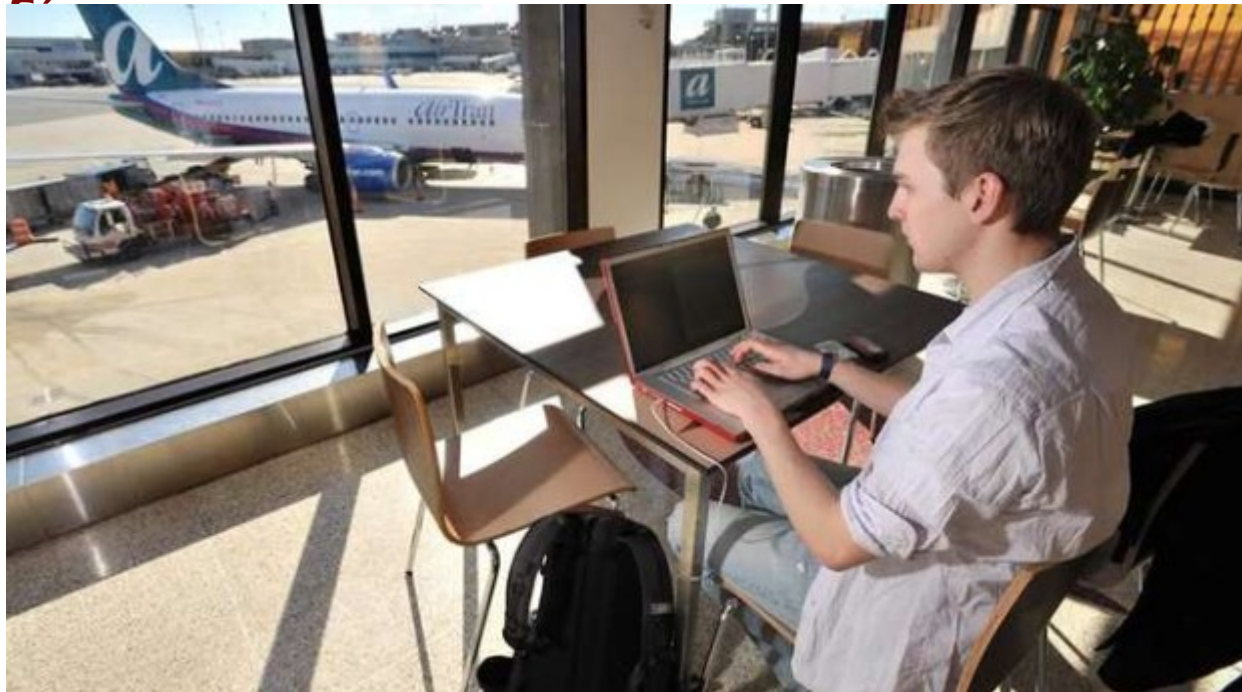


Γιατί πρέπει να αποφεύγουμε τα ανοικτά WiFi



κωδικοί παρέχουν προστασία

Πιο συχνά τους καλοκαιρινούς μήνες, όταν είμαστε μακριά από το σπίτι ή τον χώρο εργασίας, αναζητούμε ένα WiFi δίκτυο για να συνδεθούμε ασύρματα στο Internet και να έχουμε πρόσβαση σε online υπηρεσίες μέσω φορητών συσκευών.

Η αναζήτηση ελεύθερων, ανοικτών, χωρίς την προστασία κωδικού WiFi hotspots εξελίσσεται σε ένα ιδιότυπο σαφάρι, το οποίο όμως κρύβει κινδύνους, όπως προειδοποιούν οι ειδικοί σε θέματα ψηφιακής ασφάλειας.

Αν χρειάζεται οπωσδήποτε να γίνει χρήση ευαίσθητων πληροφοριών, οι χρήστες θα πρέπει να χρησιμοποιούν ασφαλή σύνδεσης, τονίζουν οι αναλυτές της Kaspersky Lab. Γενικά, είναι καλό να αποφεύγεται η χρήση δημόσιων δικτύων WiFi, ειδικά αν εν είναι προστατευμένα με κωδικό πρόσβασης, καθώς οι χάκερ μπορούν να στήσουν WiFi hotspots σε δημόσιους χώρους (όπως αεροδρόμια), ώστε να υποκλέψουν δεδομένα -παρέχοντας την ίδια στιγμή στα θύματά τους πρόσβαση στο Internet.

Συχνά, τα hotspots αυτά έχουν κάποιο όνομα που μοιάζει να ανήκει σε επίσημο φορέα ή μοιάζει με την ονομασία ενός παρακείμενου εστιατορίου, καταστήματος

κοκ. Για το λόγο αυτό, είναι χρήσιμο να επιβεβαιώνεται κάθε φορά το ακριβές όνομα της πραγματικής υπηρεσίας WiFi. Επιπλέον, συνιστάται η χρήση δικτύων που προστατεύονται με κωδικό.

Ακόμη και αν ο κωδικός του WiFi είναι ελεύθερα διαθέσιμος σε όλους, εξακολουθεί να παρέχει προστασία. Αυτό συμβαίνει γιατί αυτός ο κοινός κωδικός χρησιμοποιείται για να παράγει μοναδικά κλειδιά για κάθε χρήστη, έτσι ώστε τα δεδομένα των χρηστών να μη μπορούν να αποκρυπτογραφηθούν από οποιονδήποτε άλλον, ακόμα και αν ξέρει τον κωδικό του WiFi.

Πηγή: protothema.gr