DUOMENŲ APSAUGOS PAREIGŪNAS

MB „Teisės labirintai“
Juridinio asmens kodas 305412893
El. p. info@teiseslabirintai.lt; Mob. Tel. Nr. +370 (630) 17 959

INFORMACINIS PRANEŠIMAS – REKOMENDACIJA KAIP APSISAUGOTI NUO SUKČIAVIMO INTERNETE

(parengta pagal VDAI rekomendacijas)

DUOMENŲ APSAUGA KARO UKRAINOJE METU

Prasidėjus kariniams veiksmams Ukrainoje, Nacionalnis kibernetinio saugumo centras fiksuoja išaugusį pranešimų apie sukčių veiklą socialiniuose tinkluose skaičių. Sukčiai, prisidengę fiktyviais paramos fondais, naudojasi pilietiškai nusiteikusių asmenų noru padėti Ukrainai ir bando nukreipti aukojamas lėšas į fiktyvias sukčių valdomas sąskaitas. NKSC taip pat fiksuoja atvejų, kai sukčiai, naudodami tikrų ir patikimų paramos fondų ar organizacijų pavadinimus, simboliką ir stilistiką prašo aukoti nurodydami netikrą gavėjo pavadinimą ir sąskaitos numerį.

Kibernetiniai nusikaltėliai nuolat ieško būdų, kaip užsidirbti pinigų Jūsų sąskaita ir bando išnaudoti žmogiškas emocijas, kad, pasinaudodami socialinės inžinerijos technikomis, išgautų jiems reikalingą informaciją tiesiogiai iš Jūsų.

PATIKRINKITE INFORMACIJĄ, NESKUBĖKITE

Siekiant apsisaugoti nuo įvairių sukčiavimo ar svarbių asmens duomenų viliojimo metodų, svarbu išsiugdyti įprotį pasitikrinti pateikiamą informaciją ar pasitarti su patikimais žmonėmis prieš atliekant veiksmus, kurie potencialiai gali Jums pridaryti žalos, jei aplinkybės susiklostys ne taip, kaip tikėjotės. Kitas svarbus veiksnys yra dėmesingumas, nes socialinė inžinerija remiasi skubinimu priimti sprendimus, nespėjus apgalvoti ir pasverti jų būtinumo ir reikalingumo, tikintis, kad elgsitės impulsyviai ir neracionaliai.

Prieš darydami bet kokį pavedimą ar teikdami kitokio pobūdžio apmokėjimo prašymą, prieš nurodydami banko kortelės duomenis ir pan., būtinai įsitikinkite, kad informacija gauta iš patikimų asmenų (Jūsų draugų, kolegų, giminių). Įsitikinkite, kad patikimo paramos fondo ar organizacijos nurodytos sąskaitos vienodos (sutampa) bent keliuose šaltiniuose.

KAIP ATPAŽINTI NEPATIKIMAS INTERNETO SVETAINES

SAUGAUS NARŠYMO INTERNETE PATARIMAI

- Nenaršyti ir ypač nesuvedinėti jokių duomenų internetinėse svetainėse, kurios nenaudoja duomenų šifravimo, t. y. neturi adreso pradžioje „https“;
- Visuomet įsitikinti, ar svetainėje paskelbta privatumo politika (angl. website privacy policy);
- Įsitikinti, kad svetainės valdytojas skelbia savo kontaktinę informaciją;
- Turėti įsidiegus programinę įrangą, kuri blokuotų neįprastą tinklalapių veiklą, „iššokančius“ langus bei siūlymus atsisiųsti ir įdiegti neaiškios kilmės dokumentus ar programas;
- Užėjus į įtarimų keliančią interneto svetainę, nespausti jokių nuorodų, prie jų nesijungti naudojantis asmeninių paskyrų (pavyzdžiui, socialinių tinklų, el. pašto paslaugų ir pan.) prisijungimo duomenimis, nevesti jokios asmeninės informacijos;
- Nepasitikėti pateikta informacija apie galimus laimėjimus ar kitus prizus, kai prašoma pateikti asmens duomenis, mokėjimų kortelių duomenis, kitą asmeninę informaciją ar atsisiųsti papildomas aplikacijas, kad galėtumėte atsiimti savo laimėjimus ar prizus.

NESAUGIŲ INTERNETO SVETAINIŲ POŽYMIAI

- Net jei svetainė turi SSL sertifikatą, privatumo politiką, kontaktinę informaciją, ji vis tiek gali būti nesaugi, jei yra užkrėsta kenkėjiška programine įranga. Apie tai, kad svetainė užkrėsta kenkėjiška programine įranga, galima sužinoti iš tam tikrų kibernetinių atakų požymių:
- Turinio iškraipymo ataka (angl. defacement). Ši ataka lengvai atpažįstama – kibernetiniai sukčiai pakeičia svetainės turinį savo vardu, logotipu ir (arba) ideologiniais vaizdais, iššaukiančia reklama ar pan.;
- Iššokantys langai (angl. suspicious pop ups). Reikia būti atsargiems dėl iššokančių langų, kurie pateikia su svetainės turiniu nesusijusią informaciją. Greičiausiai bandoma privilioti svetainės lankytoją spustelėti ir netyčia atsisiųsti kenkėjiškas programas;
- Kenkėjiška reklama (angl. malvertising). Dažniausiai kenkėjišką reklamą nesunku atpažinti. Paprastai ji atrodo neprofesionali, joje yra rašybos, gramatikos klaidų, reklamuojami „stebuklingi“ išgydymai ar garsenybių skandalai. Svarbu atminti, kad ir tvarkingoje reklamoje ar skelbimuose, atitinkančiuose Jūsų naršymo istoriją, taip pat gali būti kenkėjiškų programų, todėl reikia būti atsargiems ir ieškoti dominančių dalykų patikimose paieškos sistemose;
- „Fišingo“ rinkiniai (angl. phishing kits). Tai yra svetainės, imituojančios dažniausiai lankomas svetaines, pvz., bankininkystės svetaines, socialinių tinklų svetaines ir pan., siekiant apgauti vartotojus perimant privačią informaciją. Reikia atkreipti dėmesį į naršyklėje matomą svetainės adresą, ar svetainės vardas (URL adresas) neturi gramatinių klaidų, ar jis nėra neįprastos sandaros;

- Kenkėjiškas peradresavimas (angl. malicious redirect). Jei įvedant URL adresą esate nukreipiami į kitą svetainę, ypač į tą, kuri atrodo įtartina, Jus paveikė kenkėjiškas peradresavimas, kuris dažnai naudojamas kartu su „fišingo“ rinkiniais. Nenaršykite tokioje svetainėje, perkraukite naršyklę prieš tolimesnį naršymą internete;
- Paieškos šlamštas (angl. SEO spam). Neįprastų nuorodų atsiradimas svetainėje, dažnai komentarų skiltyje, yra tikras paieškos šlamšto ženklas;
- Įspėjimai paieškos sistemose. Populiarios paieškos sistemos tikrina svetaines dėl kenkėjiškų programų ir deda įspėjimą apie tai. Neverta ignoruoti šių įspėjimų, nes jie vienareikšmiškai parodo, kad svetainė užkrėsta kenkėjiška programine įranga.

Teisės labirintai
+370 630 17 959
info@teiseslabirintai.lt
www.teiseslabirintai.lt