*Pranešimas žiniasklaidai  
2025 m. gruodžio 8 d.*

**Šventinis skubėjimas pildo ne tik dovanų maišus, bet ir sukčių sąskaitas: tūkstantinius nuostolius patiria net budriausi**

**Kalėdinis laikotarpis – tikras darbymetis kibernetiniams sukčiams – žmonės skuba pirkti dovanas, o dažnai tai daro internetu. Mokėjimų patvirtinimų žinutės, pranešimai apie išsiųstas ar gautas siuntas – gyventojų telefonai tiesiog kaista nuo informacijos, tačiau svarbiausia suprasti, kad vienas neatsargus mygtuko spustelėjimas gali kainuoti net dešimtis tūkstančių eurų. Draudimo bendrovės BTA duomenys rodo, kad šiandien nuo kibernetinių sukčių nukenčia ne tik mažiau patyrę ar vyresnio amžiaus žmonės – į itin profesionaliai surežisuotas pinkles vis dažniau patenka net ir patys budriausi interneto vartotojai.**

Pasak BTA draudimo produkto vadovo Ramūno Juso, šventiniu laikotarpiu sukčiams atsiveria itin palankios sąlygos – žmonės laukia ne vienos, o keleto siuntų vienu metu.

„Matome augantį fiksuojamų sukčiavimo atvejų skaičių – nuo kelių dešimčių iki keliolikos tūkstančių eurų. Žmonės dažnai patenka į pinkles tiesiog todėl, kad skubėdami neatkreipia dėmesio į detales. Ypač dabar, kai visi laukia kelių siuntų, viena po kitos atkeliaujančios žinutės atrodo natūralios ir apgaulingą nuorodą paspausti tampa labai lengva“, – sako R. Jusas.

Kibernetinio saugumo ekspertas, „Baltimax“ vyresnysis inžinierius ir „ESET“ atstovas Lukas Apynis atkreipia dėmesį, jog šiandien sukčiai naudoja žymiai pažangesnes technologijas ir psichologines taktikas.

„Pasitelkdami dirbtinį intelektą sukčiai generuoja itin tikroviškus laiškus, žinutes ar net imituoja balsą. Taip pat dirbtinis intelektas padeda automatizuoti tam tikrus programišių veiksmus – sukuriami bankų ar įmonių puslapiai, logotipai, SMS siuntėjų vardai. Be to, sukčiai renka informaciją ir iš socialinių tinklų, juodojo interneto (angl. „dark web“) ir taikosi į konkrečius žmones ar įmones. Taip pat Lietuvoje pastebėjome ir naujų kanalų, tokių kaip „Messenger“, „WhatsApp“, bei „Viber“ išnaudojimą“, – pažymi L. Apynis.

**Kalėdinis bumas – piktavalių darbymetis**

Vienas iš dažniausiai šiuo laikotarpiu sutinkamų sukčiavimo scenarijų – suklastotos žinutės apie siuntų nukreipimą ar papildomus mokesčius.

„Apgaulingas žinutes atpažinti sudėtinga net tiems, kurie kasdien dirba su sukčiavimo atvejais. Kai vienu metu lauki keleto siuntų iš skirtingų parduotuvių, žinutė apie tariamą siuntos nukreipimą atrodo visiškai logiška ir atitinka natūralių įvykių seką – užsisakiau prekes, jos turi keliauti, reiškia, taip ir turi būti – mygtuko paspaudimas tampa automatišku veiksmu. Deja, būtent nuo tokio, atrodytų, nekalto paspaudimo dažniausiai ir prasideda visa pinigų nuskaitymo grandinė“, – dėmesį atkreipia R. Jusas.

Būtent dėl augančių sukčiavimo mastų BTA prieš kelerius metus rinkai pasiūlė unikalų sukčiavimo rizikų draudimą, vadinamą apsauga nuo sukčių, o šiandien sukaupta statistika rodo, kad tokių įvykių daugėja ir nuostolių suma dažnai siekia ne simbolines, o kelių ar net keliolikos tūkstančių eurų sumas.

„Per pastaruosius porą metų matome vis daugiau situacijų, kai žmonės apgaunami per fiktyvias nuorodas, skelbimų portalus ar tariamus kurjerių pranešimus. Tai nėra pavienės istorijos – tokių žalų skaičius nuolat auga, jos kartojasi ir aiškiai formuoja atskiras sukčiavimo scenarijų grupes“, – teigia R. Jusas.

**Sukčių taikiniais tampa įvairaus amžiaus žmonės**

Visuomenėje vis dar gajus įsitikinimas, kad dažniausiai apgaunami vyresnio amžiaus žmonės. Visgi, pasak L. Apynio, realybė yra kiek kitokia.

„Dažniausiai nukenčia įvairaus amžiaus, taip pat ir 25–55 metų žmonės, kadangi jie aktyviausiai naudojasi skaitmeninėmis paslaugomis. Dažnai pasitaiko ir jaunimo, kadangi jie dažniau spaudžia nuorodas iš įpročio arba skubėdami. Šiuolaikinės apgaulės yra labai įtikinamos, o žmonės dažnai reaguoja skubotai“, – atkreipia dėmesį L. Apynis.

R. Jusas priduria, kad įmonės duomenys rodo vis pasikartojančias grupes žalų, kai žmonės apsigauna tiek per telefoninius skambučius, tiek per skelbimų portalus, tiek per apgaulingus kurjeriais apsimetusių sukčių pranešimus. Tai rodo, jog sukčiai nuolat ieško naujų būdų pasinaudoti tais pačiais mūsų įpročiais – skubėjimu ir pasitikėjimu įprastais procesais.

**Ką daryti, jei visgi apsigavote?**

Deja, į sukčių pinkles gali pakliūti net budriausias interneto vartotojas, tad jei vis dėlto paspaudėte nuorodą ar perdavėte prisijungimo duomenis, anot L. Apynio, svarbiausia – nedelsiant veikti.

„Pirmiausia reikėtų iš karto susisiekti su banku ir paprašyti sustabdyti įtartinas operacijas bei užblokuoti kortelę ar prisijungimo priemones. Tuomet būtina pakeisti slaptažodžius, įjungti dviejų veiksnių autentifikavimą ir patikrinti, ar nebuvo pakeisti paskyros atkūrimo nustatymai“, – akcentuoja L. Apynis.

Kitas būtinas žingsnis – kreiptis į policiją ir fiksuoti įvykį. Pasak R. Juso, tik tinkamai užfiksuotas įvykis leidžia draudimo bendrovei išsamiai įvertinti situaciją ir atlyginti dalį patirtų nuostolių.

„Kad galėtume padėti klientui, mums būtina turėti visus faktą patvirtinančius dokumentus. Pirmiausia – policijos registracijos numerį ir banko informaciją apie atliktus pavedimus: kam ir kada buvo pervesti pinigai, kokios sumos nuskaičiuotos, kada žmogus pastebėjo apgaulę. Gali prireikti ir papildomos informacijos – žinučių, ekrano nuotraukų, net fiktyvių puslapių nuorodų, kurios padeda suprasti, kaip tiksliai vyko apgaulė“, – tvirtina draudimo produkto vadovas.