SaferInternet4Kids.gr
ΓΙΑ ΕΝΑ ΑΣΦΑΛΕΣΤΕΡΟ ΔΙΑΔΙΚΤΥΟ

ΚΛΟΠΗ ΤΑΥΤΟΤΗΤΑΣ

Τι είναι, πώς να προστατευτείτε, προειδοποιητικά σημάδια και συμβουλές

Η κλοπή ταυτότητας συμβαίνει όταν κάποιος πλαστοπροσωπεί εσάς χρησιμοποιώντας τα προσωπικά σας στοιχεία, όπως το όνομά σας, τον αριθμό κοινωνικής ασφάλισης, την ημερομηνία γέννησης κ.λπ., συνήθως για να διαπράξει ένα έγκλημα εναντίον σας.

Κύριοι τύποι κλοπής ταυτότητας που μπορεί να σας επηρεάσουν

Κλοπή οικονομικής ταυτότητας

Όταν κάποιος χρησιμοποιεί τις πληροφορίες ενός άλλου ατόμου για οικονομικό όφελος, αυτός είναι ο πιο ευρέως αναγνωρισμένος τύπος κλοπής ταυτότητας. Για παράδειγμα, ένας κλέφτης ταυτότητας μπορεί να ανοίξει μια νέα πιστωτική κάρτα χρησιμοποιώντας τον αριθμό Κοινωνικής Ασφάλισης ή τα στοιχεία του τραπεζικού λογαριασμού σας για να κλέψει χρήματα ή να κάνει αγορές.

Κλοπή Ταυτότητας Κοινωνικής Ασφάλισης

Ο Αριθμός Κοινωνικής Ασφάλισης μπορεί να χρησιμοποιηθεί από κλέφτες ταυτότητας για να υποβάλουν αίτηση για πιστωτικές κάρτες και δάνεια και στη συνέχεια να τον χρησιμοποιήσουν για να αποφύγουν την επιστροφή τυχόν υπαρχόντων λογαριασμών. Ο αριθμός σας ενδέχεται να χρησιμοποιηθεί από απατεώνες για να λάβουν ασφάλιση, πληρωμές αναπηρίας και άλλα οφέλη.

Κλοπή Ιατρικής Ταυτότητας

Η μη εξουσιοδοτημένη χρήση της ασφάλισης υγείας ενός ατόμου για τη λήψη πληρωμής για ιατρικές υπηρεσίες που παρέχονται σε ένα άτομο που δεν καλύπτεται από το συμβόλαιο είναι γνωστή ως κλοπή ιατρικής ταυτότητας. Μερικές φορές, υπάλληλοι ή εξωτερικοί χάκερ κλέβουν τα δεδομένα για να πουλήσουν τα προσωπικά δεδομένα και να βγάλουν χρήματα.

Κλοπή εγκληματικής ταυτότητας

Η κλοπή εγκληματικής ταυτότητας συμβαίνει όταν ένα άτομο που συλλαμβάνεται από τις αρχές επιβολής του νόμου χρησιμοποιεί το όνομα κάποιου άλλου αντί να δώσει το δικό του. Μπορεί να μπορέσουν να το κάνουν δημιουργώντας μια ψεύτικη ταυτότητα ή χρησιμοποιώντας μια κλεμμένη ταυτότητα, όπως η άδεια οδήγησής σας, για να τη δείξουν στην αστυνομία.

Τύποι επιθέσεων phishing

Email phishing
Λήψη προσωπικών πληροφοριών από ένα θύμα, από ένα email από μια επιχείρηση που παρουσιάζεται ως αξιόπιστη.
email, ιστοσελίδες, social media, mobile apps
Λαμβάνετε μια ψεύτικη προειδοποίηση ασφαλείας από την τράπεζά σας που ζητά να επαληθεύσετε τα όνομα χρήστη και τον κωδικό πρόσβασής σας.

