

Nuolat tobulėjant skaitmeniniams atsiskaitymams jau kelerius metus mokėjimo kortelių duomenų vagystės išlieka dažniausia vagysčių rūšimi. 2021 m. bendra tokio sukčiavimo vertė Europoje siekė 1,28 mlrd. eurų, rodo naujausi Europos centrinio banko duomenys. Kaip šiandien galime nuo to apsisaugoti, pasakoja „Luminor“ banko sukčiavimo rizikos valdymo skyriaus vadovas Linas Sadeckas.

Duomenų nusavinimas perkant internetu

Duomenų nuskaitymas – tai mokėjimo kortelių informacijos vagystė iš internetinės parduotuvės klientų. Sandorio duomenys pavagiami registracijos bei pirmojo mokėjimo metu realiuoju laiku, klientams nepastebint nieko neįprasto.

„Pirmiausia sukčiai gauna prieigą prie internetinės parduotuvės arba trečiosios šalies serverio. Taip gali nutikti dėl sistemos pažeidžiamumo ar konfigūravimo klaidų. Tuomet vagys įterpia kenkėjišką programinę įrangą į mokėjimo procesą tarsi blakę, kuri paslapčia renka visą kliento informaciją. Duomenys renkami iš karto mokėjimo metu arba vėliau, kad vagystė nebūtų aptikta“, – pasakoja L. Sadeckas.

Nukentėję klientai įprastai nežino, kad jų kortelės duomenys buvo nutekinti. Pasak eksperto, jų požiūriu, užsakymas buvo pateiktas ir prekė bus gauta. Todėl nėra jokios galimybės įtarti, kad kažkas nutiko ne taip, o nuostoliai paaiškėja žymiai vėliau.

Duomenų pasisavinimas per įmones

Kibernetiniai nusikaltėliai taip pat gali pasisavinti jūsų kortelės duomenis, suradę silpnų vietų saugumo sistemose el. parduotuvių, kuriose dėl patogumo išsaugojate savo mokėjimo kortelės duomenis. Šiuo atveju jie taikosi į jau išsaugotos mokėjimo informacijos saugyklą.

Pasak eksperto, tokios sistemų spragos gali atsirasti dėl pasenusios programinės įrangos, netinkamos konfigūracijos ar netinkamų saugumo protokolų. Tai žinodamos, patikimos el. parduotuvės investuoja daug resursų, kad jose neliktų jokių spragų, tačiau labai retais atvejais jų visgi gali likti.

„Nustatę pažeidžiamą vietą sistemose, sukčiai naudoja įvairius metodus į jas įsiskverbti. Pavyzdžiui, gali įdiegti virusus arba išpirktos reikalaujančias programas, taip siekdami sistemą palaužti ir gauti neteisėtą prieigą prie duomenų. Pavogę mokėjimo kortelių informaciją, nusikaltėliai paprastai stengiasi iš jos pasipelnyti parduodami ją kitiems juodojoje rinkoje arba pinigais pasinaudoja patys“, – sako L. Sadeckas.

Apgaulingi pranešimai

Jūsų tapatybę sukčiai gali pasisavinti ir apgaulingais pranešimais (angl. – „*phishing*“). Paprastai apgavikai prisistato žinoma įmone ar patikima institucija, pavyzdžiui, banku ar pašto paslaugų bendrove, ir bando priversti pateikti konfidencialią informaciją.

„Galite gauti netikėtą elektroninį laišką arba SMS žinutę, pranešimą socialinėse medijose. Įprastai nurodomas tam tikras įvykis dėl kurio reikia skubiai imtis veiksmų bei spustelėti pranešime prikabinatą nuorodą. Tokių įvykių pavyzdžiai – neva užstrigusios pašto arba kitos siuntų tarnybos siuntos, apsimestiniai kurjeriai, neva iš policijos gaunamos žinutės apie neegzistuojančias baudas ir pan.“, – sako ekspertas.

Pasak L. Sadecko, tokie pranešimai gali teigti, kad rasta problemų su jūsų mokėjimo informacija, galbūt turite patvirtinti tam tikrus asmeninius duomenis arba pastebėta neįprastos veiklos jūsų paskyroje.

Vis dėlto, tai tik triukas, skirtas nukreipti žmogaus dėmesį ir išgauti konfidencialius duomenis – slaptažodžius, mokėjimo kortelių numerius ir su turima informacija pasiekti jūsų banko sąskaitą, sako ekspertas.

Kaip apsisaugoti?

Siekdami apsisaugoti nuo mokėjimo kortelių duomenų vagysčių, be reikalo nesidalykite kortelių informacija neaiškios reputacijos tinklalapiuose – naudokitės tik jums gerai žinomomis svetainėmis.

Taip pat patartina turėti atskirą mokėjimo kortelę internetiniams mokėjimams bei reguliariai stebėti sąskaitų išrašus. Prisijungimams prie jautrių paskyrų aktyvuokite papildomas saugumo funkcijas, kaip, pavyzdžiui, dviejų veiksmų autentifikavimą.

„Jei tapote mokėjimo kortelės duomenų vagystės auka, nedelsdami susisieki su savo banku ir praneškite Lietuvos policijai, taip padidinsite tikimybę užkardyti neteisėtą lėšų nuskaitymą ir duomenų nusavinimą“, – sako L. Sadeckas.

Eksperto teigimu, šansų atgauti lėšas, inicijuotas mokėjimo kortele yra maži, tačiau skubūs nukentėjusio asmens veiksmai įvykus kortelės duomenų vagystei gali padėti šią tikimybę padidinti.

