

6 Ιουλίου 2018

Αυτά είναι τα πέντε πράγματα που πρέπει να κάνετε πριν φύγετε για διακοπές

/ [Επιστήμες, Τέχνες & Πολιτισμός](#)





Οι διακοπές αποτελούν την ιδανική ευκαιρία χαλάρωσης, αλλά ακόμη και τότε δεν πρέπει να αμελούμε την κυβερνοασφάλεια, καθώς όταν βρισκόμαστε εκτός του γνωστού μας ψηφιακού περιβάλλοντος μπορεί να εκτεθούμε σε απρόβλεπτες απειλές. Για να μη βρεθούμε στη δυσάρεστη θέση να χαλάσουμε τις διακοπές μας εξαιτίας ενός πιθανού περιστατικού στον κυβερνοχώρο, μπορούμε να εφαρμόσουμε τις παρακάτω πέντε συμβουλές της ESET.

1. **Όσο πιο λίγα gadget, τόσο το καλύτερο.** Προσπαθήστε στις φετινές διακοπές να γίνετε ένας «ψηφιακός μινιμαλιστής», παίρνοντας μαζί σας μόνο τις βασικές και απολύτως απαραίτητες συσκευές και αφήνοντας τις υπόλοιπες στο σπίτι ή το γραφείο. Όσο πιο λίγες έχετε μαζί σας, τόσο περισσότερο μειώνετε τις πιθανότητες να θέσετε σε κίνδυνο τις συσκευές, τις πληροφορίες και τα δεδομένα σας. Εξετάστε επίσης το ενδεχόμενο ειδικά για τις διακοπές να χρησιμοποιήσετε μία προσωρινή συσκευή με αποθηκευμένα όσο το δυνατόν λιγότερα προσωπικά στοιχεία.
2. **Λογισμικό και εφαρμογές που δουλεύουν.** Βεβαιωθείτε ότι το λειτουργικό σύστημα και οι εφαρμογές είναι ενημερωμένες με τις πιο πρόσφατες επιδιορθώσεις. Μην αμελήσετε να εγκαταστήσετε ενημερώσεις,

ειδικά τις σημαντικότερες, για να μην βρεθείτε εκτεθειμένοι ή για να μην αναγκαστείτε να βασιστείτε σε μια αναξιόπιστη, μη ασφαλή δημόσια σύνδεση Wi-Fi ή στα δεδομένα σας. Συστήνεται επίσης η απενεργοποίηση παλιού και αχρησιμοποίητου λογισμικού και η απενεργοποίηση λογαριασμών που δεν χρησιμοποιούνται πλέον. Τέλος, βεβαιωθείτε ότι χρησιμοποιείτε αξιόπιστο λογισμικό προστασίας από κακόβουλο λογισμικό, το οποίο επίσης είναι ενημερωμένο.

3. **Δυσκολέψτε τη ζωή των κυβερνοεγκληματιών.** Ενισχύστε την άμυνα των συσκευών σας όσο μπορείτε χρησιμοποιώντας ισχυρούς και μοναδικούς κωδικούς πρόσβασης, φράσεις πρόσβασης, κωδικούς PIN ή μια από τις διαθέσιμες μεθόδους βιομετρικού ελέγχου ταυτότητας, όπως σάρωση δακτυλικών αποτυπωμάτων ή αναγνώριση προσώπου. Ρυθμίστε επίσης τη συσκευή να κλειδώνει αυτόματα την οθόνη της, όσο είναι αδρανής. Οι πιθανότητες να πέσουν τα δεδομένα σας σε λάθος χέρια μπορούν να μειωθούν σημαντικά με την κρυπτογράφηση, μία λειτουργία που, ανάλογα με τη συσκευή, μπορεί να προσφέρεται ως ενσωματωμένη λύση (αν και όχι απαραίτητα ενεργοποιημένη) είτε ως λογισμικό τρίτου κατασκευαστή. Τέλος, ενεργοποιήστε τη λειτουργία προστασίας από την κλοπή, που σας επιτρέπει να παρακολουθείτε τη συσκευή σας ακόμη και από απόσταση και να διαγράψετε όλο το περιεχόμενό της.
4. **Μη ξεχνάτε το back up.** Η απώλεια των προσωπικών δεδομένων που είναι αποθηκευμένα σε ένα φορητό υπολογιστή ή ένα smartphone μπορεί να είναι σημαντικότερη από την απώλεια της συσκευής. Αυτός είναι ο λόγος για τον οποίο τα αντίγραφα ασφαλείας μπορεί να φανούν ιδιαίτερα χρήσιμα ακόμη και αν μία συσκευή παραβιαστεί, χαθεί ή κλαπεί. Με τα κρυπτογραφημένα αντίγραφα ασφαλείας των δεδομένων που έχετε αποθηκεύσει σε μια ασφαλή τοποθεσία εκτός σύνδεσης, μπορείτε επίσης να γλιτώσετε από τις αρνητικές συνέπειες μιας μόλυνσης από malware, μίας επίθεσης ransomware ή, ακόμη και εξαιτίας μιας απλής δυσλειτουργίας της συσκευής.
5. **Και τέλος, προσοχή και μετριοπάθεια.** Με απλά λόγια, καλό θα ήταν να αποφύγετε να ανακοινώσετε σε όλα τα social media ότι εσείς και η οικογένειά σας θα είστε μακριά από το σπίτι για διακοπές. Ο πειρασμός να το μοιραστείτε μπορεί να μεγάλος, αλλά σκεφτείτε ότι μπορεί να σας εκθέσει σε μια φυσική εισβολή στο σπίτι σας, η οποία μπορεί να θέσει σε κίνδυνο πολλά περισσότερα τις συσκευές και τα αντίγραφα ασφαλείας σας. Τα όρια μεταξύ εικονικών και πραγματικών κόσμων μπορεί να είναι πολύ θολά και ακόμη και οι φαινομενικά αβλαβείς ψηφιακές ενέργειες μπορεί να έχουν υπερβολική σημαντικές επιδράσεις στην πραγματική ζωή.

Πηγή: techgear.gr