Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS KIBERNETINIO SAUGUMO ATMINTINĖ KELIAUJANTIEMS

2018 m. birželio 11 d.

Atostogaujant, išmanieji įrenginiai: telefonai, planšetės – o kartais ir nešiojamieji kompiuteriai, keliauja kartu. Kelionėse šie prietaisai patiria daugiau grėsmių nei įprastai, todėl reikėtų pasirūpinti jų saugumu, žinoti pagrindines kylančias grėsmes bei kaip jų išvengti.

Patarimai keliaujantiems, kaip apsaugoti savo prietaisus ir duomenis

Atnaujinimai. Reguliariai atnaujinkite savo prietaisų operacinę sistemą ir naudojamas programas. Prieš išvyką yra tikslinga pasirūpinti, kad turite naujausias versijas, kurios bus labiau apsaugotos nuo įvairių kibernetinių grėsmių.

Fizinė apsauga. Nepamirškite fizinės savo prietaisų apsaugos net trumpam laikui. Įsilaužėliui gali užtekti vos kelių akimirkų, kad patektų į jūsų įrenginį, o viduje saugoma informacija dažnai būna vertingesnė už patį prietaisą.

Užraktai. Naudokite užrakinimo priemones savo įrenginiuose ir nustatykite, kad prietaisas užsirakintų automatiškai, jeigu juo tam tikrą laiką nesinaudojama. Nenaudokite paprastų kodų ar slaptažodžių. Tyrimais nustatyta, kad skaitinis prietaiso atrakinimo būdas yra daug saugesnis už ekrano užrakto šabloną (angl. *lock screen*

Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

pattern). Jeigu yra galimybė, įjunkite biometrines atrakinimo priemones, tokias kaip atrakinimas pirštо antspaudu ar veido atpažinimu.

Viešieji tinklai ir kompiuteriai. Būkite atsargūs naudodamiesi viešai prieinamu bevieliu internetu (angl. *Public Wi-Fi*) bei viešai prieinamais kompiuteriais - nesinaudokite elektroninėmis banko paslaugomis, nepirkite prekių ir venkite interneto svetainių, kuriose reikėtų įvesti kokius nors asmeninius duomenis. Būtinoms operacijoms atlikti būtų saugiau naudotis savo įrenginio mobiliuoju internetu.

> *Naudojantis viešuoju internetu ar kompiuteriu, jūsų duomenys gali būti lengvai nuskaityti, todėl reikėtų atsisakyti betkokių jautrių duomenų naudojimo šiais kanalais. Jeigu atostogų metu vistik naudojotės nesaugiu ryšiu ar prietaisu, grįžę namo būtinai pasikeiskite savo slaptažodžius tose sistemose, prie kurių buvote prisijungę.*

Prietaisų įkrovimas. Būkite atsargūs įkraudami savo prietaisus viešai prieinamais kompiuteriais – apskritai venkite jungti savo įrenginius į viešai prieinamus prietaisus, bet, esant tokiai būtinybei, prijungę savo įrenginį, nustatykite krovimo režimą ir nesuteikite jokios prieigos prie savo duomenų.

Išjunkite Bluetooth. Išjunkite Bluetooth ryšį kuomet jo nenaudojate. Tai sumažins piktavalių galimybes prisijungti prie jūsų prietaiso ir nuskaityti jo duomenis ar išnaudoti kitiems kenkėjiškiems tikslams.

> *Kartais prietaisuose „Bluetooth“ ryšys būna įjungtas automatiškai, dėl to vartotojas gali net nežinoti apie jo įrenginio aktyvų veikimą tokiu režimu, todėl patariame pasitikrinti ir įsitikinti tuo papildomai.*

Klastotės. Natūralu, kad atostogų metu vartotojai būna atsipalaidavę ir šiek tiek išsiblaškę, todėl labiau pažeidžiami įvairioms klastočių (angl. *Phishing*) atakoms. Siekdami apsaugoti savo asmeninius, finansinius ir kitus jautrius duomenis nuo vagystės, visuomet išlikite atidūs ir kritiškai vertinkite gaunamus pranešimus.

Tel. 8 706 82 250
El. p. cert@nksc.lt
https://www.nksc.lt

Svetimos USB laikmenos. Savo įrenginiuose nenaudokite rastų ar iš nepažįstamų asmenų gautų USB laikmenų – piktavaliui tai gali būti lengviausias ir tiesiausias kelias prieiti prie jūsų duomenų. Geriausia naudoti tik savo USB laikmenas, kadangi žalinga programinė įranga šiuo keliu plinta lengviausiai – net jei tai giminių ar draugų laikmena, jūs negalite būti tikri, kad ji saugi.

> *„Pamestos“ USB laikmenos gali būti specialiai paliktos tam, kad ją radęs asmuo įsidėtų į kompiuterį ir tokiu būdu suteiktų piktavaliui prieigą prie savo prietaiso.*

VPN paslaugos. Atostogų metu savo įrenginiuose naudokite virtualaus privataus tinklo (angl. *VPN*) paslaugas. Tokiu būdu ryšys bus šifruojamas, dėl ko piktavaliai negalės nuskaityti jūsų duomenų, tad galėsite saugiai naudotis visomis jums reikalingomis interneto paslaugomis net ir viešai prieinamuose tinkluose.

Duomenų kopijos. Apsaugokite savo duomenis nuo praradimo sukurdami atsargines duomenų kopijas (angl. *Backup*). Laikykite šias duomenų kopijas atskiruose įrenginiuose – pavyzdžiui išoriniame diske ar debesinėje duomenų saugykloje. Duomenų kopijos neapsaugos jūsų nuo duomenų vagystės ir dėl to kylančių pasekmių, bet svarbių duomenų praradimo atveju (kuomet duomenys užšifruojami ar sunaikinami), juos galima bus atstatyti ar atgauti.