

Daugelis esame prarę saugoti savo pinigus nuo sukčių internete, tačiau ne kiekvienas susimąstome, kad apsaugos nuo apgavikų reikia ir mūsų vaikams. Jiems augant rizika susidurti su sukčiavimu virtualioje erdvėje tik didėja, todėl būdais, kaip išvengti sukčių pinklių, dalinasi „Luminor“ banko Sukčiavimo rizikos valdymo skyriaus vadovas ir dviejų vaikų tėvas Linas Sadeckas.

Praėjusiais metais Lietuvoje sukčiavimo būdu inicijuotų lėšų pervedimų suma siekė apie 35 mln. Eur, sukčiavimo atvejų skaičius išaugo iki 13 tūkst. kartų, rodo Pinigų plovimo prevencijos kompetencijų centro duomenys. Anot L. Sadecko, šie skaičiai rodo, kad nuo sukčių apsisaugoti yra nelengva net suaugusiems.

„Dėl to pradėti supažindinti vaikus su galimomis grėsmėmis internete turime jau nuo mažens. Mokyti kibernetinio saugumo vaiką svarbu tolygiai su didėjančiu jo amžiumi ir smalsumu naudotis išmaniaisiais įrenginiais, kadangi augant žmogui, auga ir rizika susidurti su įvairiu sukčiavimu – ar tai būtų asmens duomenų vagystės, ar nuotraukų, ar pinigų“, – sako ekspertas.

Išvilioja duomenis

Viena dažniausių sukčiavimo schemų, su kuria gali susidurti mūsų vaikai, yra duomenų viliojimas (angl. *phishing*).

„Sukčiai vaikus pasiekia per trumpąsias žinutes ar socialinių tinklų platformas. Pranešimuose pateikiamos nuorodos į suklastotas interneto svetaines – dažniausiai apsimetama banku, policija ar kita oficialia institucija. Nukreipti į tokius puslapius vaikai raginami suvesti asmens duomenis, kurie iškart atsiduria sukčių rankose“, – pasakoja L. Sadeckas.

Be to, duomenis išvilioti galima ir tokia pačia pranešime prisegus failą, kuriame yra kenkėjiška programa. Tokios programos perima visą įrenginį, jame esančias nuotraukas, vykdo tiesioginę stebėseną per įrenginio kamerą.

„Nepamirškime ir to, kad vaikai, imituodami viešus asmenis, socialinėse medijose gali netyčia atskleisti asmeninę informaciją – kur gyvena, kuo užsiima, kada nėra namuose. Tokia informacija, patekusi į sukčių rankas, taip pat gali būti panaudota prieš jus“, – priduria ekspertas.

Siūlo lengvai užsidirbti

Kiti vaikams pavojingi sukčiavimo spąstai yra „pinigų mulų“ sukčiavimo schema. Pasak L. Sadecko, kadangi vaikams net ir menka suma gali atrodyti didelė, jaunuoliai tampa lengvu taikiniu.

„Jie gali sulaukti žinučių ar komentarų per socialinius tinklus, kur siūloma greitai ir paprastai užsidirbti – tereikia leisti pinigų pervedimui panaudoti savo sąskaitą ar net pasiimti grynųjų iš bankomato ir perduoti juos trečiajam asmeniui. Vaikas tokiu atveju tampa vadinamuoju pinigų mulu – žmogumi, kuris perneša arba perveda neteisėtai gautas lėšas, neretai pats nesuprasdamas, kad dalyvauja nusikaltime ir gali sulaukti rimtų teisinių pasekmių“, – teigia ekspertas.

Kaip apsisaugoti

Viena svarbiausių pamokų – aiškiai vaikams papasakoti, kas yra prisijungimo duomenys, slaptažodžiai, ką jie reiškia ir kodėl niekam negalima jų atskleisti. Vaikai turėtų suprasti, kad banko sąskaita yra ne tik techninis įrankis, bet ir atsakomybė. Bet koks leidimas ją pasinaudoti gali atnešti pavojų ne tik jiems, bet ir visai šeimai.

„Mokykite atžalas niekam neatskleisti savo prisijungimo duomenų, nesvarbu, ar to prašo neva pažįstamas žmogus, ar instituciją imituojanti žinutė. Pasakokite, kuo galima ir kuo negalima dalintis socialinėse medijose, mokykite vengti neaiškių būdų lengvai užsidirbti. Galiausiai, nesiekite vaikams prieinamų įrenginių su jokiais mokėjimo kortelėmis. Vaikai, ypač mažamečiai, yra smalsūs, jiems įdomu pažiūrėti, paspausti, tačiau tai netyčiomis gali privesti ir iki duomenų nutekėjimo“, – teigia L. Sadeckas.

Svarbiausia – padėkite vaikams suprasti, kad internete galioja tos pačios saugumo taisyklės kaip ir realiame gyvenime: nepasitikėti nepažįstamais, saugoti savo tapatybę ir, jei kas nors kelia įtarimų, visada pasitarti su suaugusiuoju.

