτρων για την αποτροπή περαιτέρω επιθέσεων μπορεί να απαιτήσει επιπλέον χρόνο και προσπάθεια.

Επίθεση μέσω δικτύων Wi-Fi (ιδιωτικών και δημόσιων)



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ

Μπορείτε να αποφύγετε αυτές τις συνέπειες ακολουθώντας τις παρακάτω μεθόδους για να προστατευτείτε από επιθέσεις μέσω Wi-Fi.



Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης:

Ασφαλίστε το δίκτυο Wi-Fi με έναν ισχυρό, μοναδικό κωδικό πρόσβασης. Θυμηθείτε να μην χρησιμοποιείτε προφανείς κωδικούς πρόσβασης, όπως όνομα, επώνυμο, ημερομηνία γέννησης ή άλλους εύκολους συνδυασμούς χαρακτήρων.

Ενημέρωση λογισμικού:

Ενημερώστε τακτικά το λογισμικό του δρομολογητή σας για να προστατεύεστε από τα γνωστά τρωτά σημεία ασφαλείας.



Επίθεση μέσω δικτύων Wi-Fi (ιδιωτικών και δημόσιων)



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Ενεργοποίηση κρυπτογράφησης:

Βεβαιωθείτε ότι όλα τα δεδομένα κατά τη μεταφορά είναι κρυπτογραφημένα, ακόμη και σε ασφαλή δίκτυα Wi-Fi.

Αποφύγετε τα δημόσια δίκτυα Wi-Fi:

Εάν είναι δυνατόν, αποφύγετε τη χρήση δημόσιων δικτύων Wi-Fi για τη μετάδοση ευαίσθητων δεδομένων. Εάν πρέπει να τα χρησιμοποιήσετε, χρησιμοποιήστε ένα εικονικό ιδιωτικό δίκτυο (VPN).



Παρακολουθήστε το δίκτυό σας:

Ελέγχετε τακτικά τις συσκευές που είναι συνδεδεμένες στο δίκτυο Wi-Fi για να εντοπίζετε γρήγορα μη εξουσιοδοτημένες συσκευές.

Επιθέσεις ηλεκτρονικού ταχυδρομείου



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Οι επιθέσεις μέσω ηλεκτρονικού ταχυδρομείου είναι κακόβουλες προσπάθειες απόκτησης μη εξουσιοδοτημένης πρόσβασης σε συστήματα ή πληροφορίες μέσω λογαριασμών ηλεκτρονικού ταχυδρομείου. Υπάρχουν πολλοί τύποι επιθέσεων στους οποίους οι ηλικιωμένοι είναι ευάλωτοι. Αξίζει να εξοικειωθείτε με ορισμένες από τις πιο συνηθισμένες.

Οι κύριοι τύποι επιθέσεων σε θυρίδες ηλεκτρονικού ταχυδρομείου:

Το phishing είναι μια κοινή μέθοδος κατά την οποία οι απατεώνες στέλνουν ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχονται από αξιόπιστες πηγές (π.χ. τράπεζες, κυβερνητικά γραφεία).

Δράση των απατεώνων:

- **Πεύτικοι σύνδεσμοι και συνημμένα αρχεία:** Οι απατεώνες στέλνουν μηνύματα με συνδέσμους σε ψεύτικους ιστότοπους ή συνημμένα αρχεία που έχουν σχεδιαστεί για να αποκτήσουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών.
- **Δημιουργία αίσθησης επείγοντος:** Τα μηνύματα ηλεκτρονικού ταχυδρομείου συχνά περιλαμβάνουν πληροφορίες σχετικά με προβλήματα με το λογαριασμό σας, την ανάγκη να ενημερώσετε αμέσως τις πληροφορίες σας ή προειδοποιήσεις για ύποπτη δραστηριότητα.

Το spear phishing είναι μια πιο προηγμένη μορφή phishing κατά την οποία οι επιθέσεις είναι εξατομικευμένες και απευθύνονται σε συγκεκριμένα άτομα.

Δράση των απατεώνων:

- **Εξατομικευμένα μηνύματα:** Οι απατεώνες συλλέγουν πληροφορίες σχετικά με το θύμα από δημόσιες πηγές, όπως τα μέσα κοινωνικής δικτύωσης, για να δημιουργήσουν νόμιμα μηνύματα ηλεκτρονικού ταχυδρομείου.
- **Προσωποποίηση φίλων:** Τα μηνύματα αυτά συχνά εμφανίζονται να αποστέλλονται από κάποιον που το θύμα γνωρίζει (π.χ. συνάδελφο από τη δουλειά).

Επιθέσεις
Phishing

Επιθέσεις
Spear Phishing

Επιθέσεις ηλεκτρονικού ταχυδρομείου



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Επιθέσεις Email Spoofing

Η πλαστογράφηση ηλεκτρονικού ταχυδρομείου είναι μια τεχνική κατά την οποία οι απατεώνες αλλάζουν τις επικεφαλίδες του ηλεκτρονικού ταχυδρομείου για να το κάνουν να φαίνεται ότι έχει σταλεί από μια αξιόπιστη πηγή.

Δράση των απατεώνων:

- Ψεύτικες επικεφαλίδες: Οι απατεώνες αλλάζουν τις επικεφαλίδες των μηνυμάτων για να φαίνεται ότι έχουν σταλεί από μια πραγματική διεύθυνση, όπως από έναν φίλο, προϊστάμενο ή αξιόπιστο φορέα.
- Απόκρυψη ταυτότητας: Τα μηνύματα φαίνονται αυθεντικά, καθιστώντας δύσκολο τον εντοπισμό τους από τους παραλήπτες και τα συστήματα anti-spam.

Διανομή κακόβουλου λογισμικού και ransomware

Οι εγκληματίες του κυβερνοχώρου συχνά καταλαμβάνουν λογαριασμούς ηλεκτρονικού ταχυδρομείου για να διανέμουν κακόβουλο λογισμικό.

Δράση των απατεώνων:

- Μολυσμένα συνημμένα αρχεία: Τα μηνύματα ηλεκτρονικού ταχυδρομείου περιέχουν συνημμένα αρχεία που, όταν ανοίγονται, εγκαθιστούν κακόβουλο λογισμικό στον υπολογιστή του θύματος.
- Κακόβουλοι σύνδεσμοι: Τα μηνύματα ηλεκτρονικού ταχυδρομείου ενδέχεται να περιέχουν συνδέσμους προς ιστότοπους που κατεβάζουν και εγκαθιστούν αυτόματα κακόβουλο λογισμικό στον υπολογιστή σας

Επιθέσεις Man- in-the-middle (MITM) σε επικοινωνίες ηλεκτρονικού ταχυδρομείου

Μια επίθεση MITM συμβαίνει όταν ένας επιτιθέμενος υποκλέπτει και μεταδίδει δεδομένα μεταξύ δύο μερών χωρίς να το γνωρίζει κανένα από τα δύο μέρη.

Δράση των απατεώνων:

- Υποκλοπή δεδομένων: Χάκερς υποκλέπτουν επικοινωνίες για να αποκτήσουν ευαίσθητες πληροφορίες, όπως διαπιστευτήρια σύνδεσης ή εταιρικά μυστικά.
- Spoofing: Μπορούν επίσης να στέλνουν μηνύματα για λογαριασμό ενός μέρους, επιτρέποντας τη χειραγώγηση των επικοινωνιών.

Επιθέσεις ηλεκτρονικού ταχυδρομείου



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Κατάληψη
ηλεκτρονικού
ή
ταχυδρομείου
ή επιθέσεις
κατάληψης

Επιθέσεις
υποκλοπής
διαπιστευτηρί-
ων

Οι χάκερ προσπαθούν να αποκτήσουν πρόσβαση στο λογαριασμό ηλεκτρονικού ταχυδρομείου σας μαντεύοντας τον κωδικό πρόσβασής σας ή χρησιμοποιώντας άλλες μεθόδους.

Δράση των απατεώνων:

- Υπολογισμός κωδικού πρόσβασης: για να υποθέσουν τον κωδικό πρόσβασής σας.
- Phishing: Μπορούν επίσης να χρησιμοποιήσουν phishing ή άλλες τεχνικές κοινωνικής μηχανικής για να σας ξεγελάσουν και να σας οδηγήσουν στην παροχή των στοιχείων σύνδεσής σας.

Οι χάκερ αποκτούν πρόσβαση σε λογαριασμούς ηλεκτρονικού ταχυδρομείου εξαπατώντας τους χρήστες ώστε να δώσουν στοιχεία σύνδεσης.

Δράση των απατεώνων:

- Phishing: Ο χρήστης λαμβάνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου με ένα ψεύτικο αίτημα για στοιχεία σύνδεσης.
- Κοινωνική επιρροή: Οι χάκερ προσποιούνται ότι είναι κάποιος άλλος και ζητούν όνομα χρήστη και κωδικό πρόσβασης, χρησιμοποιώντας συχνά πληροφορίες από τα μέσα κοινωνικής δικτύωσης για να κάνουν το αίτημά τους πιο αξιόπιστο.

Επιθέσεις ηλεκτρονικού ταχυδρομείου



ΣΥΝΕΠΕΙΕΣ:

Οι επιθέσεις μέσω ηλεκτρονικού ταχυδρομείου έχουν διάφορες σοβαρές συνέπειες που μπορούν να απειλήσουν τα εμπιστευτικά δεδομένα και την ασφάλεια στο διαδίκτυο. Για να προστατευτείτε, είναι σημαντικό να τις αναγνωρίζετε.

01 Επιθέσεις Phishing

- Κλοπή ταυτότητας: Αυτό οδηγεί σε κλοπή ταυτότητας.
- Οικονομικές απώλειες: Η διαβίβαση δεδομένων μπορεί να οδηγήσει σε μη εξουσιοδοτημένες συναλλαγές και οικονομικές απώλειες.

02 Επιθέσεις Spear Phishing

- Παραβίαση της ιδιωτικής ζωής: Οι ηλικιωμένοι μπορεί να μοιραστούν εμπιστευτικές πληροφορίες νομίζοντας ότι επικοινωνούν με κάποιον που εμπιστεύονται.
- Οικονομικές και συναισθηματικές απώλειες: Μπορούν να χειραγωγηθούν ώστε να προβούν σε ενέργειες που οδηγούν σε οικονομικές και συναισθηματικές απώλειες.

03 Επιθέσεις Email Spoofing

- Παραβίαση ασφαλείας: Οι ηλικιωμένοι μπορεί να ενεργήσουν με βάση ψευδείς πληροφορίες, οδηγώντας σε παραβιάσεις της ασφαλείας.
- Εγκατάσταση κακόβουλου λογισμικού: Το κλικ σε συνδέσμους ή συνημμένα αρχεία μπορεί να οδηγήσει σε εγκατάσταση κακόβουλου λογισμικού.

Επιθέσεις ηλεκτρονικού ταχυδρομείου



ΣΥΝΕΠΕΙΕΣ:

04 Διανομή κακόβουλου λογισμικού και ransomware

- Ζημιά στο σύστημα: Το κακόβουλο λογισμικό μπορεί να προκαλέσει ζημιά στον υπολογιστή σας και να τον καταστήσει άχρηστο.
- Ransomware: Το κακόβουλο λογισμικό μπορεί να κρυπτογραφήσει αρχεία στον υπολογιστή σας και να ζητήσει λύτρα για να τα ξεκλειδώσει.

05 Επιθέσεις Man-in-the-middle (MITM) σε επικοινωνίες ηλεκτρονικού ταχυδρομείου

- Απώλεια της εμπιστευτικότητας: Οι ηλικιωμένοι μπορεί να αποκαλύψουν εν αγνοία τους εμπιστευτικές πληροφορίες.
- Χειραγώγηση: Οι επιτιθέμενοι μπορούν να παραπλανήσουν και τις δύο πλευρές της επικοινωνίας.

06 Κατάληψη ηλεκτρονικού ταχυδρομείου ή επιθέσεις κατάληψης

- Κλοπή ταυτότητας: Οι χάκερ μπορούν να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες και να τις χρησιμοποιήσουν για να κλέψουν την ταυτότητά σας.
- Αποστολή ανεπιθύμητης αλληλογραφίας: Οι παραβιασμένοι λογαριασμοί μπορούν να χρησιμοποιηθούν για την αποστολή ανεπιθύμητων μηνυμάτων και κακόβουλου λογισμικού.

07 Επιθέσεις υποκλοπής διαπιστευτηρίων

- Απώλεια πρόσβασης: Οι ηλικιωμένοι ενδέχεται να χάσουν την πρόσβαση στους λογαριασμούς ηλεκτρονικού ταχυδρομείου τους.
- Παραβίαση απορρήτου: Οι χάκερ μπορούν να αποκτήσουν πρόσβαση σε προσωπικές πληροφορίες και αλληλογραφία.

Επιθέσεις ηλεκτρονικού ταχυδρομείου



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Ο Ντάνιελ χρησιμοποιεί τακτικά το ηλεκτρονικό ταχυδρομείο για να κρατάει επαφή με την οικογένειά του. Ο γιος του, ο οποίος ζούσε στο εξωτερικό, του έστελνε συχνά ενημερωτικά μηνύματα. Μια μέρα, ο Ντάνιελ έλαβε ένα e-mail που φαινόταν να έχει σταλεί από τον γιο του.

Από: tom@example.com

Θέμα: Φωτογραφίες από τις διακοπές!

Γεια σου μπαμπά, ελπίζω να είναι όλα καλά με σένα. Ήθελα να μοιραστώ μαζί σου φωτογραφίες από το τελευταίο μας ταξίδι.

Κάνε κλικ στον παρακάτω σύνδεσμο για να τις δεις.
[Δείτε τις φωτογραφίες]

Με τους καλύτερους χαιρετισμούς, ο γιος σου

Συνέπειες της μη αναγνώρισης της απειλής:

ΒΗΜΑ 1: Κάνοντας κλικ στο σύνδεσμο

Ο Ντάνιελ, νομίζοντας ότι είχε λάβει μήνυμα από τον γιο του, έκανε κλικ στον σύνδεσμο.

ΒΗΜΑ 2: Μόλυνση του υπολογιστή σας

Κάνοντας κλικ στον σύνδεσμο, κατέβηκε κακόβουλο λογισμικό που εγκαταστάθηκε στον υπολογιστή του Ντάνιελ. Τέτοιο λογισμικό μπορεί να παρακολουθεί τη διαδικτυακή σας δραστηριότητα, να κλέβει κωδικούς πρόσβασης και άλλες εμπιστευτικές πληροφορίες.

Επιθέσεις ηλεκτρονικού ταχυδρομείου



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ

Το παράδειγμα του Ντάνιελ δείχνει πόσο επικίνδυνες μπορεί να είναι οι επιθέσεις σε θυρίδες ηλεκτρονικού ταχυδρομείου.

Ο σύνδεσμος στο μήνυμα οδηγούσε σε έναν ιστότοπο που κατέβαζε και εγκαθιστούσε αυτόματα κακόβουλο λογισμικό στον υπολογιστή του.



ΒΗΜΑ 3: Μόλυνση του υπολογιστή σας

Το κακόβουλο λογισμικό κατάφερε να αποκτήσει πρόσβαση στα προσωπικά δεδομένα του Ντάνιελ, συμπεριλαμβανομένων αριθμών τραπεζικών λογαριασμών, κωδικών πρόσβασης σε διάφορες υπηρεσίες και προσωπικών εγγράφων.

ΒΗΜΑ 4: Συναισθηματικό άγχος

Ο Ντάνιελ αισθάνθηκε εξαπατημένος και ανησυχούσε ότι κάποιος υποδυόταν τον γιο του. Το περιστατικό του προκάλεσε μεγάλο άγχος και ανησυχία.

Επιθέσεις ηλεκτρονικού ταχυδρομείου



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ

Μπορείτε να αποφύγετε αυτές τις συνέπειες ακολουθώντας τις παρακάτω μεθόδους για να προστατευτείτε από επιθέσεις ηλεκτρονικού ταχυδρομείου.



Να είστε προσεκτικοί όταν ανοίγετε email:

Ο Ντάνιελ πρέπει να είναι προσεκτικός όταν θα ανοίγει τα e-mail:

Δράση:

- Ελέγχετε πάντα τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα, ιδίως όταν το μήνυμα περιέχει συνδέσμους ή συνημμένα αρχεία.
- Διαβάστε προσεκτικά τα μηνύματα και δώστε προσοχή σε ασυνήθιστα αιτήματα και γραμματικά λάθη.

Ενημερώσεις λογισμικού κατά των ιών:

Ο Ντάνιελ θα πρέπει να βεβαιωθεί ότι ο υπολογιστής και το τηλέφωνό του διαθέτουν τακτικά ενημερωμένο λογισμικό προστασίας από ιούς.

Δράση:

- Τακτική ενημέρωση του λογισμικού προστασίας από ιούς και σάρωση του συστήματος.
- Εγκατάσταση των πιο πρόσφατων ενημερώσεων του λειτουργικού συστήματος και του προγράμματος περιήγησης στο διαδίκτυο.



Επιθέσεις ηλεκτρονικού ταχυδρομείου



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ

Έλεγχος ταυτότητας δύο παραγόντων (2FA):

Ο Ντάνιελ θα πρέπει να εξετάσει το ενδεχόμενο ενεργοποίησης ενός πρόσθετου επιπέδου ασφάλειας με τη χρήση ελέγχου ταυτότητας δύο παραγόντων (2FA) σε όλους τους σχετικούς λογαριασμούς. Αυτή η προσέγγιση αυξάνει σημαντικά το επίπεδο ασφάλειας ακόμη και αν αποκαλυφθεί ο κωδικός πρόσβασης.

Ενέργεια:

Ο χρήστης θα πρέπει να έχει τη δυνατότητα να χρησιμοποιήσει τον κωδικό του:

- Ένα πρόσθετο επίπεδο ασφάλειας: Χρήση 2FA σε όλους τους σημαντικούς λογαριασμούς, η οποία αυξάνει το επίπεδο ασφάλειας ακόμη και αν ο κωδικός πρόσβασης αποκαλυφθεί.



Αξίζει να εξεταστεί το ενδεχόμενο ενεργοποίησης 2FA:

- όταν συνδέεστε στον τραπεζικό σας λογαριασμό online για να εξασφαλίσετε την πρόσβαση στα χρήματά σας.
- κατά τη σύνδεση στον λογαριασμό ηλεκτρονικού ταχυδρομείου σας, όπου αποθηκεύονται σημαντικές πληροφορίες και αλληλογραφία.
- κατά την πρόσβαση σε μια πλατφόρμα κοινωνικής δικτύωσης, ιδίως όταν χρησιμοποιείται για την επικοινωνία με την οικογένεια και τους φίλους και την κοινοποίηση προσωπικών φωτογραφιών και πληροφοριών.

Λαμβάνοντας αυτές τις προφυλάξεις, ο Ντάνιελ μπορεί να αποφύγει πολλές πιθανές απειλές που σχετίζονται με επιθέσεις μέσω ηλεκτρονικού ταχυδρομείου και άλλες μορφές εγκλήματος στον κυβερνοχώρο.

Να θυμάστε τις συμβουλές μου, γιατί θα σας βοηθήσουν να αισθάνεστε πιο σίγουροι όταν χρησιμοποιείτε το Διαδίκτυο και να προστατεύετε τα προσωπικά και οικονομικά σας δεδομένα από μη εξουσιοδοτημένη πρόσβαση.



Επιθέσεις λόγω ασθενούς κωδικού πρόσβασης



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Οι επιθέσεις που βασίζονται σε ασθενείς κωδικούς πρόσβασης είναι μία από τις πιο συνηθισμένες μεθόδους που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου.

Οι κύριοι τύποι επιθέσεων σε θυρίδες ηλεκτρονικού ταχυδρομείου:

Μια επίθεση με χρήση λεξικού περιλαμβάνει τη δοκιμή ενός μεγάλου αριθμού πιθανών κωδικών πρόσβασης από έναν προηγουμένως προετοιμασμένο κατάλογο (λεξικό). Αυτός ο κατάλογος συχνά περιλαμβάνει κοινά συνθήματα και παραλλαγές λέξεων. Αυτή είναι μια αποτελεσματική μέθοδος εάν ο χρήστης χρησιμοποιεί εύκολα προβλέψιμους κωδικούς πρόσβασης, όπως «password», «123456» ή «qwerty».

Σε μια επίθεση brute force, ο επιτιθέμενος δοκιμάζει συστηματικά όλους τους πιθανούς συνδυασμούς χαρακτήρων μέχρι να βρει τον σωστό κωδικό πρόσβασης. Ενώ αυτός ο τύπος επίθεσης μπορεί να διαρκέσει πολύ χρόνο, μπορεί να είναι αποτελεσματικός για σύντομους και απλούς κωδικούς πρόσβασης.

Αυτή η επίθεση χρησιμοποιεί δεδομένα που έχουν συλλεχθεί από προηγούμενες διαρροές πληροφοριών, όπως συνδέσεις και κωδικούς πρόσβασης. Οι επιτιθέμενοι προσπαθούν να χρησιμοποιήσουν τους ίδιους συνδυασμούς σύνδεσης-συνθηματικού σε διαφορετικούς ιστότοπους, βασιζόμενοι στο γεγονός ότι οι χρήστες τείνουν να επαναχρησιμοποιούν τα ίδια στοιχεία σύνδεσης σε πολλούς ιστότοπους.

Αν και δεν πρόκειται για άμεση επίθεση με κωδικό πρόσβασης, το phishing είναι μια τεχνική που προσπαθεί να εξαπατήσει τους χρήστες ώστε να αποκαλύψουν οικειοθελώς τα στοιχεία σύνδεσής τους. Οι επιτιθέμενοι δημιουργούν ψεύτικους ιστότοπους που μοιάζουν πανομοιότυποι με γνήσιους ιστότοπους (π.χ. τραπεζικές υπηρεσίες, ηλεκτρονικό ταχυδρομείο) και στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου που ενθαρρύνουν τους χρήστες να συνδεθούν.

Επίθεση με
χρήση λεξικού

Επίθεση Brute
force

Επίθεση
πλήρωσης
διαπιστευτηρί-
ων

Επίθεση
Phishing

Επιθέσεις λόγω ασθενούς κωδικού πρόσβασης



ΣΥΝΕΠΕΙΕΣ:

Οι επιθέσεις που αφορούν ασθενείς κωδικούς πρόσβασης έχουν πολλές σοβαρές συνέπειες για τους ηλικιωμένους και μπορούν να απειλήσουν ευαίσθητα δεδομένα και την ασφάλεια στο διαδίκτυο. Για να προστατευτείτε, είναι σημαντικό να τα γνωρίζετε.

01 Επίθεση με χρήση λεξικού

Οι ηλικιωμένοι που χρησιμοποιούν εύκολα προβλέψιμους κωδικούς πρόσβασης, όπως «password» ή «123456», μπορεί να πέσουν θύματα αυτής της επίθεσης. Ως αποτέλεσμα, μπορεί να παραβιαστεί η ιδιωτική τους ζωή και να κλαπούν προσωπικά ή οικονομικά δεδομένα.

02 Επίθεση Brute force

Οι ηλικιωμένοι που χρησιμοποιούν σύντομους και απλούς κωδικούς πρόσβασης είναι ευάλωτοι σε επιθέσεις ωμής βίας. Οι εγκληματίες μπορούν να έχουν πρόσβαση στους λογαριασμούς τους στο Wi-Fi, οδηγώντας σε πιθανή διαρροή δεδομένων και κλοπή ταυτότητας.

03 Επίθεση πλήρωσης διαπιστευτηρίων

Οι ηλικιωμένοι που τείνουν να χρησιμοποιούν τα ίδια στοιχεία σύνδεσης σε πολλούς ιστότοπους είναι ευάλωτοι σε αυτόν τον τύπο επίθεσης. Αυτό μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση στους λογαριασμούς τους σε διάφορες διαδικτυακές πλατφόρμες.

04 Επίθεση Phishing

Οι ηλικιωμένοι ενήλικες, οι οποίοι μπορεί να έχουν λιγότερη επίγνωση τέτοιων απειλών, είναι ευάλωτοι σε επιθέσεις phishing. Οι εγκληματίες μπορούν να χρησιμοποιήσουν ψεύτικους ιστότοπους ή μηνύματα ηλεκτρονικού ταχυδρομείου για να εξαπατήσουν τους ανθρώπους ώστε να αποκτήσουν τα στοιχεία σύνδεσης του λογαριασμού τους, γεγονός που μπορεί να οδηγήσει σε κλοπή ταυτότητας ή οικονομική απάτη.

Επιθέσεις λόγω ασθενούς κωδικού πρόσβασης



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Η Άννα χρησιμοποιεί το λογαριασμό της στο Facebook για να διατηρεί επαφή με τους συναδέλφους της από τη δουλειά. Σε καθημερινή βάση, δημοσιεύει εκεί φωτογραφίες, μοιράζεται σημαντικά γεγονότα και συντονίζει επαγγελματικά έργα. Δυστυχώς, έπεσε θύμα μιας επίθεσης κατά την οποία ο κωδικός πρόσβασής της στο Facebook παραβιάστηκε και ο λογαριασμός της καταλήφθηκε από εγκληματίες του κυβερνοχώρου.



Τέτοιες περιπτώσεις δεν είναι ασυνήθιστες και αφορούν όχι μόνο τους ηλικιωμένους, αλλά και τους επαγγελματικά ενεργούς και τεχνολογικά ευαισθητοποιημένους ανθρώπους. Οποιοσδήποτε, ανεξαρτήτως ηλικίας, μπορεί να πέσει θύμα κυβερνοεγκληματιών, εάν δεν λάβει τα κατάλληλα μέτρα διαδικτυακής ασφάλειας.

ΒΗΜΑ 1: Χρήση απλού κωδικού πρόσβασης

Η Άννα χρησιμοποίησε έναν απλό κωδικό πρόσβασης όπως «12345678», γεγονός που διευκόλυνε την επίθεση με χρήση λεξικού.

ΒΗΜΑ 2: Χωρίς ιδιαίτερους κωδικούς πρόσβασης

Η Άννα χρησιμοποιούσε τον ίδιο κωδικό πρόσβασης σε πολλούς ιστότοπους. Ο κωδικός πρόσβασής της χρησιμοποιήθηκε σε άλλους ιστότοπους, με αποτέλεσμα τη διαρροή δεδομένων.

Επιθέσεις λόγω ασθενούς κωδικού πρόσβασης



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ

Μπορείτε να αποφύγετε αυτές τις συνέπειες ακολουθώντας τις παρακάτω μεθόδους για την προστασία από επιθέσεις με αδύναμο κωδικό πρόσβασης.



Αλλάξτε τον κωδικό πρόσβασής σας σε έναν ισχυρό και μοναδικό:

Η Άννα θα πρέπει να αλλάξει αμέσως τον κωδικό πρόσβασής της στο Facebook σε έναν ισχυρό, μακρύ και μοναδικό κωδικό πρόσβασης που δεν χρησιμοποιείται σε κανέναν άλλο ιστότοπο. Ο κωδικός πρόσβασης θα πρέπει να περιέχει συνδυασμό γραμμάτων, αριθμών και ειδικών χαρακτήρων.

Ενεργοποιήστε τον έλεγχο ταυτότητας δύο παραγόντων (2FA):

Είναι καλή ιδέα να ενεργοποιήσετε τον έλεγχο ταυτότητας δύο παραγόντων στο λογαριασμό σας στο Facebook, ο οποίος θα σας παρέχει ένα επιπλέον επίπεδο ασφάλειας. Χάρη σε αυτό, ακόμη και αν κάποιος γνωρίζει τον κωδικό πρόσβασης, δεν θα μπορεί να συνδεθεί χωρίς έναν δεύτερο παράγοντα ελέγχου ταυτότητας, π.χ. έναν κωδικό SMS.



Ελέγξτε τις ρυθμίσεις ασφαλείας σας:

Θα πρέπει να ελέγξετε τις ρυθμίσεις ασφαλείας του Facebook για να δείτε αν έχουν προστεθεί άγνωστες συσκευές ή εφαρμογές και να αποσυνδεθείτε από όλες τις συσκευές. Θα πρέπει επίσης να αλλάξετε τις ερωτήσεις ασφαλείας σας, εάν έχουν οριστεί.

Επιθέσεις λόγω ασθενούς κωδικού πρόσβασης



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Αναφέρετε το περιστατικό στο Facebook:

Η σωστή λύση είναι να επικοινωνήσετε με την Υποστήριξη του Facebook και να αναφέρετε ότι ο λογαριασμός σας έχει παραβιαστεί. Το Facebook μπορεί να σας βοηθήσει να ανακτήσετε το λογαριασμό σας και να τον προστατεύσει από περαιτέρω επιθέσεις.

Ελέγξτε άλλους λογαριασμούς:

Αξίζει να ελέγξετε τους άλλους λογαριασμούς σας σε ιστότοπους όπου μπορεί να έχει χρησιμοποιήσει τον ίδιο κωδικό πρόσβασης και να αλλάξετε τους κωδικούς πρόσβασης σε μοναδικούς και ισχυρούς. Αυτό θα αποτρέψει περαιτέρω εξαγορές λογαριασμών.



Εκπαίδευση στο phishing:

Είναι επίσης καλή πρακτική να μάθετε πώς να αναγνωρίζετε τις απόπειρες ηλεκτρονικού «ψαρέματος», ώστε να αποφεύγετε αυτού του είδους τις επιθέσεις στο μέλλον. Η Άννα θα πρέπει να δίνει προσοχή σε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, συνδέσμους και να ελέγχει προσεκτικά τις διευθύνσεις URL των σελίδων σύνδεσης.

Phishing



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Το «ψάρεμα» είναι μια μορφή κυβερνοεπίθεσης κατά την οποία οι απατεώνες προσπαθούν να αποκτήσουν εμπιστευτικές πληροφορίες. Η λέξη «phishing» προέρχεται από την αγγλική λέξη «fishing», η οποία μεταφορικά αναφέρεται στο «ψάρεμα» των προσωπικών δεδομένων των χρηστών.

Οι τέσσερις βασικές αρχές στις οποίες βασίζεται το phishing:

- Μέθοδος: Οι απατεώνες δημιουργούν ψεύτικους ιστότοπους, μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα που φαίνεται να προέρχονται από αξιόπιστους φορείς (π.χ. τράπεζες, εταιρείες τεχνολογίας, κυβερνητικές υπηρεσίες).
- Τεχνική: Χρησιμοποιούν λογότυπα, χρώματα και στυλ επικοινωνίας που μιμούνται τις αρχικές πηγές.
- Στόχος: Κερδίζουν την εμπιστοσύνη του θύματος για να παράσχει τα στοιχεία σύνδεσής του ή άλλες εμπιστευτικές πληροφορίες.

- Μέθοδος: Χρήση της αίσθησης του επείγοντος ή του φόβου για να εξαναγκάσει το θύμα να ενεργήσει γρήγορα.
- Τεχνική: Αποστολή μηνύματος σχετικά με μια υποτιθέμενη παραβίαση λογαριασμού, μια ανεξόφλητη πληρωμή ή μια ειδική ευκαιρία που απαιτεί άμεση ανταπόκριση.
- Στόχος: Αύξηση της πιθανότητας το θύμα να ενεργήσει παρορμητικά, χωρίς προσεκτική σκέψη.

**Μίμηση
αξιόπιστων
πηγών**

**Δημιουργία
επιτακτικών
και
συναισθηματικ
ών μηνυμάτων**

Phishing



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

**Χρήση
ψεύτικων
συνδέσμων και
συνημμένων**

- Μέθοδος: Αποστολή μηνυμάτων με συνδέσμους σε ψεύτικους ιστότοπους ή συνημμένα αρχεία που περιέχουν κακόβουλο λογισμικό.
- Τεχνική: Οι σύνδεσμοι μπορεί να φαίνονται νόμιμοι, αλλά οδηγούν σε ψεύτικους ιστότοπους που συλλέγουν διαπιστευτήρια σύνδεσης ή εγκαθιστούν κακόβουλο λογισμικό στη συσκευή του θύματος.
- Σκοπός: Λήψη διαπιστευτηρίων σύνδεσης, μόλυνση της συσκευής του θύματος με κακόβουλο λογισμικό ή ψάρεμα για πληροφορίες.

**Κοινωνική
μηχανική**

- Μέθοδος: Χειραγώγηση του θύματος με τη χρήση τεχνικών ψυχολογικής εξαπάτησης.
- Τεχνική: Χρήση δημοσίως διαθέσιμων πληροφοριών, όπως τα δεδομένα των μέσων κοινωνικής δικτύωσης, για τη δημιουργία εξατομικευμένων μηνυμάτων. Οι απατεώνες μπορεί επίσης να πραγματοποιούν τηλεφωνικές κλήσεις προσποιούμενοι ότι είναι εργαζόμενοι τεχνικής υποστήριξης.
- Σκοπός: Δημιουργία ψευδούς αίσθησης ασφάλειας και εξαπάτηση του θύματος ώστε να αποκαλύψει εμπιστευτικές πληροφορίες.

Phishing



ΣΥΝΕΠΕΙΕΣ:

Γιατί το phishing είναι επικίνδυνο; Οι συνέπειες μιας επιτυχημένης επίθεσης phishing μπορεί να είναι σοβαρές - από την απώλεια χρημάτων έως την κλοπή ταυτότητας και τη μόλυνση μιας συσκευής με κακόβουλο λογισμικό. Για να προστατευτείτε, είναι σημαντικό να τις γνωρίζετε.

01 Μίμηση αξιόπιστων πηγών

- Κλοπή ταυτότητας: Οι ηλικιωμένοι μπορεί να δώσουν εν αγνοία τους προσωπικές πληροφορίες που στη συνέχεια θα χρησιμοποιηθούν για το άνοιγμα ψεύτικων τραπεζικών ή πιστωτικών λογαριασμών στο όνομά τους.
- Οικονομική απώλεια: Η κοινοποίηση των στοιχείων σύνδεσης του τραπεζικού σας λογαριασμού μπορεί να οδηγήσει σε μη εξουσιοδοτημένες συναλλαγές και απώλεια των αποταμιεύσεων.

02

Δημιουργία επειγόντων και συναισθηματικών μηνυμάτων

- Μη εξουσιοδοτημένες πληρωμές: Οι ηλικιωμένοι μπορούν γρήγορα να ανταποκριθούν σε ψευδείς ειδοποιήσεις, παρέχοντας τα τραπεζικά τους στοιχεία και πραγματοποιώντας περιττές μεταφορές.
- Απώλεια αποταμιεύσεων: Ο πειρασμός να πάρουν γρήγορες αποφάσεις μπορεί να οδηγήσει σε σημαντικές οικονομικές απώλειες, ειδικά αν οι ηλικιωμένοι παρέχουν τα στοιχεία της πιστωτικής τους κάρτας σε απατεώνες.
- Αυξημένη ευπάθεια: Οι επαναλαμβανόμενες απόπειρες απάτης μπορεί να καταστήσουν τους ηλικιωμένους πιο ευάλωτους σε μελλοντικές επιθέσεις λόγω του άγχους και της αβεβαιότητας.

Phishing



ΣΥΝΕΠΕΙΕΣ:

03 Χρήση ψεύτικων συνδέσμων και συνημμένων

- Μόλυνση συσκευής: Μπορεί να μολύνει τον υπολογιστή ή το smartphone ενός ηλικιωμένου, οδηγώντας σε απώλεια του ελέγχου της συσκευής και πρόσβαση σε εμπιστευτικές πληροφορίες.
- Κλοπή δεδομένων: Το κακόβουλο λογισμικό μπορεί να καταγράψει τα στοιχεία σύνδεσης, επιτρέποντας στους απατεώνες να αποκτήσουν πρόσβαση σε τραπεζικούς λογαριασμούς και άλλους εμπιστευτικούς πόρους.
- Κόστος επισκευής: Η αφαίρεση του κακόβουλου λογισμικού και η επισκευή μιας μολυσμένης συσκευής μπορεί να συνεπάγεται υψηλό τεχνικό κόστος για το οποίο οι ηλικιωμένοι μπορεί να μην είναι προετοιμασμένοι.

04 Κοινωνική χειραγώγηση

- Τηλεφωνικές απάτες: Οι ηλικιωμένοι μπορεί να εξαπατηθούν για να δώσουν εμπιστευτικές πληροφορίες μέσω τηλεφώνου, οδηγώντας σε κλοπή ταυτότητας και οικονομικές απώλειες.
- Απώλεια εμπιστοσύνης: Οι συχνές επιθέσεις κοινωνικής μηχανικής μπορεί να οδηγήσουν σε έλλειψη εμπιστοσύνης σε νόμιμους φορείς και ανθρώπους, καθιστώντας δύσκολη την καθημερινή ζωή και την οικονομική διαχείριση.
- Συναισθηματική χειραγώγηση: Οι ψυχολογικές επιπτώσεις, όπως ο φόβος, το άγχος και το στρες, μπορούν να επηρεάσουν αρνητικά την ψυχική υγεία των ηλικιωμένων.

Phishing



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Η Μαρία χρησιμοποιεί τακτικά το Διαδίκτυο για να επικοινωνεί με την οικογένειά της, να ελέγχει τους τραπεζικούς της λογαριασμούς και να διαβάζει ειδήσεις. Μια μέρα λαμβάνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχεται από την τράπεζά της.

Από: Θέμα: Τράπεζα XYZ no-reply@bankxyz.com:
Σημαντικό: Απαιτείται άμεση επαλήθευση λογαριασμού!

Αγαπητή κα Μαρία, Λόγω πρόσφατων προσπαθειών μη εξουσιοδοτημένης πρόσβασης στο λογαριασμό σας, παρακαλούμε συνδεθείτε άμεσα στο λογαριασμό σας για να επαληθεύσετε την ταυτότητά σας και να ασφαλίσετε το λογαριασμό σας. Παρακαλούμε κάντε κλικ στον παρακάτω σύνδεσμο και ακολουθήστε τις οδηγίες:

Κάντε κλικ εδώ για να συνδεθείτε

Σας ευχαριστούμε για τη συνεργασία σας, Τράπεζα XYZ

Συνέπειες της μη αναγνώρισης της απειλής:

ΒΗΜΑ 1: Κλικ στο σύνδεσμο

Η Μαρία, ανήσυχη για το περιεχόμενο του ηλεκτρονικού ταχυδρομείου, κάνει κλικ στο σύνδεσμο χωρίς να ελέγξει προσεκτικά τη γνησιότητά του. Ο σύνδεσμος την οδηγεί σε μια σελίδα που μοιάζει πανομοιότυπη με τη σελίδα σύνδεσης της τράπεζάς της.

ΒΗΜΑ 2: Παροχή στοιχείων σύνδεσης

Η Μαρία εισάγει τα στοιχεία σύνδεσής της στον ψεύτικο ιστότοπο, νομίζοντας ότι επαληθεύει τον λογαριασμό της.

Phishing



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ

Το παράδειγμα της Μαρίας απεικονίζει μια κοινή μέθοδο phishing, η οποία υποδύεται αξιόπιστες πηγές. Ας δούμε τις συνέπειες που μπορεί να προκύψουν από την αποτυχία της Μαρίας να αναγνωρίσει αυτή την απειλή.



ΒΗΜΑ 3: Επιπρόσθετο συνημμένο

Το μήνυμα ηλεκτρονικού ταχυδρομείου περιέχει επίσης ένα συνημμένο αρχείο. Η Μαρία κατεβάζει ένα συνημμένο που περιέχει κακόβουλο λογισμικό. Μόλις ανοίξει το αρχείο, το κακόβουλο λογισμικό εγκαθίσταται στον υπολογιστή της, επιτρέποντας στους απατεώνες να έχουν απομακρυσμένη πρόσβαση στη συσκευή της.