Smissing
Η πρακτική της εξαπάτησης ενός χρήστη για να κατεβάσει κακόβουλο λογισμικό ή έναν ιό χρησιμοποιώντας ένα μήνυμα κειμένου.
κινητό τηλέφωνα
Το τηλέφωνό σας σάς ειδοποιεί μέσω SMS ότι έχετε κερδίσει μια δωροκάρτα. Όταν κάνετε κλικ στον σύνδεσμο για εξαργύρωση, εγκαθίσταται λογισμικό που καταγράφει όλες τις πληκτρολογήσεις.

Spear phishing
Το Spear phishing στοχεύει μια συγκεκριμένη ομάδα ή άτομο, όπως ο διαχειριστής συστήματος μιας επιχείρησης.
ιστοσελίδες, email
Μια ομάδα ειδικών ανθρώπινου δυναμικού λαμβάνει ένα έγγραφο του Excel με τίτλο «Σχέδιο πληρωμών 2023», ὅμως, ένα flash αντικείμενο στο αρχείο συλλέγει πληροφορίες σύνδεσης συστήματος.

Vishing
Δόλιες τηλεφωνικές κλήσεις με σκοπό τη συλλογή ευαίσθητων προσωπικών δεδομένων.
κινητό τηλέφωνο, κλήσεις
Λαμβάνετε μια κλήση από τον «τοπικό τηλεφωνίσκο» σας με μια ειδική προσφορά για ένα φτηνό συμβόλαιο που πρέπει να πληρωθεί άμεσα με πιστωτική κάρτα.

Pharming
Pharming directs victims to an attacker-controlled website by executing malicious code on their victim's device.
ιστοσελίδες, υπολογιστές
Ο ιστότοπος της τράπεζάς σας έχει μια ειδοποίηση για απομακρυσμένη σύνδεση που σας ζητά να εισαγάγετε τα PII σας για να ξεκλειδώσετε τον λογαριασμό σας επειδή το δούμε να σας έχουν κλαπεί.

Whaling
Στην επίθεση φαλαινοθηρίας οι επιτιθέμενοι στοχεύουν υψηλόβαθμα στελέχη για να κλέψουν χρήματα ή πληροφορίες.
email, social media
Ένας οικονομικός διευθυντής δημοσιεύει τη συμμετοχή του σε ένα τουρνουά. Έντεκα από τους συν-χορηγούς στέλνει ένα email με θέμα «Καλό ταξιδάκι την Κυριακή». Στο email υπάρχει μια εικόνα που εκθέτει πολλούς πληροφορίες.

Search engine phishing
Περιλαμβάνει χάκερ που τοποθετούν τον δικό τους ιστότοπο σε νόμιμες μηχανές αναζήτησης.
ιστοσελίδες
Ψάχνετε για δωρεάν στο διαδίκτυο. Παρουσιάζεται μια ψεύτικη προσφορά εργασίας, που απαιτεί από τα άτομα να εισαγάγουν τον αριθμό κοινωνικής ασφάλισής τους.

Τρόποι για να αποτρέψετε την κλοπή ταυτότητας

Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης

Ένας σημαντικός κίνδυνος για την ασφάλεια τίθεται από τη χρήση του ίδιου κωδικού πρόσβασης για όλες τις συσκευές και λογαριασμούς σας. Εάν χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης, ένας απατεώνας χρειάζεται μόνο να σπάσει έναν κωδικό πρόσβασης για να αποκτήσει πρόσβαση σε όλους τους λογαριασμούς σας.

Bonus Tip: Χρησιμοποιήστε έναν διαχειριστή κωδικών πρόσβασης για να θυμάστε και να προστατέψετε τους κωδικούς πρόσβασής σας.

