Rekomendacijos dėl rizikų valdymo ir galimų neigiamų pasekmių išvengimo

Atsižvelgiant į Registrų centro duomenų nutekinimo aplinkybes, artimiausiu metu gali padaugėti sukčiavimo atvejų, kai nusikaltėliai naudosis tikrais gyventojų duomenimis siekdami įgyti pasitikėjimą. Vien tai, kad skambinantis asmuo žino Jūsų vardą, pavardę, asmens kodą, adresą ar kitą asmeninę informaciją, nereiškia, kad jis atstovauja teisėtai institucijai.

Neteisėtai gavę gyventojų asmens duomenis, sukčiai gali:

- Apsimesti valstybės institucijų, bankų, Registrų centro, policijos ar kitų įstaigų darbuotojais ir siekti išvilioti papildomus duomenis (pvz. asmens dokumento informaciją, dokumento ar asmens nuotraukas), prisijungimo kodus ar pinigus;

- Vykdyti tikslines telefoninio sukčiavimo atakas, naudodami tikrus asmens duomenis (vardą, pavardę, adresą, asmens kodą ar kitą informaciją), taip didindami gyventojų pasitikėjimą;

- Atvykti į namus ir bandyti apgaule išvilioti lėšas;

- Siųsti suklastotus elektroninius laiškus ir SMS žinutes su nuorodomis į netikras interneto svetaines, skirtas prisijungimo duomenims ar banko informacijai išvilioti;

- Bandyti sudaryti sutartis ar gauti paslaugas kito asmens vardu, jeigu tam tikrais atvejais pakanka pavogtų identifikacinių duomenų;

- Rizika, kad nutekinti duomenys gali būti panaudoti, gali tęstis ilgą laiką.

Rekomendacijos:

Tikrinkite savo duomenis tik oficialiuose institucijų puslapiuose bei atsargiai vertinkite SMS ir elektroninius laiškus

Informacijos apie incidentą nereikėtų tikrintis gavus nuorodas SMS žinutėmis, el. laiškais ar radus socialiniuose tinkluose. Nespauskite nuorodų, gautų iš nepažįstamų siuntėjų.

Būkite ypač atsargūs sulaukę netikėtų skambučių
Jeigu skambinantis asmuo prisistato banko, policijos, Registrų centro telekomunikacijų bendrovės ar kitos institucijos darbuotoju ir prašo pateikti asmens duomenis, prisijungimo kodus, slaptažodžius ar atlikti finansines operacijas, pokalbį nutraukite ir su institucija susisiekite oficialiais kontaktais.

Neatskleiskite prisijungimo duomenų
Bankai, policija, Registrų centras ir kitos valstybės institucijos telefonu, elektroniniu paštu ar SMS žinutėmis neprašo atskleisti interneto banko prisijungimo duomenų, PIN kodų, „Smart-ID“, mobiliojo parašo kodų, mokėjimo kortelių duomenų.

Neatskleiskite kitų asmens duomenų ar asmens dokumento informacijos

Sukčiai gali prašyti asmens dokumento ar veido nuotraukų, siekiant šią informaciją panaudoti gaunant paslaugas ar atsidarant sąskaitas.

Stebėkite savo finansines operacijas
Reguliariai tikrinkite banko sąskaitų išrašus ir nedelsdami kreipkitės į banką pastebėję įtartinas operacijas.

Keiskite slaptažodžius

Jeigu nutekinti duomenys buvo naudojami slaptažodžiuose, šie gali tapti pažeidžiami.

Jeigu tapote sukčiavimo auka
Jeigu manote, kad tapote sukčiavimo auka arba Jūsų duomenys galėjo būti panaudoti nusikalstamais tikslais, nedelsdami kreipkitės į policiją arba skambinkite skubiosios pagalbos tarnybų ryšio numeriu 112.

Informuokite vyresnio amžiaus artimuosius

Rekomenduojama su artimaisiais aptarti dažniausiai pasitaikančius sukčiavimo būdus bei sukčių galimus veiksmus žinant jų asmens bei turto duomenis.

Būkite budrūs – sukčiai dažnai naudojasi žmonių pasitikėjimu ir turima asmenine informacija.

Taip pat galimi neteisėti duomenų panaudojimo būdai gali apimti:

- Išsamesnio ir tikslesnio asmens profilio sudarymą, panaudojant soc. tinklų ar kitų viešų šaltinių informaciją;

- Tyčinį asmens tapatybės atskleidimą, kai be asmens sutikimo paskelbiama su juo susijusi informacija;

Parengė:

Policijos departamentas

Nacionalinis kibernetinio saugumo centras

Antrasis operatyvinių tarnybų departamentas

Valstybės saugumo departamentas