

20 Δεκεμβρίου 2016

Internet: πόσο κοστίζει η άγνοια και η απόλυτη εμπιστοσύνη σε ειδικούς

/ [Πεμπτούσία](#)

Image not found or type unknown



Σήμερα, ειδικούς επί του διαδικτύου βρίσκετε να προσφέρουν συμβουλές σε κάθε γωνιά του internet. Κάτι που δεν είναι κακό, καθώς και οι αρχάριοι υπάρχουν στα ίδια ίσως και μεγαλύτερα ποσοστά. Κακό όμως είναι ότι υπάρχουν και ορισμένοι που εκμεταλλεύονται τις γνώσεις τους για να αποκομίσουν κάθε δυνατό κέρδος.

Οι μέθοδοι ποικίλουν. Έχουμε δει «υπηρεσίες» support κάθε είδους που χρεώνουν με την ώρα και τα αποτελέσματα δεν είναι πάντα τα επιθυμητά ή εταιρείες ανάπτυξης λογισμικού ασφαλείας που κυκλοφορούν λογισμικά που μόνο ασφάλεια δεν προσφέρουν.

Όμως στα παραπάνω παραδείγματα αν και οι «ειδικοί» προσπαθούν να κρυφτούν πίσω από φανταχτερούς τίτλους και μεγάλες υποσχέσεις, αποκαλύπτονται σχετικά γρήγορα, από αρνητικά reviews που κατακλύζουν τεχνολογικά forums.

Παρακάτω θα δούμε ένα διαφορετικό είδος ειδικών, που προσπαθούν να αποκομίσουν όσο το δυνατόν περισσότερα από τους χρήστες που δεν κρίνουν και δεν αμφισβητούν αυτά που τους σερβίρουν μέσα από κάθε ιστοσελίδα.

Θα μιλήσουμε για το Γερμανικό Hasso-Plattner-Institute. Οι ειδικοί του Γερμανικού Ινστιτούτου εξέτασαν περίπου 1 δισεκατομμύριο λογαριασμούς χρηστών (πολλή δουλειά σε ένα πάρα πολύ μεγάλο δείγμα) και κατέληξαν στο συμπέρασμα ότι το 20% των χρηστών επαναχρησιμοποιούν τους κωδικούς πρόσβασής τους. Επιπλέον, το 27% των χρηστών χρησιμοποιούν τους ίδιους κωδικούς πρόσβασης σε όλους τους λογαριασμούς τους.

Οι ερευνητές του ινστιτούτου όπως προαναφέραμε ανέλυσαν περίπου 1 δισεκατομμύριο λογαριασμούς χρηστών, από δεδομένα που προήλθαν από 31 διαφορετικές διαρροές, είτε από τους ίδιους τους επιτιθέμενους είτε από τους αγοραστές των δεδομένων. Τα sites τα οποία «έχασαν» τα δεδομένα; Yahoo, Dailymotion, VK, MySpace, Friend Finder Network, και Brazzers.

Περίπου 68,5 εκατομμύρια διευθύνσεις ηλεκτρονικού ταχυδρομείου εμφανίζονται πολλές φορές στη βάση δεδομένων, ένας αριθμός που αντιστοιχεί στο 20% (περίπου) όλων των λογαριασμών χρηστών που υπήρχαν στα δεδομένα των ερευνητών.

Οι πιο κοινοί κωδικοί βρέθηκαν να είναι οι :«123456», «123456789», «111111», «qwerty», και «12345678» σύμφωνα με τη μελέτη. Μέχρι στιγμής τίποτα το παράξενο.

Is someone spying on you?

Everyday personal data is stolen in criminal cyber attacks. A large part of the stolen information is subsequently made public on Internet databases, where it serves as the starting point for other illegal activities.

With the HPI Identity Leak Checker, it is possible to check whether your e-mail address, along with other personal data (e.g. telephone number, date of birth or address), has been made public on the Internet where it can be misused for malicious purposes.



Please enter your e-mail address here.

The e-mail address you have entered will only be used for searching in our database and, when applicable, to subsequently send an e-mail notification. It will be saved in an obfuscated way to protect you from potential e-mail spam and is never given to a third party.

Check e-mail address!

Στο επόμενο βήμα και μετά από μία ενημέρωση που είναι ικανή να τρομοκρατήσει αρκετούς το Ινστιτούτο προσφέρει την ευκαιρία σε όλους τους ενδιαφερόμενους να εξακριβώσουν αν ο κωδικός τους κυκλοφορεί στο internet.

Τι καλοί άνθρωποι...

Πως μπορεί να γίνει αυτό; Αν δώσετε το e-mail σας στην φόρμα που υπάρχει στην σελίδα που αναφέρει την έρευνα του ινστιτούτου, θα σας αποσταλεί e-mail με τα στοιχεία που υπάρχουν στην βάση τους (αν υπάρχουν).

Τι κερδίζουν με αυτό τον τρόπο; Φυσικά πολύτιμες διευθύνσεις e-mail. Σε αυτή την περίπτωση μπορείτε να είστε σίγουροι ότι όλες οι διευθύνσεις συλλέγονται γιατί σας αποστέλλεται e-mail με τα στοιχεία που ζητάτε.

Με αυτό τον τρόπο το Ινστιτούτο θα συλλέξει χιλιάδες e-mail, και αν προωθήσει το «προϊόν» του σωστά, θα φτάσουν εκατομμύρια. Να αναφέρουμε ότι τα e-mail που θα συλλέξουν οι ειδικοί δεν θα είναι μόνο από αυτούς που έχουν ήδη διαρρεύσει μέσω κάποιου hack. Το Γερμανικό Ινστιτούτο θα αποκτήσει διευθύνσεις και από αυτούς που δεν κινδυνεύουν αλλά σκέφτονται ότι καλό θα ήταν να το εξακριβώσουν...

Τι αξία έχουν τα συγκεκριμένα e-mail; Χωρίς πολλές πολλές αναλύσεις, όλα αυτά τα e-mails έχουν ένα κοινό: Προέρχονται από ανθρώπους που τους ενδιαφέρει η

διαδικτυακή ασφάλεια. Άραγε πόσο μπορεί να πληρώσει μια εταιρεία με προϊόντα ασφαλείας για αυτές τις διευθύνσεις;

Τι θα μπορούσατε να κάνετε; Αλλάξτε τον κωδικό πρόσβασης αν είστε εγγεγραμμένοι σε ένα από τα παραπάνω sites. Έτσι δεν θα δώσετε το e-mail σας.

Το δελτίο τύπου που ανακοινώνει τα αποτελέσματα της μελέτης είναι διαθέσιμο στο παρακάτω link.

<http://www.presseportal.de/pm/22537/3503172>

Πηγή: secnews.gr