26 Οκτωβρίου 2022

Χρειάζεται ή όχι να καλύψουμε τον φακό της κάμερας του φορητού υπολογιστή μας για προστασία

/ Γενικά Θέματα

Οι ειδικοί σε θέματα ασφάλειας της τεχνολογίας εξετάζουν πόσο χρήσιμο είναι ένα κάλυμμα κάμερας ενάντια σε έναν χάκερ.

Εάν είμαστε παρανοϊκοί σχετικά με το τι οπτική πρόσβαση μπορούν να έχουν, ενώ δεν πρέπει, οι άνθρωποι σε σχέση με εμάς όταν δουλεύουμε, μπορεί να αναρωτιόμαστε αν χρειαζόμαστε ένα φυσικό κάλυμμα κάμερας πάνω από τον φακό του υπολογιστή μας.

Αρκετά δημόσια πρόσωπα υψηλού προφίλ είναι γνωστό ότι χρησιμοποιούν καλύμματα κάμερας… Ο πρώην διευθυντής του FBI Τζέιμς Κόμεϊ είπε στο NPR ότι έχει χρησιμοποιήσει κάτι τέτοιο. Σε μια φωτογραφία του 2016 που δημοσιεύτηκε στον λογαριασμό του στο Facebook, ο διευθύνων σύμβουλος της Meta Μαρκ Ζούκερμπεργκ φαινόταν να χρησιμοποιεί ένα sticker στην κάμερα του φορητού υπολογιστή του. Θα πρέπει να κάνουμε το ίδιο;

Να τι πιστεύουν οι ειδικοί σε σχέση με το πόσο χρήσιμο μπορεί να είναι ένα ειδικό

κάλυμμα κάμερας.
Δεν υπάρχουν πολλοί νόμιμοι λόγοι ασφαλείας για την ανάγκη κάλυψης, αλλά οι ειδικοί λένε ότι δεν μπορεί να μας βλάψει
Εάν ανησυχούμε μήπως αφήνουμε κατά λάθος ενεργοποιημένη τη βιντεοκάμερά ας, ένα ειδικό κάλυμμα κάμερας θα μπορούσε να «απαλύνει» τις ανησυχίες μας. Ο Τζόναθαν Γιανγκ, αναπληρωτής αντιπρόεδρος του Vantage Technology Consulting Group, χρησιμοποιεί ειδικά καλύμματα κάμερας υπολογιστή για αυτόν τον λόγο.
«Τα ειδικά καλύμματα κάμερας είναι χρήσιμα κυρίως επειδή οι άνθρωποι μερικές φορές ενεργοποιούν ή αφήνουν τις κάμερές τους ενεργοποιημένες ακούσια», λέει. «Ή, οι άνθρωποι έχουν πολλές κάμερες –– κάμερα φορητού υπολογιστή και αυτόνομη κάμερα σε εξωτερική οθόνη –– και η λανθασμένη προεπιλογή μπορεί να εμφανιστεί και να μεταδώσει πληροφορίες εργασίας ή μια ενοχλητική ή αλλιώς ακατάλληλη προβολή (προσώπου). Χρησιμοποιώ καλύμματα κάμερας στις συσκευές μου για αυτούς τους λόγους».

Πέρα από το να γλιτώσουμε τον εαυτό μας από πιθανή αμηχανία, υπάρχουν και σημαντικοί λόγοι ασφαλείας για να το κάνουμε, λέει ο Μάικλ Κόβινγκτον, αντιπρόεδρος στρατηγικής χαρτοφυλακίου στο JAMF, μια πλατφόρμα διαχείρισης συσκευών της Apple.

«Ένα φυσικό κάλυμμα κάμερας είναι το τελευταίο επίπεδο ασφαλείας που διασφαλίζει ότι ο χρήστης διατηρεί τον έλεγχο του πότε εμφανίζεται στην κάμερα, ειδικά όταν συμβαίνει κάποιο από τα ακόλουθα σενάρια: Η η κάμερα της συσκευής μπορεί να ενεργοποιηθεί κατά λάθος λόγω σφάλματος του λογισμικού. Η οι προγραμματιστές εφαρμογών μπορεί να έχουν κακόβουλη πρόθεση και να δημιουργήσουν εφαρμογές για να καταγράφουν ή να κλέβουν δεδομένα μέσω της άδειας (να λειτουργεί) η κάμερα», λέει ο ίδιος.

