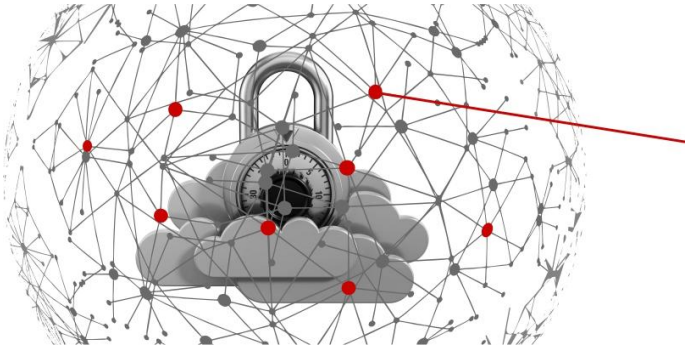

Saugumas skaitmeninėje erdvėje

Kiekvienais metais internete įvykdoma milijonai nusikaltimų. Kibernetiniai nusikaltėliai naudojasi įvairiais būdais, kad gautų prieigą prie mūsų banko sąskaitų ar duomenų, kurie gali palengvinti jų tolesnius neteisėtus veiksmus. Atrodo, kad mes esame tiesiog nekaltos tokių nusikaltimų aukos, tačiau tiesa yra ta, kad mes dažnai iš dalies esame atsakingi už tai, kas su mumis vyksta. Pagrindinių interneto saugumo taisyklių nepaisymas yra tarsi palikti atidarytas lauko duris ar raktus spynoje per naktį. Kita vertus, reikia tik nedidelių įpročių pokyčių, kad kibernetiniams nusikaltėliams būtų daug sunkiau (ar net neįmanoma) patekti į mūsų asmens duomenis.

Šiuo metu internetu naudojasi 4,5 milijardo žmonių, tai yra 60% mūsų planetos gyventojų. Pusė žmonijos, tai yra maždaug 4 milijardai žmonių, naudojasi socialine žiniasklaida ir vidutiniškai internete praleidžiamas laikas yra 6 valandos 43 minutės. Tai yra beveik 30% dienos, 100 dienų per metus!

SARS-COV-2 epidemija, prasidėjusi 2020 m. pradžioje, sustiprino šią tendenciją. Reikalavimas vengti asmeninių kontaktų, kai tik įmanoma, privertė daugelį tradicinių verslų veikti internete ir vykdyti elektroninę prekybą, o mus rinktis daugiau internetinių pramogų galimybių.

DUOMENYS NIEKADA NEMIEGA!

CLICK HERE!

Kitas veiksnys, prisidėjęs prie skaitmeninimo proceso, yra mobiliųjų įrenginių plėtra. Šiuo metu jau daugiau nei 50% laiko praleidžiame internete naudodami išmaniuosius telefonus, kuriuos visur nešiojamės. „AppAnnie“ ataskaitos duomenys rodo, kad išmaniuosiuose telefonuose praleidžiame 10 iš 11 minučių naudodamiesi mobiliosiomis programomis, tokiomis kaip įvairūs komunikatoriai, socialinė žiniasklaida, pramogos, vaizdo grotuvai, žaidimai, apsipirkimo, bankininkystės ar muzikos programos, žemėlapiai ir navigacijos ar pažinčių programos. „Ericsson Company“ duomenimis, interneto vartotojai per metus savo mobiliaisiais įrenginiais suvartoja 50 milijardų gigabaitų, iš kurių 60% naudojama vaizdo srautui perduoti.

Aukščiau pateikti skaičiai gali nustebinti, nors mes žinome, kad skaitant šį tekstą jie greičiausiai nebėra tikslūs, nes mūsų nurodoma statistika nuolat ir greitai auga. Šį procesą skatina galingos korporacijos ir pradedančiosios įmonės, gaminančios ir platinančios įrenginius ir programinę įrangą, kad vartotojai, norėdami ne tik didinti interneto prieinamumą pasaulyje, bet ir kiekvieną dieną norėtų ieškoti neribotų interneto išteklių.

