8 Φεβρουαρίου 2018

Εφαρμογές για κινητά μπορεί να «προδίδουν» προσωπικά δεδομένα

/ Επιστήμες, Τέχνες & Πολιτισμός

Οκτώ στις δέκα κινητές εφαρμογές για θέματα υγείας (mobile health apps) μεταδίδουν σε τρίτες εταιρείες ευαίσθητα στοιχεία σχετικά με την υγεία των -ανυποψίαστων- χρηστών.

Μάλιστα, μόνο οι μισές το κάνουν αυτό μέσω ασφαλούς διαδικτυακής σύνδεσης, με αποτέλεσμα να δημιουργούν και κινδύνους κυβερνο-ασφάλειας, εκτός από την παραβίαση της ιδιωτικότητας εκατομμυρίων χρηστών.

Αυτό διαπίστωσε μια έρευνα Ελλήνων και Ισπανών ερευνητών, οι οποίοι αξιολόγησαν σε βάθος τις 20 δημοφιλέστερες εφαρμογές υγείας για «έξυπνα» κινητά τηλέφωνα και άλλες κινητές συσκευές με λειτουργικό Android, που οι χρήστες μπορούν να «κατεβάσουν» δωρεάν μέσω του Google Play.

Για κάθε μία από τις εφαρμογές έχουν γίνει 100.000 έως ένα εκατομμύριο downloads, ενώ η βαθμολογία από άλλους χρήστες είναι τουλάχιστον 3,5/5.

Οι κινητές αυτές εφαρμογές διαχειρίζονται, παρακολουθούν και αποθηκεύουν διάφορα βιοϊατρικά στοιχεία των χρηστών, σχετικά με τη γενικότερη κατάσταση της υγείας τους, συγκεκριμένες παθήσεις και ιατρικά ραντεβού.

Αυτό που τέθηκε επί τάπητος από τη νέα μελέτη, η οποία διήρκεσε από τον Ιανουάριο 2016 έως τον Αύγουστιο 2017, είναι κατά πόσο αυτά τα προσωπικά δεδομένα παραμένουν μόνο στη συσκευή.

Όπως υπογραμμίζουν οι ερευνητές, το «ανησυχητικό συμπέρασμα» είναι ότι στην πραγματικότητα οι περισσότερες εφαρμογές (το 80%) προχωρούν σε ανάρμοστη και ανεξέλεγκτη χρήση αυτών των στοιχείων, αποκαλύπτοντάς ευαίσθητα δεδομένα σε τρίτα μέρη, χωρίς γνώση ή συναίνεση του χρήστη.

Πέντε ερευνητές του Τμήματος Πληροφορικής του Πανεπιστημίου του Πειραιά, οι Κώστας Πατσάκης (επίκουρος καθηγητής – υπεύθυνος της έρευνας), Αχιλλέας Παπαγεωργίου, Μιχαήλ Στρίγκος, Ευγενία Πολίτου και Ευθύμιος Αλέπης, καθώς και ο Αγκούστι Σολάνας του Πανεπιστημίου Ροβίρα ι Βιργίλι της Ταραγόνα, που έκαναν τη σχετική δημοσίευση στο περιοδικό «IEEE Access» για θέματα ηλεκτρονικών εφαρμογών, διαπίστωσαν ότι μόνο το 20% των εφαρμογών αποθηκεύουν τα δεδομένα υγείας μόνο στα smartphones και στις άλλες συσκευές των χρηστών.

Οι μισές εφαρμογές που εξετάσθηκαν, μοιράζονται με τρίτα μέρη, τόσο δεδομένα κειμένου όσο και πολυμέσων, όπως εικόνες από ακτινογραφίες. Το 50% των εφαρμογών δεν χρησιμοποποιούν ασφαλή κρυπτογραφημένη online σύνδεση (HTTPS), με αποτέλεσμα τα δεδομένα των χρηστών να είναι εύκολα προσβάσιμα από άλλους. Αυτό, πέρα από τα προσωπικά στοιχεία για την υγεία, αφορά και τους κωδικούς ασφαλείας της συσκευής (passwords) ή τις αποθηκευμένες φωτογραφίες των χρηστών.

Μερικές εφαρμογές υγείας, όταν εγκαθίστανται στη συσκευή του χρήστη, απαιτούν πρόσβαση σε στοιχεία γεωεντοπισμού της θέσης του, στο μικρόφωνο, στην κάμερα, στον κατάλογο επαφών, στην εξωτερική κάρτα αποθήκευσης δεδομένων και στο bluetooth, παρόλο που τέτοια δικαιώματα δεν είναι απαραίτητα για να λειτουργήσει σωστά η εφαρμογή.

«Υποστηρίζουμε σαφώς τη χρήση κινητών εφαρμογών υγείας, αλλά οι χρήστες πρέπει να γνωρίζουν ότι η δημοφιλία των εφαρμογών δεν διασφαλίζει την ιδιωτικότητα και την ασφάλεια. Οι άνθρωποι πρέπει να είναι ενήμεροι για τους κινδύνους που αντιμετωπίζουν», επεσήμαναν οι ερευνητές.

Έκαναν επίσης γνωστό ότι, αφότου ενημέρωσαν τους δημιουργούς των εφαρμογών για τα ευρήματα της έρευνάς τους, σε κάποιες περιπτώσεις ορισμένα ζητήματα διορθώθηκαν, όπως η ανασφαλής μετάδοση των δεδομένων.

Όμως, αναφέρει το Αθηναικό Πρακτορείο, το σημαντικότερο θέμα, η διαρροή των προσωπικών ιατρικών δεδομένων σε τρίτους, δεν αντιμετωπίσθηκε καθόλου.

Η μελέτη έγινε στο πλαίσιο του ευρωπαϊκού δικτύου CRYPTACUS, το οποίο -με χρηματοδότηση από την ΕΕ- αποσκοπεί στο να αναπτύξει καλύτερες λύσεις για την online ασφάλεια των Ευρωπαίων πολιτών.

Πηγή: real.gr