REKOMENDACIJA
DĖL SAUGAUS NARŠYMO INTERNETE

2024-12-30

Daugumos iš mūsų kasdienis gyvenimas vienaip ar kitaip susijęs su internetu: internete mes dirbame, mokomės ir bendraujame su draugais. Didėjant interneto paskyrų ir prijungtų įrenginių skaičiui, didėja ir nusikaltėlių galimybės.

Todėl svarbu žinoti interneto saugumo taisykles – jos padės apsaugoti jūsų duomenis ir įrenginius nuo grėsmių.

PAGRINDINIAI INTERNETO PAVOJAI

Interneto vartotojai susiduria su įvairiomis potencialiomis grėsmėmis, apie kurias dažnai net neįtaria. Kibernetiniai nusikaltėliai nuolat kuria naujus būdus, kaip apgauti interneto vartotojus. Štai keletas interneto grėsmių, su kuriomis interneto vartotojai dažnai susiduria: asmens duomenų vagystės, duomenų nutekėjimas, kenksmingos programos ir virusai, apgavystės ir sukčiavimo elektroniniai laiškai, netikros svetainės, nepageidaujamas turinys, kibernetinės patyčios, netinkami privatumo nustatymai ir kt. Norėdami išvengti arba sumažinti interneto pavojų, turėtumėte laikytis toliau pateikiamų rekomendacijų ir taisyklių.

PAGRINDINĖS SAUGAUS ELGESIO INTERNETE TAISYKLĖS

Stebėkite, kokias nuorodas spaudžiate	Vienas neatsargus nuorodos paspaudimas – ir jūsų asmens duomenys pateks į nusikaltėlių rankas arba įrenginys bus užkrėstas kenkėjiška programa. Todėl svarbu stebėti, kokias nuorodas spaudžiate, ir vengti tam tikro turinio: nuorodų iš nepatikimų šaltinių, šlamšto pranešimų, internetinių viktorinų, paspaudimų provokuojančių antraščių (angl. *Clickbait*), „nemokamų“ pasiūlymų ir nepageidaujamos reklamos. Gavus el. laišką, dėl kurio autentiškumo abejojate, nespauskite jo nuorodų ir neatidarykite priedų. Jei nesate tikri dėl el. laiško autentiškumo, susisiekite tiesiogiai su siuntėju. Pavyzdžiui, gavę įtartiną laišką neva iš savo banko, paskambinkite į banką ir paklauskite, ar laiškas tikrai yra jų. Naršydami svetainėje įsitikinkite, kad perėjimas per nuorodas vyksta į susijusį turinį. Pavyzdžiui, jei pereinate per nuorodą į aprašymą apie safarį Afrikoje, bet vietoj to patenkate į paspaudimus provokuojančių antraščių svetainę apie tai, kaip sulieknėjo įžymybės, arba į straipsnį su antrašte „Kur jie dabar?“, nedelsdami palikite šią svetainę.

Naudokite patikimus slaptažodžius	• Slaptažodžiai – viena silpniausių kibernetinio saugumo sistemos vietų. Vartotojai dažnai kuria slaptažodžius, kuriuos lengva prisiminti. Todėl nusikaltėliams nesunku juos atspėti naudojant specialias programas. Naudodami tą patį slaptažodį kelioms paskyroms, dar labiau rizikuojate savo duomenimis, nes, gavę prisijungimo duomenis iš vienos svetainės, nusikaltėliai gali prisijungti prie kitų jūsų paskyrų.
	• Rinkitės patikimus slaptažodžius, kuriuos sunku atspėti. Patikimas slaptažodis turi šias savybes:
	  ○ Ilgas: sudarytas iš bent 12 simbolių arba dar daugiau.
	  ○ Sudėtingas: turi didžiąsias ir mažąsias raides, specialius simbolius ir skaičius.