ΒΗΜΑ 4: Υποκλοπή δεδομένων και κλοπή χρημάτων

Όταν η Μαρία έκανε κλικ στον σύνδεσμο, οι απατεώνες υπέκλεψαν αμέσως τα στοιχεία σύνδεσής της και απέκτησαν πρόσβαση στον πραγματικό τραπεζικό λογαριασμό της Μαρίας.

ΒΗΜΑ 5: Άγχος και ανησυχία

Η Μαρία είναι συντετριμμένη από την απώλεια των αποταμιεύσεών της και φοβάται να χρησιμοποιήσει ηλεκτρονικές τραπεζικές και άλλες ηλεκτρονικές υπηρεσίες στο μέλλον.

ΒΗΜΑ 6: Μόλυνση της συσκευής σας

Το κακόβουλο λογισμικό στον υπολογιστή της Μαρίας επιτρέπει στους απατεώνες να παρακολουθούν τις διαδικτυακές δραστηριότητές της, να συλλαμβάνουν περαιτέρω στοιχεία σύνδεσης και ενδεχομένως να μολύνουν άλλα αρχεία.

Phishing



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ

Μπορείτε να αποφύγετε αυτές τις συνέπειες ακολουθώντας τις παρακάτω μεθόδους για να προστατευτείτε από τις απάτες phishing.



Έλεγχος της διεύθυνσης e-mail του αποστολέα και των συνδέσμων:

Η Μαρία θα πρέπει να ελέγχει προσεκτικά τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα και τους συνδέσμους στο μήνυμα πριν κάνει κλικ.

Δράση:

- Έλεγχος διεύθυνσης e-mail: Βεβαιωθείτε ότι το email προέρχεται από τον πραγματικό τομέα της τράπεζας.

Ρύθμιση του ελέγχου ταυτότητας δύο παραγόντων (2FA):

Η Μαρία θα πρέπει να ενεργοποιήσει τον έλεγχο ταυτότητας δύο παραγόντων (2FA) στον τραπεζικό της λογαριασμό, ο οποίος προσθέτει ένα επιπλέον επίπεδο ασφάλειας. Ακόμη και αν οι απατεώνες αποκτήσουν τον κωδικό πρόσβασής σας, χρειάζονται και ένα δεύτερο στοιχείο ελέγχου ταυτότητας, όπως έναν κωδικό SMS.

Δράση:

- Ενεργοποίηση 2FA: Μαρία θα πρέπει να επικοινωνήσει με την τράπεζά της για να ενεργοποιήσει την 2FA.



Phishing



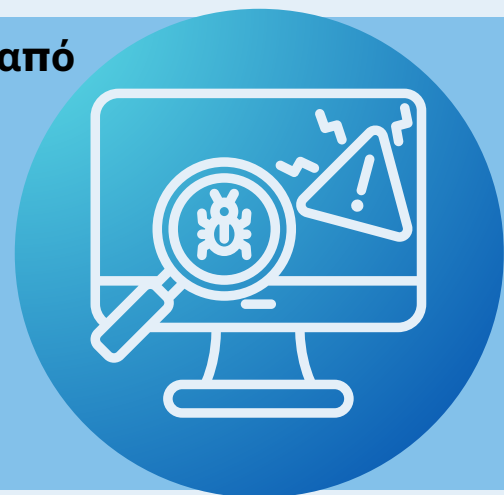
ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ

Τακτική ενημέρωση του λογισμικού προστασίας από ιούς και του λειτουργικού συστήματος:

Η Μαρία θα πρέπει να εξασφαλίζει τακτικές ενημερώσεις του λογισμικού προστασίας από ιούς και του λειτουργικού συστήματος, ώστε να διασφαλίζεται η προστασία από τις πιο πρόσφατες απειλές κακόβουλου λογισμικού και phishing.

Δράση:

- Λογισμικό προστασίας από ιούς: Μαρία θα πρέπει να εγκαταστήσει λογισμικό προστασίας από ιούς και να βεβαιωθείτε ότι είναι πάντα ενημερωμένο και να θυμάστε να το ενημερώνετε τακτικά.



Λαμβάνοντας αυτές τις προφυλάξεις, η Μαρία μπορεί να μειώσει τον κίνδυνο να πέσει θύμα phishing, προστατεύοντας τα δεδομένα και τα οικονομικά της. Ελέγχετε πάντα προσεκτικά τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα και αποφεύγετε να κάνετε κλικ σε συνδέσμους ή συνημμένα αρχεία σε απροσδόκητα μηνύματα ηλεκτρονικού ταχυδρομείου.



Κακόβουλο λογισμικό και ιοί υπολογιστών



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Ο όρος «malware» (Κακόβουλο λογισμικό) χρησιμοποιείται για να περιγράψει κακόβουλα προγράμματα που έχουν σχεδιαστεί για να βλάψουν έναν υπολογιστή ή να εκτελέσουν ανεπιθύμητες ενέργειες σε αυτόν από τον χρήστη. Ένας ιός υπολογιστή είναι μια από τις σοβαρότερες απειλές που αντιμετωπίζουν οι χρήστες υπολογιστών. Το κακόβουλο λογισμικό είναι ικανό να προκαλέσει τεράστια ζημιά - από την κλοπή δεδομένων και την επιβράδυνση ενός συστήματος έως την πλήρη καταστροφή αρχείων.

Κοινοί τύποι κακόβουλου λογισμικού:

Ένας τύπος κακόβουλου λογισμικού που εμποδίζει την πρόσβαση στα δεδομένα του χρήστη κρυπτογραφώντας τα. Ο εγκληματίας του κυβερνοχώρου απαιτεί λύτρα σε αντάλλαγμα για το κλειδί αποκρυπτογράφησης, υποσχόμενος να αποκαταστήσει την πρόσβαση στα δεδομένα. Ωστόσο, οι εγκληματίες συχνά αθετούν τη συμφωνία, πουλώντας εμπιστευτικά δεδομένα ακόμη και μετά την καταβολή των λύτρων, και τα θύματα μπορεί να γίνουν ξανά στόχος.

Ένας τύπος κακόβουλου λογισμικού που μεταμφιέζεται σε νόμιμο λογισμικό για να διεισδύσει στη συσκευή ενός χρήστη. Μόλις εγκατασταθεί, ανοίγει την πρόσβαση στη συσκευή, επιτρέποντας την εγκατάσταση άλλων τύπων κακόβουλου λογισμικού, την κατασκοπεία των χρηστών και την κλοπή εμπιστευτικών πληροφοριών. Τα trojans συχνά εξαπλώνονται χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής, όπως phishing και παραπονημένους ιστότοπους που ενθαρρύνουν τον χρήστη να κατεβάσει ένα κακόβουλο αρχείο.

Ransomware

Trojan

Κακόβουλο λογισμικό και ιοί υπολογιστών



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Worms

Ένας τύπος κακόβουλου λογισμικού παρόμοιος με τους ιούς, αλλά δεν απαιτεί αλληλεπίδραση με τον χρήστη για να εξαπλωθεί. Εκμεταλλεύεται ευπάθειες σε συσκευές εγκατάστασης και αντιγραφής. Μόλις μολύνει μια συσκευή, προσπαθεί να συνδεθεί με άλλες συσκευές στο ίδιο δίκτυο και αναζητά περαιτέρω ευπάθειες για να εξαπλωθεί σε αυτές.

Spyware

Κακόβουλο λογισμικό που εγκαθίσταται στη συσκευή του θύματος για να κατασκοπεύει και να συλλέγει ευαίσθητες πληροφορίες, όπως διαπιστευτήρια και αριθμούς πιστωτικών καρτών. Το κατασκοπευτικό λογισμικό μπορεί να συνοδεύει άλλα προγράμματα ή μπορείτε να το εγκαταστήσετε μόνοι σας κάνοντας κλικ σε μια διαφήμιση ή κατεβάζοντας δωρεάν λογισμικό από αναξιόπιστους ιστότοπους. Μόλις εγκατασταθεί, παρακολουθεί τις πληκτρολογήσεις, το ιστορικό περιήγησης και χρησιμοποιεί την κάμερα και το μικρόφωνο της συσκευής σας.

Fileless malware

Ένας τύπος κακόβουλου λογισμικού που δεν χρησιμοποιεί εκτελέσιμα αρχεία που περιέχουν κακόβουλο κώδικα για να μολύνει μια συσκευή. Αντ' αυτού, πραγματοποιεί αλλαγές στα νόμιμα εργαλεία συστήματος της συσκευής σας, επιτρέποντάς σας να εκτελείτε κακόβουλες δραστηριότητες χωρίς να χρειάζεται να κατεβάσετε αρχεία στον σκληρό σας δίσκο. Ο κακόβουλος κώδικας λογισμικού χωρίς αρχεία εκτελείται απευθείας στη μνήμη του υπολογιστή, χρησιμοποιώντας τα υπάρχοντα εργαλεία συστήματος για να επιτύχει τους στόχους του.

Κακόβουλο λογισμικό και ιοί υπολογιστών



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Ένας τύπος κακόβουλου λογισμικού που επιτίθεται σε φορητές συσκευές, όπως smartphones και tablets, για να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα. Οι συσκευές χωρίς επαρκή μέτρα ασφαλείας είναι ευάλωτες σε τέτοιου είδους επιθέσεις, επειδή συχνά δεν διαθέτουν τους προεπιλεγμένους μηχανισμούς άμυνας που είναι ενσωματωμένοι στο αρχικό λειτουργικό σύστημα.

Είναι ένας τύπος κακόβουλου λογισμικού που μολύνει συσκευές και αναπαράγεται για να εξαπλωθεί σε άλλες συσκευές. Συνήθως μεταμφιέζονται ως κακόβουλα αρχεία ή εφαρμογές που εγκαθιστούν τα θύματα. Οι επιτιθέμενοι συχνά προσπαθούν να πείσουν τους χρήστες να κατεβάσουν αυτά τα αρχεία χρησιμοποιώντας επιθέσεις phishing. Όταν το θύμα κατεβάζει το μολυσμένο αρχείο ή την εφαρμογή, ο ιός ενεργοποιείται και αρχίζει να αναπαράγεται στη συσκευή. Αλλάζει συχνά αρχεία για να αποφύγει τον εντοπισμό και μολύνει άλλες συσκευές. Ο ιός μπορεί να υποκλέψει εμπιστευτικά δεδομένα, να επιβραδύνει τη συσκευή σας, να παγώσει εφαρμογές και να αλλάξει και να καταστρέψει αρχεία.

**Malware για
κινητά
τηλέφωνα**

Ιοί

Κακόβουλο λογισμικό και ιοί υπολογιστών



CONSEQUENCES:

Οι συνέπειες της μόλυνσης από κακόβουλο λογισμικό είναι πολύ σοβαρές. Οι εγκληματίες του κυβερνοχώρου καθοδηγούνται από την επιθυμία για κέρδος. Χρησιμοποιούν μολυσμένες συσκευές για να εξαπολύσουν επιθέσεις, όπως η απόκτηση διαπιστευτηρίων για τραπεζικές υπηρεσίες, η συλλογή προσωπικών δεδομένων προς πώληση, η πώληση πρόσβασης σε πόρους υπολογιστή ή η εκβίαση αμοιβών από τα θύματα.

01 Ransomware

Το λογισμικό μπορεί να έχει ως αποτέλεσμα την απώλεια πρόσβασης σε σημαντικά δεδομένα ενός ηλίκιωμένου, όπως οικονομικά έγγραφα ή οικογενειακές φωτογραφίες. Επιπλέον, η καταβολή των λύτρων δεν εγγυάται την ανάκτηση δεδομένων, γεγονός που μπορεί να οδηγήσει σε πρόσθετες οικονομικές απώλειες.

02 Trojan horse – Δούρειος Ίππος

Το λογισμικό μπορεί να οδηγήσει στην κλοπή ευαίσθητων πληροφοριών, όπως κωδικούς πρόσβασης σε τραπεζικούς λογαριασμούς ή αριθμούς πιστωτικών καρτών, θέτοντας τους ηλίκιωμένους σε κίνδυνο κλοπής ταυτότητας και οικονομικής απώλειας.

03 Spyware

Το λογισμικό μπορεί να χρησιμοποιηθεί για την υποκλοπή των συνομιλιών των ηλίκιωμένων ή την παρακολούθηση των διαδικτυακών δραστηριοτήτων τους, γεγονός που παραβιάζει την ιδιωτική τους ζωή και μπορεί να οδηγήσει στη χρήση των συλλεγόμενων δεδομένων για εκβιασμούς ή απάτες.

Κακόβουλο λογισμικό και ιοί υπολογιστών



ΣΥΝΕΠΕΙΕΣ:

04 Worms-“Σκουλήκια”

Το λογισμικό μπορεί να βλάψει το λειτουργικό σύστημα της συσκευής ενός ηλικιωμένου ή να αναλάβει τον έλεγχο της από εγκληματίες του κυβερνοχώρου, γεγονός που μπορεί να καταστήσει αδύνατη τη χρήση της συσκευής ή να οδηγήσει στην απώλεια σημαντικών δεδομένων.

05 Fileless malware-Κακόβουλο λογισμικό χωρίς αρχείο

Το λογισμικό μπορεί να εκτελείται στο παρασκήνιο, αλλάζοντας απαραίτητα τις ρυθμίσεις της συσκευής σας ή χρησιμοποιώντας τους πόρους της, γεγονός που μπορεί να οδηγήσει στην επιβράδυνση της συσκευής σας ή να προκαλέσει προβλήματα στην απόδοσή της.

06 Malware Κινητού τηλεφώνου

Το λογισμικό μπορεί να οδηγήσει σε απώλεια δεδομένων ή σε παραβίαση της ιδιωτικής ζωής ενός ηλικιωμένου με πρόσβαση στις προσωπικές του πληροφορίες ή με εντοπισμό της τοποθεσίας του.

07 Ιοί

Οι ιοί μπορούν να υποκλέψουν εμπιστευτικά δεδομένα, όπως κωδικούς πρόσβασης, οικονομικές πληροφορίες ή προσωπικά δεδομένα, παραβιάζοντας την ιδιωτική ζωή των χρηστών. Μπορούν να αναπαραχθούν και να εξαπλωθούν σε άλλες συσκευές στο δίκτυο, προκαλώντας περαιτέρω μολύνσεις και αυξάνοντας την κλίμακα του προβλήματος.

Κακόβουλο λογισμικό και ιοί υπολογιστών



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Ο Αλέξανδρος έψαχνε τα e-mail του. Παρατήρησε κάποια νέα που δεν περίμενε και τον έκαναν περίεργο. Έκανε κλικ στο συνημμένο αρχείο αυτού του ηλεκτρονικού ταχυδρομείου. Παρατήρησε κάτι περίεργο. Κάτι άρχισε να αλλάζει αρχεία στον υπολογιστή του, προκαλώντας σημαντικές διαταραχές στην εργασία του. Τι θα μπορούσε να είχε συμβεί;

Περιπτώσεις παρόμοιες με του Αλεξάνδρου είναι δυστυχώς αρκετά συχνές. Κάνοντας κλικ σε ένα ύποπτο συνημμένο email μπορεί να οδηγήσει σε μόλυνση του υπολογιστή σας με κακόβουλο λογισμικό. Ως αποτέλεσμα, μπορεί να προκληθούν σοβαρές διαταραχές στις λειτουργίες και στην ασφάλεια των δεδομένων.



ΒΗΜΑ 1: Κλικ στο συνημμένο email

Ο Αλέξανδρος έψαχνε το ηλεκτρονικό του ταχυδρομείο και, ανυποψίαστος, έκανε κλικ στο συνημμένο αρχείο του ηλεκτρονικού ταχυδρομείου.

ΒΗΜΑ 2: Μόλυνση της συσκευής

Κάνοντας κλικ στο ψεύτικο συνημμένο αρχείο μόλυνε τη συσκευή του με έναν ιό.

ΒΗΜΑ 3: Αντιγραφή/πολλαπλασιασμός του ιού

Ο κακόβουλος κώδικας («συνημμένος») άρχισε να αναπαράγεται γρήγορα στον υπολογιστή του Αλεξάντερ, προκαλώντας αλλαγές σε αρχεία και διακοπές στην εργασία του.

ΒΗΜΑ 4: Πιθανότητα κλοπής δεδομένων

Επιπλέον, ο ιός μπορεί να είχε τη δυνατότητα να κλέψει εμπιστευτικά δεδομένα από τη συσκευή του Αλεξάνδρου, γεγονός που θα μπορούσε να οδηγήσει σε περαιτέρω ζητήματα ασφάλειας και προστασίας της ιδιωτικής ζωής.

Κακόβουλο λογισμικό και ιοί υπολογιστών



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ

Μπορείτε να αποφύγετε αυτές τις συνέπειες ακολουθώντας τις παρακάτω μεθόδους προστασίας από κακόβουλο λογισμικό.



Ενημερώστε τακτικά το λογισμικό σας κάθε φορά που διατίθενται νέα ύποπτα μηνύματα απειλών, γεγονός που μειώνει τον κίνδυνο μόλυνσης από κακόβουλο λογισμικό που εκμεταλλεύεται αυτά τα τρωτά σημεία.

Να είστε προσεκτικοί όταν ανοίγετε συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου και κατεβάζετε αρχεία, ειδικά αν προέρχονται από άγνωστους αποστολείς ή φαίνονται ύποπτα.



Αποφύγετε να κάνετε κλικ σε ύποπτους συνδέσμους ή αναδυόμενα παράθυρα, καθώς μπορεί να οδηγήσουν σε μολύνσεις ή καταγραφή δεδομένων.

Κακόβουλο λογισμικό και ιοί υπολογιστών



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Χρησιμοποιήστε τα δημόσια δίκτυα Wi-Fi με προσοχή, καθώς είναι ευάλωτα σε επιθέσεις. Σκεφτείτε να χρησιμοποιήσετε μια υπηρεσία VPN για να ασφαλίσετε τη σύνδεσή σας στο διαδίκτυο. Χρησιμοποιώντας ένα VPN, τα δεδομένα σας κρυπτογραφούνται καθώς ταξιδεύουν μέσω δημόσιων δικτύων, πράγμα που σημαίνει ότι ακόμη και αν κάποιος

Χρησιμοποιήστε προγράμματα προστασίας από ιούς και κακόβουλο λογισμικό που βοηθούν στην πρόληψη μολύνσεων και στην αφαίρεση κακόβουλου λογισμικού, συμπεριλαμβανομένων των προγραμμάτων κατασκοπείας και των προγραμμάτων διαφήμισης. Τα antivirus επικεντρώνονται κυρίως στον εντοπισμό και την εξάλειψη ιών, ενώ τα antimalware ασχολούνται με ένα ευρύ φάσμα κακόβουλου λογισμικού, συμπεριλαμβανομένων κακόβουλων εφαρμογών που δεν ταξινομούνται ως ιοί.



Ακολουθώντας αυτές τις συστάσεις, ο Αλέξανδρος και άλλοι χρήστες του Διαδικτύου μπορούν να αποφύγουν απειλές από κακόβουλο λογισμικό. Να θυμάστε να μην παίρνετε αποφάσεις πολύ γρήγορα και να ενεργείτε πάντα με προσοχή στον εικονικό κόσμο.



Περαιτέρω αναγνώσματα



ΕΠΙΘΕΣΗ ΜΕΣΩ ΔΙΚΤΥΩΝ WI-FI (ΙΔΙΩΤΙΚΩΝ ΚΑΙ ΔΗΜΟΣΙΩΝ)

- www.keepersecurity.com/pl_PL/threats/man-in-the-middle-attacks-mitm.html
- www.cdv.pl/blog/blog-ekspercki/najpopularniejsze-rodzaje-atakow-hakerskich/
- www.socialwifi.com/pl/baza-wiedzy/bezpieczenstwo-sieci/najpopularniejsze-rodzaje-atakow-na-wifi/



ΕΠΙΘΕΣΕΙΣ ΜΕΣΩ EMAIL

- www.powerdmarc.com/pl/what-are-email-based-attacks/
- <https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y>
- www.keepersecurity.com/blog/pl/2023/08/30/the-most-common-types-of-cyberattacks/



ΕΠΙΘΕΣΕΙΣ ΛΟΓΩ ΑΣΘΕΟΥΣ ΚΩΔΙΚΟΥ ΠΡΟΣΒΑΣΗΣ

- www.keepersecurity.com/blog/pl/2024/01/12/types-of-password-attacks/
- www.securivy.com/blog/brute-force/
- www.keepersecurity.com/pl_PL/threats/dictionary-attack.html



PHISHING

- www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y
- www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/
- www.kwestiabezpieczenstwa.pl/phishing/



MALWARE ΚΑΙ ΙΟΙ

- www.keepersecurity.com/blog/pl/2024/01/24/twelve-common-types-of-malware/
- www.hackeru.pl/wirus-komputerowy/
- www.powerdmarc.com/pl/types-of-malware/

ΚΕΦΑΛΑΙΟ 2.

ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΕΠΕΝΔΥΤΙΚΗ ΑΠΑΤΗ

Στον σημερινό κόσμο, οι ηλικιωμένοι πέφτουν όλο και περισσότερο θύματα οικονομικών απάτης, η οποία παίρνει διάφορες μορφές και τελειοποιείται συνεχώς από τους εγκληματίες. Αυτό το κεφάλαιο έχει ως στόχο να επισημάνει τους πιο συνηθισμένους τύπους απάτης, ώστε να βοηθήσει τους ηλικιωμένους να αναγνωρίζουν τις απειλές και να προστατεύουν τις αποταμιεύσεις τους.

Μεταξύ των πιο διαδεδομένων μεθόδων συγκαταλέγονται οι οικονομικές και επενδυτικές απάτες, οι οποίες βασίζονται σε ψευδείς υποσχέσεις για γρήγορα κέρδη, και οι φιλανθρωπικές απάτες που εκμεταλλεύονται την ενσυναίσθηση των ηλικιωμένων. Ένας άλλος κίνδυνος είναι η υπόσχεση μεγάλων κερδών μέσω ψεύτικων βραβείων και λοταριών, τα οποία απαιτούν πληρωμή για να τα διεκδικήσουν.

Οι απάτες που αφορούν ψηφιακά νομίσματα, όπως το Bitcoin, γίνονται επίσης όλο και πιο συχνές, προσφέροντας μια νέα οδό για εγκληματική δραστηριότητα. Είναι επίσης σημαντικό να αναφέρουμε τις νιγηριανές απάτες -διεθνή συστήματα απάτης που βασίζονται σε πλασματικές συναλλαγές.

Η κατανόηση αυτών των απειλών είναι ζωτικής σημασίας για τους ηλικιωμένους ώστε να προστατεύουν συνειδητά τα οικονομικά τους.

Οικονομικές και επενδυτικές χειραγωγήσεις

— ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ

Η χρηματοοικονομική και επενδυτική χειραγωγήση αναφέρεται σε παραπλανητικές πρακτικές που αποσκοπούν στο να πείσουν τα άτομα να επενδύσουν τα χρήματά τους σε δόλια ή ακατάλληλα συστήματα. Τα σχήματα αυτά συχνά υπόσχονται υψηλές αποδόσεις, αλλά τελικά καταλήγουν σε οικονομικές απώλειες για τους επενδυτές.

Είδη χειραγωγής στις χρηματοοικονομικές επενδύσεις:

Οι απατεώνες χρησιμοποιούν πειστικές τακτικές για να υποσχεθούν στους επενδυτές ασυνήθιστα υψηλές αποδόσεις στις επενδύσεις τους. Οι υποσχέσεις αυτές μπορεί να φαίνονται πολύ καλές για να είναι αληθινές και συχνά στοχεύουν σε ηλικιωμένους που αναζητούν τρόπους να συμπληρώσουν το εισόδημά τους στη σύνταξη.

**Ψευδείς
υποσχέσεις
υψηλών
αποδόσεων**

Οι απατεώνες χρησιμοποιούν συχνά τακτικές πωλήσεων υψηλής πίεσης για να πιέσουν τα άτομα να λάβουν γρήγορες επενδυτικές αποφάσεις χωρίς να ερευνήσουν ή να κατανοήσουν σε βάθος τα επενδυτικά προϊόντα. Ενδέχεται να δημιουργήσουν μια αίσθηση επείγοντος, ισχυριζόμενοι προσφορές περιορισμένης διάρκειας ή δίνοντας έμφαση στο φόβο ότι θα χάσουν επικερδείς ευκαιρίες.

**Πίεση για
γρήγορη
επένδυση**

Οι απατεώνες μπορεί να συστήνουν πολύπλοκα ή ασαφή επενδυτικά προϊόντα που είναι δύσκολο να κατανοήσουν οι επενδυτές, ιδίως οι ηλικιωμένοι. Τα προϊόντα αυτά μπορεί να περιλαμβάνουν υψηλές αμοιβές, κρυμμένους κινδύνους ή έλλειψη διαφάνειας σχετικά με τον τρόπο χρήσης των επενδυμένων κεφαλαίων.

**Πολύπλοκα και
συγκεχυμένα
επενδυτικά
προϊόντα**

Οικονομικές και επενδυτικές χειραγωγήσεις



ΣΥΝΕΠΕΙΕΣ:

Η χρηματοοικονομική και επενδυτική χειραγωγήση μπορεί να έχει σοβαρές αρνητικές επιπτώσεις, όπως:

01 Οικονομικές επιπτώσεις

Το να πέσετε θύμα οικονομικής χειραγωγήσης μπορεί να οδηγήσει στην απώλεια αποταμιεύσεων και επενδύσεων που αποκτήσατε με κόπο. Μπορεί να βρεθείτε με σημαντικά λιγότερα χρήματα από τα αναμενόμενα, επηρεάζοντας την ικανότητά σας να καλύπτετε τα καθημερινά έξοδα και να απολαμβάνετε τη συνταξιοδότησή σας

02 Συναισθηματικές επιπτώσεις

Η εξαπάτηση από οικονομικούς απατεώνες μπορεί να οδηγήσει σε αισθήματα προδοσίας και απογοήτευσης. Μπορεί να νιώθετε αμηχανία ή ντροπή που πέσατε θύμα απάτης, επηρεάζοντας την αυτοεκτίμηση και την αυτοπεποίθησή σας.

03 Προσωπικές επιπτώσεις

Το να πέσετε θύμα οικονομικής χειραγωγήσης μπορεί να υπονομεύσει την εμπιστοσύνη στους άλλους, κάνοντάς σας πιο επιφυλακτικούς και δύσπιστους απέναντι σε μελλοντικές επενδυτικές ευκαιρίες. Αυτή η απώλεια εμπιστοσύνης μπορεί να επιβαρύνει τις σχέσεις και να σας δυσκολέψει να αναζητήσετε οικονομικές συμβουλές ή υποστήριξη

Οικονομικές και επενδυτικές χειραγωγήσεις

— ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Η Σοφία λαμβάνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου από έναν άγνωστο αποστολέα που ισχυρίζεται ότι προσφέρει μια επικερδή επενδυτική ευκαιρία σε μια νέα τεχνολογική εταιρεία. Το email υπόσχεται υψηλές αποδόσεις και προτρέπει την κυρία Τζενκινς να ενεργήσει γρήγορα για να εξασφαλίσει τη θέση της στην επένδυση.

Ωστόσο, η Σοφία θυμάται τη συμβουλή που διάβασε σχετικά με την προσοχή στα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου που υπόσχονται μεγάλα κέρδη.

Η ιστορία της Σοφίας δεν είναι δυστυχώς η μοναδική περίπτωση, αλλά δείχνει τη σημασία της προστασίας των ηλικιωμένων από την οικονομική χειραγωγήση. Οι ηλικιωμένοι θα πρέπει να γνωρίζουν τις διάφορες μορφές χειραγωγής που μπορεί να συναντήσουν και να γνωρίζουν μεθόδους για να τις αποφύγουν.



ΒΗΜΑ 1: Επαλήθευση

Η Σοφία αποφασίζει να επαληθεύσει τη νομιμότητα της επενδυτικής ευκαιρίας πριν προβεί σε οποιαδήποτε ενέργεια.

ΒΗΜΑ 2: Διαβούλευση

Η Σοφία ζητά συμβουλές από το έμπιστο μέλος της οικογένειάς της που έχει εμπειρία στα οικονομικά.

ΒΗΜΑ 3: Επιβεβαίωση

Εξακολουθώντας να είναι επιφυλακτική, η Σοφία αποφασίζει να επικοινωνήσει απευθείας με την εταιρεία για να επαληθεύσει την επενδυτική ευκαιρία.

ΒΗΜΑ 4: Αναφορά

Η Σοφία αποφασίζει να αναφέρει το ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου στις αρμόδιες αρχές.

Οικονομικές και επενδυτικές χειραγωγήσεις

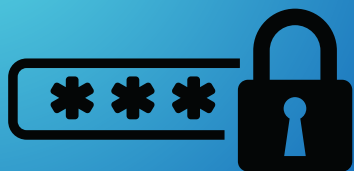


WAYS OF PROTECTION:

Η προστασία σας από οικονομικές και επενδυτικές χειραγωγήσεις είναι ζωτικής σημασίας για τη διαφύλαξη των χρημάτων που με κόπο κερδίσατε. Ακολουθούν ορισμένα απλά βήματα που μπορείτε να ακολουθήσετε.

Να είστε προσεκτικοί με τα email:

Εάν λάβετε ένα απροσδόκητο email που υπόσχεται μεγάλα κέρδη ή επείγουσες οικονομικές συμφωνίες, καλό είναι να είστε προσεκτικοί. Αφιερώστε λίγο χρόνο για να ελέγξετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα για τυχόν περίεργα σημάδια. Και αν κάτι σας φαίνεται παράξενο, μην κάνετε κλικ σε συνδέσμους ή κατεβάσετε συνημμένα αρχεία.



Ενισχύστε τους κωδικούς πρόσβασης:

Όταν δημιουργείτε κωδικούς πρόσβασης για τους διαδικτυακούς σας λογαριασμούς, βεβαιωθείτε ότι είναι ισχυροί και μοναδικοί. Χρησιμοποιήστε έναν συνδυασμό γραμμάτων, αριθμών και συμβόλων και αποφύγετε τη χρήση πληροφοριών που είναι εύκολο να μαντέψετε, όπως τα γενέθλια ή το όνομα του κατοικίδιου ζώου σας.

Οικονομικές και επενδυτικές χειραγωγήσεις



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Προσέξτε για ύποπτους συνδέσμους και ιστότοπους:

Αν συναντήσετε έναν ιστότοπο που σας φαίνεται ύποπτος ή άγνωστος, μην μοιραστείτε προσωπικές ή οικονομικές πληροφορίες. Αναζητήστε το «https://» και ένα σύμβολο λουκέτου στη γραμμή διευθύνσεων για ασφαλείς ιστότοπους.



Ενημερωθείτε για την ασφάλεια στο διαδίκτυο:

Υπάρχουν πολλές πηγές και εκπαιδευτικό υλικό διαθέσιμο για να σας βοηθήσει να μάθετε για τις κοινές απάτες που απευθύνονται σε ηλικιωμένους.

Τέλος, μη φοβάστε να ζητήσετε βοήθεια:

Αν δεν είστε σίγουροι για μια οικονομική απόφαση ή υποψιάζεστε ότι έχετε πέσει θύμα απάτης, απευθυνθείτε σε μέλη της οικογένειας, φίλους ή επαγγελματίες που εμπιστεύεστε για συμβουλές και υποστήριξη. Και αν πιστεύετε ότι πέσατε θύμα οικονομικής χειραγώγησης, αναφέρετε το περιστατικό αμέσως στις αρμόδιες αρχές, όπως στην Ομοσπονδιακή Επιτροπή Εμπορίου ή στην υπηρεσία προστασίας των καταναλωτών της πολιτείας σας.



Φαινομενικός αλτρουισμός: φιλανθρωπική απάτη

— ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ

Οι φιλανθρωπικές απάτες στο διαδίκτυο συχνά εκμεταλλεύονται τη γενναιοδωρία και την καλή θέληση των ατόμων, ιδίως με στόχο τους ηλικιωμένους ηλικίας 65 ετών και άνω. Αυτές οι απάτες μπορεί να περιλαμβάνουν ψεύτικες φιλανθρωπικές οργανώσεις που παριστάνουν τους νόμιμους οργανισμούς, ζητώντας δωρεές για υποτιθέμενους σκοπούς όπως η ανακούφιση από καταστροφές, η ιατρική έρευνα ή η βοήθεια προς τους λιγότερο τυχερούς.

Τύποι χειραγώγησης στις φιλανθρωπικές απάτες:

Οι απατεώνες μπορεί να χρησιμοποιούν πειστική γλώσσα ή συναισθηματικές εκκλήσεις για να πιέσουν τα θύματα να κάνουν γρήγορα δωρεές.

Οι απατεώνες μπορεί να δημιουργήσουν ψεύτικους ιστότοπους ή να στείλουν μηνύματα ηλεκτρονικού ταχυδρομείου που μιμούνται την επωνυμία γνωστών φιλανθρωπικών οργανώσεων για να εξαπατήσουν τα θύματα.

Οι απατεώνες μπορεί να κατασκευάσουν συγκλονιστικές ιστορίες ή να δώσουν ψεύτικες μαρτυρίες για να αποσπάσουν συμπάθεια και να ενθαρρύνουν δωρεές.

Οι ψεύτικες φιλανθρωπικές οργανώσεις παρέχουν συχνά ασαφείς ή παραπλανητικές πληροφορίες σχετικά με την αποστολή τους, τους στόχους τους και τον τρόπο χρήσης των δωρεών.

Τακτική
υψηλής
πίεσης

Προσποίηση
νόμιμων
φιλανθρωπικών
οργανώσεων

Πεύτικες
ιστορίες και
μαρτυρίες

Έλλειψη
διαφάνειας

Φαινομενικός αλτρουισμός: φιλανθρωπική απάτη



ΣΥΝΕΠΕΙΕΣ:

Το να πέσει κάποιος θύμα απάτης για φιλανθρωπικούς σκοπούς μπορεί να είναι πολύ δύσκολο για τους ηλικιωμένους, τόσο οικονομικά όσο και συναισθηματικά.

01

Οικονομική Απώλεια

Το να πέσετε θύμα απάτης με φιλανθρωπικά ιδρύματα μπορεί να έχει ως αποτέλεσμα την απώλεια αποταμιεύσεων και επενδύσεων που αποκτήσατε με κόπο. Μπορεί να βρεθείτε με σημαντικά λιγότερα χρήματα από τα αναμενόμενα, επηρεάζοντας την ικανότητά σας να καλύπτετε τα καθημερινά έξοδα και να απολαμβάνετε τη συνταξιοδότησή σας.

02

Συναισθηματική καταπόνηση

Η χειραγώγηση σε φιλανθρωπική απάτη μπορεί να σας κάνει να αισθάνεστε προδομένοι, ένοχοι και αμήχανοι που πέσατε θύμα αυτής της απάτης.

03

Προβλήματα εμπιστοσύνης

Μπορεί επίσης να δυσχεράνει την εμπιστοσύνη στις πραγματικές φιλανθρωπικές οργανώσεις στο μέλλον, επειδή γίνεται πιο δύσκολο να ξεχωρίσει κανείς τις γνήσιες από τις ψεύτικες εκκλήσεις.

Φαινομενικός αλτρουισμός: φιλανθρωπική απάτη



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Η Αλίκη λαμβάνει ένα email που υποστηρίζει ότι προέρχεται από μια φιλανθρωπική οργάνωση που ζητά δωρεές για να βοηθήσει παιδιά που έχουν ανάγκη. Το email περιλαμβάνει συγκινητικές ιστορίες και φωτογραφίες παιδιών που υποτίθεται ότι επωφελούνται από το έργο της φιλανθρωπικής οργάνωσης. Ωστόσο, η Αλίκη θυμάται τη συμβουλή που διάβασε σχετικά με το να είναι καχύποπτη με τα μηνύματα ηλεκτρονικού ταχυδρομείου που υπόσχονται δωρεές χρημάτων σε φιλανθρωπικές οργανώσεις.



Η ιστορία της Αλίκης δεν είναι δυστυχώς η μοναδική περίπτωση, αλλά δείχνει τη σημασία της προστασίας των ηλικιωμένων από τις φιλανθρωπικές απάτες. Οι ηλικιωμένοι θα πρέπει να γνωρίζουν τις διάφορες μορφές απάτης που μπορεί να συναντήσουν και να γνωρίζουν μεθόδους για να τις αποφύγουν.

Βήμα 1: Έρευνα του φιλανθρωπικού ιδρύματος

Πριν από τη δωρεά, η Αλίκη ελέγχει το καθεστώς εγγραφής της φιλανθρωπικής οργάνωσης και τις κριτικές σε αξιόπιστες ιστοσελίδες.

Βήμα 2: Προσοχή στα μη ζητηθέντα αιτήματα

Η Αλίκη αμφισβήτησε αυτό το απροσδόκητο μήνυμα ηλεκτρονικού ταχυδρομείου που ζητούσε δωρεές.

Βήμα 3: Ποτέ μην μοιράζετε προσωπικές πληροφορίες

Η Αλίκη απέφυγε να παρέχει ευαίσθητες πληροφορίες όπως αριθμούς κοινωνικής ασφάλισης ή τραπεζικά στοιχεία σε άγνωστες ή μη επαληθευμένες φιλανθρωπικές οργανώσεις.

Βήμα 4 : Δωρίστε απευθείας

Εάν η Αλίκη θέλει να κάνει δωρεά, αντί να κάνει κλικ σε συνδέσμους σε email ή να απαντά σε τηλεφωνήματα, κάνει δωρεά απευθείας μέσω της επίσημης ιστοσελίδας της φιλανθρωπικής οργάνωσης.

Φαινομενικός αλτρουισμός: φιλανθρωπική απάτη



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Η προστασία σας από τις απάτες φιλανθρωπίας και τις συνέπειές της είναι πολύ σημαντική. Ακολουθούν ορισμένα απλά βήματα που μπορείτε να υιοθετήσετε για να αποτρέψετε τον εαυτό σας από το να πέσει θύμα της φιλανθρωπικής απάτης

Ερευνήστε τις φιλανθρωπικές οργανώσεις ελέγχοντας την κατάστασή τους και τις κριτικές τους σε νόμιμους ιστότοπους φιλανθρωπικών οργανώσεων.



Να είστε προσεκτικοί σε απροσδόκητα αιτήματα για δωρεές μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, τηλεφωνημάτων ή μέσων κοινωνικής δικτύωσης, καθώς οι πραγματικές φιλανθρωπικές οργανώσεις δεν χρησιμοποιούν συνήθως τακτικές υψηλής πίεσης.

Ποτέ μην μοιράζετε προσωπικές πληροφορίες όπως αριθμούς κοινωνικής ασφάλισης ή τραπεζικά στοιχεία με άγνωστες φιλανθρωπικές οργανώσεις.



Φαινομενικός αλτρουισμός: φιланθρωπική απάτη



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Δωρίστε απευθείας μέσω της επίσημης ιστοσελίδας της φιλανθρωπικής οργάνωσης ή στέλνοντας μια επιταγή στην επαληθευμένη διεύθυνσή της.



Μείνετε ενημερωμένοι σχετικά με τις κοινές φιλανθρωπικές απάτες και μάθετε να αναγνωρίζετε τα προειδοποιητικά σημάδια.

