30 Ιανουαρίου 2017

Κινητό τηλέφωνο: ο κωδικός κλειδώματος, ασφαλέστερος του «μοτίβου»

/ Πεμπτουσία

Image not found or type unknown

Επί του παρόντος, το Android είναι το πλέον χρησιμοποιούμενο λειτουργικό σύστημα κινητών στον κόσμο, το οποίο σημαίνει ότι χρησιμοποιείται από εκατομμύρια συσκευές σε όλο τον κόσμο. Για την προστασία των συσκευών παρέχονται οι κωδικοί PIN ή κωδικοί πρόσβασης κειμένου, αλλά και ένα σύστημα κλειδώματος με μοτίβο που σας επιτρέπει να δημιουργήσετε έναν κωδικό πρόσβασης, χρησιμοποιώντας διάφορα σχέδια της επιλογής σας. Σύμφωνα, λοιπόν, με σχετική μελέτη, το μοτίβο αυτό του Android μπορεί να σπάσει με 5 προσπάθειες.

Προφανώς, περίπου το 40 τοις εκατό των ιδιοκτητών Android συσκευών, προτιμούν να χρησιμοποιούν το δημοφιλές μοτίβο κλειδώματος οθόνης, σε σύγκριση με τη χρήση κωδικών PIN ή τους κωδικούς πρόσβασης κείμενο. Η

κλειδαριά μοτίβο είναι ένα εργαλείο ξεκλειδώματος οθόνης που επιτρέπει στο χρήστη για να σχεδιάσει ένα συγκεκριμένο μοτίβο χρησιμοποιώντας τις εννέα τελείες σε ένα πλέγμα 3 × 3 χωρίς να σηκώσει το δάκτυλό του.

Ενώ κάποιος μπορεί να πιστεύει ότι το μοτίβο κλειδώματος οθόνης είναι πιο ασφαλές από ό, τι η χρήση κωδικών PIN ή κωδικών πρόσβασης κειμένου, η αλήθεια διαφέρει. Σύμφωνα με μια νέα έρευνα από το Πανεπιστήμιο του Lancaster, το Βορειοδυτικό Πανεπιστήμιο στην Κίνα και το Πανεπιστήμιο του Bath, είναι πραγματικά εύκολο να σπάσει το 95% των κλειδαριών μοτίβο οθόνης, μέσα σε πέντε προσπάθειες πρωτού η συσκευή κλειδώσει. Το χειρότερο είναι ότι τα πιο περίπλοκα μοτίβα εκεί έξω είναι ακόμα πιο εύκολο να σπάσουν από τα πιο απλά.

Για να αποδείξουν την έρευνά τους, οι ερευνητές βιντεοσκόπησαν κρυφά 120 συμμετέχοντες τη στιγμή που ξεκλείδωναν το smartphone τους σε δημόσιο χώρο. Στη συνέχεια χρησιμοποιώντας τον αλγόριθμο δακτυλικών αποτυπωμάτων παρακολούθησαν τις κινήσεις του ιδιοκτήτη σε σχέση με τη θέση της συσκευής και μέσα σε δευτερόλεπτα ο αλγόριθμος έδειξε πιθανά πρότυπα που θα μπορούσαν να ξεκλειδώσουν το smartphone ή το tablet.

Τα αποτελέσματα ήταν σε θέση να πάρει ακριβή αποτελέσματα από το βίντεο μέχρι δυόμισι μέτρα μακριά. Επίσης, λειτουργεί αξιόπιστα με σκηνές που καταγράφονται σε μια ψηφιακή φωτογραφική μηχανή SLR σε αποστάσεις μέχρι και εννέα μέτρα μακριά.

Τέλος, η μελέτη αντικρούει επίσης την ιδέα ότι χρησιμοποιώντας ένα πολύπλοκο μοτίβο με περισσότερο πολύπλοκο σχήμα είναι πιο ασφαλές. Στην πραγματικότητα, οι ερευνητές διαπίστωσαν ότι τα πιο πολύπλοκα σχήματα είναι πιο εύκολο να σπάσουν.

«Σε αντίθεση με την αντίληψη πολλών ανθρώπων ότι τα πιο πολύπλοκα σχήματα παρέχουν καλύτερη προστασία, η πεποίθηση αυτή κάνει στην πραγματικότητα τα πιο πολύπλοκα σχήματα πιο εύκολο να σπάσουν και έτσι μπορεί να είναι πιο ασφαλές να χρησιμοποιούμε μικρότερα, απλούστερα πρότυπα».

Οι ερευνητές προτείνουν ότι η χρήση μικρότερων και απλούστερων μοτίβων είναι πολύ καλύτερη. Εκτός από αυτό, οι ερευνητές προτείνουν επίσης στους χρήστες να καλύπτουν πλήρως τα δάχτυλά τους κατά το σχεδιασμό των μοτίβων τους. Πιστεύουν επίσης ότι οι διακυμάνσεις στο χρώμα και τη φωτεινότητα θα μπορούσαν ενδεχομένως να μπερδέψουν τις κάμερες που χρησιμοποιούνται από χάκερ. Επίσης, μπορούν να χρησιμοποιηθούν και άλλα μέτρα ασφαλείας.

Πηγή: Secnews.gr