	○ Ne akivaizdus: slaptažodyje nėra eilės skaičių (1234) ir asmeninės informacijos, kurią lengva sužinoti ar rasti internete: jūsų gimimo dienos, augintinio vardo ir pan. ○ Atsitiktinis: neturi įsimintinų klavišų kombinacijų. • Šiuo atveju gali būti naudinga naudoti slaptažodžių tvarkyklę. Slaptažodžių tvarkyklės padeda kurti patikimus slaptažodžius, laikyti juos skaitmeninėje saugykloje, apsaugotoje pagrindiniu slaptažodžiu.
Jeigu yra galimybė, įjunkite dviejų faktorių autentifikaciją	• Dviejų faktorių autentifikacija – tai būdas patvirtinti tapatybę, kai prieigai prie paskyros naudojami du ar daugiau patvirtinimo metodų. Pavyzdžiui, vietoj paprasto vartotojo vardo ar slaptažodžio užklausos yra naudojama dviejų faktorių autentifikacija reikalaujanti papildomos informacijos: • Papildomas vienkartinis slaptažodis, kurį svetainės autentifikavimo serveriai siunčia į telefoną ar el. pašto adresą. • Atsakymai į asmeninius saugumo klausimus. • Pirštų atspaudai ar kita biometrinė informacija, pvz., balso duomenys ar veido atpažinimas. • Dviejų faktorių autentifikacija sumažina kibernetinio išpuolio tikimybę. Norint apsaugoti internetines paskyras, rekomenduojama kiek įmanoma daugiau naudoti dviejų faktorių autentifikaciją. Interneto saugumui užtikrinti taip pat galima naudoti trečiųjų šalių autentifikavimo programas.
Atnaujinkite programinę įrangą ir operacinę sistemą	• Kūrėjai nuolat dirba ties produktų saugumu, stebi naujausias grėsmes ir išleidžia saugumo pataisas, kai aptinkamos programų pažeidžiamumas. • Naudokite naujausias operacinių sistemų ir programų versijas, kad nepraleistumėte naujų saugumo atnaujinimų.

	Tai ypač svarbu programoms, kuriose yra mokėjimo duomenų, sveikatos būklės informacijos ir kitos konfidencialios vartotojų informacijos.
Naudokite patikimą antivirusinę programinę įrangą ir reguliariai atnaujinkite ją	• Be rekomendacijų laikymosi dėl saugumo internete, svarbu naudoti patikimą antivirusinės programinės įrangos sprendimą. • Antivirusinė programinė įranga apsaugo įrenginius ir duomenis, blokuoja ne tik paplitusias grėsmes, tokias kaip virusai ir kenksmingos programos, bet ir kompleksines atakas, naudojant šnipinėjimo programas ir šifruotojus. • Kaip ir operacinių sistemų bei programų atveju, antivirusinę programinę įrangą būtina reguliariai atnaujinti, kad būtų gaunama apsauga nuo naujausių kibernetinių grėsmių.
Įsitikinkite, kad jūsų įrenginiai yra apsaugoti	• Apie 60% vartotojų naudoja mobiliuosius įrenginius pirkiniams ir informacijos paieškai internete kur kas dažniau nei kompiuterius, todėl ir tokie įrenginiai turi būti patikimai apsaugoti. • Rekomenduojama naudoti slaptažodžius, slaptus kodus ir kitas saugumo priemones, tokias kaip pirštų atspaudų nuskaitymas ar veido atpažinimo technologija visuose įrenginiuose: telefonuose, kompiuteriuose, planšetėse, išmaniuosiuose laikrodžiuose, išmaniuosiuose televizoriuose ir kituose įrenginiuose. Šios saugumo priemonės sumažins kibernetinės atakos ar jūsų asmens duomenų vagystės tikimybę.
Reguliariai atlikite atsarginių kopijų kūrimą	• Turėtumėte turėti svarbios asmeninės informacijos atsargines kopijas išoriniuose kietuosiuose diskuose ir reguliariai kurti naujas atsargines kopijas.

	• Išpirkos reikalaujančios programos – tai kenksmingos programos, blokuojančios kompiuterį ir neleidžiančios prieiti prie svarbių failų. • Atsarginių duomenų kopijų kūrimas padeda sumažinti neigiamas išpirkos reikalaujančių programų atakų pasekmes, o speciali apsaugos programinė įranga padidins jūsų saugumo lygį. • Yra ir kitų kenksmingų programų tipų, kurios blokuoja prieigą prie asmens duomenų, sukurdamos per didelę sistemos apkrovą arba tiesiog ištrindamos failus.
Būkite atsargūs atsisiųsdami įvairias nepatikrintas programas	• Kenkėjai siekia, kad atsisiųstumėte kenksmingą programą, kuri atvers jiems prieigą prie jūsų įrenginio. • Kenksmingos programos gali būti užmaskuotos kaip bet kokia programinė įranga – nuo populiarių žaidimų iki programėlių, skirtų orų ar eismo sąlygoms tikrinti. Be to, jos gali būti paslėptos sukurtose kenksmingose svetainėse, kurios bando įdiegti kenksmingas programas jūsų įrenginyje. • Kenksmingos programos daro žalą: sutrikdo įrenginio veikimą, vagia asmeninius duomenis, suteikia neautorizuotą prieigą prie kompiuterio. Paprastai kenksmingoms programoms atsisiųsti reikia keleto veiksmų iš vartotojo pusės, bet taip pat pasitaiko užkrėtimo per paslėptą atsisiuntimą, kai svetainė bando įdiegti kenksmingas programas kompiuteryje, neprašydama išankstinio leidimo. • Būkite atsargūs lankydamiesi nežinomoje svetainėje ir atsisiųsdami objektus į įrenginį. Atsisiųskite turinį tik iš patikimų ar oficialių šaltinių. Reguliariai tikrinkite atsisiuntimų aplankus ir nedelsdami ištrinkite nežinomus

	failus – jie galėjo patekti į jūsų įrenginį paslėptu atsisiuntimo būdu.