Μη διστάσετε να ζητήσετε βοήθεια από την οικογένεια, τους φίλους ή τους οικονομικούς συμβούλους όταν αξιολογείτε τα αιτήματα φιλανθρωπίας ή αν υποψιάζεστε απάτη.



Δελεαστικές απάτες: πλασματικά βραβεία και κληρώσεις



HAZARD CHARACTERISTICS:

Οι απάτες που βασίζονται σε πλαστά βραβεία, λοταρίες και κληρώσεις είναι παραπλανητικές και εκμεταλλεύονται σκόπιμα την επιθυμία των ανθρώπων να κερδίσουν, πείθοντάς τους ότι έχουν κερδίσει μεγάλα βραβεία. Οι απατεώνες ζητούν από τα θύματα να τους πληρώσουν ψεύτικα κέρδη, αλλά καταλήγουν να κλέβουν χρήματα από το πορτοφόλι του θύματος.

Τύποι χειραγώγησης σε πλασματικά βραβεία και κληρώσεις:

Οι απατεώνες συχνά παριστάνουν τους εκπροσώπους γνωστών εταιρειών ή λοταριών που διαχειρίζονται κυβερνήσεις (ιδίως ξένες) και χρησιμοποιούν τακτικές χειραγώγησης για να εκμεταλλευτούν την εμπιστοσύνη των θυμάτων τους, ελπίζοντας να εκμεταλλευτούν την επιθυμία τους για οικονομική ασφάλεια.

Οι απατεώνες προσπαθούν να πείσουν τα θύματα ότι έχουν επιλεγεί ως οι μοναδικοί ή σπάνιοι τυχεροί νικητές, προκειμένου να δημιουργήσουν μια αίσθηση μοναδικότητας και αποκλειστικής ευκαιρίας στο θύμα.

Οι απατεώνες υπόσχονται μη ρεαλιστικά χρηματικά έπαθλα, πολυτελή προϊόντα κ.λπ. που είναι πολύ καλά για να είναι αληθινά, χρησιμοποιώντας τακτικές πίεσης για να κάνουν τα θύματα να αντιδράσουν άμεσα και εμπιστευτικά.

Πλαστοπροσωπία

Αποκλειστικότητα

Μη ρεαλιστικές υποσχέσεις

Δελεαστικές απάτες: πλασματικά βραβεία και κληρώσεις



ΣΥΝΕΠΕΙΕΣ:

Οι συνέπειες της απάτης της «δελεαστικής ψευδαίσθησης» είναι ποικίλες και συχνά μακροχρόνιες.

01

Οικονομικές συνέπειες

Μία από τις χειρότερες συνέπειες αυτών των απατών είναι η οικονομική καταστροφή των θυμάτων, και τα περισσότερα θύματα συχνά υφίστανται σημαντικές οικονομικές απώλειες. Τα θύματα μπορεί να χάσουν τις οικονομίες τους, να υπερχρεωθούν ή ακόμη και να χρεοκοπήσουν. Η ανάκαμψη από τέτοιες οικονομικές καταστάσεις μπορεί να διαρκέσει χρόνια.

02

Συναισθηματικές επιπτώσεις

Τα θύματα απάτης συχνά βιώνουν βαθιά συναισθηματική οδύνη και παλεύουν με συναισθήματα προδοσίας, παραβίασης, ντροπής και ενοχής. Η συναισθηματική αναταραχή που προκαλείται από την εξαπάτηση και την απάτη μπορεί να οδηγήσει σε άγχος, κατάθλιψη, ακόμη και σε διαταραχή μετατραυματικού στρες (PTSD) και μπορεί επίσης να επηρεάσει τη σωματική υγεία.

03

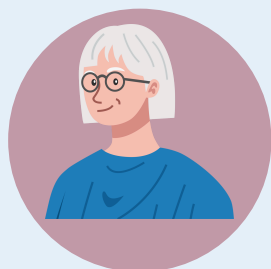
Νομικές επιπτώσεις

Σε περιπτώσεις απάτης όπου τα θύματα πείθονται να εξαργυρώσουν ψεύτικες «επιταγές βραβείων», μπορεί να αντιμετωπίσουν ακόμη και νομικές συνέπειες, όπως κατηγορίες για ξέπλυμα χρήματος και πλαστογραφία, πέραν της οικονομικής απώλειας.

Δελεαστικές απάτες: πλασματικά βραβεία και κληρώσεις



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Η Γκρέτα έλαβε ένα απροσδόκητο γραπτό μήνυμα που την ενημέρωνε ότι είχε κερδίσει ένα τζάκποτ σε μια ξένη λοταρία και ότι θα έπρεπε να πληρώσει αμέσως ένα προκαταβολικό «τέλος διαχείρισης» για να διεκδικήσει τα χρήματα του βραβείου της.

Το μήνυμα ξεκαθάριζε επίσης ότι δεν έπρεπε να μοιραστεί με κανέναν πληροφορίες σχετικά με το κέρδος της από το λαχείο και τις διαδικασίες για την παραλαβή του βραβείου της.

Δυστυχώς για τον απατεώνα ...

Η Γκρέτα παρακολούθησε πρόσφατα ένα σεμινάριο για την ασφάλεια στον κυβερνοχώρο, το οποίο περιελάμβανε συνεδρίες σχετικά με τις διαδικτυακές απάτες.



ΒΗΜΑ 1: Αναγνώριση προειδοποιητικών σημάτων

Η Γκρέτα εντόπισε αμέσως τα σημάδια της απάτης: ένα απροσδόκητο μήνυμα, ένα κέρδος από λαχείο (για το οποίο δεν είχε αγοράσει λαχνό) και ένα αίτημα για προκαταβολή.

ΒΗΜΑ 2: Εντοπισμός άλλων στρατηγικών απάτης

Η Γκρέτα αναγνώρισε την οδηγία να μην μοιραστεί λεπτομέρειες για τα κέρδη της από τη λοταρία με άλλους ως μια τακτική απομόνωσής της και για να την διευκολύνει να πέσει στην παγίδα μιας απάτης.

ΒΗΜΑ 3: Αποφυγή ανάμειξης

Η Γκρέτα δεν απάντησε στο γραπτό μήνυμα, προστατεύοντας έτσι τα προσωπικά της δεδομένα και αποφεύγοντας οικονομικές απώλειες.

ΒΗΜΑ 4: Αναφορά

Η Γκρέτα ενημέρωσε αμέσως την οικογένειά της, τους φίλους της και τις αρμόδιες αρχές για την απόπειρα απάτης και μοιράστηκε τις πληροφορίες στα μέσα κοινωνικής δικτύωσης.

Δελεαστικές απάτες: πλασματικά βραβεία και κληρώσεις



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Αν συναντήσετε μια προσπάθεια απάτης τύπου «δελεαστικής απάτης», το πρώτο πράγμα που πρέπει να θυμάστε είναι ότι δεν υπάρχουν δωρεάν χρήματα και να έχετε κατά νου τη γνωστή ρήση: «Αν κάτι φαίνεται πολύ καλό για να είναι αληθινό, μάλλον είναι». Ακολουθούν ορισμένες πρόσθετες συμβουλές σε περίπτωση που μπορεί να βρεθείτε σε μια τέτοια κατάσταση.

Χρησιμοποιήστε την κοινή λογική:

Αντισταθείτε στην παρόρμηση να ενεργήσετε γρήγορα σε απροσδόκητες ειδοποιήσεις για βραβεία που λάβατε είτε μέσω email, είτε μέσω μέσων κοινωνικής δικτύωσης, είτε μέσω γραπτού μηνύματος!

Πριν προβείτε σε οποιαδήποτε ενέργεια, σκεφτείτε αν έχετε συμμετάσχει έστω και σε κάποια κλήρωση ή λοταρία.



Έλεγχος νομιμότητας:

Ελέγξτε τον ιστότοπο ή τον αποστολέα της ειδοποίησης μέσω άλλων διαύλων.

Κάντε μια αναζήτηση στο διαδίκτυο ή συμβουλευτείτε την οικογένεια ή τους φίλους σας για να ελέγξετε την αξιοπιστία!

Μην κάνετε κλικ ή πατάτε σε συνδέσμους σε ειδοποιήσεις, ειδικά αν είναι ύποπτοι!



Δελεαστικές απάτες: πλασματικά βραβεία και κληρώσεις

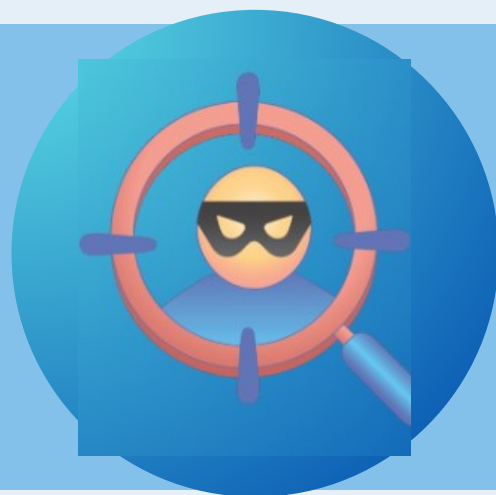


ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Ελέγξτε τις λεπτομέρειες:

Ελέγξτε προσεκτικά όλες τις πληροφορίες που λάβατε στην ειδοποίηση.

Προσέξτε τυχόν ασαφή ή ασυνήθιστα αιτήματα, όπως αιτήματα για προσωπικά στοιχεία, οικονομικές πληροφορίες ή πληρωμή εκ των προτέρων!



Θυμηθείτε:

Μην στείλετε ποτέ χρήματα ή μην πληρώσετε αμοιβή για την παραλαβή ενός βραβείου/χρήματος σε μια απροσδόκητη ειδοποίηση για ένα βραβείο!

Οι νόμιμες κληρώσεις δεν απαιτούν καμία πληρωμή για να συμμετάσχετε ή να διεκδικήσετε ένα βραβείο, ενώ η συμμετοχή σε λοταρίες απαιτεί την αγορά ενός λαχνού.

Δελεαστικές απάτες: πλασματικά βραβεία και κληρώσεις



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Εάν έχετε αποκαλύψει τα προσωπικά ή οικονομικά σας στοιχεία σε κάποιον απατεώνα, θα πρέπει να αλλάξετε αμέσως τους κωδικούς πρόσβασης του λογαριασμού ηλεκτρονικού ταχυδρομείου σας και όλων των άλλων λογαριασμών. Επίσης, αλλάξτε τους κωδικούς PIN στους τραπεζικούς σας λογαριασμούς και, αν χρησιμοποιείτε ηλεκτρονική τραπεζική, μην ξεχάσετε να αλλάξετε τον κωδικό πρόσβασης για την ηλεκτρονική σας τραπεζική.

Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης με συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμών και ειδικών χαρακτήρων!



Εάν ανοίξατε έναν ύποπτο σύνδεσμο και μοιραστήκατε τις οικονομικές ή προσωπικές σας πληροφορίες ή είχατε απώλεια, αναφέρετε το αμέσως στην αρμόδια αρχή της χώρας σας!

Απάτες με ψηφιακά νομίσματα

— ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Η απάτη με κρυπτονομίσματα αναφέρεται σε κάθε δόλια δραστηριότητα που σχετίζεται με ψηφιακά νομίσματα, όπως το Bitcoin. Μπορεί να λάβει πολλές μορφές, συμπεριλαμβανομένων των απατηλών αρχικών προσφορών νομισμάτων (ICO), των συστημάτων Ponzi και των απατηλών επενδυτικών ευκαιριών. Αυτές οι απάτες συνήθως υπόσχονται υψηλές αποδόσεις για να δελεάσουν τα θύματα, τα οποία στη συνέχεια χάνουν την επένδυσή τους όταν οι απατεώνες εξαφανίζονται με τα κεφάλαια. Οι ηλικιωμένοι είναι ιδιαίτερα ευάλωτοι σε αυτούς τους τύπους απάτης λόγω της μη εξοικείωσής τους με τις ψηφιακές τεχνολογίες και το διαδίκτυο. Οι απατεώνες συχνά εκμεταλλεύονται την εμπιστοσύνη και την οικονομική ασφάλεια των ηλικιωμένων, γεγονός που καθιστά απαραίτητη την ευαισθητοποίηση και την παροχή εκπαίδευσης για την προστασία τους από τέτοιου είδους απάτες.

Είδη απατών κρυπτονομισμάτων:

Αυτό το είδος απάτης λαμβάνει χώρα κατά τη διάρκεια του σταδίου συγκέντρωσης κεφαλαίων των νέων κρυπτονομισμάτων. Οι προγραμματιστές παρουσιάζουν ένα πολλά υποσχόμενο νέο ψηφιακό νόμισμα, συχνά με ένα λεπτομερές έγγραφο και υποσχέσεις για υψηλές αποδόσεις. Δυστυχώς, μόλις συγκεντρώσουν αρκετά κεφάλαια από τους επενδυτές, οι εν λόγω προγραμματιστές εξαφανίζονται χωρίς ίχνος, αφήνοντας τους επενδυτές με άχρηστα token.

Τα συστήματα αυτά υπόσχονται υψηλές αποδόσεις χαμηλού κινδύνου. Ωστόσο, οι αποδόσεις καταβάλλονται με κεφάλαια από νέους επενδυτές και όχι από κέρδη. Το σύστημα καταρρέει όταν δεν υπάρχουν αρκετοί νέοι επενδυτές, προκαλώντας σημαντικές απώλειες για τους τελευταίους επενδυτές.

Αυτός ο τύπος απάτης αφορά εφαρμογές ή λογισμικό που ισχυρίζονται ότι αποθηκεύουν με ασφάλεια κρυπτονομίσματα. Αυτά τα πορτοφόλια έχουν συχνά επαγγελματικής εμφάνισης διεπαφές και μπορεί ακόμη και να μιμούνται νόμιμα πορτοφόλια. Ωστόσο, στην πραγματικότητα είναι σχεδιασμένα για να απομυζούν ψηφιακά νομίσματα. Μόλις ένας χρήστης καταθέσει τα κρυπτονομίσματά του σε αυτά τα ψεύτικα πορτοφόλια, οι απατεώνες αποκτούν πρόσβαση σε αυτά, με αποτέλεσμα συχνά την πλήρη απώλεια των ψηφιακών περιουσιακών στοιχείων του χρήστη.

**Απάτη Initial
Coin
Offerings
(ICOs)**

**Συστήματα
Ponzi**

**Απάτες
ψεύτικου
πορτοφολιού**

Απάτες με ψηφιακά νομίσματα



ΣΥΝΕΠΕΙΕΣ:

Η χρηματοοικονομική και επενδυτική χειραγώγηση μπορεί να έχει σοβαρές αρνητικές επιπτώσεις, όπως:

01 Οικονομικές απώλειες

Η πιο άμεση και προφανής συνέπεια της απάτης με κρυπτονομίσματα είναι η οικονομική απώλεια. Τα θύματα συχνά χάνουν ολόκληρη την επένδυσή τους, γεγονός που μπορεί να είναι καταστροφικό, ειδικά αν έχουν επενδύσει μεγάλο μέρος των αποταμιεύσεών τους.

02 Απώλεια εμπιστοσύνης

Τα θύματα απάτης με κρυπτονομίσματα συχνά χάνουν την εμπιστοσύνη τους στα ψηφιακά νομίσματα και μπορεί να διστάζουν να επενδύσουν ή να συμμετάσχουν στην ψηφιακή οικονομία στο μέλλον. Αυτό μπορεί να εμποδίσει την ανάπτυξη και την αποδοχή των κρυπτονομισμάτων.

03 Νομικές συνέπειες

Σε ορισμένες περιπτώσεις, οι συμμετέχοντες σε δόλια σχήματα, ακόμη και εν αγνοία τους, ενδέχεται να αντιμετωπίσουν νομικές συνέπειες. Αυτό μπορεί να περιλαμβάνει έρευνα από τις ρυθμιστικές αρχές και πιθανές κατηγορίες εάν εν αγνοία τους βοήθησαν στη διευκόλυνση της απάτης.

Απάτες με ψηφιακά νομίσματα



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Μια μέρα, η Ελένη έλαβε ένα email. Ήταν μια πρόσκληση να επενδύσει σε ένα νέο κρυπτονόμισμα που υποσχόταν σημαντικές αποδόσεις. Ενδιαφερόμενη και πρόθυμη να αυξήσει το ψηφιακό της χαρτοφυλάκιο, αποφάσισε να το διερευνήσει.

Το μήνυμα ηλεκτρονικού ταχυδρομείου προερχόταν από μια εταιρεία που ονομαζόταν «CryptoGold» και ο ιστότοπός της ήταν εντυπωσιακός, γεμάτος με μαρτυρίες ικανοποιημένων επενδυτών και υποσχέσεις για υψηλές αποδόσεις. Η ευκαιρία φαινόταν πολύ καλή για να την αφήσει να περάσει ανεκμετάλλευτη, οπότε αποφάσισε να επενδύσει ένα μικρό μέρος των αποταμιεύσεών της.

Οι μέρες έγιναν εβδομάδες, και η Ελένη έλεγχε με ανυπομονησία το διαδικτυακό πορτοφόλι της κάθε μέρα, ελπίζοντας να δει την επένδυσή της να αυξάνεται. Αλλά, αντίθετα, παρατήρησε ότι η επένδυσή της μειωνόταν. Μπερδεμένη και ανήσυχη, προσπάθησε να επικοινωνήσει με την «CryptoGold». Ωστόσο, όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου της αναπήδησαν και ο άλλοτε εντυπωσιακός ιστότοπος ήταν πλέον απρόσιτος.

Η ιστορία της Ελένης υπογραμμίζει την ανάγκη προστασίας των ηλικιωμένων από τις απάτες με κρυπτονομίσματα μέσω της ευαισθητοποίησης και της εκπαίδευσης. Οι ηλικιωμένοι μπορεί να είναι ευάλωτοι λόγω της ψηφιακής εξοικείωσης και, ως εκ τούτου, πρέπει να κατανοήσουν τους κινδύνους, τα σημάδια των απάτων και τη σημασία του σκεπτικισμού απέναντι στις υποσχέσεις υψηλής απόδοσης. Τα υποστηρικτικά δίκτυα είναι επίσης ζωτικής σημασίας για την ασφαλή ψηφιακή πλοήγηση.



ΒΗΜΑ 1: Έρευνα της εταιρείας

Η Ελένη θα έπρεπε να είχε ερευνήσει διεξοδικά το «CryptoGold» πριν επενδύσει. Αντί να εντυπωσιάζεται από την ιστοσελίδα και τις μαρτυρίες, θα έπρεπε να είχε ελέγξει αν η εταιρεία ήταν εγγεγραμμένη και να αναζητήσει κριτικές ή προειδοποιήσεις από άλλους χρήστες.

ΒΗΜΑ 3: Αποφυγή άμεσων αποφάσεων

Η Ελένη αποφάσισε γρήγορα να επενδύσει χωρίς να αφιερώσει χρόνο για να κατανοήσει πλήρως τους όρους και τους κινδύνους που ενέχει. Θα έπρεπε να αποφύγει να λάβει βιαστικές επενδυτικές αποφάσεις και να ζητήσει συμβουλές από άτομα με γνώσεις ή χρηματοοικονομικούς συμβούλους.

ΒΗΜΑ 2: Επαλήθευση επικοινωνίας

Η Ελένη έλαβε ένα ανεπιθύμητο μήνυμα ηλεκτρονικού ταχυδρομείου και το εμπιστεύτηκε χωρίς επαλήθευση. Θα έπρεπε να είναι προσεκτική και να επικυρώσει την ταυτότητα του αποστολέα διασταυρώνοντας με αξιόπιστες πηγές, όπως επίσημα στοιχεία επικοινωνίας εταιρειών ή γνωστά φόρουμ κρυπτονομισμάτων.

ΒΗΜΑ 4: Παρακολούθηση των επενδύσεων σε τακτά χρονικά διαστήματα

Η Ελένη δεν παρατήρησε άμεσα σημάδια απάτης και συνέχισε να ελπίζει σε θετικές αποδόσεις. Θα έπρεπε να παρακολουθεί τακτικά τις επενδύσεις της και να επισημαίνει αμέσως οποιαδήποτε ασυνήθιστη δραστηριότητα ή έλλειψη διαφάνειας για περαιτέρω έρευνα.

Απάτες με ψηφιακά νομίσματα



ΤΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Η προστασία από απάτες με κρυπτονομίσματα είναι ζωτικής σημασίας, ιδίως για τους ηλικιωμένους, επειδή μπορεί να είναι ιδιαίτερα ευάλωτοι λόγω της μη εξοικείωσής τους με τις ψηφιακές τεχνολογίες. Οι απατεώνες συχνά στοχεύουν τους ηλικιωμένους με υποσχέσεις για υψηλές αποδόσεις, εκμεταλλευόμενοι την εμπιστοσύνη και την οικονομική τους ασφάλεια. Το να πέσετε θύμα αυτών των απατών μπορεί να οδηγήσει σε σημαντική οικονομική απώλεια, απώλεια της εμπιστοσύνης στις ψηφιακές καινοτομίες και πιθανές νομικές συνέπειες. Η εκπαίδευση, η διεξοδική έρευνα και η διατήρηση ενός υγιούς σκεπτικισμού απέναντι στις υπερβολικά καλές για να είναι αληθινές προσφορές αποτελούν βασικά βήματα για τη διαφύλαξη των περιουσιακών στοιχείων και την εξασφάλιση της οικονομικής ευημερίας.

ΕΚΠΑΙΔΕΥΣΗ:

Η κατανόηση του τρόπου λειτουργίας των κρυπτονομισμάτων είναι το πρώτο βήμα για την αποφυγή της απάτης. Αυτό περιλαμβάνει την κατανόηση της τεχνολογίας πίσω από αυτά, τον τρόπο λειτουργίας των συναλλαγών και τον τρόπο ασφαλούς αποθήκευσης και προστασίας των ψηφιακών σας περιουσιακών στοιχείων



ΕΡΕΥΝΑ:

Πριν επενδύσετε σε οποιοδήποτε κρυπτονόμισμα, ερευνήστε διεξοδικά το ψηφιακό νόμισμα, την ομάδα που το υποστηρίζει και διαβάστε τυχόν διαθέσιμα λευκά έγγραφα. Να είστε επιφυλακτικοί με τα νέα κρυπτονομίσματα που υπόσχονται υψηλές αποδόσεις με μικρό κίνδυνο.



Απάτες με ψηφιακά νομίσματα



WAYS OF PROTECTION:

ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΠΟΡΤΟΦΟΛΙΟΥ:

Προστατέψτε τα ψηφιακά σας περιουσιακά στοιχεία χρησιμοποιώντας ένα ασφαλές πορτοφόλι. Αυτό μπορεί να είναι ένα πορτοφόλι υλικού που αποθηκεύει το νόμισμα εκτός σύνδεσης ή ένα αξιόπιστο ηλεκτρονικό πορτοφόλι με ισχυρά μέτρα ασφαλείας. Ενεργοποιείτε πάντα τον έλεγχο ταυτότητας δύο παραγόντων, εάν είναι διαθέσιμος.



ΠΑΡΑΜΕΙΝΕΤΕ ΣΚΕΠΤΙΚΟΙ:

Να είστε επιφυλακτικοί απέναντι σε κάθε επένδυση που υπόσχεται υψηλές αποδόσεις με μικρό έως καθόλου κίνδυνο. Αυτές είναι συχνά πολύ καλές για να είναι αληθινές. Να θυμάστε ότι οι νόμιμες επενδύσεις συνήθως δεν εγγυώνται αποδόσεις και ενέχουν πάντα κάποιο επίπεδο κινδύνου.

ΑΝΑΦΟΡΑ ΥΠΟΠΤΗΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ:

Εάν συναντήσετε μια πιθανή απάτη με κρυπτονομίσματα, αναφέρετε την στις τοπικές αρχές και σε οποιοσδήποτε σχετικές διαδικτυακές πλατφόρμες. Αυτό όχι μόνο συμβάλλει στην προστασία σας, αλλά και στην προειδοποίηση και προστασία άλλων.



Διεθνής οικονομική απάτη



ΧΑΡΑΚΗΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Η απάτη 419, γνωστή και ως νιγηριανή απάτη, είναι μια διαβόητη απάτη με προκαταβολικά τέλη που ξεκίνησε από τη Νιγηρία, από τις πρώτες μέρες του Διαδικτύου, και έχει γίνει μια από τις πιο διαδεδομένες απάτες παγκοσμίως.

Τύποι χειραγώγησης στην απάτη 419:

Με τη λέξη « Χαίρετε» στη γραμμή του θέματος, θα σας υποδεχτεί ένας πλούσιος Νιγηριανός πρίγκιπας, (ακόμη και ένας Νιγηριανός αστροναύτης), ένας πλούσιος δικηγόρος ή επιχειρηματίας και θα σας προσφέρει ένα μεγάλο χρηματικό ποσό για να τον βοηθήσει να μεταφέρει τα χρήματά του από τη Νιγηρία (ή να του επιτρέψει την πρόσβαση στο λογαριασμό) με αντάλλαγμα μια μικρή προκαταβολή για την κάλυψη των υποτιθέμενων εξόδων συναλλαγής.

Με τη λέξη « Χαίρετε » στη γραμμή του θέματος, θα σας υποδεχτεί ένα άτομο που αντιμετωπίζει μια δύσκολη κατάσταση ζωής, όπως η απαγωγή των παιδιών του, ή ένα άτομο που, λόγω της πολιτικής κατάστασης, έχει γίνει φυγάς ή αθώος κρατούμενος κ.λπ. Ωστόσο, όλοι τους μοιράζονται μια μακρά και θλιβερή ιστορία σχετικά με το γιατί δεν μπορούν να εισπράξουν τα χρήματά τους, γι' αυτό και ζητούν τη βοήθειά σας.

Πλαστοπροσωπία (παραλλαγή 1)

Πλαστοπροσωπία (παραλλαγή 2)

Διεθνής οικονομική απάτη

Πίσω από τις νιγηριανές απάτες κρύβονται επαγγελματίες απατεώνες που χρησιμοποιούν μια συστηματική προσέγγιση και δοκιμασμένες τεχνικές για να χειραγωγήσουν τα ανθρώπινα συναισθήματα και τα τρωτά σημεία. Χρησιμοποιούν ένα προκατασκευασμένο εγχειρίδιο, γνωστό στη νιγηριανή απάτη ως «σενάριο» ή «μορφή». Αυτό συχνά περιλαμβάνει περίτεχνες ιστορίες, ψεύτικες ταυτότητες και πλαστά έγγραφα που φαίνονται νόμιμα και απλώς αντιγράφονται και χρησιμοποιούνται από τους απατεώνες στην επικοινωνία τους με τα θύματα.

Στη νιγηριανή απάτη, η επικοινωνία γίνεται αποκλειστικά μέσω ηλεκτρονικού ταχυδρομείου, μηνυμάτων κειμένου ή κοινωνικών δικτύων. Σε αυτόν τον τύπο απάτης, οι απατεώνες δεν επικοινωνούν με τα θύματα μέσω βίντεο ή τηλεφώνου. Τα λαμβανόμενα μηνύματα περιέχουν γραμματικά λάθη και κακή μορφοποίηση του κειμένου.

Μόλις το θύμα δεν παρέχει πλέον χρήματα ή προσωπικές πληροφορίες ή συνειδητοποιήσει ότι έχει εξαπατηθεί, οι απατεώνες σταματούν αμέσως να απαντούν στην αλληλογραφία και απλά εξαφανίζονται.

**Παιχνίδι με τα
συναισθήματα
των ανθρώπων**

**Αποκλειστική
χρήση γραπτής
ψηφιακής
επικοινωνίας**

Εξαφάνιση

Διεθνής οικονομική απάτη

— ΣΥΝΕΠΕΙΕΣ:

Αυτή η απάτη μπορεί να θέσει σε κίνδυνο ανθρώπους όλων των ηλικιών, ιδίως όσους πιστεύουν σε συστήματα γρήγορου πλουτισμού ή είναι οικονομικά αφελείς. Ωστόσο, οι ηλικιωμένοι είναι ακόμη πιο ευάλωτοι, καθώς συνήθως εμπιστεύονται περισσότερο τους άλλους και γνωρίζουν λιγότερο για την ασφάλεια στο διαδίκτυο.

01 Οικονομικές συνέπειες

Τα θύματα μπορεί να χάσουν μεγάλα χρηματικά ποσά, οδηγώντας σε σοβαρά οικονομικά προβλήματα. Όταν τα θύματα ανταποκρίνονται θετικά, πέφτουν στην παγίδα να τους ζητούνται όλο και περισσότερα χρήματα από τους απατεώνες, οι οποίοι επινοούν κάθε είδους ψεύτικες δικαιολογίες ή προτάσεις για επιπλέον πληρωμές. Σε αυτή την περίπτωση μπορεί επίσης να εμφανιστεί η πλάνη του βυθισμένου κόστους (Sunk Cost Fallacy), όπου τα θύματα συνεχίζουν να επιδιώκουν κάτι στο οποίο έχουν ήδη επενδύσει πολλά (είτε πρόκειται για χρήματα, είτε για χρόνο, είτε για προσπάθεια, είτε για συναισθηματική ενέργεια κ.λπ.), παρόλο που το να τα παρατήσουν θα ήταν πολύ καλύτερη ιδέα.

02 Συναισθηματικές συνέπειες

Όταν η ντροπή ή η αμηχανία ενθαρρύνει τη μυστικοπαθή συμπεριφορά, μπορεί συχνά να οδηγήσει τα θύματα σε επανειλημμένες απάτες.

03 Κοινωνικές συνέπειες

Μετά την εξαπάτηση, η εμπιστοσύνη του ατόμου σε άλλους ανθρώπους μπορεί να μειωθεί σημαντικά, οδηγώντας σε απομόνωση και δυσκολίες στη διατήρηση και τη δημιουργία σχέσεων.

Διεθνής οικονομική απάτη



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Η Έμμα περιηγούνταν στο διαδίκτυο όταν έλαβε ένα μήνυμα ηλεκτρονικού ταχυδρομείου με τίτλο « Χαίρετε». Ο αποστολέας του email ήταν ένας Νιγηριανός «πρίγκιπας» που χρειαζόταν τη βοήθειά της για τη μεταφορά ενός μεγάλου χρηματικού ποσού από τη Νιγηρία. Σε αντάλλαγμα, θα λάμβανε ένα ποσοστό των χρημάτων για τη βοήθειά της, με αντάλλαγμα μια μικρή αμοιβή για τη διευκόλυνση της συναλλαγής. Παρά τη δελεαστική προσφορά, η Έμμα έγινε καχύποπτη!

Δυστυχώς για τον απατεώνα ...

Η Emma διάβασε πρόσφατα ένα διαδικτυακό άρθρο σχετικά με τις απάτες 419 και έμαθε για όλες τις παραλλαγές της απάτης.



ΒΗΜΑ 1: Αναγνώριση προειδοποιητικών σημάτων στην επικοινωνία

Έμμα παρατήρησε ότι το περιεχόμενο του email ήταν γραμμένο σε πολύ κακά αγγλικά και δεν έβγαζε κανένα νόημα.

ΒΗΜΑ 2: Χρήση γνώσεων

Η Έμμα έμαθε επίσης διαβάζοντας ένα διαδικτυακό άρθρο για τις απάτες 419 ότι δεν υπάρχουν βασιλικές οικογένειες στη Νιγηρία.

ΒΗΜΑ 3: Αποφασιστική δράση

Η Έμμα χαρακτήρισε αμέσως το email ως spam και το διέγραψε. Το ίδιο έκανε και με άλλα μηνύματα που ακολούθησαν, τα οποία προέρχονταν από τον «υποτιθέμενο» Νιγηριανό πρίγκιπα.

ΒΗΜΑ 4: Προώθηση μιας κοινότητας ενημερωμένων και ευαισθητοποιημένων ατόμων

Η Έμμα μοιράστηκε την εμπειρία της με τον σύζυγό της, την οικογένειά της και τους φίλους της και μοιράστηκε τις πληροφορίες στα μέσα κοινωνικής δικτύωσης.

Διεθνής οικονομική απάτη



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Αν συναντήσετε μια απόπειρα απάτης τύπου 419, το πρώτο πράγμα που πρέπει να θυμάστε είναι ότι κανείς δεν έχει πάρει ένα μεγάλο χρηματικό ποσό εξαιτίας ενός απροσδόκητου μηνύματος στα εισερχόμενά του!

Ακολουθούν ορισμένες πρόσθετες συμβουλές σε περίπτωση που μπορεί να βρεθείτε σε μια τέτοια κατάσταση.

Εάν λάβετε μια προσφορά απάτης 419 και μπίτε στον πειρασμό να την αποδεχτείτε, σταματήστε και κάντε στον εαυτό σας αυτές τις δύο απλές ερωτήσεις κοινής λογικής:

Γιατί θα μοιραζόσασταν τις προσωπικές και οικονομικές σας πληροφορίες με έναν εντελώς άγνωστο (που προέρχεται από μια χώρα με την οποία δεν έχετε καμία σχέση) και γιατί αυτός ο άγνωστος θα επέλεγε εσάς για να μοιραστεί μαζί σας μια περιουσία;



Ακόμα και αν συγκινηθείτε μέχρι τα βάθη της καρδιάς σας, από την ιστορία «της απαγωγής παιδιών», **μην στέλνετε ποτέ χρήματα** (ή άλλες οικονομικές πληροφορίες) πριν ελέγξετε τη γνησιότητα του ατόμου που σας ζητάει οικονομική βοήθεια!

Λάβετε επίσης υπόψη σας ότι οι απάτες 419 σας δελεάζουν να πληρώσετε μέσω υπηρεσιών μεταφοράς χρημάτων! (συνήθως Western Union)

Διεθνής οικονομική απάτη



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Εξετάστε τη γνησιότητα του περιεχομένου:

Καθώς οι απατεώνες του 419 χρησιμοποιούν επανειλημμένα σενάρια, μπορείτε να ελέγξετε τη γνησιότητα ενός ηλεκτρονικού ταχυδρομείου εισάγοντας απλώς ένα σύντομο τμήμα του περιεχομένου του σε μια μηχανή αναζήτησης (Google, Bing κ.λπ.). Εάν το περιεχόμενο αποτελεί μέρος γνωστών ή μη αποκαλυφθέντων μηνυμάτων απάτης, θα βρείτε ιστότοπους που προειδοποιούν για αυτή την απάτη, η οποία έχει ήδη αναφερθεί από άλλα θύματα.



Μην απαντάτε σε ανεπιθύμητα e-mail (ούτε καν ως φάρσα)!

Διαγράψτε τα αμέσως!

Να θυμάστε ότι αν απαντήσετε - πιθανότατα θα πέσετε σε οικονομική παγίδα!

Διεθνής οικονομική απάτη



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Εάν έχετε αποκαλύψει τα οικονομικά σας στοιχεία σε έναν απατεώνα, αλλάξτε τα PIN και τον κωδικό πρόσβασής σας (εάν χρησιμοποιείτε ηλεκτρονική τραπεζική).

Λάβετε πρόσθετα μέτρα ασφαλείας για οικονομικές συναλλαγές, όπως ο έλεγχος ταυτότητας δύο παραγόντων (2FA) και η λειτουργία ειδοποίησης συναλλαγών και παρακολουθείτε τακτικά το υπόλοιπο του λογαριασμού σας.



REPORT

Εάν έχετε υποστεί οικονομική ζημία, αναφέρετε την αμέσως στην τράπεζά σας και σε άλλες αρμόδιες αρχές της χώρας σας!

Περαιτέρω αναγνώσματα



ΟΙΚΟΝΟΜΙΚΕΣ ΚΑΙ ΕΠΕΝΔΥΤΙΚΕΣ ΧΕΙΡΑΓΩΓΗΣΕΙΣ

- <https://faircanada.ca/investing-basics/protecting-vulnerable-investors-from-financial-abuse/>
- <https://economictimes.indiatimes.com/wealth/legal/will/how-can-senior-citizens-protect-themselves-from-financial-exploitations-by-their-own-families/articleshow/103877992.cms?from=mdr>
- <https://www.morganstanley.com/articles/elder-financial-abuse-protecting-loved-ones>
- <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6044329/>
- <https://www.psychiatrist.com/pcc/financial-abuse-older-adults-screening-prevention-interventions-primary-care-providers/>
- <https://www.youtube.com/watch?v=7G8lil8Yupg>
- <https://www.c-span.org/video/?324176-1/financial-exploitation-senior-citizens>



ΦΑΙΝΟΜΕΝΙΚΟΣ ΑΛΤΡΟΥΙΣΜΟΣ: ΑΠΑΘΗ ΓΙΑ ΦΙΛΑΝΘΡΩΠΙΑ

- <https://www.bbc.com/news/uk-34530586>
- <https://www.youtube.com/watch?app=desktop&v=MTm-fq0OUQQ>
- https://www.americansenioralliance.com/episode_5
- <https://www.youtube.com/watch?v=vR53sRLVgpc>
- <https://www.theguardian.com/society/2015/sep/01/charities-face-scrutiny-over-trading-of-elderly-mans-data>

Περαιτέρω αναγνώσματα



ΔΕΛΕΑΣΤΙΚΕΣ ΨΕΥΔΑΙΣΘΗΣΕΙΣ: ΠΛΑΣΜΑΤΙΚΑ ΕΠΑΘΛΑ ΚΑΙ ΛΑΧΕΙΑ

- <https://www.identityguard.com/news/lottery-scams>
- <https://www.pcrisk.com/> <https://www.naperville.il.us/services/naperville-police-department/community-education-and-crime-prevention/frauds-and-scams/>
- <https://www.scamwatch.gov.au/system/files/Little%20Black%20Book%20of%20Scams%20-%20Final.pdf>
- <https://www.gamblingcommission.gov.uk/public-and-players/guide/lottery-scams-and-fraud>
- <https://www.identityguard.com/news/online-safety-tips-for-seniors>
- <https://www.liveabout.com/warning-signs-of-sweepstakes-scams-886996>
- <https://surfshark.com/research/data-breach-impact/crime-lottery-inheritance-scam> <https://www.aura.com/learn/sweepstakes-scams>



ΑΠΑΤΕΣ ΜΕ ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ

- <https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams> <https://www.coindesk.com/learn/crypto-scams-types-of-crypto-schemes-and-how-to-avoid-getting-scammed>
- <https://www.fastex.com/en/learn/crypto-scams-explained>
- <https://cointelegraph.com/explained/impersonation-scams-in-crypto-explained> <https://www.ftc.gov/news-events/news/press-releases/2022/06/new-analysis-finds-consumers-reported-losing-more-1-billion-cryptocurrency-scams-2021>
- <https://www.mdpi.com/2227-9091/11/3/51>
- <https://www.cybertrace.com.au/cryptocurrency-fraud-explained>
- <https://www.arkoselabs.com/guide-to-cryptocurrency-security>
- <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-new-analysis-reveals-consumers-lost-nearly-500-million-cryptocurrency-scams>
- <https://www.kaspersky.com/resource-center/threats/top-seven-tips-for-preventing-cryptocurrency-scams>

Περαιτέρω αναγνώσματα



ΔΙΕΘΝΗΣ ΟΙΚΟΝΟΜΙΚΗ ΑΠΑΤΗ

- <https://www.altospam.com/en/glossary/scam-nigerian419/>
- <https://www.comparitech.com/identity-theft-protection/nigerian-scam/>
- <https://www.comparitech.com/identity-theft-protection/nigerian-scam/>
- <https://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy#ref829190>
- <https://www.wallstreetmojo.com/nigerian-scam/#nigerian-letter-scam-explained>
- <https://whatismyipaddress.com/nigerian-fraud-combines-scams>
- <https://hackernoon.com/the-nigerian-prince-email-and-the-history-of-social-engineering-techniques>
- <https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html>

ΚΕΦΑΛΑΙΟ 3.