Didžiausi virtualios rinkos dalyviai, tokie kaip „Google“ ar „Facebook“, teikia mums paslaugas ir programas, palengvinančias arba daugeliu atvejų įgalinančias darbą ir bendravimą. Jie teikia pramogas, suteikia lengvesnę prieigą prie žinių, sukuria galimybes tyrinėti ir ieškoti pasaulinių mokslo šaltinių. Mes noriai naudojamės tokiomis galimybėmis, nes jos yra

nemokamos. Bet ar jie tikrai nemokami? Iš tiesų yra įvairių programų ir programinės įrangos, už kurias nereikia atsiskaityti grynaisiais pinigais ar banko pavedimu. Tačiau tai nereiškia, kad už juos visiškai nemokama. Skaitmeninis pasaulis vertina ne tik pinigus, bet ir dar labiau vertina mūsų duomenis, asmeninius duomenis, kuriais dalinamės atsisiųsdami „nemokamą“ programinę įrangą, filmus, žaidimus, naršydami socialiniuose tinkluose, apsipirkdami virtualiose parduotuvėse, informaciją apie naudojamus įrenginius, savo vietą, elgesys - tiek internete, tiek realiame pasaulyje. Informacija apie mūsų išvaizdą, šeimą, draugus, pomėgius, veiklą, darbą, finansus, svajones, planus ir kt.

KIBERNETINIŲ NUSIKALTIMŲ STATISTIKA
CLICK HERE and HERE

XXI amžiaus pradžioje pasiūlymas įdėti identifikavimo lustą, pavyzdžiui, į asmens tapatybės dokumentą, sukėlė ginčų ir pasipriešinimą. Tai buvo vertinama kaip neteisėtas kišimasis į privatumą ir asmens orumą. Šiais laikais esame pasirengę savanoriškai dalytis daug daugiau nei tik savo asmens duomenimis.

TOP 5 DIDŽIAUSIOS KIBERNETINĖS ATAKOS
CLICK HERE

Tačiau yra teigiamas tokio elgesio aspektas. Didelių duomenų bazių rinkimas leidžia mums surinkti tokią statistiką, kokios nebuvo anksčiau. Tyrėjai iš viso pasaulio gali dirbti kartu ir naudoti vienas kito tyrimų rezultatus, taip pat savarankiškai sukurtus metodus ir mokslinius modelius.

Didieji duomenys turi daug privalumų visai žmonijai, tačiau kibernetiniams piratams taip pat suteikia daugybę galimybių. Duomenys, kurie taip noriai ir dažnai siunčiami į pasaulį, pavogus gali tapti rimtų bėdų šaltiniu. Galima užsipulti bet ką: slaptažodžius banko sistemose, privačias nuotraukas ar prisijungimo prie svetainės istoriją. Tokie išpuoliai vyksta kiekvieną dieną, o elektroninių nusikaltimų statistika įrodo, kokia ši problema tapo rimta.

Pažiūrėkime, kiek kibernetinių nusikaltimų buvo padaryta per vieną 24 valandų laikotarpį (nuo 2020 m. Gegužės mėn.):

- apie 62,4 mln. įsilaužimų į sistemą

- įsilaužėlių ataka kas 39 sekundes

- išsiųsta 6,4 mln. Melagingų el. Laiškų

- 4 739 svetainės nulaužė daugiau nei 100 kartų

- daugiau nei 1200 skundų dėl asmeninių kompiuterių įsilaužimo vien JAV.

Ataskaitos ir statistika taip pat rodo, kad per praėjusių 3 mėnesių laikotarpį kenkėjiška programa buvo užkrėsti 232 292 individualūs vartotojai. Tuo pačiu metu įvyko 260 000 sėkmingų sukčiavimo išpuolių tų, kurie maskavosi kaip patikimi subjektai. Praradus duomenis atsiranda socialinio ir ekonominio pobūdžio pasekmės. Išpirkos programa (blokuojanti prieigą prie kompiuterio, nebent bus sumokėta išpirkos kaina) pernai patyrė 3,5 mlrd. 2019 m. Kriptovaliuta buvo užpulta 52,7 mln.

