VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

DUK PATARIMAI, ką daryti, jeigu Jūsų paskyra buvo „nulaužta“

2021-12-31

Valstybinė duomenų apsaugos inspekcija atkreipia dėmesį, kad įvairūs asmens duomenų saugumo incidentai gali įvykti su kiekvieno iš mūsų asmens duomenimis. Todėl labai svarbu ir patiems pasirūpinti savo duomenų saugumu. Dalijamės keletu patarimų, kaip galime labiau apsaugoti savo asmens duomenis.

PAKEISKITE SLAPTAŽODŽIUS

Nedelsdami pakeiskite visų naudojamų „online“ paslaugų (socialinių tinklų, internetinių parduotuvių, internetinės komunikacijos ir pan.), taip pat su jomis susijusių paslaugų slaptažodžius. Niekada daugiau nenaudokite senojo slaptažodžio. Slaptažodžiai turėtų būti keičiami kas pusmetį – tai svarbus Jūsų saugumo internete aspektas. Jokiais būdais nenaudokite tokių slaptažodžių kaip qwerty ar 123456 ir pan. Kiekvienai paslaugai kurkite skirtingus slaptažodžius. Pakartotinis slaptažodžių naudojimas yra didžiausia blogybė. Svetainėse gali būti taikomi slaptažodžio reikalavimai, pvz., skaičiai, didžiosios raidės ar simboliai. Tačiau jos negali uždrausti vartotojams naudoti tų pačių slaptažodžių ir neleisti jiems pakartotinai naudoti pažeistų slaptažodžių.

SUSIGRĄŽINKITE SAVO PASKYRŲ KONTROLĘ

Jeigu pastebėjote, kad yra pasikėsinta į daugiau Jūsų valdomų paslaugų, susigražinkite jų kontrolę. Daugelis interneto paslaugų turi savo mechanizmus, kaip grąžinti paskyrą tikram savininkui, kai ją perima užpuolikai. „Apple“, „Facebook“, „Google“, „Microsoft“, „Twitter“ , „Yahoo“ ir pan. turi šiuos mechanizmus. Dažniausiai reikia atsakyti į kelis klausimus apie savo sąskaitą. „Facebook“ naudoja naujoviškesnį būdą patikrinti Jūsų tapatybę pagal draugus. Kraštutiniu atveju turėsite kreiptis į vietinį paslaugos biurą ir parodyti dokumentus, po kurių Jums bus grąžinta paskyros kontrolė.

IEŠKOKITE „ATVIRŲ DURŲ“ (ANGL. BACKDOOR)

Gali būti, kad įsilaužėlis jau pabuvojo Jūsų paskyrose. Protingas įsilaužėlis nenurims paprasčiausiai įsiskverbęs į Jūsų paskyrą. Jis pasirūpins galimybe vėl į ją patekti, įdiegdamas tam reikalingas priemones. Todėl, kai tik atgausite savo paskyrų kontrolę, nedelsdami patikrinkite, ar nėra „atvirų durų“, pro kurias galėtų sugrįžti įsibrovėliai. Jei tai el. paštas, patikrinkite nustatymus – ar yra sukonfigūruoti korespondencijos persiuntimai į kitas pašto dėžutes, ar išjungti šlamšto filtrai ir ar pasikeitė atsakymai į Jūsų saugos klausimus kitų paslaugų paskyrose.

STEBĖKITE SAVO FINANSUS

Atidžiai stebėkite, kas vyksta su Jūsų sąskaitomis ir lėšų judėjimu per jas. Įsitikinkite, kad atsiskaitymo sąskaitose ar internetinių parduotuvių ir kitų mokamų paslaugų paskyrose nebuvo pridėti

nauji pristatymo adresai, pridėti nauji mokėjimo metodai ar prijungtos naujos paskyros. Tai ypač aktualu dėl paslaugų, leidžiančių sumokėti už pirkinį vienu paspaudimu.

PASIŠALINKITE IŠ VISŲ ATVIRĄ AUTORIZACIJOS PROTOKOLĄ PALAIKANČIŲ PASLAUGŲ

„Google“, „Twitter“, „Facebook“, „Dropbox“ ir daugelis kitų palaiko „OAuth“ – atvirą autorizacijos protokolą, leidžiantį suteikti trečiajai šaliai ribotą prieigą prie saugomų vartotojo išteklių, kai nereikia perduoti savo vartotojo vardo ir slaptažodžio trečiajai šaliai. Pasitikrinkite ir sukurkite atskirą prisijungimą su vartotojo vardu ir slaptažodžiu arba pašalinkite tokias paslaugas.