ΚΟΙΝΩΝΙΚΗ ΧΕΙΡΑΓΩΓΗΣΗ ΚΑΙ ΣΥΝΑΙΣΘΗΜΑΤΙΚΗ ΕΞΑΠΑΤΗΣΗ

Οι σύγχρονες απάτες λαμβάνουν όλο και περισσότερο τη μορφή κοινωνικής και συναισθηματικής χειραγώγησης, καθιστώντας τους ηλικιωμένους ιδιαίτερα εύάλωτους σε αυτές τις απειλές. Οι εγκληματίες εκμεταλλεύονται τα συναισθήματα, την εμπιστοσύνη και την αφέλεια για να επιτύχουν τους στόχους τους, καταστρέφοντας συχνά την οικονομική και συναισθηματική ευημερία των θυμάτων τους. Αυτό το κεφάλαιο έχει ως στόχο να συζητήσει τις πιο συνηθισμένες απάτες που βασίζονται στη συναισθηματική και κοινωνική χειραγώγηση, βοηθώντας τους ηλικιωμένους να αναγνωρίζουν και να προστατεύονται από αυτούς τους κινδύνους.

Μεταξύ των πιο επικίνδυνων είναι οι ρομαντικές απάτες, όπου οι εγκληματίες οικοδομούν σχέσεις για να αποσπάσουν χρήματα. Οι απάτες «smishing» και οι τηλεφωνικές απάτες αποτελούν επίσης σοβαρές απειλές, καθώς οι απατεώνες υποδύονται έμπιστα άτομα ή ιδρύματα για να αποκτήσουν προσωπικές πληροφορίες ή χρήματα.

Οι απάτες με παππούδες, όπου οι απατεώνες παριστάνουν τα μέλη της οικογένειας, και οι απάτες που αφορούν ιατρικά προϊόντα είναι πρόσθετες μέθοδοι χειραγώγησης. Η κατανόηση αυτών των απειλών είναι ζωτικής σημασίας για την προστασία της οικονομικής και συναισθηματικής ευημερίας των ηλικιωμένων.

Απάτη στις σχέσεις ανδρών-γυναικών



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Μια απάτη διαδικτυακής γνωριμίας, επίσης γνωστή ως απάτη ρομαντισμού, συμβαίνει όταν ένα θύμα εξαπατάται πιστεύοντας ότι είναι σε μια ρομαντική σχέση με κάποιον που γνώρισε στο διαδίκτυο. Ωστόσο, ο υποτιθέμενος σύντροφός τους είναι απατεώνας.

Τύποι παραπλάνησης σε ένα διαδικτυακό ειδύλλιο:

Οι απατεώνες δημιουργούν ψεύτικα διαδικτυακά προφίλ και παρουσιάζονται ως άτομα που βρίσκονται μακριά από το θύμα, τις περισσότερες φορές στο εξωτερικό, σε αποστολή (γιατρός, στρατιώτης, φιλόanthropos), εργάζονται σε εξέδρα άντλησης πετρελαίου κλπ.

Τα ενδιαφέροντα και τα χόμπι του απατεώνα είναι σχεδόν ακριβώς τα ίδια με τα θύματα ... και οι φωτογραφίες είναι απλά ... ΟΥΑΟΥ! Αν και εκτός από μερικές «τέλειες φωτογραφίες», δεν υπάρχουν πολλές (ή καθόλου) άλλες φωτογραφίες του/της σε διάφορες καταστάσεις της ζωής.

Μόλις όλα φαίνονται ρόδινα (δήλωση αγάπης, πρόταση γάμου κ.λπ.), ο απατεώνας καλεί τα θύματα να επικοινωνήσουν ιδιωτικά (αποκτώντας έτσι τον αριθμό τηλεφώνου, τη διεύθυνση ηλεκτρονικού ταχυδρομείου και άλλες πληροφορίες) και υπόσχεται να τα δει σύντομα από κοντά.

Και εκεί που όλα φαίνονται ακόμα πιο ρόδινα, έρχεται το αίτημα για χρήματα, συνοδευόμενο από μια ιστορία που προκαλεί ενσυναίσθηση και ένα αίτημα για συγκεκριμένες μεθόδους πληρωμής (έμβασμα, νεοσύστατος τραπεζικός λογαριασμός στο όνομα του θύματος κ.λπ.).

Πλαστή
ταυτότητα

Τελειότητα

Γρήγορη
εξέλιξη

Αίτημα
για...
ΧΡΗΜΑΤΑ

Απάτη στις σχέσεις ανδρών-γυναικών



ΣΥΝΕΠΕΙΕΣ:

Οι ρομαντικές απάτες μπορεί να οδηγήσουν σε σοβαρές οικονομικές απώλειες και σημαντική συναισθηματική οδύνη για τα θύματα.

01 Οικονομικές συνέπειες

Επειδή τα θύματα συχνά πιστεύουν ότι βοηθούν ένα αγαπημένο τους πρόσωπο που έχει ανάγκη, είναι πρόθυμα να χρησιμοποιήσουν τα χρήματά τους και να τα επενδύσουν στη σχέση. Για χάρη της «αγάπης» ορισμένα θύματα θυσιάζουν ακόμη και το σύνολο των αποταμιεύσεών τους, παίρνουν πρόσθετα δάνεια ή ακόμη και πωλούν τα περιουσιακά τους στοιχεία. Τα δεδομένα που αποκτούν οι απατεώνες από τα θύματα (στοιχεία τραπεζικών λογαριασμών, πιστωτικών καρτών) μπορούν να χρησιμοποιηθούν για μη εξουσιοδοτημένες συναλλαγές ή αναλήψεις, οδηγώντας σε σημαντικές οικονομικές απώλειες.

02 Συναισθηματικές συνέπειες

Η απάτη στις διαδικτυακές γνωριμίες είναι ιδιαίτερα σκληρή, καθώς παίζει με τα συναισθήματα των ανθρώπων. Η αποκάλυψη ότι μια διαδικτυακή σχέση είναι απάτη προκαλεί παρόμοια συναισθηματική ζημιά στο θύμα με το ξαφνικό τέλος μιας σχέσης που βασίζεται στη φυσική αλληλεπίδραση. Αυτό συχνά δυσκολεύει τα θύματα να σπάσουν την αγάπη που νιώθουν για τον απατεώνα, ακόμη και όταν συνειδητοποιούν ότι έχουν εξαπατηθεί.

03 Ψυχολογικές συνέπειες

Τα θύματα ρομαντικής απάτης είναι επιρρεπή σε ψυχολογικό πόνο, όπως ντροπή, αμηχανία, άγχος, κατάθλιψη και φόβο. Τα θύματα μπορεί να εμφανίσουν συμπτώματα που μοιάζουν με μείζονα καταθλιπτική διαταραχή, θλίψη ή διαταραχή μετατραυματικού στρες (PTSD).

Απάτη στις σχέσεις ανδρών-γυναικών



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΤΗΝ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Δύο χρόνια μετά το θάνατο του συζύγου της, τα εγγόνια της Μαργκώ την έπεισαν να εγγραφεί σε μια διαδικτυακή ιστοσελίδα γνωριμιών. Σύντομα, άρχισε να συνομιλεί με έναν άνδρα ονόματι Τομ, γιατρό σε ανθρωπιστική αποστολή στην Αφρική.

Μετά από μερικές εβδομάδες ειλικρινών συζητήσεων, ο Τομ ισχυρίστηκε ότι είχε «προβλήματα ρευστότητας» και χρειαζόταν χρήματα για να καλύψει τα έξοδα. Η Μάργκοτ έγινε καχύποπτη και συζήτησε το ασυνήθιστο αίτημα με τα εγγόνια της. Μαζί ερεύνησαν το προφίλ του και ανακάλυψαν ότι ο Τομ ήταν απατεώνας.

Δυστυχώς για τον απατεώνα ...

Η Μαργκώ πήρε τη σωστή απόφαση όταν μίλησε ανοιχτά στους οικείους της για τις υποψίες της περί απάτης.



ΒΗΜΑ 1: Ακολουθήστε τη διαίσθηση

Η Μαργκώ αισθάνθηκε ότι κάτι δεν πήγαινε καλά. Εμπιστεύτηκε το ένστικτό της και δεν έσπευσε να τον βοηθήσει, αλλά πρώτα σκέφτηκε το παράξενο του αιτήματός του.

ΒΗΜΑ 2: Αναζήτηση συμβουλών από έμπιστα άτομα

Αντί να πάρει η ίδια την απόφαση, η Μαργκώ συμβουλευτηκε τα εγγόνια της. Μοιράστηκε μαζί τους τις λεπτομέρειες του αιτήματος του Τομ και ζήτησε τη συμβουλή τους.

ΒΗΜΑ 3: Έρευνα

Μαζί ερεύνησαν το προφίλ του Τομ και διαπίστωσαν ότι επρόκειτο για απατεώνα. Αυτή η συνειδητοποίηση απέτρεψε τη Μαργκώ από το να του στείλει χρήματα και να πέσει θύμα της απάτης του.

ΒΗΜΑ 4: Αναφορά

Η Μαργκώ ενημέρωσε τον ιστότοπο γνωριμιών, επικοινωνώντας με τον διαχειριστή του ιστότοπου και ανέφερε τον Τομ για υποψία απάτης.

Απάτη στις σχέσεις ανδρών-γυναικών



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Οι απατεώνες που εκμεταλλεύονται τη μοναξιά των ηλικιωμένων, ιδίως των πρόσφατα χήρων ή διαζευγμένων, εκμεταλλευόμενοι την ευαλωτότητα και τους οικονομικούς τους πόρους για να αναπτύξουν ψεύτικες ρομαντικές σχέσεις στο διαδίκτυο σε πλατφόρμες κοινωνικής δικτύωσης, ιστοσελίδες γνωριμιών κ.λπ.

Ακολουθούν ορισμένες πρόσθετες συμβουλές σε περίπτωση που μπορεί να βρεθείτε σε μια τέτοια κατάσταση.

Προσέξτε τι μοιράζεστε στο διαδίκτυο:

Οι πληροφορίες που μοιράζεστε δημοσίως (ενδιαφέροντα, χόμπι, τρόπος ζωής κ.λπ.) μπορούν να χρησιμοποιηθούν από τους απατεώνες για να δημιουργήσουν μια ψεύτικη προσωπικότητα για να προσελκύσουν το ρομαντικό σας ενδιαφέρον.



Σε οποιαδήποτε διαδικτυακή σχέση, κρατήστε τις προσωπικές/οικονομικές σας πληροφορίες για τον εαυτό σας:

Μην μοιράζεστε πολλές προσωπικές πληροφορίες με έναν πιθανό διαδικτυακό ερωτικό σύντροφο και σίγουρα μην αποκαλύπτετε τα οικονομικά σας στοιχεία. Αλλά πάνω απ' όλα - **Μην στέλνετε χρήματα ή αγοράζετε τιμαλφή σε κανέναν που δεν έχετε γνωρίσει ποτέ!**

Απάτη στις σχέσεις ανδρών-γυναικών



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Επαλήθευση:

Αν και δεν μπορείτε να επαληθεύσετε όλα όσα σας λέει ένας διαδικτυακός ερωτικός σύντροφος, μπορείτε να ελέγξετε ορισμένες συγκεκριμένες λεπτομέρειες **χρησιμοποιώντας το διαδίκτυο για να επαληθεύσετε** το όνομα, το επώνυμο, τον τόπο διαμονής, τα προφίλ στα μέσα κοινωνικής δικτύωσης, **τη γνησιότητα** των αναρτημένων και αποσταλμένων φωτογραφιών και να ελέγξετε αν χρησιμοποιούν ανακυκλωμένες ιστορίες ή εκφράσεις στην επικοινωνία, καθώς οι απατεώνες συχνά επαναλαμβάνουν τις ίδιες ιστορίες και ατάκες επανειλημμένα.



Θυμηθείτε!

Εάν ο ρομαντικός διαδικτυακός σύντροφός σας αρνείται να σας συναντήσει πρόσωπο με πρόσωπο, επινοεί δικαιολογίες για το γιατί δεν μπορεί να συναντηθεί ή δεν συμμετέχει ποτέ σε βιντεοκλήσεις ή άλλες μορφές ζωντανής «αλληλεπίδρασης», μπορεί να έχετε μπλέξει με έναν απατεώνα.



Απάτη στις σχέσεις ανδρών-γυναικών



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Εάν έχετε κοινούς κωδικούς πρόσβασης στους λογαριασμούς σας και έχετε εντοπίσει ύποπτη δραστηριότητα, **ελέγξτε αμέσως εάν έχουν αλλάξει οποιεσδήποτε ρυθμίσεις και ελέγξτε τις τελευταίες συνδέσεις και δραστηριότητες στους λογαριασμούς σας**. Εάν παρατηρήσετε άγνωστες ή ύποπτες συνδέσεις, ενημερώστε τον πάροχο υπηρεσιών σας και τις επαφές σας και προειδοποιήστε τους να είναι σε εγρήγορση για ύποπτα μηνύματα που μπορεί να φαίνεται ότι προέρχονται από εσάς.

Η καλύτερη συμβουλή είναι να αλλάξετε όλους τους κωδικούς πρόσβασης στους οποίους έχετε δώσει πρόσβαση!



REPORT

Αν υποψιάζεστε ότι η διαδικτυακή σας σχέση είναι απάτη, σταματήστε αμέσως την επικοινωνία και **μπλοκάρτε τον απατεώνα στα μέσα κοινωνικής δικτύωσης**, στο ηλεκτρονικό ταχυδρομείο, στις εφαρμογές ανταλλαγής μηνυμάτων, στις ιστοσελίδες γνωριμιών κ.λπ.

Εάν χρησιμοποιήθηκαν οι τραπεζικοί ή πιστωτικοί σας λογαριασμοί, επικοινωνήστε με την τράπεζα ή την αστυνομία!

Διαδώστε το μήνυμα!

"Smishing" απάτες μέσω μηνυμάτων



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Το «Smishing» είναι ένα αρκτικόλεξο των λέξεων «SMS» (υπηρεσία σύντομων μηνυμάτων) και «phishing». Σε αυτές τις επιθέσεις, οι εγκληματίες του κυβερνοχώρου στέλνουν απατηλά μηνύματα κειμένου και προσπαθούν να εξαπατήσουν ή να χειραγωγήσουν τα θύματα ώστε να αποκαλύψουν προσωπικές ή οικονομικές πληροφορίες, να πατήσουν σε κακόβουλους συνδέσμους ή να κατεβάσουν επιβλαβές λογισμικό ή εφαρμογές.

Τύποι χειραγώγησης στο smishing:

Οι απατεώνες εξαπατούν τα θύματα υποδυόμενοι νομικά ιδρύματα, επιχειρήσεις ή άλλους οργανισμούς μέσω μηνυμάτων κειμένου. Τα μηνύματα αυτά προτρέπουν τα θύματα να προβούν σε άμεσες ενέργειες, όπως να πατήσουν έναν σύνδεσμο στο μήνυμα, να απαντήσουν με προσωπικές πληροφορίες ή να καλέσουν έναν συγκεκριμένο αριθμό.

Η αξιοποίηση μιας κατάστασης που θα μπορούσε να είναι οικεία για τα θύματα (μήνυμα από την τράπεζα, τις υπηρεσίες πιστωτικών καρτών, την υποστήριξη πελατών κλπ.) επιτρέπει στους απατεώνες να δημιουργήσουν μια αποτελεσματική μεταμπίεση και τους βοηθά να παρακάμψουν κάθε υποψία ότι μπορεί να πρόκειται για ανεπιθύμητη αλληλογραφία.

Εντείνοντας τα συναισθήματα του θύματος, το μήνυμα μοιάζει εξατομικευμένο και προκαλεί μια συγκεκριμένη συναισθηματική αντίδραση, όπως επείγον, φόβο ή περιέργεια. Χρησιμοποιώντας αυτές τις τακτικές, οι απατεώνες δημιουργούν μηνύματα που έχουν σχεδιαστεί για να ωθήσουν τα θύματα να αναλάβουν άμεση δράση.

Πλαστοπροσω
πία

Πιθανό και
αληθοφανές
πλαίσιο

Παιχνίδι με τα
συναισθήματα

"Smishing" απάτες μέσω μηνυμάτων



ΣΥΝΕΠΕΙΕΣ:

Λόγω της περιορισμένης εμπειρίας τους με τις σύγχρονες τεχνολογίες και τις γνώσεις κυβερνοασφάλειας, οι ηλικιωμένοι συχνά δυσκολεύονται να αναγνωρίσουν τα σημάδια κινδύνου στα μηνύματα smishing, όπως ψευδείς κλήσεις σε δράση ή ύποπτους συνδέσμους. Τείνουν να είναι λιγότερο υποψιασμένοι και είναι πιο πιθανό να πιστέψουν τα παραπλανητικά μηνύματα smishing.

01 Οικονομικές συνέπειες

Εάν τα θύματα αποκαλύψουν τις προσωπικές ή οικονομικές τους πληροφορίες, όπως αριθμούς πιστωτικών καρτών ή τραπεζικών λογαριασμών, μπορεί να υποστούν μεγαλύτερη οικονομική ζημία, καθώς οι απατεώνες χρησιμοποιούν αυτές τις πληροφορίες για να πραγματοποιήσουν μη εξουσιοδοτημένες συναλλαγές ή να αποσύρουν χρήματα από το λογαριασμό του θύματος. Οι συνέπειες αυτές μπορεί να προκαλέσουν σοβαρά οικονομικά προβλήματα και μακροχρόνιες ζημιές.

02 Κλοπή ταυτότητας

Σε περίπτωση κλοπής ταυτότητας, τα προσωπικά σας δεδομένα χρησιμοποιούνται καταχρηστικά, γεγονός που επηρεάζει την προσωπική σας ασφάλεια και ιδιωτικότητα. Εάν συνδεθούν με παράνομες δραστηριότητες, ενδέχεται επίσης να αντιμετωπίσετε νομικές συνέπειες. Η ανάκτηση της ταυτότητάς σας μπορεί να είναι πολύ χρονοβόρα, καθώς περιλαμβάνει πολλές διοικητικές (καθώς και νομικές) διαδικασίες.

03 Ψυχολογικές επιπτώσεις

Τα μηνύματα «Smishing» συχνά εκμεταλλεύονται συναισθήματα όπως ο φόβος, ο πανικός ή η σύγχυση, τα οποία μπορούν να επηρεάσουν την ψυχολογική ευημερία των θυμάτων.

"Smishing" απάτες μέσω μηνυμάτων



WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND



Ο Πέτρος έλαβε ένα γραπτό μήνυμα στο smartphone του από την τράπεζά του, το οποίο τον ενημέρωνε ότι ο λογαριασμός του είχε μπλοκαριστεί προσωρινά. Το μήνυμα περιείχε ένα ασυνήθιστο αίτημα να πατήσει ΑΜΕΣΑ έναν σύνδεσμο για να ενεργοποιήσει τον λογαριασμό του.

Παρόλο που ο Πέτρος πανικοβλήθηκε για μια στιγμή, αποφάσισε να μην πατήσει τον σύνδεσμο επειδή βρήκε το μήνυμα πολύ ύποπτο.

Δυστυχώς για τον απατεώνα ...
Ο Πέτρος παρακολούθησε πρόσφατα ένα διαδικτυακό εκπαιδευτικό βίντεο σχετικά με το «smishing» και έμαθε να αναγνωρίζει τα χαρακτηριστικά αυτού του τύπου απάτης..



ΒΗΜΑ1:Αναγνώριση των προειδοποιητικών σημάτων

Ο Πέτρος παρατήρησε επίσης ορθογραφικά λάθη ή αδέξια διατυπωμένες προτάσεις στο μήνυμα, τα οποία έδειχναν ότι το μήνυμα δεν ήταν επικυρωμένο.

ΒΗΜΑ 2: Διαπίστωση έλλειψης προσωπικής επαφής

Ο Πέτρος παρατήρησε επίσης ότι το μήνυμα ήταν ανώνυμο και δεν περιείχε τα στοιχεία της τράπεζας ή κάποιο πρόσωπο επικοινωνίας με το οποίο ο πελάτης θα μπορούσε να επικοινωνήσει για περισσότερες πληροφορίες.

ΒΗΜΑ 3: Επαλήθευση πληροφοριών

Αντί να πατήσει τον σύνδεσμο, ο Πέτρος κάλεσε την τράπεζα, χρησιμοποιώντας τον αριθμό τηλεφώνου από τον τηλεφωνικό του κατάλογο, και έλεγξε με την τράπεζα αν το μήνυμα ήταν αληθινό.

ΒΗΜΑ 4: Ενημέρωση/αναφορά

Αφού ο Πέτρος ενημέρωσε την τράπεζα, η οποία επιβεβαίωσε την απόπειρα απάτης, η τράπεζα ενημέρωσε όλους τους πελάτες της και κατήγγειλε την απόπειρα απάτης στην αρμόδια αρχή.

"Smishing" απάτες μέσω μηνυμάτων



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Είναι εύκολο να προστατευτείτε από τις πιθανές συνέπειες αυτών των επιθέσεων – απλά αγνοήστε τις. Φυσικά, δεν θα πρέπει να αγνοείτε όλα τα μηνύματα, καθώς τα μηνύματα κειμένου είναι ένα νόμιμο εργαλείο για πολλούς εμπόρους λιανικής πώλησης και άλλους φορείς για να επικοινωνούν μαζί σας.

Ακολουθούν ορισμένες πρόσθετες συμβουλές σε περίπτωση που μπορεί να βρεθείτε σε μια τέτοια κατάσταση.

Μην απαντάτε:

Εάν λάβετε ένα απροσδόκητο ή ύποπτο μήνυμα, ακόμη και αιτήματα να απαντήσετε, όπως να στείλετε το μήνυμα «ΣΤΟΠ» για να διαγραφείτε, μπορεί να είναι μια τακτική που χρησιμοποιείται για τον εντοπισμό ενεργών τηλεφωνικών αριθμών και να οδηγήσει σε απάτη.



• Example 3



Μην πανικοβάλλεστε:

Πάρτε το χρόνο σας και καθυστερήστε αν ένα μήνυμα φαίνεται επείγον.

Αντιμετωπίστε τις επείγουσες ενημερώσεις λογαριασμού ή τις επείγουσες προσφορές περιορισμένου χρόνου ως πιθανές ενδείξεις smishing.

Μείνετε προσεκτικοί!

"Smishing" απάτες μέσω μηνυμάτων



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Μην χρησιμοποιείτε τους συνδέσμους ή τα στοιχεία επικοινωνίας που παρέχονται στο μήνυμα!

Επαληθεύστε, ελέγξτε και επικοινωνήστε απευθείας μέσω των επίσημων διαύλων επικοινωνίας και όχι μέσω των λεπτομερειών ή των πληροφοριών που παρέχονται στο κείμενο.

Να θυμάστε!

Οι νόμιμοι φορείς (π.χ. τράπεζες, κυβερνητικές υπηρεσίες κ.λπ.) δεν ζητούν ποτέ ευαίσθητα δεδομένα μέσω SMS ή μη πιστοποιημένων συνδέσεων.



Εάν υποψιάζεστε απόπειρα επίθεσης smishing, **αλλάξτε αμέσως όλους τους κωδικούς πρόσβασης και τους κωδικούς PIN των λογαριασμών σας.**

Επιπλέον, **παρακολουθείτε τα οικονομικά σας και τους ηλεκτρονικούς σας λογαριασμούς** για ασυνήθιστες θέσεις σύνδεσης ή οποιεσδήποτε ύποπτες δραστηριότητες.

Εάν πέσετε θύμα «smishing», επικοινωνήστε με τους αρμόδιους φορείς που μπορούν να σας βοηθήσουν άμεσα. Σε περίπτωση οικονομικής επίθεσης, επικοινωνήστε με την τράπεζά σας για να παγώσετε τον λογαριασμό σας ή να ακυρώσετε τις πιστωτικές σας κάρτες.



Τηλεφωνικές απάτες σε ηλικιωμένους



HAZARD CHARACTERISTICS:

Οι τηλεφωνικές απάτες, γνωστές και ως «vishing», είναι ιδιαίτερα αποτελεσματικές σε βάρος των ηλικιωμένων. Οι τυπικές τακτικές περιλαμβάνουν απροσδόκητες κλήσεις από άγνωστους ή ξένους αριθμούς, ψεύτικους αριθμούς ή πλατφόρμες όπως το Viber και το WhatsApp. Οι κλήσεις vishing μπορεί να προέρχονται από πραγματικό πρόσωπο ή από προηχογραφημένη ρομποτική κλήση. Οι απατεώνες χρησιμοποιούν τη φωνητική τακτική για να κλέψουν εμπιστευτικά προσωπικά δεδομένα, όπως στοιχεία ταυτότητας, αριθμούς τραπεζικών λογαριασμών, στοιχεία σύνδεσης και κωδικούς πρόσβασης.

Τύποι χειραγώγησης στο vishing:

Οι απατεώνες συχνά παριστάνουν τους υπαλλήλους τραπεζών, κυβερνητικών υπηρεσιών, ασφαλιστικών ή άλλων γνωστών εταιρειών για να φανούν νόμιμοι και να αποκτήσουν οικονομικές και προσωπικές πληροφορίες. Χρησιμοποιούν ψυχολογικές τακτικές για να δημιουργήσουν την αίσθηση του επείγοντος, πείθοντας τα θύματα ότι βρίσκονται σε κίνδυνο. Μπορεί να τα απειλούν και να προσπαθούν να τα τρομάξουν

Οι απατεώνες μπορεί επίσης να χρησιμοποιούν πειστική γλώσσα και τόνο για να πείσουν το θύμα ότι είναι με το μέρος τους. Για το λόγο αυτό συχνά οδηγούν τη συζήτηση με φιλικό, προσιτό, συμπονετικό τρόπο και εμφανίζονται να είναι εξυπηρετικοί και συχνά χρησιμοποιούν διφορούμενη γλώσσα ή αλλάζουν θέμα κατά τη διάρκεια μιας συζήτησης για να αποσπάσουν την προσοχή του θύματος.

Οι απατεώνες χαρακτηρίζονται από επιμονή και επαναλαμβανόμενες κλήσεις από τον ίδιο αριθμό (μπορεί ακόμη και να επικοινωνούν με το θύμα πολλές φορές την ημέρα κ.λπ.). Με τον τρόπο αυτό, αργά και σταθερά, κερδίζουν την εμπιστοσύνη του θύματος. Αυτή η τακτική χρησιμοποιείται για να κερδίσει την εμπιστοσύνη του θύματος και να το παρασύρει στην αποκάλυψη ευαίσθητων πληροφοριών.

Πλαστοπροσωπία

Πειθώ

Επιμονή

Τηλεφωνικές απάτες σε ηλικιωμένους



ΣΥΝΕΠΕΙΕΣ:

Οι ηλικιωμένοι συχνά θεωρούν τις τηλεφωνικές κλήσεις σημαντικό τρόπο επικοινωνίας και εκτιμούν την προσωπική αλληλεπίδραση που προσφέρει ένα τηλεφώνημα. Αυτό το υψηλό επίπεδο εμπιστοσύνης στην προσωπική επικοινωνία μέσω τηλεφώνου είναι που τους καθιστά πιο ευάλωτους σε διάφορους τύπους τηλεφωνικών απάτης και πιο εύκολα να πιστεύουν παραπλανητικά αιτήματα για πληροφορίες ή ενέργειες από απατεώνες.

01 Οικονομικές συνέπειες

Τα θύματα τηλεφωνικών απατών συχνά υφίστανται άμεσες οικονομικές απώλειες. Οι απατεώνες μπορούν να εξαπατήσουν τα θύματα ώστε να προβούν σε πληρωμές ή να παράσχουν τραπεζικές πληροφορίες, οδηγώντας σε μη εξουσιοδοτημένες συναλλαγές ή στην αφαίμαξη τραπεζικών λογαριασμών. Αυτό μπορεί να επηρεάσει σημαντικά τις αποταμιεύσεις και την οικονομική τους ασφάλεια.

02 Κλοπή ταυτότητας

Οι τηλεφωνικές απάτες συχνά περιλαμβάνουν την κλοπή προσωπικών πληροφοριών, όπως αριθμούς κοινωνικής ασφάλισης, ημερομηνίες γέννησης και διευθύνσεις. Τα θύματα ενδέχεται να αντιμετωπίσουν σημαντικές προκλήσεις για την επίλυση αυτών των προβλημάτων και την ανάκτηση της ταυτότητάς τους.

03 Φθορά της υπόληψης

Σε περιπτώσεις όπου η απάτη είναι αποτέλεσμα μη εξουσιοδοτημένων οικονομικών δραστηριοτήτων ή συναλλαγών, το θύμα μπορεί επίσης να υποστεί ζημία στην οικονομική του φήμη. Η αποκατάσταση της φήμης μπορεί να είναι δύσκολη και απαιτεί εκτεταμένη τεκμηρίωση και επικοινωνία με τα χρηματοπιστωτικά ιδρύματα.

Τηλεφωνικές απάτες σε ηλικιωμένους



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Ο Ανδρέας δέχτηκε τηλεφώνημα από άτομο που ισχυριζόταν ότι ήταν από ασφαλιστική εταιρεία υγείας και ότι χρειαζόταν περισσότερες πληροφορίες για να ενημερώσει τον ιατρικό του φάκελο. Ο καλών ήταν πολύ φιλικός, αλλά δεν συστήθηκε με το όνομα και το επώνυμό του. Είπε απλώς ότι καλούσε εκ μέρους της ασφαλιστικής εταιρείας και εξήγησε ότι επρόκειτο για έναν έλεγχο ρουτίνας.

Όταν άρχισε να ζητά προσωπικά στοιχεία, όπως τον αριθμό ασφάλισης και την ημερομηνία γέννησης, ο Andrew έγινε καχύποπτος.

Δυστυχώς για τον απατεώνα ...

Ο Ανδρέας συμμετέχει ενεργά σε διαδικτυακά φόρουμ και κοινότητες όπου συζητούνται θέματα ασφάλειας και ανταλλάσσονται εμπειρίες από απάτες.



ΒΗΜΑ 1: Επαλήθευση της ταυτότητας του καλούντος

Ο Ανδρέας δεν μπόρεσε να επαληθεύσει την ταυτότητα του καλούντος στον επίσημο ιστότοπο της ασφαλιστικής εταιρείας, επειδή ο υποτιθέμενος υπάλληλος της ασφαλιστικής εταιρείας δεν έδωσε το πλήρες όνομά του - οπότε ο Ανδρέας έγινε καχύποπτος.

ΒΗΜΑ 2: Προσοχή σε ύποπτα αιτήματα

Όταν ο καλών άρχισε να ζητά προσωπικά στοιχεία, όπως τον αριθμό ασφάλισης και την ημερομηνία γέννησης, ο Ανδρέας αμφισβήτησε τη γνησιότητα της κλήσης και διέκοψε αμέσως την κλήση.

ΒΗΜΑ 3: Χρήση προηγούμενων γνώσεων

Ο Ανδρέας αναγνώρισε τα σημάδια εξαπάτησης λόγω της ενεργής συμμετοχής του σε διαδικτυακά φόρουμ που συζητούν θέματα ασφάλειας, γεγονός που τον βοήθησε να εντοπίσει γρήγορα τα ύποπτα στοιχεία της κλήσης.

ΒΗΜΑ 4: Ενημέρωση/αναφορά

Ο Ανδρέας κάλεσε απευθείας τον ασφαλιστή υγείας του για να ελέγξει αν η κλήση ήταν απόπειρα απάτης και το διέδωσε σε φόρουμ και κοινότητες όπου δραστηριοποιείται.

Τηλεφωνικές απάτες σε ηλικιωμένους



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Λόγω της επιταχυνόμενης προόδου της τεχνολογίας των τηλεπικοινωνιών, οι απατεώνες έχουν εκμεταλλευτεί την ανωνυμία και την εύκολη πρόσβαση στις τηλεφωνικές κλήσεις για να διεξάγουν δόλιες δραστηριότητες. Ως εκ τούτου, είναι ζωτικής σημασίας οι ηλικιωμένοι να διατηρούν υψηλό επίπεδο επαγρύπνησης και να γνωρίζουν τους κινδύνους που συνδέονται με την επικοινωνία μέσω τηλεφώνου.

Ακολουθούν ορισμένες πρόσθετες συμβουλές σε περίπτωση που μπορεί να βρεθείτε σε μια τέτοια κατάσταση.

Αγνοήστε τις απροσδόκητες κλήσεις από άγνωστους αριθμούς ή απλά αφήστε τις να πάνε στον τηλεφωνητή και αποφασίστε αν θα απαντήσετε στην κλήση με βάση τις πληροφορίες που σας παρέχονται.

Αποφύγετε τη χρήση οποιουδήποτε αριθμού επανάκλησης που σας παρέχουν, καθώς μπορεί να αποτελεί μέρος απάτης. Αντ' αυτού, αναζητήστε τον επίσημο αριθμό τηλεφώνου και καλέστε τους απευθείας για να επιβεβαιώσετε τη νομιμότητα του αιτήματος.



Ποτέ μην μοιράζετε οικονομικές ή προσωπικές πληροφορίες μέσω τηλεφώνου!

Κλείστε αμέσως το τηλέφωνο αν προσπαθήσουν να σας αποσπάσουν τέτοιου είδους πληροφορίες!

Τηλεφωνικές απάτες σε ηλικιωμένους



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Ελέγξτε τη γραμμή:

Λάβετε υπόψη ότι οι απατεώνες μπορούν να κρατήσουν την τηλεφωνική σας γραμμή ανοιχτή ακόμη και αφού κλείσετε το τηλέφωνο.

Χρησιμοποιήστε ένα άλλο τηλέφωνο για να ελέγξετε αν η γραμμή είναι ελεύθερη ή **περιμένετε τουλάχιστον 10 έως 15 λεπτά** για να βεβαιωθείτε ότι οι απατεώνες έχουν κλείσει το τηλέφωνο.



Δοκιμάστε τον αποκλεισμό κλήσεων:

Ενεργοποιήστε τις λειτουργίες αποκλεισμού κλήσεων του τηλεφώνου σας για να φιλτράρετε πιθανές απάτες «vishing». Τα περισσότερα κινητά τηλέφωνα προσφέρουν αυτές τις λειτουργίες.

Αν δεν έχετε smartphone, επικοινωνήστε με τον πάροχο τηλεφωνικών υπηρεσιών σας για να μάθετε τι υπηρεσίες προσφέρει για τον αποκλεισμό ανεπιθύμητων κλήσεων.

Εάν πέσετε θύμα «vishing», επικοινωνήστε αμέσως με τους αρμόδιους φορείς που μπορούν να σας βοηθήσουν.



Τηλεφωνικές απάτες σε ηλικιωμένους



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Η εξαπάτηση «παππούδων και γιαγιάδων» είναι ένα είδος απάτης όπου οι απατεώνες εκμεταλλεύονται τους συναισθηματικούς δεσμούς μεταξύ των παππούδων και των εγγονών τους. Ο απατεώνας συνήθως προσποιείται ότι είναι ένα εγγόνι που βρίσκεται σε κίνδυνο και χρειάζεται άμεση οικονομική βοήθεια.

Τύποι χειραγώγησης στην απάτη:

Ο απατεώνας δημιουργεί μια αίσθηση έκτακτης ανάγκης για να αποτρέψει τον παππού και τη γιαγιά από το να σκεφτεί πολύ ή να επικοινωνήσει με άλλα μέλη της οικογένειας.

Οι απατεώνες μπορεί να ζητήσουν από τους παππούδες και τις γιαγιάδες να κρατήσουν την κατάσταση μυστική, επικαλούμενοι αμηχανία ή φόβο μήπως μπλέξουν περισσότερο.

Οι απατεώνες εκμεταλλεύονται την αγάπη και το ενδιαφέρον του παππού και της γιαγιάς για το εγγόνι τους για να αποσπάσουν μια γρήγορη απάντηση.

**Επείγουσα
ανάγκη**

Μυστικότητα

**Συναισθηματικό
χειρισμός**

Απάτες που εκμεταλλεύονται συναισθηματικούς οικογενειακούς δεσμούς



ΣΥΝΕΠΕΙΕΣ:

Το να πέσετε θύμα εξαπάτησης μπορεί να έχει σοβαρές συνέπειες.

01 Οικονομικές απώλειες

Οικονομικά, μπορεί να χάσετε τα χρήματα που με κόπο κερδίσατε, καθώς οι απατεώνες συχνά ζητούν μεγάλα ποσά που μπορούν να εξαντλήσουν τις αποταμιεύσεις σας. Αν δώσετε τα τραπεζικά σας στοιχεία, μπορούν να κλέψουν ακόμη περισσότερα.

02 Συναισθηματική πίεση

Συναισθηματικά, οι ψεύτικες καταστάσεις έκτακτης ανάγκης δημιουργούν σημαντικό στρες και άγχος και η ανακάλυψη ότι επρόκειτο για απάτη μπορεί να σας αφήσει να νιώσετε βαθιά προδομένοι και πληγωμένοι.

03 Απώλεια εμπιστοσύνης

Αυτή η εμπειρία μπορεί να οδηγήσει σε απώλεια εμπιστοσύνης, κάνοντάς σας να αμφιβάλλετε για τα πραγματικά επείγοντα περιστατικά και να αισθάνεστε καχύποπτοι απέναντι σε κάθε απροσδόκητη επαφή, ακόμη και από νόμιμες πηγές.

04 Απομόνωση

Επιπλέον, μπορεί να νιώσετε αμηχανία ή ντροπή, με αποτέλεσμα να μην είστε πρόθυμοι να επικοινωνήσετε για οικονομικά θέματα με την οικογένεια ή τους φίλους σας, και οι απατεώνες μπορεί να σαςβάλουν ξανά στο στόχαστρο, βλέποντάς σας ως εύκολο θύμα.

Απάτες που εκμεταλλεύονται συναισθηματικούς οικογενειακούς δεσμούς

— ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΑ ΣΤΟ ΥΠΟΒΑΘΡΟ



Η Μαρία ζει μόνη της και απολαμβάνει μια στενή σχέση με την οικογένειά της, ιδίως με τα εγγόνια της. Ένα βράδυ, η Μαρία δέχτηκε ένα τηλεφώνημα από κάποιον που ισχυριζόταν ότι ήταν ο εγγονός της, ο Τζακ, ο οποίος ζητούσε επείγοντως ένα μεγάλο χρηματικό ποσό. Το τηλεφώνημα αυτό οδήγησε σε μια οδυνηρή και δαπανηρή εμπειρία για τη Μαρία.

Ωστόσο, η Μαρία θυμάται τη συμβουλή που της έδωσε ο εγγονός της να είναι προσεκτική στα τηλεφωνήματα με άτομα που ζητούν χρήματα.

Η εμπειρία της Μαίρης υπογραμμίζει τη σημασία της ενημέρωσης σχετικά με τις κοινές απάτες και της επαλήθευσης κάθε επείγοντος και συναισθηματικού αιτήματος για χρήματα. Με την κατανόηση των τακτικών που χρησιμοποιούν οι απατεώνες, όπως η δημιουργία επείγουσας ανάγκης, η απαίτηση μυστικότητας και η χειραγώγηση των συναισθημάτων, οι ηλικιωμένοι μπορούν να προστατευτούν καλύτερα από το να πέσουν θύματα. Αν έχετε αμφιβολίες, να επαληθεύετε πάντα τις πληροφορίες με άλλα μέλη της οικογένειας και να μη βιάζεστε ποτέ να στείλετε χρήματα.