Εάν το τελευταίο ζήτημα είναι αυτό που μας απασχολεί περισσότερο – ότι οι χάκερ ψάχνουν στο σπίτι μας μέσω του υπολογιστή μας – τότε ίσως δεν χρειάζεται να ανησυχούμε τόσο πολύ, σύμφωνα με τον Νάιζτελ Ανταμς, ιδιοκτήτη της Nizel Corp, μιας εταιρείας συμβούλων τεχνολογίας πληροφοριών στο Σικάγο.

«Καταλαβαίνω την παράνοια. Σε κανέναν δεν αρέσει να νιώθει ευάλωτος», λέει ο Άνταμς. «Αλλά αν λαμβάνουμε προληπτικά μέτρα, οι πιθανότητες να χακαριστεί κάποιος ή κάποιος να μας παρακολουθεί στην κάμερά μας είναι από ελάχιστες ως μηδαμινές»...

Ακόμα κι αν ένας χάκερ γνωρίζει τον κωδικό πρόσβασης του υπολογιστή μας, ο ίδιος λέει ότι θα πρέπει επίσης να έχει πρόσβαση σε πολλές πρόσθετες πληροφορίες σχετικά με τον υπολογιστή μας για να εισβάλει στην οθόνη μας,

όπως η εξωτερική διεύθυνση IP του δικτύου στο οποίο βρίσκεται η συσκευή, η ακριβή διεύθυνση IP ή το όνομα του υπολογιστή και έναν αριθμό θύρας που είναι ανοιχτή και έχει οριστεί για απομακρυσμένη πρόσβαση.

Δεδομένου ότι πολλά συστήματα υπολογιστών απενεργοποιούν αυτόματα αυτή τη δυνατότητα απομακρυσμένης πρόσβασης από προεπιλογή, ένας χάκερ θα πρέπει επίσης να μας εξαπατήσει ώστε να εγκαταστήσουμε λογισμικό για να αποκτήσουμε πρόσβαση, λέει ο Άνταμς.

Η δεύτερη ανησυχία που έχει ο Άνταμς από τους ανθρώπους είναι ότι ένας επαγγελματίας πληροφορικής μπορεί να είναι αυτός που θα κάνει το ατόπημα να ρίξει μια ματιά στην οθόνη ενός υπαλλήλου. Ωστόσο, σημειώνει ότι οι υπάλληλοι πληροφορικής συνήθως έχουν όλες τις ενέργειές τους καταγεγραμμένες σε ένα ασφαλές σύστημα που θα έκρουε τον κώδωνα του κινδύνου εάν κάποιος προσπαθούσε να αποκτήσει πρόσβαση στη βιντεοκάμερα άλλου ατόμου.

Επιπλέον, «στα 20 και πλέον χρόνια που εργάζομαι στην επιχείρηση, γνωρίζω ότι η συντριπτική πλειονότητα των IT δεν έχουν ιδέα πώς να έχουν άμεση πρόσβαση στην κάμερα κάποιου από απόσταση», ειδικά όχι μ΄ έναν τρόπο που σημαίνει ότι το φως της κάμερας θα άναβε και δεν θα το έβλεπες, λέει.

«Τα φίλτρα που αποκλείουν την κάμερα, δεν είναι χρήσιμα όσον αφορά την ιδιωτικότητα, αλλά έχουν κάποια μικρή χρησιμότητα ως κάλυμμα για τον φακό», προσθέτει ο Ανταμς.
Υπάρχουν μερικοί άλλοι τρόποι με τους οποίους μπορούμε να διατηρήσουμε τα βίντεό μας όσο το δυνατόν πιο ιδιωτικά, πέρα από τη χρήση καλύμματος οθόνης

Ας ελέγξουμε ξανά ότι το βίντεό μας δεν είναι ενεργοποιημένο πριν και μετά από κάθε συνάντηση.

Ας έχουμε το νου μας τι φόντο έχουμε κατά την διάρκεια των ψηφιακών μας συναντήσεων

Ας απεγκαταστήσουμε εφαρμογές που δεν χρησιμοποιούμε συνήθως κι ας διπλοτσεκάρουμε ποιες έχουν πρόσβαση στην κάμερά μας

Ας μην ανοίγουμε mail από ανθρώπους που δεν γνωρίζουμε

Ας μην χρησιμοποιούμε απλούς κωδικούς

Πηγή: huffingtonpost.gr