Kaip atpažinti programišius ir apsaugoti savo nuosavybę?

Visame pasaulyje spalį minimo kibernetinio saugumo mėnesio proga, Nacionalinio kibernetinio saugumo centro (NKSC) specialistai atkreipia gyventojų dėmesį į keletą šiuo metu populiarių programišių taktikų ir ragina gyventojus būti budriais.

Skambina pažįstamas telefono numeris? Tai dar nieko nereiškia

Dalis gyventojų vasaros pabaigoje jau galėjo susidurti su *„Google“* darbuotojais apsimetančiais sukčiais. Jie dažniausiai skambino iš lietuviško numerio, kalbėjo rusiškai ir, įvairiais būdais gąsdindami bei skubindami, bandė išvilioti gyventojų asmeninius duomenis. Tam, kad skambutis nesukeltų įtarimo, programišiai naudoja mobiliojo numerio klastojimo (angl. „spoofing“) techniką, kai skambinančiojo numeris telefone atvaizduojamas kaip kitas. Perskambinę tokiam numeriui būsite sujungti su tikruoju numerio savininku, kuris neturės nieko bendra su įvykusia situacija. Svarbu žinoti, kad sukčiai gali apsimesti jūsų pažįstamu ir skambinti prisidengdami numeriu iš jūsų kontaktų knygelės. Gavę įtarimą keliantį skambutį, patikrinkite, ar tikrai kalbate su tuo žmogumi, užduodami klausimus, į kuriuos atsakymus žino tik jis. Jei kyla abejonių, nutraukite pokalbį ir paskambinkite atgal naudodami patikimą kontaktą.

Kai pasiūlymai per geri, kad būtų tikri

Artėjant rudens išpardavimams į duomenis nusitaikę programišiai vilios didelėmis nuolaidomis, ragins kuo greičiau „pirkti“ ir naudotis riboto laiko pasiūlymais. Prieš registruojantis ar apsiperkant nematytoje parduotuvėje rekomenduojama peržiūrėti atsiliepimus internete, patikrinti kontaktų skiltį – įtarimą turėtų kelti įmonės rekvizitų, kontaktinio telefono, oficialaus el. pašto nebuvimas. Sukčiai taip pat kuria gerai žinomų elektroninių parduotuvių kopijas ir leidžia reklamas socialiniuose tinkluose naudodamiesi gera prekės ženklo reputacija, todėl peržiūrėkite prekes reklamuojantį profilį, jo įrašų istoriją. Atkreipkite dėmesį į reakcijas ir komentarus. Jei komentarų yra išskirtinai daug, jie parašyti lietuvių kalba, o komentuojančiųjų vardai ir pavardės yra nelietuviški – tai netikri komentarai.

Neskubėkite džiaugtis sulaukę entuziastingo pirkėjo

Pardavinėdami daiktą internetinėse platformose arba socialiniuose tinkluose, būkite atidūs gavę panašaus pobūdžio žinutę: „Prekę rezervuoju, padariau pavedimą, patvirtinkite pinigų gavimą: (nuoroda arba QR kodas)“. Paspaudę šią nuorodą būtumėte nukreipti į naršyklės langą, kur reikėtų pasirinkti savo naudojamą banką. Tai padarius atsidarytų nuo tikrojo

beveik niekuo nesiskirianti prisijungimo prie el. banko svetainė. Matydami jūsų vedamus prisijungimo duomenis ir patvirtinimo kodus, programišiai tuo pačiu metu jungtųsi prie tikrosios jūsų sąskaitos ir kiltų pavojus, kad sukčiams pavyks inicijuoti pinigų pervedimą į savo sąskaitą.

Melagingų SMS žinučių siuntėjai tobulėja

Kenkėjiškos SMS žinutės tampa vis sunkiau atpažįstamos ir labiau personalizuotos. Dažniausi sukčių naudojami scenarijai yra susiję su siuntų pristatymu, teigiant, kad kurjeriui nepavyko pristatyti siuntos, siunta „užstrigo“ muitinėje, reikia atnaujinti duomenis. Taip pat dažnai pasitaiko mokesčių grąžinimą arba įsiskolinimą imituojančios žinutės, kuriose manipuliuojama gyventojų baime prarasti pinigus. Žinute pasitikėti neverta net joje matote savo teisingai nurodytą vardą ar adresą. Šiuos duomenis programišiai galėjo gauti, jei į kenkėjišką puslapį savo duomenis suvedėte praeityje. Kenkėjišką SMS dažnai išduoda lietuviškų raidžių nenaudojimas, rašybos klaidos, raginimas veikti kuo greičiau, bandymas sukelti stresą ir nuoroda.

Ką daryti nukentėjus?

Jeigu susidūrėte su situacija, kurioje nukentėjote finansiškai, nedelsdami kreipkitės į savo banką, nes kai kuriais atvejais dar būna galimybė sustabdyti pinigų pervedimą sukčiams. Apie įvykį taip pat informuokite policiją, o jeigu susidūrėte su įtarimą keliančia nuoroda arba sukčiavimo svetaine, apie tai pranešti galite www.nksc.lt skiltyje „Pranešti apie incidentą“.