Βήμα 1: Επαλήθευση

Η Μαίρη έκανε στον καλούντα ερωτήσεις που μόνο ο Τζακ θα ήξερε, και πήρε ένα λεπτό για να καλέσει απευθείας τον Τζακ για να αποφύγει την απάτη.

Βήμα 2: Ευαισθητοποίηση

Η εκ των προτέρων γνώση αυτών των απατών βοήθησε τη Μαίρη να αναγνωρίσει τα προειδοποιητικά σημάδια.

Βήμα 3: Επικοινωνία

Η Μαίρη έχει ήδη συζητήσει με την οικογένειά της για πιθανές απάτες και η δημιουργία μιας οικογενειακής κωδικής λέξης για καταστάσεις έκτακτης ανάγκης μπορεί να προσφέρει πρόσθετη προστασία.

Απάτες που εκμεταλλεύονται συναισθηματικούς οικογενειακούς δεσμούς



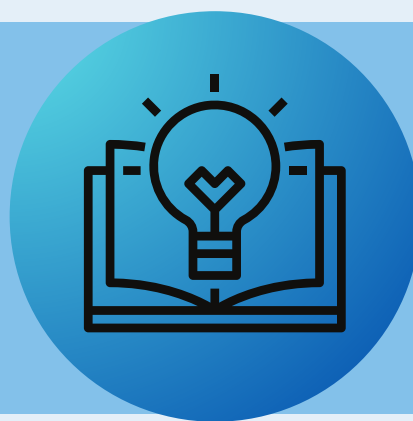
WAYS OF PROTECTION:

Η προστασία σας από απάτες που εκμεταλλεύονται τους συναισθηματικούς οικογενειακούς δεσμούς είναι ζωτικής σημασίας για τη διαφύλαξη των χρημάτων που με κόπο κερδίσατε. Ακολουθούν ορισμένα απλά βήματα που μπορείτε να ακολουθήσετε.

Μείνετε ενημερωμένοι:

Ενημερώστε τον εαυτό σας και τα αγαπημένα σας πρόσωπα σχετικά με τις κοινές απάτες που στοχεύουν τους ηλικιωμένους, συμπεριλαμβανομένης της απάτης των παππούδων και των γιαγιάδων.

Μείνετε ενημερωμένοι για τις νέες τακτικές που μπορεί να χρησιμοποιούν οι απατεώνες, ακολουθώντας αξιόπιστες πηγές πληροφοριών.



Επαλήθευση ταυτοτήτων:

Να κάνετε πάντα ερωτήσεις που μόνο το πραγματικό μέλος της οικογένειας θα ήξερε, όπως το όνομα ενός κατοικίδιου ή ένα συγκεκριμένο οικογενειακό γεγονός.

Εάν έχετε αμφιβολίες, καλέστε ξανά χρησιμοποιώντας έναν γνωστό αριθμό για να επαληθεύσετε την ταυτότητα του καλούντος.



Ορίστε μια οικογενειακή λέξη-κώδικα:

Καθιερώστε μια μυστική κωδική λέξη με την οικογένειά σας, την οποία θα γνωρίζουν μόνο έμπιστα άτομα.

Χρησιμοποιήστε αυτή την κωδική λέξη σε περιπτώσεις έκτακτης ανάγκης για να επαληθεύσετε την ταυτότητα των καλούντων που ισχυρίζονται ότι είναι μέλη της οικογένειας.



Απάτες που εκμεταλλεύονται συναισθηματικούς οικογενειακούς δεσμούς



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Αποφύγετε τις βιαστικές αποφάσεις:

Μη βιάζεστε όταν λαμβάνετε απροσδόκητα ή επείγοντα αιτήματα για χρήματα.

Οι απατεώνες χρησιμοποιούν το επείγον για να σας εμποδίσουν να αμφισβητήσετε την ιστορία τους ή να ζητήσετε συμβουλές από άλλους.



Χρησιμοποιήστε αναγνώριση καλούντος και φραγή κλήσεων:

Χρησιμοποιήστε την αναγνώριση κλήσης για να ελέγχετε τις εισερχόμενες κλήσεις και να αποκλείετε άγνωστους ή ύποπτους αριθμούς. Αναφέρετε τις απατηλές κλήσεις στον πάροχο τηλεφωνικών υπηρεσιών σας ή στις αρμόδιες αρχές.

Φύλαξη προσωπικών δεδομένων

Να είστε προσεκτικοί όταν μοιράζεστε προσωπικές και οικονομικές πληροφορίες μέσω τηλεφώνου ή διαδικτύου.

Αποφεύγετε να παρέχετε ευαίσθητες λεπτομέρειες, εκτός εάν είστε σίγουροι για την ταυτότητα του παραλήπτη.



Απάτες με ιατρικά προϊόντα



HAZARD CHARACTERISTICS:

Τα τελευταία χρόνια, οι απατεώνες στοχεύουν όλο και περισσότερο σε ευάλωτα άτομα, συμπεριλαμβανομένων των ηλικιωμένων, με δόλια σχέδια που αφορούν ιατρικά προϊόντα. Αυτές οι απάτες συχνά εκμεταλλεύονται συναισθήματα και φόβους που σχετίζονται με θέματα υγείας, υποσχόμενες θαυματουργές θεραπείες, θεραπείες ή θεραπείες που είναι πολύ καλές για να είναι αληθινές.

Τύποι χειραγώγησης στην απάτη με ιατρικά προϊόντα:

Οι απατεώνες κάνουν τολμηρούς ισχυρισμούς για τα προϊόντα τους, υποσχόμενοι θαυματουργά αποτελέσματα με ελάχιστα έως καθόλου επιστημονικά στοιχεία.

Συχνά χρησιμοποιούν τακτικές πωλήσεων υψηλής πίεσης, προτρέποντάς σας να αγοράσετε γρήγορα πριν λήξει η «προσφορά περιορισμένου χρόνου».

Αυτές οι απάτες παίζουν με τα συναισθήματά σας, εκμεταλλευόμενες τους φόβους σας για θέματα υγείας και προσφέροντας ψεύτικες ελπίδες για μια γρήγορη και εύκολη λύση.

Ψευδείς
υποσχέσεις

Τακτικές
υψηλής
πίεσης

Συναισθηματική
χειραγώγηση

Απάτες με ιατρικά προϊόντα



ΣΥΝΕΠΕΙΕΣ:

Η απάτη με ιατρικά προϊόντα μπορεί να έχει σοβαρές αρνητικές επιπτώσεις, όπως:

01 Οικονομικές απώλειες

Το να πέσετε θύμα απάτης με ιατρικά προϊόντα μπορεί να έχει ως αποτέλεσμα να ξοδέψετε μεγάλα χρηματικά ποσά σε αναποτελεσματικά ή και επικίνδυνα προϊόντα, εξαντλώντας τις αποταμιεύσεις σας.

02 Κίνδυνοι στην υγεία

Σε ορισμένες περιπτώσεις, οι απατεώνες χρησιμοποιούν μη ελεγχόμενα ή παραποιημένα ιατρικά προϊόντα, τα οποία μπορεί να οδηγήσουν σε σοβαρές επιπλοκές για την υγεία ή σε αλληλεπιδράσεις με υπάρχοντα φάρμακα.

03 Συναισθηματική πίεση

Η εξαπάτηση μπορεί να οδηγήσει σε αισθήματα ντροπής, ενοχής και αμηχανίας. Μπορεί να νιώσετε προδομένοι και ανήσυχοι, γεγονός που μπορεί να επηρεάσει αρνητικά τη συνολική ψυχική σας υγεία και ευεξία.

04 Υποβάθμιση της ποιότητας ζωής

Οι συνδυασμένες επιπτώσεις της οικονομικής απώλειας, των κινδύνων για την υγεία και της συναισθηματικής δυσφορίας μπορούν να οδηγήσουν σε σημαντική μείωση της ποιότητας ζωής των θυμάτων. Μπορεί να δυσκολεύονται να διαχειριστούν τις καθημερινές τους δραστηριότητες και να διατηρήσουν την ανεξαρτησία τους.

Απάτες με ιατρικά προϊόντα



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΙΣΤΟΡΙΚΟ ΥΠΟΒΑΘΡΟ



Ο Θωμάς λαμβάνει ένα email που διαφημίζει ένα νέο «θαυματουργό συμπλήρωμα» που ισχυρίζεται ότι θεραπεύει την αρθρίτιδα, τον διαβήτη και την υψηλή αρτηριακή πίεση μέσα σε μια νύχτα. Το email προσφέρει έκπτωση περιορισμένου χρόνου και τον προτρέπει να αγοράσει τώρα για να μη χάσει την ευκαιρία για καλύτερη υγεία. Ωστόσο, ο Θωμάς θυμάται τη συμβουλή που είχε διαβάσει σχετικά με την προσοχή στις θαυματουργές θεραπείες.

Η ιστορία του Θωμά δεν είναι δυστυχώς η μοναδική περίπτωση. Οι απάτες με ιατρικά προϊόντα εκμεταλλεύονται τα τρωτά σημεία και τα συναισθήματα των ηλικιωμένων, υποσχόμενες γρήγορες λύσεις για πολύπλοκα ζητήματα υγείας. Παραμένοντας ενημερωμένοι, επιφυλακτικοί και συμβουλευόμενοι τους επαγγελματίες υγείας, μπορείτε να προστατευτείτε από το να πέσετε θύμα αυτών των δόλιων συστημάτων. Να θυμάστε, η υγεία σας είναι ανεκτίμητη και δεν υπάρχουν συντομεύσεις για πραγματική ευεξία.



Βήμα 1: Μείνετε επιφυλακτικοί

Ο Θωμάς θυμήθηκε ότι οι νόμιμες ιατρικές ανακαλύψεις δοκιμάζονται αυστηρά και επαληθεύονται από ειδικούς.

Βήμα 2: Συμβουλευτείτε επαγγελματίες

Ο Θωμάς κάλεσε τον προσωπικό του γιατρό και συζήτησε τυχόν νέες θεραπείες ή συμπληρώματα.

Βήμα 3: Ερευνήστε

Ο Θωμάς έψαξε για αμερόληπτες κριτικές και επιστημονικά στοιχεία που να υποστηρίζουν τους ισχυρισμούς του προϊόντος προτού εξετάσει την αγορά.

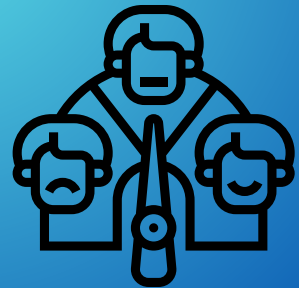
Απάτες με ιατρικά προϊόντα



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Να θυμάστε ότι η προστασία σας από την απάτη με ιατρικά προϊόντα είναι ζωτικής σημασίας για την προστασία των χρημάτων που με κόπο κερδίσατε και της υγείας σας. Ένα από τα πιο κρίσιμα βήματα είναι η αναζήτηση συναισθηματικής υποστήριξης. Ακολουθούν ορισμένα απλά βήματα που μπορείτε να ακολουθήσετε.

Αναζητήστε συναισθηματική υποστήριξη: Η προσωπική υποστήριξη από την οικογένεια, τους φίλους και τα μέλη της κοινότητας μπορεί να προσφέρει στους ηλικιωμένους τη συναισθηματική δύναμη και τη διαβεβαίωση που χρειάζονται για να αντισταθούν στη χειραγώγηση. Όταν οι ηλικιωμένοι αισθάνονται ότι τους υποστηρίζουν και τους εκτιμούν, είναι λιγότερο πιθανό να πέσουν θύματα απάτεων που εκμεταλλεύονται συναισθηματικά τρωτά σημεία.



Παραμείνετε ενημερωμένοι:

Τα κοινωνικά δίκτυα μπορούν να αποτελέσουν ζωτικής σημασίας πηγή πληροφοριών. Τα μέλη της οικογένειας και οι φίλοι μπορούν να μοιραστούν προειδοποιήσεις για τρέχουσες απάτες, να παρέχουν συμβουλές για το πώς να αναγνωρίζουν την απάτη και να προτείνουν αξιόπιστες πηγές για ιατρικά προϊόντα και θεραπείες. Η διατήρηση της ενημέρωσης μέσω της κοινωνικής υποστήριξης μπορεί να μειώσει σημαντικά τον κίνδυνο να πέσετε θύμα απάτης.

Απάτες με ιατρικά προϊόντα



WAYS OF PROTECTION:

Συμβουλευτείτε τους επαγγελματίες υγείας:

Πριν δοκιμάσετε οποιοδήποτε νέο ιατρικό προϊόν ή θεραπεία, συμβουλευτείτε τον πάροχο υγειονομικής περίθαλψης για να βεβαιωθείτε ότι είναι ασφαλές και αποτελεσματικό.



Να είστε επιφυλακτικοί με τους ισχυρισμούς περί θαυματουργών φαρμάκων:

Εάν ένα προϊόν ισχυρίζεται ότι θεραπεύει πολλαπλές ασύνδετες παθήσεις της υγείας ή προσφέρει γρήγορα και αβίαστα αποτελέσματα, είναι πιθανό να είναι πολύ καλό για να είναι αληθινό.

Ερευνήστε διεξοδικά:

Αφιερώστε χρόνο για να ερευνήσετε το προϊόν και την εταιρεία πίσω από αυτό. Αναζητήστε κριτικές από αξιόπιστες πηγές και ελέγξτε αν το προϊόν είναι εγκεκριμένο από ρυθμιστικούς φορείς.



Περαιτέρω αναγνώσματα



ΑΠΑΤΗ ΣΤΙΣ ΣΧΕΣΕΙΣ ΑΝΔΡΩΝ-ΓΥΝΑΙΚΩΝ

- <https://www.sciencedirect.com/science/article/pii/S2949791423000441>
- <https://hu.usembassy.gov/be-wary-of-online-romance-scams/>
- <https://consumer.ftc.gov/articles/what-know-about-romance-scams#whatis> <https://us.norton.com/blog/online-scams/romance-scams>
- <https://www.unit21.ai/fraud-aml-dictionary/romance-fraud>
- <https://www.hsbc.co.uk/help/security-centre/romance-scams-case-study/>
- <https://www.equifax.co.uk/resources/identity-protection/how-to-spot-and-avoid-romance-scams.html>
- <https://dfpi.ca.gov/2024/03/05/romance-scams-what-consumers-need-to-know/>
- <https://complyadvantage.com/insights/what-is-a-romance-scam/>



SMISHING ΑΠΑΤΕΣ ΜΗΝΥΜΑΤΩΝ

- <https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it>
- <https://www.proofpoint.com/us/threat-reference/smishing>
- <https://www.sinch.com/blog/what-is-smishing/>
- <https://business.bofa.com/en-us/content/what-is-smishing-how-to-prevent-it.html>
- https://www.forbes.com/advisor/business/what-is-smishing/#how_to_protect_against_smishing_section
- <https://www.techtarget.com/searchmobilecomputing/definition/SMiShing>
- <https://cybeready.com/category/the-complete-guide-to-smishing>
- <https://www.rd.com/article/what-is-smishing/>

Περαιτέρω αναγνώσματα



ΤΗΛΕΦΩΝΙΚΕΣ ΑΠΑΤΕΣ ΜΕ ΗΛΙΚΙΩΜΕΝΟΥΣ

- <https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud/phone-scams/>
- https://www.ageuk.org.uk/globalassets/age-uk/documents/information-guides/ageukig05_avoiding_scams_inf.pdf
- <https://www.helpguide.org/articles/abuse/elder-scams-and-senior-fraud-abuse.htm>
- <https://www.seniorliving.org/research/common-elderly-scams/>
- <https://www.ooma.com/blog/home-phone/protect-seniors-from-elderly-phone-scams>
- https://taking.care/blogs/resources-advice/scams-targeting-the-elderly#How_to_avoid
- <https://www.terranovasecurity.com/solutions/security-awareness-training/what-is-vishing>
- <https://www.kaspersky.com/resource-center/definitions/vishing>
- <https://www.proofpoint.com/us/threat-reference/vishing>



ΑΠΑΤΕΣ ΠΟΥ ΕΚΜΕΤΑΛΛΕΥΟΝΤΑΙ ΣΥΝΑΙΣΘΗΜΑΤΙΚΟΥΣ ΟΙΚΟΓΕΝΕΙΑΚΟΥΣ ΔΕΣΜΟΥΣ

- <https://www.homeinstead.com/location/347/news-and-media/the-grandparent-scam/>
- <https://www.europol.europa.eu/media-press/newsroom/news/crime-against-elderly-four-arrests-in-germany-and-poland>
- <https://www.identityguard.com/news/grandparent-scam#:~:text=The%20most%20common%20grandparent%20scam,often%20claim%20to%20be%20overseas.>
- <https://www.cbsnews.com/news/what-being-targeted-by-grandparent-scam-sounds-like-60-minutes/>
- <https://www.youtube.com/watch?v=v2VFy2igHPE>
- <https://globalnews.ca/video/9901367/calgary-senior-falls-victim-to-grandparents-scam-costing-her-thousands>

Περαιτέρω αναγνώσματα



ΑΠΑΤΕΣ ΜΕ ΙΑΤΡΙΚΑ ΠΡΟΪΟΝΤΑ

- <https://www.forres-gazette.co.uk/news/older-people-targeted-by-medical-scam-116453/>
- <https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products>
- <https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview>
- <https://www.bbc.com/news/business-58029113>
- <https://www.europol.europa.eu/media-press/newsroom/news/544-arrests-and-%E2%82%AC63-million-of-fake-pharmaceuticals-and-illegal-doping-substances-seized>

ΚΕΦΑΛΑΙΟ 4.

ΑΠΑΤΗ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Στην εποχή των ηλεκτρονικών πληρωμών και συναλλαγών, υπάρχουν όλο και περισσότερες αναφορές για ηλεκτρονικές απάτες. Οι εγκληματίες έχουν πρόσβαση σε πολλούς ηλικιωμένους στη χρήση των νέων τεχνολογιών, γεγονός που τους καθιστά πιο εξελιγμένους στις πρακτικές απάτης. Σε αυτή την ενότητα, θα συζητήσουμε τις πιο συνηθισμένες απάτες με διαδικτυακές διαδικασίες για να βοηθήσουμε τους ηλικιωμένους να τις επιλύσουν και να τις αποφύγουν.

Οι απάτες με ταξίδια και εισιτήρια περιλαμβάνουν την προσφορά πλασματικών προσφορών που δεν υλοποιούνται ποτέ. Στις απάτες με συνδρομές, οι ηλικιωμένοι εξαπατώνται για να αποδεχτούν υπηρεσίες που χρεώνουν αυτόματα τέλη. Τα ψεύτικα ηλεκτρονικά καταστήματα εκβιάζουν πληρωμές για προϊόντα που δεν έχουν παραδοθεί. Οι απάτες αγοράς-πώλησης περιλαμβάνουν δόλιες αγορές όπου τα προϊόντα δεν αναφέρονται ή δεν είναι διαθέσιμα και όπου οι ηλικιωμένοι πωλούν δωρεάν τα υπάρχοντά τους σε ιστοσελίδες αγγελιών.

Η κατανόηση αυτών των απειλών είναι ζωτικής σημασίας, ώστε οι ηλικιωμένοι να μπορούν να επωφεληθούν με ασφάλεια από τις ευκαιρίες που προσφέρει το Διαδίκτυο και να προστατεύσουν τα οικονομικά τους από απάτες.

Απάτες με ταξίδια και εισιτήρια



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Η απάτη με ταξίδια και εισιτήρια αναφέρεται σε δόλια σχέδια που περιλαμβάνουν την πώληση πλαστών πακέτων ταξιδιών, εκδρομών και εισιτηρίων. Αυτός ο τύπος απάτης εμφανίζεται συχνά στο διαδίκτυο, όπου οι απατεώνες δημιουργούν επαγγελματικούς ιστότοπους ή στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου προσφέροντας προσφορές με μεγάλες εκπτώσεις. Οι ηλικιωμένοι, οι οποίοι μπορεί να είναι λιγότερο εξοικειωμένοι με τις σύγχρονες τακτικές ηλεκτρονικής απάτης, είναι ιδιαίτερα ευάλωτοι σε αυτές τις απάτες. Οι ανυποψίαστοι πελάτες, ιδίως οι ηλικιωμένοι που προσελκύονται από αυτές τις προσφορές, πραγματοποιούν πληρωμές για αυτές τις ανύπαρκτες υπηρεσίες και δεν έχουν καμία δυνατότητα προσφυγής όταν συνειδητοποιούν ότι έχουν εξαπατηθεί. Είναι ζωτικής σημασίας η ενημέρωση των ηλικιωμένων σχετικά με αυτά τα απατηλά συστήματα, ώστε να τους βοηθήσουμε να αποφύγουν σημαντικές οικονομικές απώλειες και συναισθηματική οδύνη.

Τύποι απάτης στα ταξίδια και στα εισιτήρια:

Πρόκειται για απατεώνες που πωλούν ανύπαρκτα αεροπορικά εισιτήρια. Μπορεί να δημιουργήσουν ψεύτικους ιστότοπους που μοιάζουν με αυθεντικούς ιστότοπους αεροπορικών εταιρειών, να δελεάσουν τους πελάτες με μειωμένες τιμές εισιτηρίων και στη συνέχεια να εξαφανιστούν αφού εισπράξουν την πληρωμή.

Αυτό συμβαίνει όταν οι απατεώνες προσφέρουν ολοκληρωμένα πακέτα διακοπών σε πολύ μειωμένες τιμές. Αφού ο πελάτης κάνει την πληρωμή, ανακαλύπτει ότι το πακέτο δεν υπάρχει ή δεν περιλαμβάνει αυτό που του υποσχέθηκαν.

Οι απατεώνες μπορεί να παριστάνουν τους πωλητές ή μεταπωλητές χρονομεριστικών ακινήτων, υποσχόμενοι εξαιρετικές προσφορές σε ιδιοκτησίες χρονομεριστικών ακινήτων. Μπορεί να ζητήσουν προκαταβολικά τέλη και στη συνέχεια να εξαφανιστούν μόλις γίνει η πληρωμή.

**Ψεύτικα
αεροπορικά
εισιτήρια**

**Παραπλανητικά
πακέτα
διακοπών**

**Απάτες
χρονομεριστικής
μίσθωσης**

Απάτες με ταξίδια και εισιτήρια



ΣΥΝΕΠΕΙΕΣ::

Η απάτη στα ταξίδια και τα εισιτήρια μπορεί να έχει σοβαρές αρνητικές επιπτώσεις, όπως:

01 Οικονομικές απώλειες

Η πιο άμεση συνέπεια της απάτης στα ταξίδια και τα εισιτήρια είναι η οικονομική απώλεια. Οι απατεώνες παίρνουν πληρωμές για ανύπαρκτες υπηρεσίες, αφήνοντας τα θύματα χωρίς καμία δυνατότητα να ανακτήσουν τα χρήματά τους.

02 Κλοπή ταυτότητας

Συχνά, αυτές οι απάτες περιλαμβάνουν την παροχή ευαίσθητων προσωπικών και οικονομικών πληροφοριών από το θύμα με το πρόσχημα της κράτησης ενός ταξιδιού. Οι πληροφορίες αυτές μπορούν στη συνέχεια να χρησιμοποιηθούν για κλοπή ταυτότητας.

03 Συναισθηματική δυσφορία

Το να πέσει κανείς θύμα μιας τέτοιας απάτης μπορεί να οδηγήσει σε σημαντική συναισθηματική οδύνη. Ο ενθουσιασμός ενός προγραμματισμένου ταξιδιού μετατρέπεται σε απογοήτευση και απογοήτευση, για να μην αναφέρουμε τα συναισθήματα παραβίασης και ευαλωτότητας μετά την εξαπάτηση.

Απάτες με ταξίδια και εισιτήρια



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΦΟΝΤΟ ΤΗΝ ΙΣΤΟΡΙΑ



Μια μέρα, ο Γιώργος έλαβε ένα email από ένα διαδικτυακό ταξιδιωτικό πρακτορείο που προσέφερε μια φανταστική προσφορά για ένα πακέτο ευρωπαϊκών διακοπών. Η προσφορά περιελάμβανε πτήσεις, διαμονή και περιηγήσεις στα αξιοθέατα της Ρώμης, του Παρισιού και του Λονδίνου. Το πακέτο είχε μεγάλη έκπτωση και ο Γιώργος, ενθουσιασμένος από την προοπτική του ταξιδιού των ονείρων του, αποφάσισε να το διερευνήσει περαιτέρω.

Έκανε κλικ στον ιστότοπο του ταξιδιωτικού γραφείου, ο οποίος φαινόταν επαγγελματικός με εικόνες υψηλής ποιότητας από τους προορισμούς και λαμπερές μαρτυρίες από ευχαριστημένους πελάτες. Πεισμένος, ο Γιώργος αποφάσισε να κλείσει το πακέτο διακοπών. Εισήγαγε τα στοιχεία της πιστωτικής του κάρτας και έλαβε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που επιβεβαίωνε την κράτησή του.

Οι μέρες έγιναν εβδομάδες και ο Γιώργος δεν έλαβε καμία περαιτέρω επικοινωνία σχετικά με το ταξίδι του. Άρχισε να ανησυχεί και προσπάθησε να επικοινωνήσει με το ταξιδιωτικό γραφείο, αλλά διαπίστωσε ότι ο αριθμός τηλεφώνου τους ήταν αποσυνδεδεμένος και τα email του έμεναν αναπάντητα.

Η ιστορία του Γιώργου υπογραμμίζει την ανάγκη ενημέρωσης των ηλικιωμένων για τις ηλεκτρονικές απάτες. Καθώς αποκτούν περισσότερες γνώσεις τεχνολογίας, διατρέχουν μεγαλύτερο κίνδυνο. Η ενημέρωσή τους για τα σημάδια απάτης, όπως οι υπερβολικά ελκυστικές προσφορές, και η σημασία της επαλήθευσης της αυθεντικότητας μιας εταιρείας πριν από την αγορά μπορεί να τους βοηθήσει να παραμείνουν ασφαλείς. Η ανταλλαγή τέτοιων εμπειριών μπορεί να προειδοποιήσει αποτελεσματικά τους ηλικιωμένους για την ηλεκτρονική απάτη.



ΒΗΜΑ 1: Επαλήθευση της αυθεντικότητας vs. άμεση εμπιστοσύνη

Ο Γιώργος εμπιστεύτηκε το ταξιδιωτικό πρακτορείο με βάση την επαγγελματική του ιστοσελίδα και τις μαρτυρίες του χωρίς περαιτέρω έλεγχο. Ο Γιώργος θα έπρεπε να είχε επαληθεύσει τη γνησιότητα του ταξιδιωτικού πρακτορείου ελέγχοντας τις κριτικές των πελατών, επιβεβαιώνοντας την εγγραφή και τη φυσική του διεύθυνση και αξιολογώντας το ποσοστό ανταπόκρισης τους επικοινωνώντας απευθείας μαζί τους.

ΒΗΜΑ 2: Χρησιμοποιήστε ασφαλείς μεθόδους πληρωμής vs. εισαγωγή στοιχείων πιστωτικής κάρτας

Ο Γιώργος εισήγαγε τα στοιχεία της πιστωτικής του κάρτας απευθείας στον ιστότοπο του ταξιδιωτικού πρακτορείου χωρίς να διασφαλίσει την ασφάλεια της διαδικασίας πληρωμής. Ο Γιώργος θα έπρεπε να χρησιμοποιήσει ασφαλείς μεθόδους πληρωμής που προσφέρουν προστασία στον αγοραστή, όπως πιστωτικές κάρτες μέσω μιας αξιόπιστης πλατφόρμας πληρωμών, και να αποφύγει την απευθείας κοινοποίηση στοιχείων πιστωτικής κάρτας σε άγνωστους ιστότοπους.

ΒΗΜΑ 3: Επακόλουθη επικοινωνία vs. αναμονή χωρίς δράση

Ο Γιώργος περίμενε εβδομάδες χωρίς να λάβει καμία περαιτέρω επικοινωνία σχετικά με το ταξίδι του και προσπάθησε να επικοινωνήσει με το πρακτορείο μόνο όταν άρχισε να ανησυχεί. Ο Γιώργος θα έπρεπε να είχε επικοινωνήσει με το ταξιδιωτικό γραφείο αμέσως μετά την πραγματοποίηση της κράτησης για να επιβεβαιώσει τις λεπτομέρειες και να εξασφαλίσει συνεχή επικοινωνία.

ΒΗΜΑ 4: Αναφορά ύποπτης δραστηριότητας vs. καθυστερημένη αντίδραση

Ο Γιώργος καθυστέρησε να επικοινωνήσει με την εταιρεία της πιστωτικής του κάρτας μέχρι να συνειδητοποιήσει ότι κάτι δεν πήγαινε καλά. Ο Γιώργος θα έπρεπε να είχε αναφέρει οποιαδήποτε ύποπτη δραστηριότητα ή έλλειψη επικοινωνίας στην εταιρεία πιστωτικών καρτών του αμέσως, ώστε να σταματήσει ενδεχομένως τη συναλλαγή και να διερευνήσει το ζήτημα.

Απάτες με ταξίδια και εισιτήρια



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Είναι ζωτικής σημασίας για τους ηλικιωμένους να προστατεύονται από την απάτη με ταξίδια και τα εισιτήρια για να αποφύγουν σημαντικές οικονομικές απώλειες, συναισθηματική δυσφορία και πιθανή κλοπή ταυτότητας. Οι απατεώνες συχνά έχουν ως στόχο τους ηλικιωμένους, οι οποίοι μπορεί να είναι λιγότερο εξοικειωμένοι με τις τακτικές της ηλεκτρονικής απάτης, εκμεταλλευόμενοι την εμπιστοσύνη και τον ενθουσιασμό τους για τις ταξιδιωτικές προσφορές. Προστατεύοντας τον εαυτό τους, οι ηλικιωμένοι μπορούν να διασφαλίσουν ότι τα χρήματα που έχουν κερδίσει με κόπο δεν θα κλαπούν, ότι οι προσωπικές τους πληροφορίες θα παραμείνουν ασφαλείς και ότι τα ταξιδιωτικά τους σχέδια δεν θα καταστραφούν από δόλια σχέδια.

Ερευνήστε διεξοδικά την εταιρεία:

Προτού προβείτε σε οποιαδήποτε αγορά, φροντίστε πάντα να διεξάγετε μια ολοκληρωμένη έρευνα για την εταιρεία. Φροντίστε να αναζητήσετε κριτικές και αξιολογήσεις πελατών για να προσδιορίσετε την αξιοπιστία της εταιρείας και να διασφαλίσετε τη νομιμότητά της. Αυτό θα σας δώσει μια καλύτερη κατανόηση της φήμης της εταιρείας μεταξύ των προηγούμενων πελατών της.



Χρησιμοποιήστε μόνο ασφαλείς μεθόδους πληρωμής:

Όταν κάνετε αγορές μέσω διαδικτύου, είναι ζωτικής σημασίας να χρησιμοποιείτε μόνο ασφαλείς μεθόδους πληρωμής. Αποφύγετε τις άμεσες τραπεζικές μεταφορές και αποφύγετε να μοιράζεστε τα στοιχεία της πιστωτικής σας κάρτας σε πλατφόρμες που δεν είναι ασφαλείς. Είναι πάντα ασφαλέστερο να χρησιμοποιείτε επιλογές πληρωμής που προσφέρουν προστασία στον αγοραστή.



Απάτες με ταξίδια και εισιτήρια



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Να είστε προσεκτικοί με τις προσφορές που φαίνονται πολύ καλές για να είναι αληθινές:

Αν μια προσφορά ή έκπτωση φαίνεται πολύ καλή για να είναι αληθινή, μάλλον είναι. Να είστε ιδιαίτερα προσεκτικοί σε τιμές με μεγάλες εκπτώσεις για είδη όπως αεροπορικά εισιτήρια ή πακέτα διακοπών. Είναι πάντα προτιμότερο να κάνετε μια μικρή έρευνα αγοράς προτού πέσετε πάνω σε τέτοιες προσφορές.



• Example 3



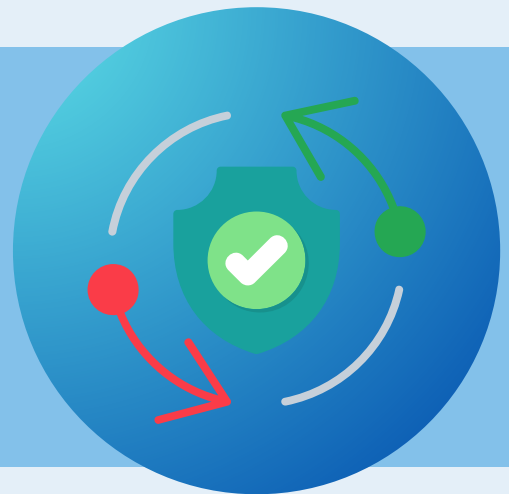
CONTACT US

Επικοινωνήστε απευθείας με την αεροπορική εταιρεία ή το ξενοδοχείο:

Εάν λάβετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που σας προσφέρει έκπτωση σε πτήση ή διαμονή σε ξενοδοχείο, καλό είναι να επικοινωνήσετε απευθείας με την αεροπορική εταιρεία ή το ξενοδοχείο για να επαληθεύσετε την προσφορά. Αυτό θα διασφαλίσει ότι η προσφορά είναι νόμιμη και όχι απάτη.

Εξασφαλίστε ότι οι προσωπικές πληροφορίες είναι ασφαλείς:

Να είστε προσεκτικοί όταν μοιράζετε προσωπικές πληροφορίες. Ελέγχετε πάντα ότι η πλατφόρμα είναι ασφαλής προτού εισαγάγετε οποιαδήποτε ευαίσθητη πληροφορία. Ποτέ μην μοιράζετε σημαντικά προσωπικά στοιχεία σε πλατφόρμες που δεν διαθέτουν επαρκή μέτρα ασφαλείας.



Απάτη με συνδρομές



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Η απάτη με τις συνδρομές είναι ένα είδος απάτης όπου τα άτομα εξαπατώνται για να υπογράψουν ακριβές συνδρομές ή υπηρεσίες χωρίς να το γνωρίζουν. Αυτές οι απάτες συχνά οδηγούν σε επαναλαμβανόμενες χρεώσεις που είναι δύσκολο να ακυρωθούν, με αποτέλεσμα να πλήττονται ευάλωτα άτομα, συμπεριλαμβανομένων των ηλικιωμένων.

Τύποι χειραγώγησης σε απάτες συνδρομής:

Οι απατεώνες χρησιμοποιούν παραπλανητικές διαφημίσεις ή αναδυόμενους συνδέσμους για να σας δελεάσουν να εγγραφείτε σε κάτι που φαίνεται να είναι μια δωρεάν δοκιμή ή μια υπηρεσία χαμηλού κόστους.

Οι όροι και οι προϋποθέσεις της συνδρομής, συμπεριλαμβανομένου του κόστους και της διάρκειας, συχνά κρύβονται στα ψιλά γράμματα ή δεν εξηγούνται με σαφήνεια.

Μόλις εγγραφείτε, η συνδρομή ανανεώνεται αυτόματα, οδηγώντας σε απροσδόκητες χρεώσεις στην πιστωτική σας κάρτα ή στον τραπεζικό σας λογαριασμό.

Η ακύρωση της συνδρομής γίνεται σκόπιμα δύσκολη, με περίπλοκες διαδικασίες, μη ανταποκρινόμενη εξυπηρέτηση πελατών ή ασαφείς πολιτικές ακύρωσης.

Παραπλανητικές
διαφημίσεις και
σύνδεσμοι

Κρυφοί όροι

Αυτόματες
ανανεώσεις

Δυσκολία
ακύρωσης

Απάτη με συνδρομές

— ΣΥΝΕΠΕΙΕΣ:

Η απάτη στις συνδρομές μπορεί να έχει σοβαρές αρνητικές επιπτώσεις, όπως:

01 Οικονομική ζημία

Το να πέσετε θύμα απάτης συνδρομής μπορεί να οδηγήσει στην απώλεια των αποταμιεύσεων που αποκτήσατε με κόπο. Μπορείτε να χάσετε σημαντικά χρηματικά ποσά λόγω επαναλαμβανόμενων χρεώσεων που δεν είχαν προβλέψει ή συμφωνήσει.

02 Κλοπή ταυτότητας

Η παροχή προσωπικών πληροφοριών και πληροφοριών πληρωμής σε δόλιους ιστότοπους μπορεί να οδηγήσει σε κλοπή ταυτότητας και περαιτέρω οικονομική ζημία.

03 Συναισθηματικό στρες

Η απογοήτευση και το άγχος της αντιμετώπισης μη εξουσιοδοτημένων χρεώσεων και της προσπάθειας ακύρωσης της συνδρομής μπορεί να επηρεάσει τη συναισθηματική σας ευημερία.

Απάτη με συνδρομές



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΤΗΝ ΙΣΤΟΡΙΑ ΣΤΟ ΠΑΡΑΣΚΗΝΙΟ



Ο David είδε μια διαδικτυακή διαφήμιση για μια δωρεάν δοκιμή ενός νέου συμπληρώματος βιταμινών. Η διαφήμιση ισχυριζόταν ότι χρειαζόταν να πληρώσει μόνο ένα μικρό ποσό αποστολής για να εγγραφεί και στη συνέχεια θα έπαιρνε απεριόριστες βιταμίνες για το υπόλοιπο του έτους. Ενθουσιασμένος που ήθελε να δοκιμάσει το συμπλήρωμα, αποφάσισε να εισάγει τα στοιχεία της πιστωτικής του κάρτας για να καλύψει τα έξοδα αποστολής.

Ενώ το έκανε αυτό, ο David θυμήθηκε τι είχε διαβάσει για κάποιες ιστοσελίδες που αφαιρούσαν χρήματα από αθώους ανθρώπους. Τι έκανε λοιπόν ο Ντέιβιντ;

Η απάτη στις συνδρομές μπορεί να είναι μια δαπανηρή και απογοητευτική εμπειρία, ιδίως για τους ηλικιωμένους. Αν είστε σε εγρήγορση, διαβάζετε τα ψιλά γράμματα και λαμβάνετε μέτρα για την προστασία των προσωπικών και οικονομικών σας πληροφοριών, μπορείτε να αποφύγετε να πέσετε θύμα αυτών των απατών. Προσεγγίζετε πάντα τις δωρεάν δοκιμές και τις προσφορές με έκπτωση με προσοχή και βεβαιωθείτε ότι έχετε κατανοήσει τους πλήρεις όρους πριν δώσετε τα στοιχεία πληρωμής σας. Μείνετε ενημερωμένοι, παραμείνετε προσεκτικοί και προστατευθείτε από απάτες με συνδρομές.



Βήμα 1. Διαβάστε τα ψιλά γράμματα

Πριν από την εγγραφή του, έψαξε για οποιαδήποτε αναφορά σε τρέχουσες συνδρομές ή πρόσθετες χρεώσεις.

Βήμα 2. Έρευνα

Έψαξε την εταιρεία και διάβασε κριτικές για να δει αν άλλοι έχουν αντιμετωπίσει παρόμοια προβλήματα

Βήμα 3. Παρακολούθηση καταθέσεων

Έλεγε τακτικά τους λογαριασμούς του για να εντοπίζει έγκαιρα τις μη εξουσιοδοτημένες χρεώσεις.

