13 Ιουνίου 2016

Πως κλέβουν την ταυτότητά σας στο internet

/ Πεμπτουσία

Image not found or type unknown

Hacker waiting for something with binary code in background

Ένα ωραίο πρωί ξυπνάτε και έχετε υποστεί αυτό που λέμε «κλοπή ταυτότητας». Παρόλο που η κλοπή ταυτότητας κάποιου, δεν είναι νόμιμη, υπάρχουν διάφοροι ύπουλοι, αλλά νόμιμοι τρόποι που απατεώνες και χάκερ μπορούν να χρησιμοποιήσουν ώστε να υποστείτε τη λεγόμενη «κλοπή ταυτότητας». Το πρώτο βήμα για να σταματήσει αυτό το ανησυχητικό σενάριο είναι να γνωρίζετε τα πιο κοινά συστήματα συλλογής δεδομένων που θα μπορούσαν να σας κάνουν ευπαθή.

Παρακάτω θα δούμε πέντε τακτικές που πρέπει να γνωρίζετε, ώστε να μπορείτε να έχετε τον «έλεγχο» της ταυτότητά σας.

Κατασκοπεία των Social media

Οι άνθρωποι έχουν αρχίσει να μοιράζονται, περισσότερο από ποτέ, πράγματα σχετικά με την προσωπική τους ζωή μέσω του διαδικτύου με την εμφάνιση των

μέσων κοινωνικής δικτύωσης. Ενώ μπορείτε ουσιαστικά να συνδεθείτε με παλιούς φίλους που είχατε χάσει και συγγενείς, παράλληλα γίνεται απλούστερο για έναν απατεώνα ή χάκερ να πάρει στα χέρια του τα προσωπικά σας στοιχεία που θα μπορούσαν να οδηγήσουν σε κλοπή ταυτότητας. Σε γενικές γραμμές, αν αποφασίσετε να αποκαλύψετε προσωπικές σας πληροφορίες, όπως τα γενέθλιά σας ή οποιαδήποτε άλλα προσωπικά στοιχεία, προτείνεται να κρατάτε τις ρυθμίσεις του προφίλ σας ιδιωτικές και να έχετε εξετάσει τις συνέπειες από οτιδήποτε δημοσιεύετε. Για παράδειγμα, το να προβάλετε παντού τις διακοπές σας θα μπορούσε να κάνει έναν κλέφτη να καταλάβει ότι το σπίτι σας είναι αφύλακτο ή ότι δεν έχετε πρόσβαση στο ηλεκτρονικό σας ταχυδρομείο.

Social engineering

Μερικοί απατεώνες και χάκερ θα δημιουργήσουν παγίδες που εξαρτώνται κυρίως από την ανθρώπινη αλληλεπίδραση για να αποκτήσουν πρόσβαση, αντί να ξοδεύουν το χρόνο τους προσπαθώντας να μαντέψουν ή να εντοπίσουμε τα προσωπικά σας στοιχεία. Αυτή η τακτική είναι γνωστή ως «Social engineering». Συχνά, αυτοί οι χάκερ λοιπόν, εμφανίζονται ως ένα φιλικό πρόσωπο ή μια εταιρεία που ψάχνει για πληροφορίες. Τα κόλπα της κοινωνικής μηχανικής εξαρτώνται από την περιέργεια των ανθρώπων και την εμπιστοσύνη που δείχνουν. Μπορεί να θέλετε να είστε προσεκτικοί στα “επείγοντα” μηνύματα ηλεκτρονικού ταχυδρομείου που προσπαθούν να επιβεβαιώσουν τα στοιχεία σύνδεσής σας ή επισφαλείς αιτήσεις φίλων στασocial media.

Υποκλοπή από τον παλιό σας σκληρό δίσκο ή υπολογιστή

Μην δίνετε απλά τον παλιό σας υπολογιστή με τον υπάρχοντα σκληρό δίσκο ανέπαφο, αν ψάχνετε να τον πουλήσετε ή να τον ξεφορτωθείτε. Θα μπορούσατε έτσι ακούσια να παραδώσετε τα κλειδιά για τις προσωπικές σας πληροφορίες σε κάποιον που θέλει να κλέψει την ταυτότητά σας. Βεβαιωθείτε ότι ο σκληρός δίσκος έχει αντικατασταθεί και καταστραφεί πριν τον πετάξετε ή αναβαθμίσετε ένα παλιό μηχάνημα.

Phishing που βασίζεται στο Malware

Υπάρχουν πιθανότητες να είστε πιο ευάλωτοι σε απάτες που κρύβονται πίσω από «διορθώσεις» στο πρόβλημα, όταν αισθάνεστε ότι ο υπολογιστής σας τρέχει κάποιο κακόβουλο λογισμικό. Εάν αισθάνεστε ότι ο υπολογιστής σας έχει μολυνθεί ή έχει κατεβάσει παράνομο περιεχόμενο και αν σας προσφερθεί μια άμεση λύση στο πρόβλημα, τότε σκεφτείτε την δύο φορές. Μπορείτε πραγματικά να καταλήξετε στην εγκατάσταση ενός κακόβουλου λογισμικού αντ' αυτού.

Vishing ή «voice phishing»

Οι voice phishing ή "vishing" απάτες είναι φωνητικά μηνύματα ή robocalls τίθενται από απατεώνες και χάκερ που κρύβονται πίσω από επιχειρήσεις ή κρατικούς φορείς με μόνο τους στόχο να αποκτήσουν την προσοχή σας. Θα θελήσουν να σας κάνουν να αποκαλύψετε σημαντικές πληροφορίες ταυτοποίησης όπως τον αριθμό κοινωνικής σας ασφάλισης ή της πιστωτικής κάρτας σας γρήγορα από το τηλέφωνο. ***Μια συμβουλή***: Ένας αξιόπιστος οργανισμός δεν λειτουργεί με αυτόν τον τρόπο.

Πηγή: secnews.gr