Ikmēneša informācijas drošības biļetens ikvienam

OUCH!

ŠAJĀ NUMMURĀ …

Drošība ceļojot

Pārskats

Mēs visi gribam iespēju izmantot tehnoloģijas jebkurā laikā, tajā skaitā ceļojumā. Šajā izdevumā mēs aplūkosim, kā droši pieslēgties internetam un izmantot ierīces ceļojot.

Viesredaktors

Mark Williams ir BlueCross Blueshield uzņēmumu drošības arhitekts Tenesijā. Viņš ir arī SANS pasniedzējs un ISSA Chattanooga nodaļas prezidents. Viņš ir daudz ceļojis un izprot problēmas, kas saistītas ar tehnikas izmantošanu ceļojumā.

Sagatavošanās

Jūsu mājas tīkls var būt ir drošs, taču ceļojuma laikā labāk uzskatiet, ka visi tīkli, kam jūs pieslēdzaties, ir nedroši. Jūs nevarat zināt, kas vēl ir šajā tīklā un kas tiek darīts. Zemāk ir daži vienkārši principi, kā aizsargāt sevi un savus datus ceļojuma laikā.

- Drošākā ir informācija, kas jums nav līdzi. Saprotiet, kādus datus jums nevajag līdzi ceļā, un izdzēsiet tos no ierīcēm. Tādā veidā būtiski samazinās zaudējumi, ja jūsu ierīce pazūd, tiek nozagta, vai tiek aizturēta muitā vai robežapsardzē. Ja ceļojums ir saistīts ar darbu, pavaicājiet priekšniecībai, vai organizācijā ir ierīces, kas ir domātas izmantošanai darba vajadzībām ceļojumā.
- Uzstādiet mobilajām ierīcēm un/vai portatīvajam datoram drošu paroli. Ja tas tiks nozagts, citiem nebūs iespējams piekļūt jūsu informācijai. Papildus uzstādiet pilnu diska šifrēšanu jūsu mobilajās ierīcēs un portatīvajos datoros. Vairumam mobilo ierīču šī funkcija tiek automātiski ieslēgta, ja jūs izmantojat ekrāna bloķēšanu.
- Uzstādiet vai iespējojiet programmu, kas ļauj attālināti noteikt ierīces atrašanās vietu vai pat attālināti izdzēst datus, ja ierīce ir nozagta vai pazaudēta.
- Atjauniniet ierīces aplikācijas un antivīrusa programmas pirms izceļošanas. Daudzi uzbrukumi koncentrējas uz novecojušu programmatūru.
- Veiciet pilnu rezerves kopēšanu ierīcēm. Tādā veidā, ja kaut kas notiek ar tām ceļojuma laikā, jūsu dati būs drošībā.
- Starptautiskajiem ceļojumiem pārliecinieties, kādas ir mobilo pakalpojumu iespējas attiecīgajā valstī. Bieži vien

Drošība ceļojot

starptautiskajai datu pārraidei tiek piemēroti augsti tarifi, tādēļ varbūt labāk atspējojiet mobilo datu pārraidi vai iegādājieties un izmantojiet vietējo priekšapmaksas SIM karti.

Lai ceļojuma laikā būtu drošībā, sagatavojiet ierīces pirms ceļojuma, turiet tās fiziski drošībā un šifrējiet jebkādas tiešsaistes aktivitātes.

Nozaudētas/ Nozagtas ierīces

Ceļojumā nodrošiniet ierīču fizisko drošību. Piemēram, neatstājiet ierīces automašīnā, kur garāmgājēji var tās viegli ieraudzīt, jo noziedznieki var vienkārši izsist automašīnas logu un nozagt visu vērtīgo. Noziedzība, protams, ir risks, tomēr daudz biežāk cilvēki pazaudē ierīces. To apliecina arī nesensVerison pētījums, kurš rāda, ka 100 reiz lielāka iespēja ir pazaudēt ierīci, nekā ka to nozags. Vienmēr pārbaudiet, vai jūsu ierīces joprojām ir pie jums, piemēram, pēc drošības pārbaudēm lidostā, izkāpjot no taksometra vai ejot prom no restorāna, izrakstoties no viesnīcas vai izkāpjot no lidmašīnas. Vienmēr pārbaudiet priekšējā krēsla kabatu lidmašīnā!

Wi-Fi piekļuve

Piekļuve internetam ceļojumā bieži nozīmē publiskā Wi-Fi pieejas punkta izmantošanu, piemēram, viesnīcā, kafejnīcā vai lidostā. Publiskajiem Wi-Fi tīkliem ir divas galvenās problēmas: jūs nezināt, kas tos ir uzstādījis, un jūs nezināt, kas ir pieslēdzies. Tādēļ tie ir jāuzskata par nedrošiem. Tieši tādēļ bija jāveic visas iepriekšminētās darbības pirms ceļojuma sākuma. Bez tam, Wi-Fi izmanto radioviļņus, kas nozīmē, ka jebkurš, kas atrodas jūsu tuvumā, var potenciāli pārtvert un novērot visus savienojumus. Tādēļ, izmantojot publisko Wi-Fi tīklu, pārliecinieties, ka visas jūsu aktivitātes tiešsaistē ir šifrētas. Piemēram, ieejot tīmekļa pārlūkprogrammā, pārbaudiet, vai jūsu apmeklētās interneta vietnes izmanto šifrētu savienojumu. Par to liecinās “https://” un/vai atslēgas attēls URL adreses laukā. Papildu drošībai jūs varat izmantot VPN (Virtuālo privāto tīklu), kas šifrē jūsu tiešsaistes aktivitātes. Šo iespēju jums var nodrošināt darbs, vai jūs varat iegādāties VPN pakalpojumu privātai lietošanai. Ja nav uzticama Wi-Fi tīkla, izmantojiet mobilā telefona datu pieslēgumu. Brīdinājums: kā minēts iepriekš tas var būt dārgi, tādēļ vispirms konsultējieties ar savu mobilo sakaru pakalpojumu sniedzēju.

Drošība ceļojot

Publiskie resursi

No publiski pieejamiem datoriem, piemēram, viesnīcu vestibilos vai interneta kafejnīcās, neejiet savos tiešsaistes kontos un nepiekļūstiet sensitīvai informācijai. Jūs nezināt, kas izmantojis šos datorus pirms jums, tādēļ tie var būt nejauši vai apzināti inficēti. Kad vien iespējams, izmantojiet tikai jūsu kontrolētas un uzticamas ierīces. Publiskos datorus var lietot, piemēram, laika prognozes pārbaudīšanai vai ziņu lasīšanai. Pierakstīšanās kādā no jūsu privātajiem kontiem, piemēram, jūsu Google kontā, var izraisīt interesi hakeros, kas novēro šo publisko datoru.

UZZINIET VAIRĀK

Parakstieties uz OUCH! - ikmēneša biļetenu par informācijas tehnoloģiju drošību datoru lietotājiem, apmeklējiet OUCH! arhīvu, uzziniet vairāk par SANS informācijas tehnoloģiju drošības risinājumiem, apmeklējot tīmekļa vietni securingthehuman.sans.org/ouch/archives.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Resursi

Paroles:	https://securingthehuman.sans.org/ouch/2015#april2015
Rezerves kopijas:	https://securingthehuman.sans.org/ouch/2015#august2015
Ļaunatūra:	https://securingthehuman.sans.org/ouch/2016#march2016
Šifrēšana:	https://securingthehuman.sans.org/ouch/2016#june2016
OUCH Arhīvi/ Tulkojumi:	https://securingthehuman.sans.org/ouch/archives

License

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Tulkojums: Edgars Tauriņš