

OUCH!

Ikmēneša informācijas drošības izdevums tev

## Labākie kiberdrošības padomi brīvdienām

### Pārskats

Tuvojoties svētku sezonai, miljoniem cilvēku dosies ceļojumos. Ja esat viens no viņiem, lūk, daži padomi, ko ņemt vērā par kiberdrošību.

- **Mobilās ierīces:** Ņemiet līdzi pēc iespējas mazāk ierīču. Jo mazāk ierīču ņemat līdzi ceļojumā, jo mazāk ierīču var tikt pazaudētas vai nozagtas. Bet vai zinājat, ka ir daudz lielāka iespēja pazaudēt mobilo ierīci nekā tai tikt nozagtai? Izejot no viesnīcas numura, restorāna, izkāpjot no taksometra, vilciena vai lidmašīnas, ātri pārbaudiet savas ierīces un pārliecinieties, ka nekā netrūkst. Atgādiniet draugiem vai ģimenei, kas ceļo ar jums, par tām un pārliecināties, ka viņiem ir savas ierīces, jo, piemēram, bērni mēdz mobilās ierīces atstāt uz sēdekļiem vai restorānā.

Attiecībā uz ierīcēm, kuras izvēlaties ņemt līdzi, pārliecinieties, vai tās ir atjauninātas un tajās ir jaunākā operētājsistēma un lietotnes. Izmantojiet ekrāna bloķēšanas funkciju. Ja iespējams, nodrošiniet iespēju attālināti izsekot ierīces, ja tās tiek pazaudētas. Turklāt, iespējams, var noderēt iespēja attālināti formatēt ierīci. Tādējādi ierīces nozaudēšanas vai zādzības gadījumā varat attālināti izsekot un/vai izdzēst visus sensitīvos datus un kontus no ierīces. Visbeidzot izveidojiet rezerves kopiju visām ierīcēm, ko ņemat līdzi, lai pazaudēšanas vai zādzības gadījumā varētu viegli atjaunot datus.

- **Wi-Fi savienojumi:** Ceļojot var būt nepieciešams izveidot savienojumu ar publisku Wi-Fi tīklu. Paturiet prātā, ka bieži vien nezināt, kas šo Wi-Fi tīklu ir konfigurējis, kas un kā to uzrauga un kurš vēl tam ir pieslēdzies. Tā vietā, lai pieslēgtos publiskam Wi-Fi tīklam, kad vien iespējams, izmantojiet iespēju izveidot savienojumu ar viedtālruņa mobilo tīklāju. Šādi jūs zināsiet, ka ir izveidots uzticams Wi-Fi savienojums. Ja tas nav iespējams un ir nepieciešams izveidot savienojumu ar publisku Wi-Fi tīklu (piemēram, lidostā, viesnīcā vai kafejnīcā), izmantojiet virtuālo privāto tīklu, ko bieži sauc par VPN. Tā ir programmatūra, ko iespējams instalēt savā klēpj datorā vai mobilajās ierīcēs, lai palīdzētu aizsargāt un anonimizēt Wi-Fi savienojumu. Daži VPN risinājumi ietver iestatījumus, lai automātiski iespējotu VPN, pieslēdzoties neuzticamiem Wi-Fi tīkliem.
- **Publiskās lietošanas datori:** Izvairieties no publiski pieejamu datoru, kas pieejami, piemēram, viesnīcu vestibilos vai kafejnīcās, izmantošanas, lai piekļūtu saviem kontiem vai citai sensitīvai informācijai. Jūs nezināt, kas šo datoru izmantojis pirms jums, un, iespējams, tas ir nejauši vai apzināti inficēts ar ļaunatūru, piemēram, taustiņu reģistrētāju. Izmantojiet tikai uzticamas ierīces, kuras kontrolējat pats.

- **Sociālie tīkli:** Mums patīk informēt citus par saviem ceļojumiem un piedzīvojumiem, izmantojot sociālos tīklus, taču ne vienmēr zinām, kas ir katrs tiešsaistes draugs vai skatītājs. Atvaļinājuma laikā pēc iespējas izvairieties no pārlietu detalizētas informācijas koplietošanas un apsveriet iespēju veidot publikācijas par ceļojumu tikai, atgriežoties mājās. Turklāt npublicējiet iekāpšanas karšu, autovadītāja apliecību vai pasu attēlus, jo tas var rezultēties ar identitātes zādzību.
- **Darbs:** Ja atvaļinājuma laikā strādāsiet (ceram, ka ne!), iepriekš pārliecinieties, kādi ir jūsu darba ceļojumu noteikumi, tostarp kādas ierīces vai datus varat ceļojumā varat izmantot un kā droši attālināti pieslēgties darba sistēmām.

Atvaļinājumam ir jābūt atpūtas, izpētes un izklaides laikam. Šie vienkāršie soļi palīdzēs izplānot drošu un neapdraudētu ceļojumu.

## Viesredaktors

Princesa Janga (Princess Young) ir Southwest Airlines vecākā analītiķe un vada kiberdrošības izglītības un apmācības pasākumus 60 000 darbiniekiem visā valstī. Princesai patīk sadarboties ar darbiniekiem, lai viņi neatkarīgi no sava amata vai nodarbošanās varētu justies pilnvaroti uzņemties līdztbildību par kiberdrošību.



## Resursi

**Mobilo ierīču aizsargāšana:** <https://www.sans.org/newsletters/ouch/securing-mobile-devices/>

**Atjauninājumu nozīme:** <https://www.sans.org/newsletters/ouch/the-power-of-updating/>

**Virtualie privātie tīkli:** <https://www.sans.org/newsletters/ouch/Virtual-Private-Networks/>

**Tālrūņa rezerves kopija:** <https://www.sans.org/newsletters/ouch/got-backups/>

**Tulkojums:** CERT.LV

OUCH! izdod SANS institūts programmas "Security Awareness" ietvaros un tas tiek izplatīts saskaņā ar [Creative Commons BY-NC-ND 4.0 licences nosacījumiem](https://creativecommons.org/licenses/by-nc-nd/4.0/). Jūs varat brīvi dalīties ar šo biļetenu vai izplatīt, kamēr jūs to nepārdodat un nepārveidojat. Redakcijas kolēģija Valters Skrivenšs (Walter Scrivens), Fils Hofmans (Phil Hoffman), Alans Vagoners (Alan Waggoner), Leslija Rīdauta (Leslie Ridout), Princesa Janga (Princess Young).

