

Το 31% των χρηστών του διαδικτύου είναι απρόσεκτοι στις online συναλλαγές τους

/ [Επιστήμες, Τέχνες & Πολιτισμός](#)



Έρευνα της Kaspersky Lab και της B2B International

Ένας στους πέντε χρήστες δεν παίρνει κανένα μέτρο για την προστασία των κωδικών που χρησιμοποιεί για την πρόσβαση σε ευαίσθητες πηγές

Σύμφωνα με έρευνα της Kaspersky Lab και της B2B International, σχεδόν το ένα τρίτο των χρηστών συνεχίζει να είναι απρόσεκτο όταν πραγματοποιεί online συναλλαγές. Η συμπεριφορά αυτή θέτει σε κίνδυνο τα χρήματά τους, αλλά δημιουργεί και προβλήματα στις τράπεζες και τα συστήματα ηλεκτρονικών πληρωμών, καθώς ενδέχεται να κληθούν να αποζημιώσουν τους πελάτες τους για απώλεια χρημάτων. Στη βάση αυτή, όλοι όσοι εμπλέκονται σε μια online συναλλαγή, θα πρέπει να λαμβάνουν τα κατάλληλα μέτρα ασφαλείας, ώστε να ελαχιστοποιούνται οι πιθανοί κίνδυνοι.

Οι ψηφιακοί εγκληματίες δεν ενδιαφέρονται μόνο για αριθμούς πιστωτικών ή χρεωστικών καρτών. Τα στοιχεία σύνδεσης σε online τραπεζικούς λογαριασμούς και σε υπηρεσίες ηλεκτρονικών πληρωμών βρίσκονται επίσης σταθερά στο στόχαστρό τους. Παρόλα αυτά, το 31% των ερωτηθέντων παραδέχτηκε ότι δεν δίνει πολύ προσοχή στο επίπεδο ασφάλειας των σελίδων όπου εισάγει προσωπικά ή οικονομικά δεδομένα. Ένας στους πέντε χρήστες δεν παίρνει κανένα μέτρο για την

προστασία των κωδικών που χρησιμοποιεί για την πρόσβαση σε αυτές τις ευαίσθητες πηγές. Μάλιστα, σε ποσοστό 16%, οι ερωτηθέντες δήλωσαν με βεβαιότητα ότι «το ψηφιακό έγκλημα που αποσκοπεί στην κλοπή χρημάτων είναι ένα σπάνιο φαινόμενο» και ότι είναι «απίθανη η περίπτωση να συμβεί στους ίδιους κάτι τέτοιο».

Το 30% των ερωτηθέντων αποθηκεύει οικονομικά δεδομένα σε συσκευές με πρόσβαση στο Διαδίκτυο. Αυτό δεν θα ήταν τόσο επικίνδυνο, αν οι χρήστες φρόντιζαν πάντα να χρησιμοποιούν ειδικά προγράμματα ασφαλούς αποθήκευσης δεδομένων. Αυτό όμως δεν γίνεται. Για παράδειγμα, μόνο το 58% των Android smartphones, αναφέρει το techgear.gr, έχει εγκατεστημένη μια λύση ασφάλειας. Ακόμη χειρότερα, στο 31% των έξυπνων τηλεφώνων και στο 41% των Android tablets δεν χρησιμοποιούνται ούτε βασικά μέτρα ασφάλειας, όπως ο ορισμός ενός κωδικού πρόσβασης για το ξεκλείδωμα της συσκευής πριν τη χρήση της.

Εν τω μεταξύ, πολλοί χρήστες έρχονται συχνά αντιμέτωποι με στοιχεία που αποδεικνύουν ότι οι ψηφιακοί εγκληματίες αναζητούν διαρκώς οικονομικές πληροφορίες. Μέσα στους τελευταίους 12 μήνες, το 33% των ερωτηθέντων ανέφερε ότι είχε λάβει ύποπτα email που ισχυρίζονταν ότι προέρχονταν από κάποια τράπεζα και ζητούσαν κωδικούς πρόσβασης ή άλλες πληροφορίες. Ακόμη, το 14% των χρηστών ανακατευθύνθηκε σε ιστοσελίδες που ζητούσαν στοιχεία σύνδεσης για λογαριασμούς ηλεκτρονικών πληρωμών.

Σύμφωνα με τον Ross Hogan, Global Head of the Fraud Prevention Division της Kaspersky Lab: “Όταν οι χρήστες αγνοούν τα μέτρα ασφάλειας, μπορεί να πέσουν θύματα απατεώνων. Ταυτόχρονα, οι τράπεζες καταλήγουν συχνά να πληρώνουν για την αμέλεια αυτή. Βλέποντας ότι υπάρχουν πολλοί χρήστες που αμελούν την ασφάλεια τους, οι τράπεζες και οι διαχειριστές συστημάτων ηλεκτρονικών πληρωμών οφείλουν οι ίδιοι να λάβουν μέτρα προστασίας ενάντια στους οικονομικούς κινδύνους, αλλά και διαφυλάξουν τη φήμη τους, χρησιμοποιώντας εξειδικευμένες λύσεις ασφάλειας που έχουν τη δυνατότητα να αποτρέψουν το ψηφιακό έγκλημα”

Η πλατφόρμα Kaspersky Fraud Prevention παρέχει εξειδικευμένες λύσεις που επιτρέπουν στις τράπεζες, στα συστήματα επεξεργασίας πληρωμών και στις εταιρείες ηλεκτρονικού εμπορίου να προλαμβάνουν τις απάτες στα online και mobile κανάλια τους. Οι λύσεις αυτές προστατεύουν ενεργά και τους τελικούς χρήστες και τις επιχειρήσεις, δημιουργώντας μια ασφαλή εμπειρία για τους χρήστες των online υπηρεσιών. Επιπλέον, η πλατφόρμα Kaspersky Fraud Prevention αποτρέπει προσπάθειες παραβίασης λογαριασμών και phishing, ενώ ταυτόχρονα διακόπτει και εξουδετερώνει τις «μολύνσεις» που έχουν προκληθεί

από κακόβουλο λογισμικό.

Τέλος, η Kaspersky Lab συμβουλεύει τους χρήστες να εγκαταστήσουν λύσεις ασφάλειας που καλύπτουν ταυτόχρονα πολλαπλές συσκευές, ακόμη και με διαφορετικές λειτουργικές πλατφόρμες, όπως το Kaspersky Internet Security - Multi-Device και το Kaspersky Total Security - Multi-Device. Οι λύσεις αυτές εκτός του ότι παρέχουν γενική προστασία ενάντια σε ψηφιακές απειλές, διαθέτουν και την τεχνολογία Safe Money, ένα ειδικό εργαλείο προστασίας των online συναλλαγών (κατάλληλο για λογισμικά Windows και OS X). Το Kaspersky Total Security - Multi-Device περιλαμβάνει επίσης μια ειδική εφαρμογή για την ασφαλή αποθήκευση κωδικών πρόσβασης και τον συγχρονισμό των στοιχείων σύνδεσης μεταξύ διαφορετικών συσκευών.

Πηγή: protothema.gr