**Juodasis lapkritis: kaip išlikti saugiems internete masinių išpardavimų laikotarpiu?**

*Informacija žiniasklaidai, 2024 m. lapkričio 7 d.*

**Juodasis penktadienis (*angl. Black Friday*) pamažu tampa juoduoju lapkričiu, mat gyventojai vis dažniau yra viliojami nuolaidomis nebe vieną dieną, o beveik visą mėnesį. Kol daugelis skuba pasinaudoti patraukliausiais pasiūlymais, sukčiai taip pat nesėdi rankų sudėję. Skirtingais duomenimis, didžiųjų išpardavimų laikotarpiu sukčiavimo atvejų padaugėja kone penktadaliu. Elektroninės atpažinties ekspertas sako, jog šiuo laikotarpiu ypač svarbu išlikti budriems ir dalijasi patarimais, kaip apsaugoti savo asmeninius duomenis bei pinigus.**

„Prasidėjus masiniams išpardavimams gyventojai dažnai susigundo patraukliais pasiūlymais, o saugumas lieka antrame plane. Šiuo laikotarpiu pardavimų kiekis padidėja 30 procentų, o tuo skuba pasinaudoti sukčiai. Jie tik ir laukia, kol budrumą pamiršę asmenys užkibs ant kabliuko – patvirtins neinicijuotą transakciją ar paspaus nesaugią nuorodą. Todėl prieš įsibėgėjant išpardavimų karštinei svarbu dar kartą pasikartoti pagrindines kibernetinės higienos taisykles“, – sako Viktoras Kamarevcevas, e. atpažinties priemones kuriančios bendrovės „SK ID Solutions“ verslo vadovas Lietuvoje.

**Netvirtinkite to, ko neinicijavote**

Anot V. Kamarevcevo, didžiųjų nuolaidų mėnuo finansiniams sukčiams – puiki terpė „sumedžioti“ ne vieną auką. Prisidengdami šurmuliu, įvairiais pasiūlymais, jie naudojasi žmonių neapdairumu, siekia sukurti netikėtumo momentą ir taip apgauti gyventojus. Viena dažniausių klaidų, kurias skubėdami padaro žmonės – patvirtina neinicijuotą „Smart-ID“ transakciją.

„Kartais transakcijos inicijavimas įvyksta dėl žmogiškosios klaidos, pavyzdžiui, kuomet asmens informacija yra labai panaši į kito naudotojo ir šis padarė klaidą bandydamas prisijungti prie savo „Smart-ID“ paskyros. Visgi, pasitaiko ir tokių atvejų, kuomet sukčiai, gavę jūsų asmeninius duomenis, juos suveda e. paslaugos teikėjo platformoje ir taip bando inicijuoti operaciją. Tuomet programėlėje gali atsirasti transakcijos patvirtinimo užklausa. Jeigu tuo metu nieko neperkate internetu, nesijungiate prie banko ar kitų paslaugų ir neinicijavote šios transakcijos, jokiais būdais neveskite PIN kodų. Kol veiksmas nebus patvirtintas paties asmens suvedus tik jam žiniomis PIN kodus, asmeniniai duomenys liks saugūs“, – primena ekspertas.

Jo teigimu, pati „Smart-ID“ programėlė dėl joje naudojamos padalinto viešojo rakto infrastruktūros yra saugi ir į ją įsilaužti sukčiai negali. Tačiau nusikaltėliai vis ieško naujų būdų, kaip apgauti gyventojus, todėl svarbu netvirtinti jūsų neinicijuotų transakcijų.

**Devynis kartus patikrink, dešimtą pirk**

„SK ID Solutions“ atstovas pabrėžia, jog perkant internetu, kur įmanoma, reikėtų naudoti saugias el. atpažinties priemonės ir visada sutikrinti kontrolinius kodus:

„Pavyzdžiui, jei elektroninėje parduotuvėje apsiperkate su „Smart-ID“, prieš patvirtindami transakciją įsitikinkite, jog jūsų telefone rodomas kontrolinis keturių skaitmenų kodas sutampa su e. paslaugos elektroninėje parduotuvėje pateiktu kodu. Taip būsite ramūs, jog tvirtinate tą operaciją, kurią inicijuojate patys.“

Be to, V. Kamarevcevas pažymi, jog prieš atliekant transakcijas „Smart-ID“ programėlėje visuomet nurodoma papildoma informacija: „Tiek vedant PIN1, tiek PIN2, svarbu skaityti pranešimus išmaniojo įrenginio ekrane. Jeigu prašoma įvesti PIN1 kodą, reiškia, jog jungiatės prie e. paslaugų – interneto banko, e. parduotuvės ir pan. Jeigu PIN2 – tuomet autorizuojate veiksmą, pavyzdžiui, mokėjimą, dokumento pasirašymą ir panašiai. Šis programėlėje atsirandantis pranešimas – papildomas saugumo žingsnis, nurodantis, kokia operacija yra atliekama. Tačiau jei jums kyla bent menkiausias įtarimas ar pastebite nesutapimų – atšaukite transakciją.“

Pasak eksperto, ypač svarbi ir PIN kodų apsauga – jais negalima dalintis su niekuo, net ir šeimos nariais. „Smart-ID“ naudotojų PIN kodai nėra saugomi vidinėse bendrovės sistemose, jų negalima keisti, o juos pamiršus, reikia susikurti naują paskyrą.

**Nespauskite neaiškių nuorodų**

Prasidėjus išpardavimams, ypatingus pasiūlymus jums gali siųsti ne tik autorizuotos e. parduotuvės ir gerai žinomi prekių ženklai, bet ir jais apsimetantys sukčiai. V. Kamarevcevas pastebi, jog šiuo laikotarpiu ypač išauga nesaugių nuorodų siuntimas gyventojams trumposiomis žinutėmis ar el. paštu.

„Tikėtina, kad įsisukus lapkričio nuolaidų viesului sukčiai bandys iš jūsų išvilioti duomenis siųsdami nesaugias nuorodas pranešdami apie momentinius išpardavimus, nepristatytą siuntą arba kad ji yra „užstrigusi“ muitinėje ir panašiai. Jokiais būdais jų nespauskite. Visada yra saugiau pačiam jungtis prie norimų puslapių, suvedant internetinės svetainės adresą tiesiai į naršyklę. Be to, reikėtų atkreipti dėmesį, jog siųsdami nuorodas sukčiai sukuria skubos jausmą, pavyzdžiui, nurodydami itin trumpą akcijos galiojimo laiką. Tokiu atveju taip pat svarbu išlaikyti šaltą protą ir neužkibti ant kabliuko“, – sako V. Kamarevcevas.

Jis taip pat primena, jog nei paslaugos teikėjas „SK ID Solutions“, nei institucijos, nei e. paslaugas teikiančios bendrovės niekada nesiunčia jokių aktyvių nuorodų su prašymu pateikti asmens duomenis ar patvirtinti transakcijas. O gavus tokią užklausą apie tai reikėtų informuoti paslaugos teikėją.