Απάτη με συνδρομές

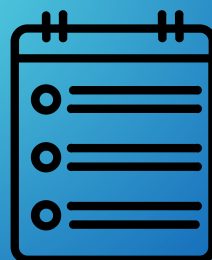


ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Η προστασία σας από απάτες με συνδρομές είναι ζωτικής σημασίας για τη διαφύλαξη των χρημάτων που με κόπο κερδίσατε. Ακολουθούν ορισμένα απλά βήματα που μπορείτε να ακολουθήσετε.

Διαβάστε τα φιλά γράμματα:

Διαβάζετε πάντα τους όρους και τις προϋποθέσεις πριν εγγραφείτε σε οποιαδήποτε υπηρεσία, ειδικά αν πρόκειται για δωρεάν δοκιμή ή προσφορά με έκπτωση.

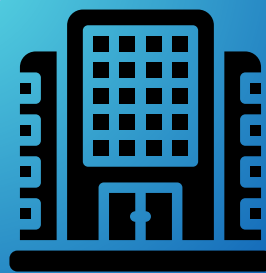


Προσοχή στις δωρεάν δοκιμές:

Να είστε προσεκτικοί στις δωρεάν δοκιμές που απαιτούν τα στοιχεία της πιστωτικής σας κάρτας. Ελέγξτε αν η δοκιμή μετατρέπεται σε συνδρομή επί πληρωμή και ποιο θα είναι το κόστος.

Ερευνήστε την εταιρεία:

Αναζητήστε κριτικές και αξιολογήσεις της εταιρείας που προσφέρει τη συνδρομή. Βεβαιωθείτε ότι έχουν καλή φήμη και αξιόπιστη εξυπηρέτηση πελατών.



Απάτη με συνδρομές



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Παρακολούθηση τραπεζικών καταστάσεων:

Ελέγχετε τακτικά τους λογαριασμούς της τράπεζας και της πιστωτικής σας κάρτας για τυχόν μη εξουσιοδοτημένες ή ύποπτες χρεώσεις.



Ρύθμιση ειδοποιήσεων:

Χρησιμοποιήστε τις ειδοποιήσεις λογαριασμού για να σας ειδοποιήσουν για τυχόν νέες χρεώσεις ή συναλλαγές. Με αυτόν τον τρόπο, μπορείτε να εντοπίζετε και να αμφισβητείτε γρήγορα μη εξουσιοδοτημένες χρεώσεις.

Ζητήστε βοήθεια:

Εάν πέσετε θύμα απάτης με συνδρομές, επικοινωνήστε αμέσως με την τράπεζα ή την εταιρεία πιστωτικών καρτών σας για να αναφέρετε τις μη εξουσιοδοτημένες χρεώσεις. Μπορούν να σας βοηθήσουν να σταματήσετε περαιτέρω χρεώσεις και να ανακτήσετε τα χρήματά σας.



Απάτη με τη δημιουργία ψεύτικων ηλεκτρονικών καταστημάτων



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Τα ψεύτικα ηλεκτρονικά καταστήματα είναι δόλιοι ιστότοποι που δημιουργήθηκαν για να μοιάζουν με νόμιμους ιστότοπους αγορών. Αυτοί οι απατεώνες χρησιμοποιούν παραπλανητικές τακτικές πωλήσεων για να ξεγελάσουν τους ανθρώπους και να τους οδηγήσουν σε αγορές. Αντί να λάβουν τα αντικείμενα που παρήγγειλαν, τα θύματα συχνά λαμβάνουν πλαστά προϊόντα, αντικείμενα χαμηλής ποιότητας ή τίποτα απολύτως. Αυτός ο τύπος απάτης μπορεί να επηρεάσει σημαντικά τα ευάλωτα άτομα, συμπεριλαμβανομένων των ηλικιωμένων.

Τύποι χειραγώγησης σε ψεύτικα ηλεκτρονικά καταστήματα:

Οι απατεώνες προσελκύουν αγοραστές με απίστευτα χαμηλές τιμές ή τεράστιες εκπτώσεις σε δημοφιλή είδη.

Ενώ ορισμένοι ψεύτικοι ιστότοποι είναι πολύ εξελιγμένοι, πολλοί έχουν κακό σχεδιασμό, σπασμένους συνδέσμους ή εικόνες χαμηλής ποιότητας.

Οι νόμιμες επιχειρήσεις παρέχουν σαφείς πληροφορίες επικοινωνίας, συμπεριλαμβανομένων φυσικών διευθύνσεων και τηλεφωνικών αριθμών εξυπηρέτησης πελατών.

Η έλλειψη γνώσιων κριτικών πελατών ή η ύπαρξη μόνο υπερβολικά θετικών, γενικών κριτικών μπορεί να αποτελέσει κόκκινο πανί.

Οι νόμιμοι ιστότοποι αγορών χρησιμοποιούν ασφαλείς συνδέσεις για την προστασία των δεδομένων σας. Αναζητήστε το «https» και το εικονίδιο του λουκέτου στη γραμμή διευθύνσεων του προγράμματος περιήγησης.

Πολύ καλές
για να είναι
αληθινές
τιμές

Κακή
σχεδίαση
ιστοσελίδας

Περιορισμένες
πληροφορίες
επικοινωνίας

Χωρίς
κριτικές ή
ψεύτικες
κριτικές

Δεν υπάρχει
ασφαλής
σύνδεση

Απάτη με τη δημιουργία ψεύτικων ηλεκτρονικών καταστημάτων

— ΣΥΝΕΠΕΙΕΣ:

Η απάτη σχετικά με τα ψεύτικα ηλεκτρονικά καταστήματα μπορεί να προκαλέσει σοβαρές αρνητικές επιπτώσεις, όπως:

01 Οικονομική ζημία

Το να πέσετε θύμα απάτης σχετικά με ψεύτικα ηλεκτρονικά καταστήματα μπορεί να οδηγήσει στην απώλεια των αποταμιεύσεων. Μπορεί να βρεθείτε με σημαντικά λιγότερα χρήματα από τα αναμενόμενα, επηρεάζοντας την ικανότητά σας να καλύπτετε τα καθημερινά έξοδα και να απολαμβάνετε τη σύνταξή σας.

02 Συναισθηματικό στρες

Η συνειδητοποίηση ότι έχουν εξαπατηθεί μπορεί να προκαλέσει σημαντική συναισθηματική οδύνη. Οι ηλικιωμένοι μπορεί να αισθάνονται αμηχανία, ντροπή ή ενοχή επειδή έπεσαν στην απάτη. Αυτός ο συναισθηματικός αντίκτυπος μπορεί να οδηγήσει σε άγχος, κατάθλιψη και μειωμένη αίσθηση εμπιστοσύνης στις ηλεκτρονικές αγορές και στα χρηματοπιστωτικά ιδρύματα.

03 Κλοπή προσωπικών πληροφοριών

Τα ψεύτικα ηλεκτρονικά καταστήματα συχνά συλλέγουν προσωπικές και οικονομικές πληροφορίες κατά τη διαδικασία πληρωμής. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για κλοπή ταυτότητας, οδηγώντας σε μη εξουσιοδοτημένες συναλλαγές, άνοιγμα νέων πιστωτικών λογαριασμών στο όνομα του θύματος και άλλες μορφές απάτης.

Απάτη με τη δημιουργία ψεύτικων ηλεκτρονικών καταστημάτων



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΦΟΝΤΟ ΤΗΝ ΙΣΤΟΡΙΑ



Η Εύα είδε μια διαφήμιση στα μέσα κοινωνικής δικτύωσης για ένα υψηλής ποιότητας μπλέντερ με έκπτωση 75%. Ενθουσιασμένη από τη μεγάλη προσφορά, έκανε κλικ στον σύνδεσμο και οδηγήθηκε σε έναν ιστότοπο που έδειχνε επαγγελματικός, αλλά προσέφερε περιορισμένα στοιχεία επικοινωνίας. Ο ιστότοπος επέμενε στην πληρωμή μέσω εμβάσματος για να εξασφαλίσει τη χαμηλή τιμή. Αφού πραγματοποίησε την πληρωμή, δεν παρέλαβε ποτέ το μπλέντερ και οι προσπάθειες να επικοινωνήσει με την υπηρεσία εξυπηρέτησης πελατών έμειναν αναπάντητες.

Τι έπρεπε να είχε κάνει η Εύα για να αποφύγει την απάτη;

Τα ψεύτικα ηλεκτρονικά καταστήματα μπορούν να εξαπατήσουν και να προκαλέσουν σημαντική οικονομική και συναισθηματική ζημία, ιδίως στους ηλικιωμένους. Παραμένοντας ενημερωμένοι και ακολουθώντας τα μέτρα προστασίας που περιγράφονται παρακάτω, μπορείτε να μειώσετε τον κίνδυνο να πέσετε θύμα αυτών των απατών. Αφιερώνετε πάντα χρόνο για να ερευνήσετε και να επαληθεύσετε τα ηλεκτρονικά καταστήματα πριν κάνετε οποιαδήποτε αγορά, ώστε να εξασφαλίσετε μια ασφαλή και προστατευμένη εμπειρία αγορών.



Βήμα 1. Έρευνα για τον ιστότοπο

Έπρεπε να ελέγξει τις κριτικές και να αναζητήσει τα στοιχεία επικοινωνίας του καταστήματος.

Βήμα 2. Επαλήθευση ασφαλών συνδέσεων

Βεβαιωθείτε ότι ο ιστότοπος έχει την ένδειξη «https» και ένα εικονίδιο λουκέτου.

Βήμα 3. Να είστε επιφυλακτικοί με τις συμφωνίες

Αμφισβητήστε την πολύ καλή για να είναι αληθινή έκπτωση.

Βήμα 4. Χρήση ασφαλών μεθόδων πληρωμής

Avoid wire transfers; use a credit card instead.

Απάτη με τη δημιουργία ψεύτικων ηλεκτρονικών καταστημάτων



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Να θυμάστε, αγαπητοί ηλικιωμένοι, ότι η προστασία σας από τα ψεύτικα ηλεκτρονικά καταστήματα είναι ζωτικής σημασίας για τη διαφύλαξη των χρημάτων και των συναισθημάτων σας. Ακολουθούν ορισμένα απλά βήματα που μπορείτε να ακολουθήσετε.

Ερευνήστε τον ιστότοπο:

Ελέγξτε για σχόλια και αξιολογήσεις από άλλους πελάτες. Χρησιμοποιήστε αξιόπιστους ιστότοπους αναθεωρήσεων για να επαληθεύσετε τη νομιμότητα του καταστήματος. Αναζητήστε τα στοιχεία επικοινωνίας του καταστήματος και προσπαθήστε να επικοινωνήσετε μαζί του πριν προβείτε σε αγορά.



Επαλήθευση ασφαλών συνδέσεων:

Βεβαιωθείτε ότι ο ιστότοπος χρησιμοποιεί ασφαλή σύνδεση («https» και εικονίδιο λουκέτου). Αποφύγετε την εισαγωγή προσωπικών πληροφοριών ή πληροφοριών πληρωμής σε ιστότοπους χωρίς ασφαλή σύνδεση.

Να είστε επιφυλακτικοί σε υπερβολικά καλές για να είναι αληθινές προσφορές:

Αν οι τιμές φαίνονται απίστευτα χαμηλές ή οι προσφορές είναι πολύ καλές για να είναι αληθινές, μάλλον είναι. Συγκρίνετε τις τιμές με άλλες αξιόπιστες επιχειρήσεις λιανικής πώλησης.



Απάτη με τη δημιουργία ψεύτικων ηλεκτρονικών καταστημάτων



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Χρησιμοποιήστε ασφαλείς μεθόδους πληρωμής:

Χρησιμοποιήστε πιστωτικές κάρτες για ηλεκτρονικές αγορές, καθώς προσφέρουν καλύτερη προστασία από απάτες. Αποφύγετε τη χρήση εμβασμάτων, προπληρωμένων καρτών ή κρυπτονομισμάτων για πληρωμές.



Ελέγξτε τα στοιχεία του ιστότοπου:

Αναζητήστε σαφείς, λεπτομερείς περιγραφές προϊόντων και επαγγελματικές εικόνες. Επαληθεύστε τα στοιχεία επικοινωνίας του ιστότοπου, συμπεριλαμβανομένων τηλεφωνικών αριθμών και φυσικών διευθύνσεων.

Γνωρίστε την πολιτική επιστροφών:

Τα νόμιμα καταστήματα έχουν σαφείς πολιτικές επιστροφής. Να είστε επιφυλακτικοί εάν αυτές οι πληροφορίες λείπουν ή είναι ασαφείς.



Αθέμιτες αγορές μέσω διαδικτυακών διαφημίσεων (αγορά)



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Η διαδικτυακή δόλια διαφήμιση αποτελεί σημαντική απειλή, με τους απατεώνες να αξιοποιούν πλατφόρμες κοινωνικής δικτύωσης, δημοφιλείς ιστότοπους, ακόμη και μηχανές αναζήτησης όπως η Google. Οι ψεύτικες διαφημίσεις μπορούν να λάβουν πολλές μορφές, όπως αναδυόμενα παράθυρα, banners, διαφημίσεις στα μέσα κοινωνικής δικτύωσης και χορηγούμενο περιεχόμενο. Αυτές οι παραπλανητικές διαδικτυακές διαφημίσεις έχουν σχεδιαστεί για να ξεγελούν ανυποψίαστους χρήστες ώστε να κάνουν κλικ σε αυτές, οδηγώντας ενδεχομένως σε δόλιες αγορές.

Τύποι χειραγώγησης στις αγορές μέσω διαδικτυακών διαφημίσεων

Οι απατεώνες χρησιμοποιούν συνήθως διαφημιστικό υλικό (λογότυπα, λεζάντες, σλόγκαν κ.λπ.) από πραγματικά γνωστές μάρκες. Στη συνέχεια, αρχίζουν να τρέχουν στοχευμένες διαφημίσεις για να εξαπατήσουν τα θύματα. Οι απατεώνες μπορεί επίσης να χρησιμοποιούν τακτικές κοινωνικής μηχανικής, όπως δελεαστικές προσφορές, για να παρασύρουν τους χρήστες να κάνουν κλικ σε αυτές τις ψεύτικες διαφημίσεις.

Καθώς οι ψεύτικες διαφημίσεις μπορούν να φαίνονται πολύ επαγγελματικές και πειστικές, είναι δύσκολο να τις διακρίνετε από τις νόμιμες διαφημίσεις. Όταν ένα θύμα κάνει κλικ σε μια διαφήμιση, συνήθως καταλήγει σε ένα ψεύτικο κατάστημα - όπου μπορεί να συμβεί phishing - ή σε ένα κατάστημα που πουλάει απομιμήσεις. Σε αυτές τις περιπτώσεις (εκτός από το phishing), υπάρχει επίσης ο κίνδυνος το θύμα να μην παραλάβει το προϊόν ή να παραλάβει ένα προϊόν χαμηλότερης ποιότητας από αυτή που πλήρωσε.

Οι απατεώνες χρησιμοποιούν συχνά ψεύτικες διαφημίσεις με ενσωματωμένο κακόβουλο κώδικα που μπορεί να μολύνει τις συσκευές των χρηστών όταν κάνουν κλικ. Αυτή η μέθοδος, γνωστή ως malvertising, έχει γίνει μια ευρέως διαδεδομένη τακτική που χρησιμοποιείται από εγκληματίες του κυβερνοχώρου για τη διάδοση κακόβουλου λογισμικού μέσω ψεύτικων διαφημίσεων.

Απομίμηση

Δεν υπάρχουν
«πραγματικά»
αγαθά

Κακόβουλη
διαφήμιση

Αθέμιτες αγορές μέσω διαδικτυακών διαφημίσεων (αγορά)

— ΣΥΝΕΠΕΙΕΣ:

Ανεξάρτητα από τη μέθοδο που επιλέγεται, οι απατεώνες που κρύβονται πίσω από ψεύτικες διαφημίσεις επιδιώκουν πάντα οικονομικό κέρδος.

01 Οικονομικές συνέπειες – Άμεση οικονομική κλοπή

Οι ψεύτικες διαφημίσεις που προσφέρουν προϊόντα με μεγάλες εκπτώσεις από γνωστές μάρκες συχνά κρύβουν καταστήματα που στοχεύουν στη συλλογή στοιχείων πληρωμής και ευαίσθητων πληροφοριών κατά το στάδιο της πληρωμής μιας συναλλαγής. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για την κλοπή χρημάτων από λογαριασμούς, την έναρξη πρόσθετων επιθέσεων στον κυβερνοχώρο ή την πώληση σε άλλους εγκληματίες του κυβερνοχώρου. Σε πολλές περιπτώσεις, τα θύματα λαμβάνουν πλαστά προϊόντα ή δεν λαμβάνουν τίποτα απολύτως.

02 Οικονομικές συνέπειες – Κόστος Ransomware

Η παραβίαση συστημάτων και δεδομένων μέσω της μεθόδου της κακόβουλης διαφήμισης μπορεί επίσης να έχει οικονομικές συνέπειες. Κάνοντας κλικ στη διαφήμιση, το κακόβουλο λογισμικό αρχίζει να κατεβάζει και να εγκαθιστά ransomware – έναν τύπο κακόβουλου λογισμικού που κρυπτογραφεί τα αρχεία σας – οι απατεώνες απαιτούν πληρωμή για την απελευθέρωσή τους. Το κόστος που συνδέεται με την καταβολή των λύτρων, την επισκευή του συστήματός σας και την αφαίρεση του κακόβουλου λογισμικού μπορεί να είναι σημαντικό.

03 Κλοπή ταυτότητας

Μέσω της μεθόδου phishing, οι απατεώνες υποδύονται νόμιμες μάρκες σε μια προσπάθεια να εξαπατήσουν τα θύματα ώστε να μοιραστούν προσωπικές πληροφορίες ή εγκαθιστώντας spyware (μέσω της μεθόδου malvertisig) το οποίο συλλέγει κρυφά ευαίσθητες πληροφορίες από τη συσκευή, όπως διαπιστευτήρια σύνδεσης και οικονομικά δεδομένα, μπορεί να οδηγήσει σε σοβαρή κλοπή ταυτότητας, όπου τα ευαίσθητα δεδομένα των θυμάτων χρησιμοποιούνται καταχρηστικά.

Αθέμιτες αγορές μέσω διαδικτυακών διαφημίσεων (αγορά)



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΦΟΝΤΟ ΤΗΝ ΙΣΤΟΡΙΑ



Η Λίζα, τακτικός χρήστης διαφόρων πλατφορμών κοινωνικής δικτύωσης, περιφερόταν στο Facebook όταν έπεσε πάνω σε μια διαδικτυακή διαφήμιση που προσέφερε ένα πολύ ωραίο μπλέντερ. Η διαφήμιση έδειχνε την εικόνα ενός κορυφαίου μπλέντερ σε εξαιρετικά χαμηλή τιμή με την υπόσχεση γρήγορης παράδοσης.

Η διαφήμιση φαινόταν πολύ καλή για να είναι αληθινή, αλλά έκανε κατά λάθος κλικ πάνω της και ανακατευθύνθηκε σε κάτι που αρχικά φαινόταν να είναι ένα νόμιμο ηλεκτρονικό κατάστημα ... Ωστόσο, η Λίζα αναγνώρισε τα προειδοποιητικά σημάδια!

Δυστυχώς για τον απατεώνα ...

Η Λίζα παρακολούθησε ένα σεμινάριο για προχωρημένους σχετικά με τις απάτες στα μέσα κοινωνικής δικτύωσης.



ΒΗΜΑ 1: Έλεγχος ποιότητας

Μετά την ανακατεύθυνση, η Λίζα παρατήρησε αμέσως ότι ο ιστότοπος ήταν κακοσχεδιασμένος, είχε πολλά γραμματικά λάθη και ότι οι φωτογραφίες ήταν κακής ποιότητας σε αντίθεση με τη διαφήμιση.

ΒΗΜΑ 3: Έλεγχος νομιμότητας

Όταν η Λίζα έλεγξε τον ιστότοπο, διαπίστωσε ότι έλειπαν βασικά στοιχεία επικοινωνίας, όπως η διεύθυνση της εταιρείας, ο αριθμός τηλεφώνου και το email της υπηρεσίας εξυπηρέτησης πελατών.

ΒΗΜΑ 2: Τεχνικός έλεγχος

Η Λίζα παρατήρησε ότι η διεύθυνση URL του ιστότοπου δεν ταίριαζε με το εμπορικό σήμα. Αντίθετα, ο τίτλος αποτελούνταν από τυχαία γράμματα και αριθμούς.

ΒΗΜΑ 4: Έλεγχος των σχολίων

Η Λίζα παρατήρησε επίσης ότι δεν υπήρχαν κριτικές ή σχόλια πελατών στον ιστότοπο. Ένας νόμιμος διαδικτυακός έμπορος παρέχει συνήθως σχόλια και γνώμες από προηγούμενους πελάτες.

Αθέμιτες αγορές μέσω διαδικτυακών διαφημίσεων (αγορά)



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Απάτες με ψεύτικες διαφημίσεις, όπου οι εγκληματίες προωθούν πλαστά ή ανύπαρκτα προϊόντα σε ελκυστικές τιμές και εκμεταλλεύονται το ενδιαφέρον των ηλικιωμένων για εκπτώσεις. Οι απατεώνες μπορεί να παρατείνουν την απάτη επινοώντας δικαιολογίες για καθυστερήσεις στην παράδοση, γεγονός που αυξάνει περαιτέρω την οικονομική ζημία των θυμάτων.

Ακολουθούν ορισμένες πρόσθετες συμβουλές σε περίπτωση που μπορεί να βρεθείτε σε μια τέτοια κατάσταση.

Για να προστατευτείτε από πιθανές απάτες, **είναι ασφαλέστερο να αγνοείτε τις διαφημίσεις**, ειδικά εκείνες που σας φαίνονται ύποπτες!

Επίσης, **προσέξτε πού κάνετε κλικ!** Προσέχοντας πού βρίσκεται το ποντίκι στην οθόνη και προσέχοντας σε ποιο σημείο της σελίδας κάνετε scrolling μπορεί να σας βοηθήσει να αποφύγετε τυχαία κλικ!



Να είστε προσεκτικοί όταν κάνετε κλικ σε οποιονδήποτε σύνδεσμο, ακόμη και σε αυτούς που βρίσκονται στην κορυφή των αποτελεσμάτων των μηχανών αναζήτησης.

Δώστε μεγάλη προσοχή για να διακρίνετε τις διαφημίσεις από τα γνήσια αποτελέσματα αναζήτησης. Οι διαφημίσεις εμφανίζονται συνήθως πρώτες και επισημαίνονται με την ένδειξη «Ad» ή «Advertisement».

Λάβετε υπόψη ότι οι απατεώνες πληρώνουν σκόπιμα για την τοποθέτηση διαφημίσεων στις μηχανές αναζήτησης!

Αθέμιτες αγορές μέσω διαδικτυακών διαφημίσεων (αγορά)



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Πληκτρολογείτε πάντα τη διεύθυνση URL του ιστότοπου απευθείας στο πρόγραμμα περιήγησής σας:

Αναζητήστε ένα εικονίδιο κλειδαριάς και το «https» στο πρόγραμμα περιήγησής σας για να επιβεβαιώσετε ότι είναι ασφαλές, επαληθεύστε τη διεύθυνση URL (τοποθετήστε τον κέρσορα πάνω από τη διεύθυνση URL).



Προστατέψτε τον υπολογιστή σας:

Είναι σημαντικό να εγκαθιστάτε και να ενημερώνετε τακτικά το λογισμικό προστασίας από ιούς και λογισμικό ασφαλείας στον υπολογιστή σας. Αυτό θα διασφαλίσει ότι ο υπολογιστής σας προστατεύεται από διάφορους τύπους απειλών, όπως ιούς, επιθέσεις χάκερ και κακόβουλο λογισμικό.

Ενεργοποιήστε τη λειτουργία αποκλεισμού αναδυόμενων παραθύρων στα προγράμματα περιήγησής σας!

Αθέμιτες αγορές μέσω διαδικτυακών διαφημίσεων (αγορά)



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Οι ψεύτικοι διαδικτυακοί πωλητές/απατεώνες συνήθως ζητούν πληρωμή μέσω αναξιόπιστων μεθόδων, όπως τραπεζικές μεταφορές (καθώς προσφέρουν λιγότερη προστασία σε περίπτωση απάτης, σε σύγκριση με άλλες μεθόδους πληρωμής, όπως οι πιστωτικές κάρτες) ή άγνωστες πλατφόρμες πληρωμών.

Μην κάνετε ποτέ πληρωμή με αυτόν τον τρόπο! Επίσης, μην αποκαλύπτετε ποτέ τις οικονομικές ή άλλες ευαίσθητες πληροφορίες σας!

Εάν πέσετε θύμα απάτης, **προσπαθήστε να συγκεντρώσετε όσο το δυνατόν περισσότερα αποδεικτικά στοιχεία και αναφέρετε την απάτη αμέσως στην αρμόδια αρχή!**



Αναφορά! Οι περισσότερες πλατφόρμες διαθέτουν μηχανισμούς αναφοράς για την αντιμετώπιση τέτοιων ζητημάτων.

Χρησιμοποιήστε τη λειτουργία αναφοράς στην πλατφόρμα, η οποία είναι συνήθως προσβάσιμη μέσω του κουμπιού «Αναφορά» στη διαφήμιση ή στο προφίλ χρήστη.

Περιμένετε οδηγίες από την ομάδα υποστήριξης της πλατφόρμας και σταματήστε κάθε αλληλεπίδραση με το ύποπτο άτομο μετά την αναφορά.

Αθέμιτες αγορές μέσω δικτυακών τόπων αγγελιών (πώληση)



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Οι διαδικτυακές αγορές μπορούν να αποτελέσουν έναν εξαιρετικό τρόπο για τους ηλικιωμένους να βγάλουν μερικά επιπλέον χρήματα, καθώς μπορούν να πουλήσουν τα αντικείμενά τους, όπως χειροποίητες κατασκευές, αντίκες ή περιττά οικιακά αντικείμενα κ.λπ. Αυτό τους δίνει τη δυνατότητα να κερδίσουν πρόσθετα χρήματα, τα οποία μπορούν να χρησιμοποιηθούν για τη βελτίωση του βιοτικού τους επιπέδου ή για ειδικές περιστάσεις. Οι ηλικιωμένοι πρέπει να είναι ιδιαίτερα προσεκτικοί όταν πωλούν, καθώς οι αγορές αυτές είναι επίσης επιρρεπείς σε απατεώνες που εμφανίζονται ως πιθανοί αγοραστές.

Τύποι χειραγώγησης σε απάτες αγοραστών με αγγελίες:

Οι απατεώνες είναι πρόθυμοι να «αγοράσουν» ένα αντικείμενο χωρίς να το δουν και συχνά χρησιμοποιούν διάφορες δικαιολογίες, όπως ασθένεια, μήνα του μέλιτος ή ταξίδι στο εξωτερικό κ.λπ. Επικοινωνούν με τα θύματα μόνο μέσω γραπτών μηνυμάτων ή ηλεκτρονικού ταχυδρομείου και αποφεύγουν τις τηλεφωνικές κλήσεις ή τις βιντεοκλήσεις. Συχνά ζητούν να αποσταλεί το αντικείμενο στον «πράκτορα αποστολής» τους ή κανονίζουν να το παραλάβει ένας ταχυμεταφορέας. Όλες αυτές οι μέθοδοι επικοινωνίας επιτρέπουν στους απατεώνες να αποκρύψουν την ταυτότητά τους.

Οι απατεώνες ζητούν αποκλειστικά την πληρωμή με επιταγή, έμβασμα, τραπεζικό έμβασμα, διεθνές έμβασμα, εφαρμογές πληρωμών μέσω κινητού τηλεφώνου κ.λπ., στέλνοντας ψεύτικες επιβεβαιώσεις πληρωμής και ελπίζοντας ότι τα θύματα θα στείλουν το προϊόν πριν συνειδητοποιήσουν ότι πρόκειται για απάτη. Μπορεί να χρησιμοποιήσουν «δικαιολογίες», όπως ότι υπήρξε πρόβλημα με την πληρωμή που έστειλαν, μπορεί να ζητήσουν από τα θύματα να προκαταβάλουν τα έξοδα μεταφοράς ή αποστολής και να υποσχεθούν ότι θα επιστρέψουν τα έξοδα κ.λπ.

Οι απατεώνες συνήθως προσφέρουν στα θύματα περισσότερα χρήματα από την τιμή που ζητούν. Οι λόγοι ποικίλλουν – μπορεί να ισχυρίζονται ότι αποζημιώνουν για τα «προβλήματα» του θύματος, καλύπτουν υποτιθέμενα έξοδα αποστολής ή προσποιούνται ότι έκαναν λάθος στο ποσό πληρωμής. Ωστόσο, μόλις τα θύματα λάβουν μια υπερπληρωμή, οι απατεώνες θα ζητήσουν πίσω τα πλεονάζοντα χρήματα.

**Καμία
προσωπική
επαφή**

**Χωρίς
μετρητά**

Υπερπληρωμή

Αθέμιτες αγορές μέσω ιστοσελίδων αγγελιών (πώληση)



ΣΥΝΕΠΕΙΕΣ:

Τα θύματα απάτης με αγγελίες αγοραστών μπορεί να βιώσουν τις ακόλουθες αρνητικές επιπτώσεις:

01 Οικονομικές συνέπειες

Τα θύματα μπορεί να αντιμετωπίσουν οικονομικές συνέπειες, όπως η χρηματική απώλεια της αξίας των αντικειμένων, εάν έχουν στείλει αντικείμενα χωρίς να λάβουν πληρωμή. Εάν υπήρξε υπερπληρωμή και τα θύματα έχουν επιστρέψει τα χρήματα, είναι πιθανό να διαπιστώσουν ότι η αρχική πληρωμή ήταν δόλια - η επιταγή θα αφαιρεθεί ή η ηλεκτρονική πληρωμή του πελάτη θα απορριφθεί - σε αυτή την περίπτωση, τα θύματα έχουν χάσει τα χρήματα που «επέστρεψαν» και τη χρηματική αξία των αντικειμένων.

02 Συναισθηματικές συνέπειες

Το θύμα μπορεί να αναπτύξει μια σειρά από συμπτώματα, συμπεριλαμβανομένων αρνητικών σκέψεων για τον εαυτό του. Τα θύματα μπορεί να πιστεύουν ότι δεν είναι έξυπνα ή ότι υπάρχει κάτι λάθος με την ικανότητά τους να κρίνουν τους άλλους. Συχνά κατηγορούν τον εαυτό τους για το έγκλημα, νιώθοντας ότι ήταν υπερβολικά έμπιστοι, και νιώθουν θυμό, θλίψη, προδοσία, αδυναμία και αμηχανία.

03 Νομικές συνέπειες

Εάν το θύμα συμφώνησε και αποδέχθηκε την πληρωμή με επιταγή, αλλά η επιταγή ήταν πλαστή, το ανυποψίαστο θύμα θα θεωρηθεί νομικά υπεύθυνο για την προσπάθεια εξαργύρωσης της παράνομης επιταγής όταν η τράπεζα εντοπίσει την πλαστογραφία. Επιπλέον, το θύμα ενδέχεται να αντιμετωπίσει δυσκολίες σε μελλοντικές οικονομικές συναλλαγές.

Αθέμιτες αγορές μέσω ιστοσελίδων αγγελιών (πώληση)



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΦΟΝΤΟ ΤΗΝ ΙΣΤΟΡΙΑ



Ο Leon δημοσίευσε μια αγγελία στο Facebook Marketplace για ένα μεταχειρισμένο ποδήλατο προς 200 ευρώ και έλαβε αμέσως ένα μήνυμα από τον «Tim», ο οποίος ήθελε να το αγοράσει χωρίς να διαπραγματευτεί την τιμή και μάλιστα προσέφερε 30 ευρώ επιπλέον για τα έξοδα αποστολής. Ο Leon βρήκε περίεργο το γεγονός ότι ο Tim δεν ήθελε να δει το προϊόν από κοντά, παρά το γεγονός ότι ζούσε στην ίδια πόλη. Ο Tim ήθελε επίσης να πληρώσει για το προϊόν μέσω PayPal και ζήτησε τον αριθμό κοινωνικής ασφάλισης και τη διεύθυνση κατοικίας του Leon. Τότε ήταν που ο Λεόν έκανε γρήγορα πίσω!

Δυστυχώς για τον απατεώνα ...

Ο Leon παρακολούθησε την εκστρατεία ευαισθητοποίησης στην κοινότητα των χρηστών και εκπαιδεύτηκε σχετικά με τις συνήθειες απόπειρες αυτού του τύπου απάτης και τα προληπτικά μέτρα.



ΒΗΜΑ 1: Αναγνώριση ύποπτης συμπεριφοράς

Ο Leon βρήκε περίεργο το γεγονός ότι ο Tim δεν ήθελε να δει το προϊόν από κοντά, παρόλο που ζούσε στην ίδια πόλη. Αυτό ήταν το πρώτο προειδοποιητικό σημάδι, καθώς οι νόμιμοι αγοραστές συνήθως προτιμούν να επιθεωρούν τα αντικείμενα πριν προβούν σε αγορά.

ΒΗΜΑ 2: Έρευνα

Ο Leon ερεύνησε το προφίλ του Tim και βρήκε ύποπτα στοιχεία επικοινωνίας και ασυνεπή επικοινωνία. Ο Leon μπλόκαρε τον Tim και διέκοψε αμέσως κάθε επικοινωνία, αποτρέποντας έτσι περαιτέρω κινδύνους.

ΒΗΜΑ 3: Προστασία

Ο Tim ήθελε να πληρώσει μέσω PayPal, κάτι που δεν είναι από μόνο του ύποπτο, αλλά ζήτησε επίσης τον αριθμό κοινωνικής ασφάλισης και τη διεύθυνση κατοικίας του Leon, κάτι που είναι εξαιρετικά ασυνήθιστο και περιττό. Ο Leon αποφάσισε συνειδητά να μην μοιραστεί αυτές τις πληροφορίες.

ΒΗΜΑ 4: Ενημέρωση/αναφορά

Ο Leon μοιράστηκε την εμπειρία του με την κοινότητα και ανέφερε το προφίλ του Tim στην πλατφόρμα. Με τον τρόπο αυτό, βοήθησε στην ευαισθητοποίηση και την προστασία και άλλων χρηστών.

Αθέμιτες αγορές μέσω ιστοσελίδων αγγελιών (πώληση)



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Εάν διαφημίζετε τα αντικείμενά σας προς πώληση μέσω διαδικτυακών πυλών αγγελιών, παραθέτουμε ορισμένα απλά βήματα που μπορείτε να λάβετε για να ενδυναμώσετε και να προστατευτείτε από απατεώνες που προσποιούνται ότι είναι πιθανοί αγοραστές.

Να είστε επιφυλακτικοί όταν κάποιος σας προσφέρει περισσότερα από την τιμή που ζητάτε (εκτός αν πουλάτε ένα αντικείμενο με πολλαπλές ανταγωνιστικές προσφορές). Μην εμπλακείτε με οποιονδήποτε σας προσφέρει να σας στείλει πληρωμή σε υψηλότερο ποσό, περιμένοντας να στείλετε πίσω το πλεόνασμα.

Απορρίψτε αμέσως την πληρωμή αυτή και επιμείνετε να λάβετε το σωστό ποσό σε νέα συναλλαγή.



Ζητήστε πληρωμή σε μετρητά:

Εάν αυτό δεν είναι δυνατό, μην στείλετε ένα αντικείμενο πριν λάβετε την πληρωμή και βεβαιωθείτε ότι η πληρωμή είναι νόμιμη.

Εάν στείλετε πριν πληρώσουν, δεν θα έχετε κανένα τρόπο να πάρετε πίσω το προϊόν σας!

Αθέμιτες αγορές μέσω ιστοσελίδων αγγελιών (πώληση)



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Μην εμπιστεύεστε τις επιβεβαιώσεις πληρωμής μέσω email - μπορεί να είναι ψεύτικες! Ελέγξτε απευθείας τον τραπεζικό σας λογαριασμό για να δείτε αν η πληρωμή έχει παραληφθεί.

Είναι καλύτερο να **συναλλάσσετε με τοπικούς αγοραστές** που μπορείτε να συναντήσετε προσωπικά και να δέχεστε μόνο μετρητά για να αποφύγετε πιθανές απάτες. **Μην πληρώνετε προφανή έξοδα αποστολής ή έξοδα μεταφοράς.** Συνιστάται ιδιαίτερη προσοχή όταν πουλάτε σε αγοραστές στο εξωτερικό.



Ignore

Αγνοήστε τυχόν αιτήματα παροχής περιττών πληροφοριών. Παρέχετε μόνο τις πληροφορίες που είναι απολύτως απαραίτητες για την ολοκλήρωση της συναλλαγής.

Εάν πουλάτε ένα αντικείμενο, **μην κάνετε κλικ σε κανένα σύνδεσμο που σας στέλνει ο αγοραστής και μην στέλνετε στον αγοραστή καμία πληροφορία που θα μπορούσε να του δώσει πρόσβαση σε οποιονδήποτε τραπεζικό σας λογαριασμό.**

Αναφορά! Οι περισσότερες πλατφόρμες διαθέτουν μηχανισμούς αναφοράς για την αντιμετώπιση τέτοιων ζητημάτων.