Įsitikinkite, kad svetainė yra patikima	• Patikimumas yra svarbi visų lankomų svetainių savybė, ypač tų, kuriose atliekamos operacijos. Ypač svarbu elektroninės prekybos svetainėms. Patekę į nepažįstamą svetainę, patikrinkite, ar ji apsaugota SSL sertifikatu.
	• Tokių svetainių adresai prasideda nuo HTTPS vietoj HTTP (raidė S reiškia „saugus“), o adresų juostoje rodoma užrakto piktograma. Kiti svetainės patikimumo požymiai yra šie:
	  ○ Gramatikos klaidų neturintis tekstas, be rašybos ir skyrybos klaidų. Autoritetingi prekės ženklai deda dideles pastangas, kad jų svetainės būtų kokybiškos.
	  ○ Kokybiški vaizdai, atitinkantys ekrano plotį.
	  ○ Skelbimai, kurie organiškai įsilieja į svetainės struktūrą ir neperkrauna jos.

Ištrinkite nenaudojamas paskyras	• Daugelis turi paskyras, kurios ilgai nenaudojamos. Jų buvimas gali tapti silpna vieta, naudojant internetą. • Senos paskyros dažnai turi silpnesnius slaptažodžius, o svetainės, kuriose jos buvo naudojamos, gali turėti nepatikimą duomenų apsaugos politiką. • Be to, pagal duomenis senose socialinių tinklų profiliuose kibernetiniai nusikaltėliai gali surinkti apie jus įvairią informaciją, pavyzdžiui, gimimo datą ir buvimo vietą, ir naudoti juos tolesniam išpuoliui. • Todėl rekomenduojame ištrinti senas paskyras ir pateikti prašymą ištrinti jūsų duomenis iš išorinių serverių.
Būkite atsargūs dalindamiesi	• Internete nėra galimybės ištrinti paskelbtos informacijos. Visi paskelbti komentarai ir nuotraukos gali likti tinkle

informacija internete	amžinai, nes ištrinant originalą jūs neištrinate kopijų, kurias galėjo padaryti kiti vartotojai. • Būkite atsargūs, skelbdami asmeninę informaciją internete: nenurodykite jautrių asmens duomenų socialinių tinklų profiliuose. Realiame gyvenime jūs neatskleistumėte asmens duomenų nepažįstamiems asmenims, todėl nereikėtų skelbti jų internete ir padaryti prieinamus milijonams vartotojų. • Būkite atsargūs, nurodydami savo el. pašto adresą. Naudinga turėti papildomą laikiną el. pašto paskyrą, naudojamą tik registracijoms ir prenumeratoms. Ji turėtų skirtis nuo darbo paskyros ir nuo naudojamos bendravimui su draugais ir artimaisiais.
Būkite atsargūs naudodamiesi internetinėmis pažinčių svetainėmis	• Jūsų internetiniai pažįstami ne visada yra tie, kuo prisistato. • Naudodami netikrus profilius socialiniuose tinkluose, piktavaliai medžioja neatsargius vartotojus, siekdami pavogti jų asmens duomenis ar pasinaudoti jų finansinėmis lėšomis. • Su socialiniu gyvenimu internete reikia elgtis taip pat atsargiai, kaip ir su socialiniu gyvenimu realiame pasaulyje. Tai ypač svarbu, atsižvelgiant į pastaraisiais metais padidėjusį sukčiavimo atvejų skaičių internetinių pažinčių srityje.

Patikrinkite privatumo nustatymus ir susipažinkite su privatumo politika	• Rinkodaros specialistai, kaip ir nusikaltėliai, nori apie jus sužinoti viską. Jie gali gauti šią informaciją iš paieškos istorijos ir socialinių tinklų. Bet jūs galite kontroliuoti prieinamą informaciją. Interneto naršyklėse ir mobiliųjų operacinių sistemų parametruose yra numatyti nustatymai, skirti užtikrinti privatumą internete. • Daugelis sutinka su privatumo politikos sąlygomis jų neskaitę. Tačiau didžiulis duomenų kiekis tvarkomas rinkodaros ir reklamos (ir nusikalstamais) tikslais, todėl rekomenduojama susipažinti su naudojamų svetainių ir programų privatumo politikomis ir suprasti, kaip vykdomas duomenų rinkimas ir analizė.