30 Ιανουαρίου 2014

Συμβουλές προστασίας πιστωτικών και

 Τα

πρόσφατα περιστατικά διαρροής προσωπικών δεδομένων σε κατόχους καρτών, ως αποτέλεσμα της επίθεσης κυβερνοεγκληματιών στην αμερικανική αλυσίδα καταστημάτων λιανεμπορίου Target, καταδεικνύουν ακόμη μία φορά το ζήτημα της προστασίας των καταναλωτών που πραγματοποιούν αγορές με χρεωστικές ή πιστωτικές κάρτες. Με αφορμή το γεγονός αυτό, η ESET συμβουλεύει τους κατόχους καρτών για το πώς μπορούν να προστατεύσουν τους λογαριασμούς τους αλλά και την ταυτότητά τους.

Ελέγξτε το λογαριασμό σας για ύποπτη δραστηριότητα, ειδικά αν είχατε πραγματοποιήσει αγορές το διάστημα Νοεμβρίου – Δεκεμβρίου 2013, οπότε και παρατηρήθηκε έξαρση στα περιστατικά διαρροής. Να είστε σε επιφυλακή ακόμη κι αν δεν φανούν ύποπτες συναλλαγές στην κίνηση της κάρτας, καθώς οι κυβερνοεγκληματίες πολλές φορές διατηρούν τα στοιχεία και τα χρησιμοποιούν μόλις το θέμα ξεχαστεί από την επικαιρότητα.

Αντικαταστήστε την χρεωστική/πιστωτική σας κάρτα σε περίπτωση που δεν επιθυμείτε να είστε διαρκώς σε επιφυλακή και να την ελέγχετε. Σε περίπτωση που

στην κάρτα σας έχετε δώσει εντολές αυτόματης πληρωμής κάποιων λογαριασμών, θα χρειαστεί αλλαγή των στοιχείων.

Αλλάξτε το PIN της χρεωστικής σας κάρτας, καθώς οι κυβερνοεγκληματίες προσπαθούν διαρκώς να «σπάσουν» την κρυπτογράφηση και πολλοί χρήστες καρτών δεν χρησιμοποιούν ισχυρά PIN.

Ελέγχετε τακτικά τις πιστοληπτικές σας αναφορές δίνοντας ιδιαίτερη προσοχή για δραστηριότητες όπως νέοι λογαριασμοί στο όνομά σας, για τους οποίους δεν είχατε δώσει σχετική εντολή. Μπορείτε επίσης να δημιουργήσετε μία ειδοποίηση (fraud alert) ή να «παγώσετε» την πιστωτική σας για επιπλέον προστασία, λαμβάνοντας ωστόσο υπόψη ότι θα πρέπει, κατά το διάστημα αυτό, να υποβάλλεστε σε επιπλέον διαδικασίες εξακρίβωσης των στοιχείων σας κάθε φορά που θα χρησιμοποιείτε την κάρτα.

Αλλάξτε τα passwords που χρησιμοποιείτε για τις online αγορές σας, δεδομένου ότι δεν έχουν ολοκληρωθεί όλες οι έρευνες για τις απάτες των τελευταίων ημερών, οποιοδήποτε προληπτικό μέτρο προστασίας θα σας βοηθήσει να παραμείνετε ασφαλείς.

Να είστε επιφυλακτικοί σε scams, καθώς σε περίπτωση που κλαπούν στοιχεία της κάρτας, οι κυβερνοεγκληματίες συνήθως αποκτούν πρόσβαση σε ακόμη περισσότερα στοιχεία, τα οποία και χρησιμοποιούν στέλνοντας scam ή phishing email. Φανείτε προσεκτικοί σε links ή email που φαίνονται ύποπτα και μην τα ανοίγετε, αλλά αντίθετα πληκτρολογήστε απευθείας την διεύθυνση URL στο browser σας.

Πηγή: kathimerini.gr