Χρησιμοποιήστε τη λειτουργία αναφοράς στην πλατφόρμα, η οποία συνήθως είναι προσβάσιμη μέσω του κουμπιού **«Αναφορά» στη διαφήμιση ή στο προφίλ χρήστη.**

Περιμένετε οδηγίες από την ομάδα υποστήριξης της πλατφόρμας και **σταματήστε όλες τις αλληλεπιδράσεις με το ύποπτο άτομο μετά την αναφορά.**

REPORT

Περισσότερες πληροφορίες



ΑΠΑΤΗ ΣΕ ΤΑΞΙΔΙΑ ΚΑΙ ΕΙΣΙΤΗΡΙΑ

- <https://www.comparitech.com/blog/information-security/avoid-common-ticket-and-travel-scams-online/> <https://www.aura.com/learn/airline-scams>
- <https://www.interpol.int/en/Crimes/Financial-crime/Airline-ticket-fraud>
- <https://www.nyccriminallawyer.com/ticket-scams/>
- <https://www.chargebackgurus.com/blog/travel-agency-chargebacks>
- <https://chargebacks911.com/otas-lose-billions-every-year-to-travel-fraud/>
- <https://www.traveldailynews.com/post/how-fraudsters-exploit-travel-agencies>
- <https://www.consumerreports.org/travel/avoiding-travel-scams/>
- <https://www.bbb.org/all/travel-scams>
- <https://www.consumer.ftc.gov/articles/travel-scams>



ΑΠΑΤΗ ΤΩΝ ΣΥΝΔΡΟΜΩΝ

- <https://balkaninsight.com/2023/08/22/subscription-scams-the-mobile-users-paying-for-unwanted-services/>
- https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/consumer-frequent-traps-and-scams_en
- <https://www.evz.de/en/shopping-internet/internet-fraud/subscription-traps.html>
- <https://www.europe-consommateurs.eu/en/shopping-internet/internet-fraud-and-scams/subscription-traps.html>
- <https://www.flagright.com/post/understanding-subscription-fraud>
- <https://www.which.co.uk/news/article/5-subscription-scams-and-traps-to-watch-out-for-aYwJA0u8EFZ9>

Περισσότερες πληροφορίες



ΑΠΑΤΗ ΜΕ ΤΗ ΔΗΜΙΟΥΡΓΙΑ ΨΕΥΤΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΚΑΤΑΣΤΗΜΑΤΩΝ

- <https://www.statista.com/statistics/1182221/online-shopping-fraud-incidents-uk/>
- <https://www.northyorkshire.police.uk/news/north-yorkshire/news/news/2024/04-april/online-shopping-fraud/>
- <https://us.norton.com/blog/online-scams/fake-e-shops>
- <https://www.youtube.com/watch?v=ItI7DXrNQCA>
- https://www.youtube.com/watch?v=CQYmfcLW_oc



ΔΟΛΙΕΣ ΑΓΟΡΕΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΑΚΩΝ ΔΙΑΦΗΜΙΣΕΩΝ (ΑΓΟΡΑ)

- <https://www.rd.com/list/fake-ads-on-social-media/>
- <https://www.seniorlifestyle.com/resources/blog/protect-your-parents-from-common-digital-traps/>
- <https://www.takefive-stopfraud.org.uk/advice/general-advice/purchase-fraud/> primeri <https://bolster.ai/glossary/fake-ads>
- <https://www.investigatetv.com/2023/11/14/how-determine-if-social-media-ads-are-real-or-fake/>
- https://thegratifiedblog.com/social-media-marketing/how-to-spot-fake-ads-on-facebook/#What_Are_Fake_Ads
- <https://trafficwatchdog.pl/en/articles/85/ad-frauds-in-social-media>
- https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_fraudulentadvertising_online_execsummary_july2020_final.pdf
- https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

Περισσότερες πληροφορίες



ΔΟΛΙΕΣ ΑΓΟΡΕΣ ΜΕΣΩ ΙΣΤΟΣΕΛΙΔΩΝ ΑΓΓΕΛΙΩΝ (ΠΩΛΗΣΕΙΣ)

- <https://www.westpac.com.au/security/types-of-scams/online-shopping-scams/>
- <https://www.ccpc.ie/consumers/money/scams/social-media-scams/>
- <https://www.desjardins.com/qc/en/tips/spot-avoid-scams-online-classifieds.html> <https://www.obvy-app.com/en/magazine/individuals/avoid-scams/scam-sites-small-ads/2341>
- <https://www.interbank.com/fraud-protection/beware-of-online-scams-how-to-spot-fake-listings-on-social-media-sale-groups/>
- <https://www.dropzone.com/help/classifieds/classifieds-buyer-scams-r23/>
- <https://www.nab.com.au/about-us/security/online-safety-tips/buying-selling-scams>
- <https://fastercapital.com/content/Classified-ads-site--Safety-Measures-When-Using-Classified-Ad-Websites.html>
- <https://consumer.ftc.gov/consumer-alerts/2022/07/selling-stuff-online-heres-how-avoid-scam>

ΚΕΦΑΛΑΙΟ 5.

ΧΕΙΡΑΓΩΓΗΣΗ ΤΗΣ ΤΑΥΤΟΤΗΤΑΣ ΚΑΙ ΕΚΜΕΤΑΛΛΕΥΣΗ ΤΗΣ ΕΜΠΙΣΤΟΣΥΝΗΣ ΤΟΥ ΚΟΣΜΟΥ

Οι σύγχρονες απάτες βασίζονται όλο και περισσότερο στη χειραγώγηση της ταυτότητας και στην εκμετάλλευση της εμπιστοσύνης στους δημόσιους φορείς, γεγονός που φέρνει τους ηλικιωμένους σε ιδιαίτερα ευάλωτη θέση. Οι εγκληματίες όχι μόνο υποδύονται αξιόπιστα ιδρύματα, αλλά χρησιμοποιούν και προηγμένες τεχνολογίες για να επιτύχουν τους στόχους τους. Σε αυτό το κεφάλαιο, θα συζητήσουμε τις πιο συνηθισμένες απάτες ταυτότητας και εμπιστοσύνης για να βοηθήσουμε τους ηλικιωμένους να αναγνωρίσουν και να αποφύγουν αυτές τις απειλές.

Οι σοβαρές απειλές για τους ηλικιωμένους περιλαμβάνουν ψευδείς κατηγορίες για κάποιο έγκλημα, όπου οι απατεώνες κατηγορούν ψευδώς τους ηλικιωμένους προκειμένου να εκβιάσουν χρήματα ή πληροφορίες. Η πλαστοπροσωπία της κυβέρνησης είναι μια άλλη επικίνδυνη μέθοδος, όπου οι εγκληματίες παριστάνουν την κυβέρνηση για να αποκτήσουν προσωπικές πληροφορίες ή χρήματα. Η τεχνολογία Deepfake επιτρέπει τη δημιουργία ψεύτικων αλλά πειστικών ηχογραφήσεων, οι οποίες μπορεί να οδηγήσουν σε σοβαρές συνέπειες. Οι απάτες υπηρεσιών που υποδύονται κυβερνητικούς φορείς συχνά περιλαμβάνουν ψεύτικες προσφορές που αποσκοπούν στην απόσπαση χρημάτων. Οι ψεύτικοι λογαριασμοί χρησιμοποιούνται για τον εκβιασμό ηλικιωμένων με την απειλή ότι θα αποκαλύψουν ψευδείς πληροφορίες.

Η κατανόηση αυτών των απειλών και των μηχανισμών τους είναι ζωτικής σημασίας για τους ηλικιωμένους ώστε να προστατεύσουν αποτελεσματικά την ταυτότητά τους, τα οικονομικά τους και την εμπιστοσύνη τους στους δημόσιους φορείς. Σε αυτό το κεφάλαιο, θα συζητήσουμε αυτά τα θέματα λεπτομερώς για να σας βοηθήσουμε να αναγνωρίσετε και να αποφύγετε τέτοιου είδους απάτες.

Ισχυρισμοί εμπλοκής σε εγκληματικές ενέργειες



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Εξαπάτηση χρημάτων από έναν χρήστη ισχυριζόμενος ότι είναι δικαστής, αστυνομικός ή εισαγγελέας και ότι το όνομά του συνδέεται με την τρομοκρατία. Οι «ισχυρισμοί για συμμετοχή σε εγκληματικές ενέργειες» αναφέρονται σε ισχυρισμούς ή κατηγορίες ότι ένα πρόσωπο, μια οργάνωση ή ακόμη και ηλικιωμένοι έχουν συμμετάσχει σε παράνομες δραστηριότητες. Οι ισχυρισμοί αυτοί δεν έχουν ακόμη αποδειχθεί και απαιτούν έρευνα για να διαπιστωθεί η εγκυρότητά τους. Η φύση του εγκλήματος μπορεί να ποικίλλει ευρέως, συμπεριλαμβανομένης της απάτης, της κλοπής ή άλλων παράνομων ενεργειών, και οι ισχυρισμοί αυτοί μπορεί να έχουν σοβαρές νομικές και κοινωνικές επιπτώσεις για τους κατηγορούμενους, συμπεριλαμβανομένων των ηλικιωμένων. Οι ηλικιωμένοι μπορεί να είναι ιδιαίτερα ευάλωτοι σε τέτοιους ισχυρισμούς λόγω της πιθανής έλλειψης εξοικείωσής τους με την ψηφιακή τεχνολογία και τις συνήθειες τακτικής απάτης.

Είδη ισχυρισμών για συμμετοχή σε εγκληματικές ενέργειες:

Ο ισχυρισμός ότι ο τραπεζικός λογαριασμός του θύματος έχει συνδεθεί με συναλλαγές που χρηματοδοτούν τρομοκρατικές δραστηριότητες είναι ένα είδος απάτης που αποσκοπεί στον εκφοβισμό του θύματος και στην πρόκληση πανικού. Σε αυτό το σενάριο, ο απατεώνας τονίζει τη σοβαρότητα του ισχυρισμού. Ο απατεώνας συνήθως απαιτεί άμεση δράση από το θύμα, η οποία μπορεί να είναι η καταβολή ενός «προστίμου» ή « αμοιβής». Καθ' όλη τη διάρκεια της αλληλεπίδρασης, ο απατεώνας χρησιμοποιεί τακτικές ψυχολογικής χειραγώγησης για να πανικοβάλει το θύμα και να το χειραγωγήσει ώστε να μοιραστεί τις προσωπικές του πληροφορίες ή/και τα χρήματά του. Μπορεί ακόμη και να προειδοποιήσουν το θύμα να μην επικοινωνήσει με κανέναν και να το κρατήσει μυστικό.

Σε αυτό το σενάριο, ο απατεώνας μπορεί να επικοινωνήσει με το θύμα και να παρουσιαστεί ως έγκυρο πρόσωπο, ισχυριζόμενος ότι ανήκει σε υπηρεσία επιβολής του νόμου ή σε δικαστικό σύστημα. Προειδοποιεί το θύμα ότι το όνομά του βρέθηκε σε κατάλογο ατόμων που συνδέονται με γνωστή τρομοκρατική οργάνωση. Ενδέχεται να δώσουν κατασκευασμένες λεπτομέρειες για να τρομάξουν και να πανικοβάλουν το θύμα. Απαιτώντας από το θύμα να λάβει άμεσα μέτρα, μπορεί να χρησιμοποιήσουν απειλές ή εκφοβιστικό λόγο για να διατηρήσουν τον έλεγχο.

Σε αυτό το σενάριο, ο απατεώνας επικοινωνεί με το θύμα παριστάνοντας τον αστυνομικό, τον δικαστή ή τον εισαγγελέα. Ενημερώνει το θύμα ότι το ταξιδιωτικό του ιστορικό ή ορισμένες δραστηριότητές του κίνησαν υποψίες. Ενδέχεται να αναφέρουν συγκεκριμένα μέρη που το θύμα επισκέφθηκε στην πραγματικότητα. Για να το κάνουν πιο πιστευτό, μπορεί να προσθέσουν λεπτομέρειες όπως ημερομηνίες ταξιδιού ή ονόματα ύποπτων τρομοκρατών με τους οποίους πιστεύουν ότι ήρθατε σε επαφή. Όπως και στα άλλα σενάρια, ο απατεώνας πιέζει το θύμα να λάβει γρήγορες αποφάσεις και χρησιμοποιεί τακτικές χειραγώγησης για να πείσει το θύμα να παράσχει προσωπικές πληροφορίες

Συμμετοχή σε
δίκτυο
χρηματοδότησης
της τρομοκρατίας

Σύνδεση με
γνωστές
τρομοκρατικές
οργανώσεις

Ύποπτο
ταξιδιωτικό
ιστορικό ή
δραστηριότητες

Ισχυρισμοί εμπλοκής σε εγκληματικές ενέργειες



ΣΥΝΕΠΕΙΕΣ:

Ο ισχυρισμός της εμπλοκής στο έγκλημα μπορεί να έχει σοβαρές αρνητικές επιπτώσεις, όπως:

01 Ζημία στη φήμη

Η σύνδεση με ένα έγκλημα, ακόμη και αν οι ισχυρισμοί δεν αποδειχθούν, μπορεί να έχει σοβαρές επιπτώσεις στη φήμη ενός ατόμου. Αυτό μπορεί να επηρεάσει τις προσωπικές σχέσεις, καθώς και τις επαγγελματικές ευκαιρίες.

02 Νομικές συνέπειες

Εάν οι ισχυρισμοί οδηγήσουν σε ποινική έρευνα και το άτομο κριθεί ένοχο, μπορεί να αντιμετωπίσει νομικές συνέπειες. Αυτές μπορεί να περιλαμβάνουν πρόστιμα, αναστολή ή ακόμη και φυλάκιση.

03 Συναισθηματική δυσφορία

Η κατηγορία για έγκλημα μπορεί να προκαλέσει σημαντική συναισθηματική οδύνη. Το άτομο μπορεί να βιώνει συναισθήματα φόβου, ντροπής ή αμηχανίας και αυτά τα συναισθήματα μπορεί να έχουν μακροπρόθεσμες επιπτώσεις στην ψυχολογική του ευημερία.

Ισχυρισμοί για συμμετοχή σε εγκληματικές ενέργειες



ΣΥΝΕΠΕΙΕΣ::

04

Κλοπή ταυτότητας και χρήση της για τη διάπραξη άλλων εγκλημάτων

Ισχυρισμοί που αφορούν κλοπή ταυτότητας μπορεί να οδηγήσουν σε περαιτέρω εγκληματικές δραστηριότητες στο όνομα του θύματος, επιδεινώνοντας τις νομικές και προσωπικές επιπτώσεις.

05

Απώλεια κεφαλαίων

Τα θύματα καταγγελιών για εγκλήματα, ιδίως εκείνων που αφορούν οικονομική απάτη, μπορεί να υποστούν σημαντικές οικονομικές απώλειες, είτε άμεσα λόγω κλοπής είτε έμμεσα λόγω νομικών εξόδων και άλλων δαπανών που σχετίζονται με την υπεράσπισή τους.

06

Μόλυνση συσκευών με ιούς

Σε υποθέσεις που αφορούν κατηγορίες για εγκλήματα στον κυβερνοχώρο, υπάρχει κίνδυνος οι συσκευές του κατηγορουμένου να αποτελέσουν στόχο και να μολυνθούν με ιούς ή κακόβουλο λογισμικό, οδηγώντας σε παραβιάσεις δεδομένων και περαιτέρω επιπλοκές.

Ισχυρισμοί για συμμετοχή σε εγκληματικές ενέργειες

— ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΦΟΝΤΟ ΤΗΝ ΙΣΤΟΡΙΑ



Μια μέρα, η Ρίτα έλαβε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο την ενημέρωνε ότι το όνομά της εμπλέκεται σε μια έρευνα εγκλήματος υψηλού προφίλ που σχετίζεται με μια απατηλή ηλεκτρονική συναλλαγή. Το email φαινόταν να προέρχεται από το τοπικό αστυνομικό τμήμα και ήταν αρκετά λεπτομερές, δημιουργώντας μια αίσθηση επείγοντος και φόβου.

Το email έδινε εντολή στη Ρίτα να κάνει κλικ σε έναν σύνδεσμο και να εισάγει τα προσωπικά της στοιχεία, συμπεριλαμβανομένου του αριθμού κοινωνικής ασφάλισης και των στοιχείων του τραπεζικού της λογαριασμού, υποτίθεται για να επαληθεύσει την ταυτότητά της και να απαλλάξει το όνομά της από την έρευνα. Τρομοκρατημένη από τους ισχυρισμούς και απελπισμένη να επιλύσει το ζήτημα άμεσα, η Ρίτα ακολούθησε τις οδηγίες.

Λίγες ημέρες αργότερα, έλαβε ένα τηλεφώνημα από την τράπεζά της, το οποίο την ενημέρωνε για ύποπτες δραστηριότητες στο λογαριασμό της. Σε αυτό το σημείο η Ρίτα συνειδητοποίησε ότι είχε εξαπατηθεί από έναν απατεώνα, ο οποίος χρησιμοποιούσε ως τέχνασμα τους ισχυρισμούς περί εμπλοκής της σε εγκληματική δραστηριότητα.

Αυτή η ιστορία υπογραμμίζει τη σημασία της εκπαίδευσης των ηλικιωμένων σχετικά με τους κινδύνους και τις τακτικές των διαδικτυακών απάτης. Όπως αποδείχθηκε στην περίπτωση της Ρίτα, οι απατεώνες μπορούν να εκμεταλλευτούν την έλλειψη εξοικείωσής τους με τον ψηφιακό κόσμο και να χρησιμοποιήσουν τακτικές εκφοβισμού για να τους εξαπατήσουν ώστε να αποκαλύψουν ευαίσθητες προσωπικές πληροφορίες. Ενημερώνοντας τους ηλικιωμένους για αυτές τις απειλές και διδάσκοντάς τους πώς να επαληθεύουν τη νομιμότητα τέτοιων αιτημάτων, μπορούμε να τους προστατεύσουμε από το να πέσουν θύματα τέτοιων απάτων.



ΒΗΜΑ 1: Επαλήθευση

Εάν η Ρίτα λάβει ένα απροσδόκητο μήνυμα ηλεκτρονικού ταχυδρομείου, ιδίως από υποτιθέμενο κυβερνητικό φορέα ή από τις αρχές επιβολής του νόμου, δεν θα πρέπει να απαντήσει άμεσα. Θα πρέπει να βρει ανεξάρτητα τα επίσημα στοιχεία επικοινωνίας και να τα επαληθεύσει.

ΒΗΜΑ 2: Προστασία προσωπικών πληροφοριών

Η Ρίτα δεν θα πρέπει να μοιράζεται ευαίσθητες πληροφορίες όπως τον αριθμό κοινωνικής ασφάλισης ή τα τραπεζικά της στοιχεία μέσω ηλεκτρονικού ταχυδρομείου. Οι νόμιμοι οργανισμοί δεν ζητούν κάτι τέτοιο μέσω ηλεκτρονικού ταχυδρομείου.

ΒΗΜΑ 3: Παρακολούθηση λογαριασμών

Η Ρίτα θα πρέπει να ελέγχει τακτικά τους οικονομικούς και διαδικτυακούς λογαριασμούς της για ύποπτη δραστηριότητα, ώστε να εντοπίζει έγκαιρα την απάτη και να διασφαλίζει τους λογαριασμούς της.

ΒΗΜΑ 4: Χρήση λογισμικού ασφαλείας

Η εγκατάσταση και η ενημέρωση του λογισμικού ασφαλείας μπορεί να προστατεύσει την Ρίτα από διαδικτυακές απειλές όπως ιούς, κακόβουλο λογισμικό και ηλεκτρονικό ψάρεμα. Το λογισμικό μπορεί να σαρώνει για απειλές και να μπλοκάρει ύποπτους ιστότοπους.

Ισχυρισμοί για συμμετοχή σε εγκληματικές ενέργειες



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Οι ηλικιωμένοι πρέπει να προστατεύονται από κατηγορίες για εγκλήματα, οι οποίες μπορεί να βλάψουν τη φήμη τους, να οδηγήσουν σε νομικά προβλήματα και να προκαλέσουν συναισθηματική οδύνη. Συχνά στοχοποιούνται λόγω της μη εξοικείωσής τους με την ψηφιακή τεχνολογία, γεγονός που τους καθιστά ευάλωτους σε απάτες. Τα προληπτικά μέτρα μπορούν να διασφαλίσουν τα οικονομικά τους, τις προσωπικές τους πληροφορίες και την ευημερία τους.

Επαλήθευση απροσδόκητων αιτημάτων:

Να είστε πάντα σε εγρήγορση όταν λαμβάνετε απροσδόκητα μηνύματα ηλεκτρονικού ταχυδρομείου ή επικοινωνία, ειδικά από πηγή που ισχυρίζεται ότι είναι κυβερνητικός φορέας, υπηρεσία επιβολής του νόμου ή υπηρεσία που χρησιμοποιείτε. Αντί να απαντάτε απευθείας στο μήνυμα ηλεκτρονικού ταχυδρομείου ή να κάνετε κλικ σε τυχόν συνδέσμους, βρείτε ανεξάρτητα τα επίσημα στοιχεία επικοινωνίας του οργανισμού και επικοινωνήστε μαζί τους για επαλήθευση. Με αυτόν τον τρόπο, μπορείτε να επιβεβαιώσετε αν το αίτημα είναι νόμιμο ή μια πιθανή απάτη.



Να είστε προσεκτικοί σχετικά με την κοινοποίηση προσωπικών πληροφοριών:

Οι προσωπικές σας πληροφορίες είναι πολύτιμες και πρέπει να προστατεύονται με κάθε κόστος. Ποτέ μην παρέχετε ευαίσθητες προσωπικές πληροφορίες, όπως τον αριθμό κοινωνικής ασφάλισης, τα στοιχεία του τραπεζικού σας λογαριασμού ή άλλες προσωπικές πληροφορίες, ανταποκρινόμενοι σε αίτημα ηλεκτρονικού ταχυδρομείου ή σε μη επαληθευμένη πηγή. Οι νόμιμοι οργανισμοί συνήθως δεν ζητούν αυτού του είδους τις πληροφορίες μέσω ηλεκτρονικού ταχυδρομείου ή μη ζητηθείσας επικοινωνίας.



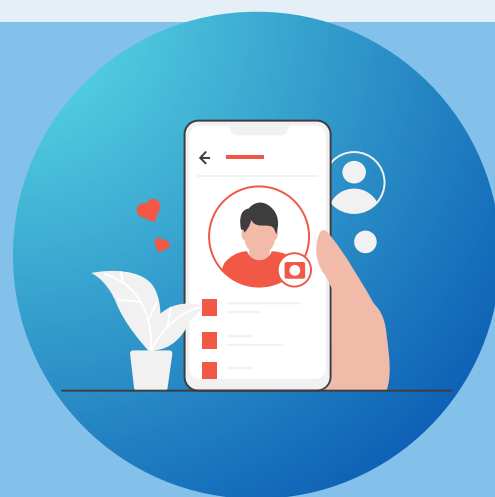
Ισχυρισμοί για συμμετοχή σε εγκληματικές ενέργειες



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

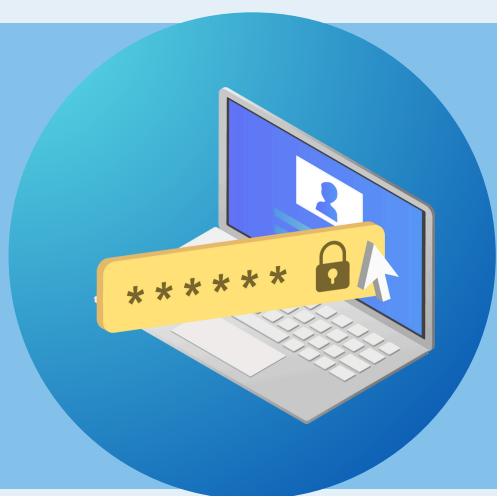
Τακτική παρακολούθηση των λογαριασμών:

Η τακτική παρακολούθηση των οικονομικών και ηλεκτρονικών λογαριασμών σας μπορεί να σας βοηθήσει να εντοπίσετε έγκαιρα τυχόν ύποπτη δραστηριότητα. Αυτό είναι ζωτικής σημασίας για την πρόληψη περαιτέρω ζημιών, καθώς μπορείτε να αναφέρετε αμέσως τη δραστηριότητα στις αρμόδιες αρχές ή στον πάροχο υπηρεσιών και να λάβετε μέτρα για την ασφάλεια του λογαριασμού σας.



Χρήση ασφαλών και μοναδικών κωδικών πρόσβασης:

Η χρήση ισχυρών και μοναδικών κωδικών πρόσβασης για όλους τους διαδικτυακούς σας λογαριασμούς αποτελεί θεμελιώδες μέτρο ασφαλείας. Ένας ισχυρός κωδικός πρόσβασης περιλαμβάνει έναν συνδυασμό γραμμάτων, αριθμών και συμβόλων και δεν είναι εύκολα μαντεύσιμος. Μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης σε πολλούς λογαριασμούς. Εάν ένας λογαριασμός παραβιαστεί, οι υπόλοιποι παραμένουν ασφαλείς.



Εγκατάσταση λογισμικού ασφαλείας:

Η εγκατάσταση και η τακτική ενημέρωση του λογισμικού ασφαλείας στον υπολογιστή σας παρέχει μια πρώτη γραμμή άμυνας ενάντια σε πολλές διαδικτυακές απειλές. Αυτό περιλαμβάνει ιούς, κακόβουλο λογισμικό, ransomware και απόπειρες phishing. Μπορεί να σαρώνει το σύστημά σας για απειλές, να αποκλείει ύποπτους ιστότοπους και να παρέχει προστασία σε πραγματικό χρόνο από επιθέσεις κακόβουλου λογισμικού.



Χειραγωγήσεις που υποδύονται κρατικούς θεσμούς



ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Η μίμηση κυβερνητικών υπαλλήλων είναι ένα είδος απάτης όπου οι απατεώνες προσποιούνται ότι προέρχονται από διάφορες κυβερνητικές υπηρεσίες, όπως οι φορολογικές αρχές, η αστυνομία ή τα συνταξιοδοτικά ταμεία. Αυτές οι απάτες αποτελούν σημαντική απειλή για τις προσωπικές πληροφορίες και την οικονομική ασφάλεια των ατόμων. Οι απατεώνες χρησιμοποιούν διαφορετικές τακτικές για να εξαπατήσουν τα θύματά τους, αλλά υπάρχουν ορισμένα κοινά σημάδια που πρέπει να προσέξετε.

Είδη χειραγωγησης στην πλαστοπροσωπία κρατικών θεσμών:

Οι απατεώνες επικοινωνούν συνήθως απροσδόκητα με τα θύματα μέσω τηλεφώνου, ηλεκτρονικού ταχυδρομείου, μηνυμάτων ή ακόμη και μέσω διαδικτυακής διαφήμισης. Ο αρχικός στόχος είναι να εξαπατήσουν τα θύματα ώστε να ξεκινήσουν επικοινωνία με τους απατεώνες. Συνήθως έχουν τα βασικά προσωπικά στοιχεία του υποψήφιου θύματος για να τους κάνουν να φαίνονται νόμιμοι. Μόλις επιτευχθεί η επαφή, οι απατεώνες απαιτούν από το θύμα να παράσχει ευαίσθητες πληροφορίες, να πληρώσει «πρόστιμα» (μέσω ασυνήθιστων μεθόδων πληρωμής) ή να προβεί σε άλλες ενέργειες.

Στις συνομιλίες με τα θύματα, παρέχουν πολλές ψευδείς πληροφορίες για τους εαυτούς τους και τα καθήκοντά τους και χρησιμοποιούν όρους που ακούγονται επίσημα, υπονοώντας ψευδώς κυβερνητική ένταξη. Στην επικοινωνία μέσω ταχυδρομείου ή στο διαδίκτυο χρησιμοποιούν επίσημης εμφάνισης κυβερνητικές σφραγίδες, λογότυπα, ονόματα πραγματικών αξιωματούχων στις θέσεις, ψεύτικους ιστότοπους και τομείς ηλεκτρονικού ταχυδρομείου για να ξεγελάσουν τα θύματα και να τους εμπιστευτούν. Τα μηνύματα ηλεκτρονικού ταχυδρομείου συχνά περιέχουν επίσης ένα συνημμένο συνήθως αρχείο PDF) και μια προειδοποίηση να διαβάσετε τα συνημμένα έγγραφα.

Οι απατεώνες χρησιμοποιούν τον εκφοβισμό και τις προθεσμίες και απειλούν με νομικές ενέργειες ή πρόστιμα για να εξαναγκάσουν σε άμεσες απαντήσεις. Για παράδειγμα, ένα μήνυμα ηλεκτρονικού ταχυδρομείου που υποτίθεται ότι προέρχεται από την αστυνομία μπορεί να απειλήσει ότι θα κινήσει ποινικές διαδικασίες εάν το θύμα δεν απαντήσει εντός συγκεκριμένου χρονικού πλαισίου. Αυτές οι τακτικές μπορούν να προκαλέσουν πανικό και να επηρεάσουν την κρίση, κάνοντας ακόμη και τα συνήθως λογικά άτομα να αντιδράσουν από φόβο.

**Ανεπιθύμητη
επικοινωνία**

**Προσποιείται ότι
να είναι
αξιόπιστος**

**Απειλές και
επείγουσα
ανάγκη**

Χειραγωγήσεις που υποδύονται κρατικούς θεσμούς



ΣΥΝΕΠΕΙΕΣ:

Οι κυβερνητικές απάτες εξαπάτησης βασίζονται κυριολεκτικά στο γεγονός ότι οι ηλικιωμένοι αποτελούν μεγάλα πιθανά θύματα, καθώς οι μεγαλύτερες γενιές συχνά εμπιστεύονται περισσότερο τα κυβερνητικά ιδρύματα και έχουν συνηθίσει να σέβονται περισσότερο την εξουσία και τους θεσμούς. Επιπλέον, έχουν αποταμιεύσεις και πιθανότατα λαμβάνουν κάποιας μορφής κρατικές παροχές.

01 Οικονομικές συνέπειες

Τα θύματα χάνουν χρήματα που μεταφέρουν στους απατεώνες ως πληρωμή για την επίλυση πλασματικών φορολογικών, νομικών ή άλλων υποχρεώσεων. Εκτός από τα χαμένα χρήματα, τα θύματα ενδέχεται να επιβαρυνθούν με πρόσθετα έξοδα για την επίλυση της κατάστασης. Εάν οι απατεώνες αποκτήσουν πρόσβαση στον τραπεζικό τους λογαριασμό, αυτό μπορεί να οδηγήσει σε περαιτέρω οικονομικές απώλειες λόγω μη εξουσιοδοτημένων αγορών. Στη χειρότερη περίπτωση, ο λογαριασμός μπορεί να αδειάσει, προκαλώντας ανεπανόρθωτη ζημιά, ιδίως στους ηλικιωμένους που μπορεί να έχουν χάσει τις αποταμιεύσεις τους που έχουν κερδίσει με κόπο.

Χειραγωγήσεις που υποδύονται κρατικούς θεσμούς

02 Κλοπή ταυτότητας

Εάν ένα θύμα υποστεί απώλεια ευαίσθητων προσωπικών δεδομένων, αυτό μπορεί να οδηγήσει σε περαιτέρω οικονομικές απώλειες, καθώς οι απατεώνες μπορούν να χρησιμοποιήσουν πληροφορίες από ένα διαβατήριο ή μια ταυτότητα για να ανοίξουν νέους τραπεζικούς λογαριασμούς και να πάρουν δάνεια στο όνομα του θύματος εν αγνοία του. Στην περίπτωση κλοπής ταυτότητας υγειονομικής περίθαλψης, το θύμα μπορεί να χάσει τις παροχές υγειονομικής περίθαλψης, ενώ στην περίπτωση κλοπής ταυτότητας φορολογικού χαρακτήρα, μπορεί να μείνει χωρίς επιστροφή φόρου. Η κλοπή ταυτότητας είναι μια τραυματική εμπειρία και έχει πολλές άλλες συνέπειες, όπως το ότι οι εγκληματίες χρησιμοποιούν την ταυτότητα του θύματος για να διαπράξουν εγκλήματα (συμπεριλαμβανομένων των εγκλημάτων στον κυβερνοχώρο), οδηγώντας ενδεχομένως το θύμα να αντιμετωπίσει νομικές συνέπειες για πράξεις που δεν διέπραξε.

03 Απώλεια εμπιστοσύνης στους δημόσιους θεσμούς

Αυτού του είδους οι απάτες μπορεί να έχουν σημαντικό αντίκτυπο στην εμπιστοσύνη των ατόμων στους δημόσιους θεσμούς, καθώς τα θύματα μπορεί να αισθάνονται βαθιά προδοσία και απώλεια εμπιστοσύνης προς αυτούς τους θεσμούς. Αυτό μπορεί να τους κάνει να γίνουν επιφυλακτικοί απέναντι στις γνήσιες επικοινωνίες και λιγότερο πρόθυμοι να συνεργαστούν, καθώς μπορεί να αρχίσουν να αμφισβητούν τα νόμιμα αιτήματα και τις πληροφορίες, γεγονός που οδηγεί σε έλλειψη προθυμίας να συνεργαστούν με τα κυβερνητικά θεσμικά όργανα. Η αυξημένη ανησυχία για το ενδεχόμενο απάτης μπορεί επίσης να επηρεάσει την κοινή γνώμη και να μειώσει την εμπιστοσύνη στην ικανότητα των κυβερνητικών φορέων να προστατεύουν και να εξυπηρετούν αποτελεσματικά τους πολίτες.

Χειραγωγήσεις που υποδύονται κρατικούς θεσμούς



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΦΟΝΤΟ ΤΗΝ ΙΣΤΟΡΙΑ



Ο Simon δέχτηκε μια κλήση από ένα άτομο που, σε επίσημο τόνο, αυτοπροσδιορίστηκε ως υπάλληλος της φορολογικής αρχής. Του είπε ότι χρωστούσε καθυστερούμενους φόρους και ότι θα συλληφθεί και θα οδηγηθεί στη φυλακή, αν δεν διευθετούσε αμέσως το χρέος του πληρώνοντας σε ένα από τα κρυπτονομίσματα. Παρά το γεγονός ότι η καλούσα ήταν επίμονη και εκφοβιστική, ο Simon έκλεισε το τηλέφωνο.

Λίγο μετά τον τερματισμό της κλήσης, έλαβε ένα μήνυμα με το ίδιο περιεχόμενο με τη συνομιλία, το οποίο περιείχε επίσης έναν ύποπτο σύνδεσμο προς τον ιστότοπο της φορολογικής αρχής.

Δυστυχώς για τον απατεώνα ...

Ο Simon παρακολούθησε μια εκπαιδευτική διάλεξη σχετικά με τις απάτες με πλαστοπροσωπία της κυβέρνησης που διοργάνωσε η Φορολογική Διοίκηση.



ΒΗΜΑ 1: Αναγνωρίζοντας τα προειδοποιητικά σημάδια

Ο Simon αρχικά φοβήθηκε, αλλά αναγνώρισε σημάδια απάτης όταν ο τηλεφωνητής ανέφερε την πληρωμή εκκρεμών φορολογικών υποχρεώσεων με κρυπτονόμισμα, το οποίο δεν αποτελεί συνήθη μέθοδο πληρωμής φόρων.

ΒΗΜΑ 2: Εντοπισμός μιας ασυνήθιστης συμπεριφοράς

Επειδή ο τηλεφωνητής απείλησε με σύλληψη και φυλάκιση, ο Simon αμφέβαλε για τη νομιμότητα τέτοιων απειλών και τερμάτισε αμέσως την κλήση.

ΒΗΜΑ 3: Επαλήθευση

Ο Simon έλεγξε αμέσως αν ο αριθμός τηλεφώνου συνδέεται με την αρμόδια φορολογική αρχή και διαπίστωσε ότι δεν ήταν. Ο ύποπτος τομέας που περιείχε το γραπτό μήνυμα απλώς επιβεβαίωσε τις υποψίες του, οπότε μπλόκαρε τον αριθμό.

ΒΗΜΑ 4: Αναφορά

Ο Simon επικοινωνήσε με την επίσημη φορολογική αρχή χρησιμοποιώντας τον επίσημο αριθμό τηλεφώνου της και την ενημέρωσε για την απόπειρα απάτης.

Χειραγωγήσεις που υποδύονται κρατικούς θεσμούς



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Ακολουθούν ορισμένες πρόσθετες συμβουλές σε περίπτωση που βρεθείτε σε μια τέτοια κατάσταση.

Κλείστε το τηλέφωνο, Διαγράψτε, Μην απαντήσετε:

Αγνοήστε κλήσεις, μηνύματα ηλεκτρονικού ταχυδρομείου, γραπτά μηνύματα και μηνύματα στα μέσα κοινωνικής δικτύωσης που ισχυρίζονται ότι προέρχονται από κυβερνητικά ιδρύματα και σας ζητούν να πληρώσετε, να επιβεβαιώσετε ευαίσθητες πληροφορίες ή να δώσετε άλλες πληροφορίες.

Το πραγματικό κυβερνητικό ίδρυμα δεν θα σας καλέσει ποτέ, δεν θα σας στείλει email, δεν θα σας στείλει μήνυμα ή δεν θα σας στείλει μήνυμα στα μέσα κοινωνικής δικτύωσης για να σας ζητήσει χρήματα ή πληροφορίες.



Μην διατηρείτε επαφή με τους απατεώνες και μην παρέχετε τα προσωπικά σας στοιχεία και μην πραγματοποιείτε πληρωμές!

Τα νόμιμα ιδρύματα τηρούν συγκεκριμένες διαδικασίες και κανόνες σχετικά με τις πληρωμές, τις οικονομικές υποχρεώσεις και άλλα διοικητικά θέματα και δεν θα σας ζητήσουν ποτέ να πληρώσετε χρησιμοποιώντας μεθόδους πληρωμής όπως κρυπτονομίσματα, υπηρεσίες μεταφοράς χρημάτων, πλατφόρμες πληρωμών κ.λπ.

Χειραγωγήσεις που υποδύονται κρατικούς θεσμούς



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Μην βασίζεστε στα στοιχεία επικοινωνίας που παρέχονται σε μηνύματα ηλεκτρονικού ταχυδρομείου και SMS!

Βεβαιωθείτε ότι επιβεβαιώνετε ανεξάρτητα την ταυτότητα του αποστολέα προτού απαντήσετε σε αλληλογραφία που υποτίθεται ότι προέρχεται από κυβερνητικό φορέα.

Για να διασφαλίσετε τη νομιμότητα της επικοινωνίας, αναζητήστε τα επίσημα στοιχεία επικοινωνίας της αρμόδιας υπηρεσίας και επικοινωνήστε απευθείας μαζί της!



Διακόψτε αμέσως την επαφή με οποιονδήποτε προσπαθεί να σας απειλήσει ή να σας εκφοβίσει!

Οι απειλές και ο εκφοβισμός μπορεί να οδηγήσουν σε συναισθηματική δυσφορία και ψυχολογική βλάβη.

Θυμηθείτε!

Τα νόμιμα κυβερνητικά όργανα δεν χρησιμοποιούν απειλές σύλληψης ή φυλάκισης για να επιτύχουν την πληρωμή φορολογικών υποχρεώσεων ή άλλων χρεών.

Εάν έχετε πέσει θύμα απάτης και έχετε μεταφέρει χρήματα μόνο και μόνο για να συνειδητοποιήσετε αργότερα ότι επρόκειτο για απάτη, επικοινωνήστε αμέσως με την τράπεζά σας και υποβάλλετε καταγγελία. Αναφέρετε τη ζημία στην αστυνομία.

Εάν έχουν αποκαλυφθεί άλλες προσωπικές πληροφορίες κατά τη διάρκεια της απάτης, ενημερώστε αμέσως το σχετικό ίδρυμα που χρησιμοποίησαν οι απατεώνες για τους σκοπούς της απάτης τους.

REPORT

Χειραγώγηση με χρήση τεχνολογίας deepfake

— ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Η απάτη Deepfake αναφέρεται σε έναν τύπο απάτης όπου η τεχνητή νοημοσύνη χρησιμοποιείται για τη δημιουργία ή την αλλοίωση βίντεο, ήχου ή εικόνων με σκοπό την εξαπάτηση. Αυτό συχνά περιλαμβάνει τη δημιουργία συνθετικού περιεχομένου ενός ατόμου, μιμούμενο τη φωνή, τις εκφράσεις του προσώπου και τους τρόπους συμπεριφοράς του, ώστε να φαίνεται ότι κάνει ή λέει κάτι που δεν έκανε. Αυτά τα απατηλά βίντεο, ηχητικά αποσπάσματα ή εικόνες χρησιμοποιούνται συχνά για να εξαπατήσουν τα θύματα ώστε να αποχωριστούν χρήματα, να αποκαλύψουν ευαίσθητες πληροφορίες ή να βλάψουν τη φήμη τους. Οι ηλικιωμένοι, ιδίως, γίνονται συχνά στόχος λόγω της αντιληπτής ευπάθειάς τους και της έλλειψης εξοικείωσης με τέτοιες εξελιγμένες τεχνολογικές απειλές. Η απάτη Deepfake μπορεί επίσης να χρησιμοποιηθεί για εκβιασμό, εκβιασμό, διάδοση ψευδών πληροφοριών ή παραβίαση συστημάτων ασφαλείας. Δεδομένου του σημαντικού συναισθηματικού και οικονομικού αντίκτυπου στους ηλικιωμένους, είναι ζωτικής σημασίας η ευαισθητοποίηση και η εκπαίδευσή τους σχετικά με το πώς να αναγνωρίζουν και να προστατεύονται από αυτές τις παραπλανητικές απάτες.