Ελέγχετε συχνά τις πιστωτικές σας αναφορές

Η δραστηριότητα του χρηματοοικονομικού λογαριασμού σας, συμπεριλαμβανομένων των τελευταίων κινήσεων, αντικατοπτρίζεται στις πιστωτικές σας αναφορές. Επομένως, ο συχνός έλεγχος των κινήσεων του λογαριασμού σας είναι ένας καλός τρόπος για να βρείτε σφάλματα.

Bonus Tip: Εάν δεν δείτε μία πληρωμή, καλέστε ή συνδεθείτε απευθείας στον λογαριασμό σας για να βεβαιωθείτε ότι κάποιος κλέφτης δεν έχει ανακατευθύνει την ηλεκτρονική αλληλογραφία σας σε άλλη διεύθυνση.

Χρησιμοποιήστε ένα εικονικό ιδιωτικό δίκτυο

Γενικά, θα πρέπει να αποφεύγετε να χρησιμοποιείτε δημόσια δίκτυα Wi-Fi για να συνδεθείτε σε σημαντικούς λογαριασμούς ή να εισαγάγετε στοιχεία πληρωμής.

Ένα VPN μπορεί να δημιουργήσει μια κρυπτογραφημένη σύνδεση μεταξύ του υπολογιστή ή της κινητής συσκευής σας και του διακομιστή VPN, εάν σκοπεύετε να χρησιμοποιήσετε δημόσιο Wi-Fi. Αυτή η διαμόρφωση μπορεί να μειώσει την πιθανότητα κάποιος να κλέψει τις πληροφορίες σας.

Bonus Tip: Θυμηθείτε να προσθέσετε έναν κωδικό πρόσβασης στο οικιακό σας δίκτυο αν δεν έχει ήδη.

Προσέξτε για ύποπτα email/ιστοσελίδες

Ποτέ μην κάνετε κλικ σε συνδέσμους που φαίνονται ύποπτοι σε email ή μηνύματα κειμένου. Οι κλέφτες ταυτοτήτων χρησιμοποιούν μηνύματα ηλεκτρονικού ταχυδρομείου και ιστότοπους που φαίνεται να προέρχονται από την τράπεζά σας για να σας εξαπατήσουν ώστε να εισαγάγετε τα στοιχεία του λογαριασμού σας ή άλλα προσωπικά δεδομένα.

Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου μπορεί ακόμη και να σας ζητήσουν να ανοίξετε ένα συνημμένο που εγκαθιστά επιβλαβές κακόβουλο λογισμικό στη συσκευή σας.

Προστατέψτε τα προσωπικά σας έγγραφα

Σε περίπτωση ακατάλληλου χειρισμού, τα φυσικά έγγραφα μπορεί να θέσουν σε κίνδυνο την ασφάλεια σας. Ο αριθμός κοινωνικής ασφάλισης και πληροφορίες σχετικά με τους τραπεζικούς λογαριασμούς σας θα μπορούσαν να βρεθούν στα χέρια κλεφτών ταυτότητας.

Τα γραμματοκιβώτια σας δεν πρέπει ποτέ να μένουν χωρίς επιτήρηση, επειδή οι κλέφτες ταυτότητας συχνά τα στοχοποιούν.

Χρησιμοποιήστε έλεγχο ταυτότητας δύο παραγόντων

Το 2FA είναι ένα πρόσθετο μέτρο ασφαλείας που χρησιμοποιείται για να επιβεβαιώσει ότι οι χρήστες που προσπαθούν να συνδεθούν σε έναν διαδικτυακό λογαριασμό είναι αυτοί που ισχυρίζονται ότι είναι. Ένας χρήστης πρέπει πρώτα να εισάγει ένα όνομα χρήστη και έναν κωδικό πρόσβασης. Μετά από αυτό, δεν θα τους παραχωρηθεί αμέσως πρόσβαση, αλλά θα πρέπει να παράσχουν περισσότερες πληροφορίες.

SaferInternet4Kids.gr · safeLine.gr · help line · ITE · INHOPE · insafe · Co-funded by the European Union