Τύποι απάτης deepfake

Αυτός ο τύπος απάτης deepfake περιλαμβάνει τη δημιουργία ενός συνθετικού βίντεο ενός ατόμου για να το υποδυθεί. Ο απατεώνας μπορεί να χρησιμοποιήσει αυτό το βίντεο για να ξεγελάσει τα θύματα και να τα κάνει να πιστέψουν ότι αλληλεπιδρούν με το πραγματικό πρόσωπο, οδηγώντας σε πιθανή οικονομική απώλεια ή κλοπή προσωπικών πληροφοριών.

Σε αυτόν τον τύπο απάτης, τα deepfakes χρησιμοποιούνται για τη διάδοση παραπληροφόρησης ή προπαγάνδας. Αυτό θα μπορούσε να περιλαμβάνει τη δημιουργία βίντεο με δημόσια πρόσωπα να λένε ή να κάνουν πράγματα που δεν έκαναν ποτέ, παραπλανώντας έτσι το κοινό και επηρεάζοντας γνώμες ή πράξεις.

Τα deepfakes μπορούν επίσης να χρησιμοποιηθούν για την παραβίαση συστημάτων ασφαλείας που βασίζονται στην τεχνολογία αναγνώρισης προσώπου. Δημιουργώντας ένα συνθετικό βίντεο ενός εξουσιοδοτημένου ατόμου, οι απατεώνες μπορούν να ξεγελάσουν αυτά τα συστήματα και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες περιοχές ή διαβαθμισμένες πληροφορίες.

**Κλοπή
ταυτότητας**

**Διάδοση
ψευδών
πληροφοριών**

**Παραβίαση
ασφάλειας**

Χειραγώγηση με χρήση τεχνολογίας deepfake



ΣΥΝΕΠΕΙΕΣ:

Η απάτη Deepfake μπορεί να έχει σοβαρές αρνητικές επιπτώσεις, όπως:

01 Οικονομικές απώλειες

Τα θύματα της απάτης deepfake μπορεί να υποστούν σημαντικές οικονομικές απώλειες. Αυτό μπορεί να συμβεί όταν εξαπατηθούν για να μεταφέρουν χρήματα ή να αποκαλύψουν οικονομικές πληροφορίες με βάση παραπλανητικό περιεχόμενο deepfake.

02 Συναισθηματική δυσφορία

Το να είσαι θύμα απάτης deepfake μπορεί να οδηγήσει σε σοβαρή συναισθηματική οδύνη. Η παραβίαση της προσωπικής ταυτότητας και η πιθανή έκθεση προσωπικών πληροφοριών μπορεί να αφήσει τα θύματα να αισθάνονται ευάλωτα και παραβιασμένα.

03 Ζημία στη φήμη

Η απάτη Deepfake μπορεί να προκαλέσει σοβαρή ζημία στη φήμη ατόμων και οργανισμών. Οι ψευδείς πληροφορίες που διαδίδονται μέσω των deepfakes μπορούν να υπονομεύσουν την εμπιστοσύνη του κοινού και να οδηγήσουν σε απώλεια επιχειρήσεων, νομικά ζητήματα και άλλες αρνητικές συνέπειες.

Χειραγώγηση με χρήση τεχνολογίας deepfake



ΣΥΝΕΠΕΙΕΣ:

04 Παραπληροφόρηση

Τα deepfakes μπορούν να χρησιμοποιηθούν για τη διάδοση ψευδών πληροφοριών ή προπαγάνδας, παραπλανώντας το κοινό και επηρεάζοντας γνώμες ή ενέργειες. Αυτό μπορεί να έχει σοβαρές κοινωνικές και πολιτικές προεκτάσεις, όπως η υπονόμηση της εμπιστοσύνης στους θεσμούς ή η χειραγώγηση των εκλογικών αποτελεσμάτων.

05 Κλοπή ταυτότητας

Η τεχνολογία Deepfake μπορεί να χρησιμοποιηθεί για τη δημιουργία συνθετικών βίντεο ή ηχητικών αποσπασμάτων ατόμων, οδηγώντας σε κλοπή ταυτότητας. Οι απατεώνες μπορούν να υποδυθούν κάποιον για να αποκτήσουν πρόσβαση σε προσωπικές πληροφορίες, οικονομικούς πόρους ή ασφαλή συστήματα.

06 Νομικές συνέπειες

Η χρήση της τεχνολογίας deepfake για τη διάπραξη απάτης ή τη διάδοση ψευδών πληροφοριών μπορεί να οδηγήσει σε νομικές συνέπειες τόσο για τους δράστες όσο και για τα θύματα. Τα θύματα μπορεί να αντιμετωπίσουν νομικές προκλήσεις για την απόδειξη της αθωότητάς τους ή την ανάκτηση της φήμης τους, ενώ οι δράστες μπορεί να βρεθούν αντιμέτωποι με ποινικές διώξεις.

07 Διάβρωση της κοινωνικής εμπιστοσύνης

Η επικράτηση των απομιμήσεων μπορεί να διαβρώσει την κοινωνική εμπιστοσύνη, κάνοντας τους ανθρώπους δύσπιστους ως προς τη γνησιότητα του ψηφιακού περιεχομένου. Αυτό μπορεί να οδηγήσει σε μια γενική δυσπιστία απέναντι στα μέσα ενημέρωσης και τις πληροφορίες που μοιράζονται στο διαδίκτυο, περιπλέκοντας την επικοινωνία και τη διάδοση των γνήσιων πληροφοριών.

Χειραγώγηση με χρήση τεχνολογίας deepfake



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΦΟΝΤΟ ΤΗΝ ΙΣΤΟΡΙΑ



Μια μέρα, ο Bill έλαβε ένα email από τον εγγονό του, τον Jack. Το email περιείχε ένα βίντεο όπου ο Jack φαινομενικά ζητούσε βοήθεια. Είπε ότι είχε χάσει το πορτοφόλι του ενώ ταξίδευε και χρειαζόταν κάποια χρήματα για να επιστρέψει στο σπίτι του. Το βίντεο φαινόταν απίστευτα γνήσιο, καθώς είχε τη φωνή και τους τρόπους του Jack μέχρι κεραίας.

Ο Bill, ανησυχώντας για τον εγγονό του, μετέφερε αμέσως τα χρήματα. Μόνο αργότερα, όταν μίλησε με την κόρη του, ανακάλυψε ότι ο Jack δεν είχε κάνει ποτέ το ταξίδι από την αρχή.

Μπερδεμένος και σοκαρισμένος, ο Bill συνειδητοποίησε ότι είχε πέσει θύμα μιας απάτης που είχε γίνει σε βάθος. Το βίντεο του Jack δεν ήταν αληθινό, αλλά ήταν ένα deepfake - ένα συνθετικό βίντεο που είχε παραχθεί με τη χρήση τεχνητής νοημοσύνης.

Αυτή η ιστορία υπογραμμίζει την ευπάθεια των ηλικιωμένων στην απάτη deepfake, τονίζοντας την ανάγκη ευαισθητοποίησης και εκπαίδευσης αυτής της δημογραφικής ομάδας. Οι ηλικιωμένοι, όπως ο Bill, μπορεί να μην γνωρίζουν τέτοιες εξελιγμένες απάτες, γεγονός που τους καθιστά εύκολους στόχους. Η αφήγηση υπογραμμίζει τη σημασία της ενημέρωσης των ηλικιωμένων σχετικά με την τεχνολογία deepfake, της διδασκαλίας τους σχετικά με τον τρόπο επαλήθευσης των αιτημάτων για οικονομική βοήθεια και της ενθάρρυνσης της ανοιχτής επικοινωνίας εντός των οικογενειών για την επιβεβαίωση της αυθεντικότητας τέτοιων αιτημάτων.



ΒΗΜΑ 1: Επαλήθευση

Να επαληθεύετε πάντα κάθε αίτημα για οικονομική βοήθεια ή ευαίσθητες πληροφορίες. Για τον Bill, αυτό σημαίνει ότι πρέπει να επικοινωνήσει απευθείας με τον εγγονό του μέσω μιας γνωστής και αξιόπιστης μεθόδου, όπως ένα τηλεφώνημα, για να επιβεβαιώσει τη γνησιότητα του αιτήματος πριν προβεί σε οποιαδήποτε ενέργεια.

ΒΗΜΑ 3: Προχωρημένα μέτρα ασφαλείας

Ο Bill θα πρέπει να χρησιμοποιεί προηγμένα μέτρα ασφαλείας, όπως ο έλεγχος ταυτότητας δύο παραγόντων για τους λογαριασμούς ηλεκτρονικού ταχυδρομείου και κοινωνικών μέσων. Αυτό προσθέτει ένα επιπλέον επίπεδο προστασίας από μη εξουσιοδοτημένη πρόσβαση και πιθανές απάτες.

ΒΗΜΑ 2: Εκπαίδευση και ευαισθητοποίηση

Ο Bill θα πρέπει να ενημερώνεται για τις τελευταίες τεχνολογικές απειλές, όπως τα deepfakes. Η κατανόηση του τρόπου λειτουργίας τους και του τρόπου με τον οποίο μπορούν να χρησιμοποιηθούν σε απάτες θα τον βοηθήσει να αναγνωρίσει πιθανές απόπειρες απάτης και να λάβει μέτρα προστασίας.

ΒΗΜΑ 4: Ανοιχτή επικοινωνία

Ο Bill θα πρέπει να διατηρεί ανοιχτή επικοινωνία με την οικογένειά του σχετικά με τυχόν ασυνήθιστα αιτήματα ή μηνύματα που λαμβάνει. Συζητώντας τα με έμπιστα μέλη της οικογένειας, μπορεί να εντοπίσει και να αποφύγει γρήγορα πιθανές απάτες.

Χειραγώγηση με χρήση τεχνολογίας deepfake



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Η απάτη Deepfake μπορεί να οδηγήσει σε σημαντικές οικονομικές απώλειες, συναισθηματική οδύνη και βλάβη της φήμης κάποιου. Επιπλέον, οι ηλικιωμένοι μπορεί να αντιμετωπίσουν προκλήσεις κατά την ανάκαμψη από τέτοιες απάτες, τόσο σε οικονομικό όσο και σε συναισθηματικό επίπεδο. Γνωρίζοντας αυτές τις απειλές και λαμβάνοντας μέτρα προστασίας, οι ηλικιωμένοι μπορούν να διαφυλάξουν τις προσωπικές τους πληροφορίες, να διατηρήσουν την οικονομική τους ασφάλεια και να διατηρήσουν την αξιοπρέπεια και την ψυχική τους ηρεμία.

Εκπαίδευση και ευαισθητοποίηση:

Μείνετε ενημερωμένοι σχετικά με τα deepfakes, τις πιθανές χρήσεις τους και τα τελευταία διαθέσιμα εργαλεία για τον εντοπισμό τους. Ενημερώστε τακτικά τις γνώσεις σας σχετικά με αυτές τις απειλές και τα μέτρα προστασίας από αυτές.



Επαλήθευση:

Πάντα να επαληθεύετε την πηγή των βίντεο, ιδίως εκείνων που σας ζητούν οικονομική βοήθεια ή ευαίσθητες πληροφορίες. Επικοινωνήστε με το πρόσωπο που εμφανίζεται στο βίντεο μέσω μιας αξιόπιστης μεθόδου για να επιβεβαιώσετε τη γνησιότητά του.



Χειραγώγηση με χρήση τεχνολογίας deepfake



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Χρήση προηγμένων μέτρων ασφαλείας:

Χρησιμοποιήστε προηγμένα μέτρα ασφαλείας, όπως ο έλεγχος ταυτότητας δύο παραγόντων και η βιομετρική επαλήθευση, για να διασφαλίσετε τις προσωπικές και οικονομικές σας πληροφορίες.



Βασιστείτε σε αξιόπιστες πηγές:

Μοιραστείτε ευαίσθητες πληροφορίες μόνο με αξιόπιστες πηγές και μέσω ασφαλών πλατφορμών. Να είστε επιφυλακτικοί σε μη ζητηθείσες επικοινωνίες που ζητούν προσωπικά στοιχεία ή οικονομικές πληροφορίες.

Αναφορά ύποπτης δραστηριότητας:

Αν συναντήσετε ένα πιθανό deepfake, αναφέρετε το στις αρμόδιες αρχές. Αυτό θα μπορούσε να βοηθήσει να αποτρέψετε άλλους από το να γίνουν θύματα και να βοηθήσετε στη σύλληψη των απατεώνων.



Απάτη υπηρεσιών που υποδύεται τα κρατικά όργανα

— ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Η απάτη υπηρεσιών που υποδύεται κρατικούς φορείς περιλαμβάνει απατεώνες που προσποιούνται ότι είναι επίσημοι κυβερνητικοί οργανισμοί ή υπηρεσίες. Αυτοί οι απατεώνες προσφέρουν βοήθεια για τη διεκπεραίωση επίσημων εγγράφων, όπως διαβατήρια, βίζες ή επιδόματα κοινωνικής ασφάλισης, αλλά ο πραγματικός τους στόχος είναι να κλέψουν τις προσωπικές σας πληροφορίες ή τα χρήματά σας.

Τύποι χειραγώγησης στην απάτη στον τομέα των υπηρεσιών:

Οι απατεώνες δημιουργούν ψεύτικους ιστότοπους ή στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου που μοιάζουν να προέρχονται από κυβερνητικές υπηρεσίες. Μπορεί να χρησιμοποιούν επίσημα λογότυπα και γλώσσα για να φαίνονται νόμιμοι.

Αυτές οι απάτες χρησιμοποιούν συχνά επείγουσα γλώσσα, προειδοποιώντας σας για τις συνέπειες εάν δεν ενεργήσετε γρήγορα. Αυτό μπορεί να περιλαμβάνει απειλές για πρόστιμα, νομικές ενέργειες ή χαμένες προθεσμίες.

Ζητούν ευαίσθητες πληροφορίες, όπως τον αριθμό κοινωνικής ασφάλισης, τα στοιχεία του τραπεζικού σας λογαριασμού ή τα στοιχεία του διαβατηρίου σας.

Οι απατεώνες ζητούν πληρωμή για τις «υπηρεσίες» τους εκ των προτέρων, συχνά μέσω μη ανιχνεύσιμων μεθόδων όπως εμβάσματα, προπληρωμένες κάρτες ή κρυπτονομίσματα.

Οι γνήσιοι κυβερνητικοί ιστότοποι παρέχουν σαφείς πληροφορίες επικοινωνίας και επιλογές εξυπηρέτησης πελατών. Οι ψεύτικοι ιστότοποι έχουν συχνά περιορισμένα ή ψεύτικα στοιχεία επικοινωνίας.

Πλαστοπροσωπία
επίσημων
υπηρεσιών

Επείγουσα
και έγκυρη
γλώσσα

Αιτήματα για
προσωπικές
πληροφορίες

Προκαταβολές

Έλλειψη
άμεσων
πληροφοριών
επικοινωνίας

Απάτη υπηρεσιών που υποδύεται τα κρατικά όργανα

— ΣΥΝΕΠΕΙΕΣ:

Η απάτη στις υπηρεσίες μπορεί να έχει σοβαρές αρνητικές επιπτώσεις, όπως:

01 Νομικά και διοικητικά προβλήματα

Η χρήση ψεύτικων υπηρεσιών μπορεί να οδηγήσει σε νομικά ζητήματα εάν το θύμα υποβάλει εν αγνοία του πλαστά έγγραφα ή δεν συμμορφώνεται με τις νομικές απαιτήσεις. Αυτό μπορεί να οδηγήσει σε πρόστιμα, ποινές ή πρόσθετα νομικά έξοδα.

02 Κλοπή ταυτότητας

Οι απατεώνες συχνά συλλέγουν προσωπικές πληροφορίες με το πρόσχημα ότι τις χρειάζονται για υπηρεσίες που σχετίζονται με το κράτος. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για την κλοπή της ταυτότητας του θύματος, οδηγώντας σε μη εξουσιοδοτημένες οικονομικές συναλλαγές, άνοιγμα νέων λογαριασμών στο όνομά του και άλλες δόλιες δραστηριότητες.

03 Απώλεια της εμπιστοσύνης στους νόμιμους θεσμούς

Αφού εξαπατηθούν από κάποιον που παριστάνει τον κρατικό φορέα, οι ηλικιωμένοι μπορεί να γίνουν δύσπιστοι απέναντι στις πραγματικές κυβερνητικές υπηρεσίες και υπαλλήλους. Αυτό μπορεί να εμποδίσει την προθυμία τους να αναζητήσουν βοήθεια ή υπηρεσίες που πραγματικά χρειάζονται.

04 Οικονομικές απώλειες

Οι ηλικιωμένοι μπορεί να πληρώνουν για ψεύτικες υπηρεσίες, όπως τέλη διεκπεραίωσης για ανύπαρκτες παροχές ή βοήθεια με επίσημα έγγραφα. Αυτό έχει ως αποτέλεσμα άμεση οικονομική απώλεια, η οποία μπορεί να είναι ιδιαίτερα επιζήμια για όσους έχουν σταθερό εισόδημα.

Απάτη υπηρεσιών που υποδύεται τα κρατικά όργανα

— ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΦΟΝΤΟ ΤΗΝ ΙΣΤΟΡΙΑ



Η Grace λαμβάνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που ισχυρίζεται ότι προέρχεται από την κυβέρνηση και αναφέρει ότι το διαβατήριό της πρέπει να ανανεωθεί επείγοντως για να αποφύγει κυρώσεις. Το μήνυμα ηλεκτρονικού ταχυδρομείου παρείχε έναν σύνδεσμο προς έναν ιστότοπο που φαινόταν επίσημος, με το λογότυπο του υπουργείου και επίσημη γλώσσα. Ο ιστότοπος ζητούσε προσωπικά στοιχεία και ένα τέλος 150 ευρώ για την επίσπευση της διαδικασίας ανανέωσης. Τι πρέπει να κάνει η Grace;

Η απάτη με υπηρεσίες που υποδύονται κρατικά ιδρύματα μπορεί να οδηγήσει σε σοβαρή οικονομική και συναισθηματική βλάβη, ιδίως για τους ηλικιωμένους. Επαληθεύοντας την πηγή των πληροφοριών, αντιμετωπίζοντας με σκεπτικισμό τα επείγοντα αιτήματα, προστατεύοντας τις προσωπικές πληροφορίες και χρησιμοποιώντας ασφαλείς μεθόδους πληρωμής, μπορείτε να προστατευτείτε από αυτές τις απάτες.

Βεβαιώνετε πάντα ότι αλληλεπιδράτε με γνήσιους κυβερνητικούς ιστότοπους και υπηρεσίες για να αποφύγετε να πέσετε θύμα δόλιων συστημάτων.



Βήμα 1. Επαληθεύστε την πηγή

Ελέγξτε απευθείας τον επίσημο ιστότοπο του Υπουργείου Εξωτερικών ή καλέστε την υπηρεσία εξυπηρέτησης πελατών για να επιβεβαιώσετε τη διαδικασία ανανέωσης.

Βήμα 2. Να είστε επιφυλακτικοί απέναντι στα επείγοντα αιτήματα

Αναγνωρίστε ότι οι γνήσιες κυβερνητικές υπηρεσίες δεν θα στείλουν επείγοντα αιτήματα ανανέωσης μέσω ηλεκτρονικού ταχυδρομείου.

Βήμα 3. Μην μοιράζετε προσωπικές πληροφορίες

Αποφύγετε την εισαγωγή των προσωπικών σας στοιχείων στον παρεχόμενο ιστότοπο μέχρι να επαληθεύσετε τη γνησιότητά του.

Βήμα 4. Χρησιμοποιήστε ασφαλείς μεθόδους πληρωμής

Να είστε προσεκτικοί σχετικά με τα αιτήματα πληρωμής και να επαληθεύετε αν η κυβέρνηση παρέχει τέτοιες αμοιβές και υπηρεσίες.

Απάτη υπηρεσιών που υποδύεται τα κρατικά όργανα



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Η προστασία σας από την απάτη υπηρεσιών που υποδύεται τον κρατικό φορέα είναι ζωτικής σημασίας για την προστασία των προσωπικών σας πληροφοριών, των χρημάτων σας και των συναισθημάτων σας. Ακολουθούν ορισμένα απλά βήματα που μπορείτε να ακολουθήσετε.

Μην μοιράζεστε προσωπικές πληροφορίες:

Αποφύγετε να παρέχετε ευαίσθητες πληροφορίες, όπως τον αριθμό κοινωνικής ασφάλισης, τα τραπεζικά σας στοιχεία ή τα στοιχεία διαβατηρίου σας στο διαδίκτυο, εκτός εάν είστε βέβαιοι ότι ο ιστότοπος είναι νόμιμος.



Επαληθεύστε την Πηγή:

Βεβαιωθείτε ότι βρίσκεστε σε επίσημο κυβερνητικό ιστότοπο. Αναζητήστε τη διεύθυνση «.gov» στην ιστοσελίδα, η οποία χρησιμοποιείται από κυβερνητικά ιδρύματα. Επικοινωνήστε απευθείας με την κυβερνητική υπηρεσία χρησιμοποιώντας πληροφορίες από επίσημη πηγή και όχι τα στοιχεία επικοινωνίας που παρέχονται στο ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου ή στον ιστότοπο.

Αντιμετωπίστε με σκεπτικισμό τα επείγοντα αιτήματα:

Να είστε προσεκτικοί εάν λαμβάνετε επείγοντα ή απειλητικά μηνύματα που απαιτούν άμεση δράση ή πληρωμή. Οι γνήσιες κυβερνητικές υπηρεσίες δεν λειτουργούν με αυτόν τον τρόπο.



Απάτη μέσω ψεύτικων λογαριασμών

— ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΙΝΔΥΝΟΥ:

Ο εκβιασμός με τη χρήση ψεύτικων λογαριασμών αναφέρεται σε μια παραπλανητική πρακτική κατά την οποία οι απατεώνες δημιουργούν πλαστά προφίλ στα μέσα κοινωνικής δικτύωσης, συχνά υποδυόμενοι κάποιον που το θύμα γνωρίζει ή εμπιστεύεται. Αυτή η απάτη στοχεύει ιδιαίτερα τους ηλικιωμένους, οι οποίοι μπορεί να είναι λιγότερο εξοικειωμένοι με τις ψηφιακές πλατφόρμες. Οι απατεώνες συνήθως ξεκινούν την επαφή στέλνοντας αιτήματα φιλίας και στη συνέχεια προχωρούν σε κοινοποίηση ρητού ή επιβλαβούς περιεχομένου. Στη συνέχεια, ο απατεώνας απαιτεί χρήματα ή άλλες μορφές πληρωμής, απειλώντας να βλάψει τη φήμη του ηλικιωμένου συνδέοντάς τον με το ακατάλληλο περιεχόμενο.

Είδη εκβιασμού με τη χρήση ψεύτικων λογαριασμών:

Ο απατεώνας δημιουργεί έναν ψεύτικο λογαριασμό προσποιούμενος ότι είναι κάποιος γνωστός του θύματος, κερδίζει την εμπιστοσύνη του και στη συνέχεια χρησιμοποιεί αυτή την εμπιστοσύνη για να ξεκινήσει τον εκβιασμό.

Προσωποποίηση
φίλου ή
γνωστού

Ο απατεώνας δημιουργεί μια ψεύτικη ταυτότητα, συχνά ένα άτομο που ενδιαφέρεται ερωτικά για το θύμα. Μόλις το θύμα επενδύσει συναισθηματικά, ο απατεώνας αρχίζει τον εκβιασμό.

Catfishing

Ο απατεώνας δημιουργεί έναν ψεύτικο λογαριασμό μιας διασημότητας ή ενός δημόσιου προσώπου. Στη συνέχεια έρχεται σε επαφή με τους θαυμαστές ή τους οπαδούς του, μοιράζεται ρητό περιεχόμενο και απαιτεί χρήματα με την απειλή ότι θα αμαυρώσει τη φήμη του θαυμαστή.

Μίμηση
διασημότητας
ή δημόσιου
προσώπου

Απάτη μέσω ψεύτικων λογαριασμών



ΣΥΝΕΠΕΙΕΣ:

Ο εκβιασμός με τη χρήση ψεύτικων λογαριασμών μπορεί να έχει σοβαρές αρνητικές συνέπειες, όπως:

01 Συναισθηματική και ψυχολογική δυσφορία

Μία από τις πρωταρχικές επιπτώσεις που μπορεί να αντιμετωπίσει ένα θύμα είναι η σημαντική συναισθηματική και ψυχολογική δυσφορία. Αυτό είναι συχνά άμεσο αποτέλεσμα των αδυσώπητων απειλών και της συνεχούς παρενόχλησης που διαπράττει ο απατεώνας. Η εν λόγω δυσφορία μπορεί να εκδηλωθεί με πολλούς τρόπους, όπως φόβος, άγχος, κατάθλιψη και διαταραχή του ύπνου, επηρεάζοντας σημαντικά την καθημερινή ζωή του θύματος.

02 Οικονομικές απώλειες

Ένας επιπλέον κίνδυνος στον οποίο εκτίθενται τα θύματα είναι το ενδεχόμενο σημαντικών οικονομικών ζημιών. Αυτό συμβαίνει συνήθως όταν το θύμα, αισθανόμενο στριμωγμένο και καταβεβλημένο από τις ανυποχώρητες απαιτήσεις του απατεώνα, ενδίδει τελικά. Ως αποτέλεσμα, μπορεί να βιώσουν όχι μόνο την απώλεια των σκληρά κερδισμένων χρημάτων τους αλλά και το άγχος και την αγωνία που συνοδεύει μια τέτοια απώλεια.

03 Ζημία στη φήμη

Τέλος, υπάρχει ο κίνδυνος σοβαρής ζημίας της φήμης του θύματος. Αυτό μπορεί να συμβεί αν ο απατεώνας αποφασίσει να πραγματοποιήσει τις απειλές του, δημοσιοποιώντας δυνητικά επιζήμιες ή ευαίσθητες πληροφορίες για το θύμα. Αυτό μπορεί να οδηγήσει σε σημαντική μείωση της κοινωνικής θέσης του θύματος και να επηρεάσει τις προσωπικές και επαγγελματικές του σχέσεις, καθώς και τις μελλοντικές του ευκαιρίες.

Απάτη μέσω ψεύτικων λογαριασμών



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΦΟΝΤΟ ΤΗΝ ΙΣΤΟΡΙΑ



Μια μέρα, η Susan έλαβε ένα αίτημα φιλίας από έναν λογαριασμό που έφερε το όνομα ενός χαμένου φίλου. Ενθουσιασμένη από την προοπτική της επανασύνδεσης, αποδέχτηκε το αίτημα. Σύντομα, άρχισαν να ανταλλάσσουν μηνύματα, αναπολώντας τα παλιά. Ωστόσο, τα πράγματα έγιναν δυσοίωνα όταν ο φίλος άρχισε να μοιράζεται περιεχόμενο με ρητό περιεχόμενο και απαίτησε χρήματα, απειλώντας να αμαυρώσει τη φήμη της συνδέοντας το όνομά της με το περιεχόμενο.

Συγκλονισμένη από την απότομη αλλαγή, η Susan αποφάσισε να επικοινωνήσει με την πραγματική της φίλη μέσω ενός διαφορετικού μέσου. Όταν έμαθε ότι η φίλη της δεν γνώριζε τίποτα για αυτόν τον λογαριασμό, συνειδητοποίησε ότι είχε αλληλεπιδράσει με έναν ψεύτικο λογαριασμό.

Αυτή η ιστορία υπογραμμίζει τη σημασία της εκπαίδευσης των ηλικιωμένων σχετικά με τους πιθανούς κινδύνους που ενέχει η αλληλεπίδραση με άγνωστες οντότητες στο διαδίκτυο. Επισημαίνει πώς οι ηλικιωμένοι μπορούν να γίνουν στόχος απάτης, όπως ο εκβιασμός μέσω ψεύτικων λογαριασμών, λόγω της πιθανής έλλειψης εξοικείωσής τους με τις ψηφιακές πλατφόρμες. Η ιστορία χρησιμεύει ως υπενθύμιση προς τους ηλικιωμένους να επαληθεύουν την ταυτότητα των ατόμων προτού συνεργαστούν μαζί τους στο διαδίκτυο και να αναφέρουν τυχόν ύποπτες δραστηριότητες στην πλατφόρμα ή στις τοπικές αρχές. Τονίζει την ανάγκη για ευαισθητοποίηση και επαγρύπνηση στον ψηφιακό κόσμο για την προστασία των ευημερία και την οικονομική τους ασφάλεια.



ΒΗΜΑ 1: Επαλήθευση αιτημάτων φιλίας

Η Susan δέχτηκε ένα αίτημα φιλίας από έναν λογαριασμό που πίστευε ότι ήταν ένας χαμένος φίλος χωρίς να επαληθεύσει τη γνησιότητά του. Η Susan θα έπρεπε να είχε επικοινωνήσει με τον πραγματικό της φίλο μέσω άλλου μέσου για να επαληθεύσει τη γνησιότητα του αιτήματος φιλίας πριν το αποδεχτεί.

ΒΗΜΑ 2: Να είστε προσεκτικοί με τις προσωπικές πληροφορίες

Η Susan συμμετείχε σε συζητήσεις και μοιράστηκε προσωπικές αναμνήσεις χωρίς να υποπτεύεται κάποιο βρώμικο παιχνίδι. Η Susan θα έπρεπε να είναι προσεκτική και να αποφεύγει να μοιράζεται προσωπικές πληροφορίες ή να εμπλέκεται σε ευαίσθητες συζητήσεις μέχρι να βεβαιωθεί για την ταυτότητα του άλλου μέρους.

ΒΗΜΑ 3: Αναγνωρίστε ύποπτη συμπεριφορά

Η Susan συνέχισε να αλληλεπιδρά με τον λογαριασμό ακόμη και αφού άρχισαν να μοιράζονται ρητό περιεχόμενο και να προβάλλουν απαιτήσεις. Μόλις αντιλήφθηκε την ύποπτη συμπεριφορά, η Susan θα έπρεπε να είχε σταματήσει αμέσως την αλληλεπίδραση με τον λογαριασμό και να τον επισημάνει ως ύποπτο.

ΒΗΜΑ 4: Αναφορά και εκπαίδευση

Αφού συνειδητοποίησε ότι ο λογαριασμός ήταν ψεύτικος, η Susan ανέφερε το περιστατικό και μοιράστηκε την εμπειρία της με φίλους και συγγενείς. Οι ενέργειες της Σούζαν για την αναφορά του λογαριασμού και την ενημέρωση των άλλων ήταν κατάλληλες. Θα πρέπει να συνεχίσει να υποστηρίζει την ευαισθητοποίηση και την επαγρύπνηση απέναντι στις διαδικτυακές απάτες.

Απάτη μέσω ψεύτικων λογαριασμών



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Η προστασία σας από εκβιασμούς με τη χρήση ψεύτικων λογαριασμών είναι ζωτικής σημασίας, ιδίως για τους ηλικιωμένους, επειδή βοηθά στην αποφυγή συναισθηματικής και ψυχολογικής δυσφορίας, οικονομικής απώλειας και ζημίας στη φήμη. Οι ηλικιωμένοι μπορεί να είναι πιο ευάλωτοι σε αυτές τις απάτες λόγω πιθανής έλλειψης εξοικείωσης με τις ψηφιακές πλατφόρμες. Με την επαγρύπνηση και την προσοχή στο διαδίκτυο, οι ηλικιωμένοι μπορούν να διαφυλάξουν την ευημερία και την οικονομική τους ασφάλεια, εξασφαλίζοντας μια ασφαλέστερη και πιο ευχάριστη διαδικτυακή εμπειρία.

Επαλήθευση αιτημάτων φιλίας:

Πάντα να επαληθεύετε την ταυτότητα του ατόμου που σας στέλνει αίτημα φιλίας, ιδίως αν δεν έχετε έρθει σε επαφή μαζί του για κάποιο χρονικό διάστημα. Αυτό μπορεί να γίνει με το να επικοινωνήσετε μαζί τους μέσω ενός άλλου μέσου που έχετε χρησιμοποιήσει στο παρελθόν για να επικοινωνήσετε.



Ρυθμίσεις απορρήτου:

Βεβαιωθείτε ότι οι λογαριασμοί σας στα μέσα κοινωνικής δικτύωσης έχουν τις υψηλότερες ρυθμίσεις απορρήτου. Αυτό θα περιορίσει τον όγκο των πληροφοριών που μπορούν να δουν άτομα που δεν είναι στη λίστα των φίλων σας.



Απάτη μέσω ψεύτικων λογαριασμών



ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ:

Μην μοιράζεστε ευαίσθητες πληροφορίες:

Αποφύγετε να μοιράζεστε προσωπικές ή ευαίσθητες πληροφορίες στο διαδίκτυο. Εάν το άτομο με το οποίο επικοινωνείτε αρχίζει να συμπεριφέρεται ύποπτα ή να απαιτεί χρήματα, διακόψτε αμέσως τη συζήτηση.



Αναφορά ύποπτης δραστηριότητας:

Αν συναντήσετε έναν ύποπτο λογαριασμό ή αν κάποιος αρχίσει να μοιράζεται ακατάλληλο περιεχόμενο ή να διατυπώνει απειλές, αναφέρετε τον λογαριασμό στην πλατφόρμα κοινωνικής δικτύωσης και στις τοπικές σας αρχές.

Εκπαιδεύστε τον εαυτό σας και τους άλλους:

Μάθετε για τα κοινά σημάδια των διαδικτυακών απάτης και διδάξτε και στους άλλους για αυτά τα σημάδια. Αυτό μπορεί να βοηθήσει εσάς και τους αγαπημένους σας να αποφύγετε να πέσετε θύματα τέτοιων απάτης.



Περισσότερες πληροφορίες



ΙΣΧΥΡΙΣΜΟ ΕΜΠΛΟΚΗΣ ΣΕ ΕΓΚΛΗΜΑΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ

- <https://www.legalmatch.com/law-library/article/allegations-of-criminal-involvement.html>
- <https://www.findlaw.com/criminal/criminal-charges/defending-against-criminal-charges.html>
- <https://www.nolo.com/legal-encyclopedia/criminal-defense-strategies>
- <https://www.lawinfo.com/resources/criminal-defense/>
- <https://www.justia.com/criminal/>
- <https://www.avvo.com/topics/criminal-charges>
- <https://www.legalzoom.com/articles/what-to-do-if-youre-accused-of-a-crime>
- <https://www.hg.org/criminal.html> <https://www.lawyers.com/legal-info/criminal/>
- https://www.americanbar.org/groups/criminal_justice/



ΧΕΙΡΑΓΩΓΗΣΕΙΣ ΠΟΥ ΥΠΟΔΥΟΝΤΑΙ ΚΡΑΤΙΚΟΥΣ ΘΕΣΜΟΥΣ

- <https://www.ncoa.org/article/government-imposter-scams-what-they-are-and-how-to-spot-them>
- <https://www.nia.nih.gov/news/high-vulnerability-government-impersonation-scams-among-older-adults>
- <https://www.idnow.io/glossary/impostor-fraud/>
- <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/senior-citizens-financial-scams/>
- <https://consumer.ftc.gov/articles/how-avoid-government-impersonation-scam#whattoknow>
- <https://regtechtimes.com/government-impersonation-scams-your-shield/>
- <https://www.europol.europa.eu/media-press/newsroom/news/beware-of-scams-involving-fake-correspondence-europol>

Περισσότερες πληροφορίες



ΧΕΙΡΑΓΩΓΗΣΗ ΜΕ ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΑΣ DEEPFAKE

- <https://www.bitdefender.com/blog/labs/deepfakes-what-they-are-how-they-work-and-how-to-protect-against-malicious-usage-in-the-digital-age>
- <https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained>
- <https://www.media.mit.edu/posts/deepfakes-explained/>
- <https://www.sentinelone.com/blog/what-are-deepfakes-how-can-you-spot-them/>
- <https://www.datavisor.com/blog/how-deepfakes-are-made-and-how-fraudsters-use-them/>
- <https://www.iproov.com/blog/deepfake-fraud-identity-theft-explained>
- <https://techmonitor.ai/technology/ai-and-automation/audio-deepfake-scams-the-growing-threat-explored>
- <https://readwrite.com/are-deepfakes-illegal-ais-dark-side-explained/>



ΑΠΑΤΗ ΥΠΗΡΕΣΙΩΝ ΠΟΥ ΥΠΟΔΥΕΤΑΙ ΤΑ ΚΡΑΤΙΚΑ ΟΡΓΑΝΑ

- <https://www.c-span.org/video/?468676-1/social-security-scams>
- <https://www.nia.nih.gov/news/high-vulnerability-government-impersonation-scams-among-older-adults>
- <https://www.bressler.com/news-1882>
- <https://consumer.ftc.gov/articles/how-avoid-government-impersonation-scam>
- https://www.facebook.com/europol/videos/%EF%B8%8F-beware-scammers-impersonating-europol-officers-europol-never-contacts-members-/1097501060976901/?_rdr

Περισσότερες πληροφορίες



ΑΠΑΤΗ ΜΕΣΩ ΠΛΑΣΤΩΝ ΛΟΓΑΡΙΑΣΜΩΝ

- <https://www.malwaretips.com/i-have-your-secrets-fake-blackmail-sextortion-scam-email>
- <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/sextortion-scams>
- https://www.scamnet.wa.gov.au/scamnet/Fight_back.htm
- <https://www.antivirus.com/blackmail-and-sextortion-emails>
- <https://www.malwaretips.com/hello-perv-blackmail-emails-are-fake>
- <https://www.womenslaw.org/about-abuse/abuse-using-technology/impersonation>
- <https://www.minclaw.com/how-to-deal-with-google-chat-blackmail>
- <https://www.digitalinvestigation.com/blog/blackmail-on-tiktok>
- <https://www.justice.gov/opa/pr/us-law-enforcement-joins-international-partners-disrupt-international-sextortion-ring>
- <https://www.cyber.gov.au/acsc/view-all-content/publications/sextortion-scams>



www.cybersafesenior.eu



Cyber-Safe-Senior



Funded by
the European Union

CYBER SAFE
SENIOR 



Instytut
Nowych Technologii



SIMBIOZA
MED GENERACIJAMI

«Χρηματοδοτείται από την ΕΕ. Οι απόψεις και οι γνώμες που εκφράζονται είναι του/των συγγραφέα/ων και δεν αντανακλούν απαραίτητα τις απόψεις της Ευρωπαϊκής Ένωσης ή του Εθνικού Οργανισμού Erasmus+. Ούτε η Ευρωπαϊκή Ένωση ούτε ο χορηγός είναι υπεύθυνοι γι' αυτά».



Το υλικό αυτό διατίθεται με την ανοικτή άδεια CC.3.0 BY-NC-ND 3.0 PL license (Attribution-Non-Commercial-No Derivative Works 3.0 Polska).

Η άδεια χρήσης σας επιτρέπει να διανέμετε, να παρουσιάζετε και να εκτελείτε το έργο μόνο για μη εμπορικούς σκοπούς και υπό την προϋπόθεση ότι διατηρείται στην αρχική του μορφή (χωρίς παράγωγα έργα).

Περισσότερες πληροφορίες:

<https://creativecommons.org/licenses/by-nd/3.0/pl/legalcode>