KIEK SAUGUS YRA TAVO SLAPTAŽODIS?
CLICK HERE

Kodėl tiek daug išpuolių prieš asmens duomenis? Be abejo, yra kaltinamų kibernetinių nusikaltėlių, nes jie yra suinteresuoti pavogti mūsų duomenis ir nuolat tobulina įsilaužimo galimybes. Jie naudoja naujoviškus metodus, kad galėtų pasiekti interneto vartotojus ir jų įrenginius, kad pavogtų jiems reikalingą informaciją. Deja, neatrodo, kad didėjantis kibernetinių nusikaltimų skaičius padidino supratimą apie tokius pavojus ir sugebėjimą jų išvengti.

Dėl žinių trūkumo ir pagrindinių saugos taisyklių nepaisymo kibernetiniams nusikaltėliams lengviau gauti greitą prieigą prie mūsų duomenų. Tiksliau: 63% tinklo įsilaužimų įvyksta dėl slaptažodžių ir vartotojo vardų sulaužymo, o tai yra dėl to, kad dauguma slaptažodžių yra paprasti ženklų deriniai. Mes dažnai nežinome, kaip lengva rasti mūsų duomenis ir naudoti juos neteisėtais ar nepageidaujamais tikslais. Asmeninę informaciją, kuria noriai dalijamės su socialinės žiniasklaidos vartotojais, gali lengvai užfiksuoti įsilaužėlių. 2019 m. Pastebėta apie 849 mln. Asmens duomenų nutekėjimo per vieną populiarią socialinės žiniasklaidos paslaugą („Facebook“).

APSAUGOKITE SAVO DUOMENIS

CLICK HERE

Žemiau pateikiame interneto saugos taisykles. Jų laikydamiesi galime apsaugoti save ir savo duomenis nuo kibernetinių nusikaltėlių išpuolių.

KAIP NAUDOTIS INTERNETU SAUGIAU?

1. VISADA PASIRINKITE STIPRIUS SLAPTAŽODŽIUS

Slaptažodis, kuriame yra jūsų vardas, gimimo data, prisijungimo vardas ar bet kas, kas su jumis lengvai susiejamas, nėra nei geras, nei tvirtas. Stiprūs slaptažodžiai sujungia mažąsias ir didžiąsias raides, skaičius ir specialiuosius ženklus. Kaip mes galime sustiprinti savo slaptažodį per kelias sekundes? Jei mūsų slaptažodis yra „ersmusproject2020“, galime tiesiog pridėti kelias didžiąsias raides ir specialiuosius simbolius: „Er @ $ mu $ _pro! Ect_2020“.

2. NEIŠSAUGOKITE SLAPTAŽODŽIŲ AUTOMATIŠKAI

Atminkite, kad kiekvienai paskyrai turėtumėte pasirinkti skirtingus slaptažodžius - pakartojimai nėra priimtini. Negalima automatiškai išsaugoti slaptažodžių. Ar sukūrėte tvirtą slaptažodį ir bijote jį pamiršti? Slaptažodžių tvarkyklės programinė įranga gali padėti valdyti kelis slaptažodžius ir prisijungimo duomenis. Tai saugi vieta, kurioje galite laikyti visus savo skaitmeninio gyvenimo raktus.

3. VISADA PATVIRTINKITE SIUNTĖJĄ

Apgaulingos atakos pagrindas yra maskuotis kaip patikimas subjektas, todėl prieš tikrindami visada turėtumėte atkreipti dėmesį į siuntėjo adresą ir niekada neatidaryti nuorodų (adresą galima patikrinti užvedus pelės žymeklį ant nuorodos). Atidžiai patikrinkite, ar raidės išdėstytos teisinga tvarka ir ar siuntėjo domenas - siuntėjas, persirengęs paslaugų teikėju, naudos kitą šalies kodą iš aukščiausio lygio domeno arba tiesiog sukurs naują, padirbtą.

4. ĮSITIKINKITE, AR VISKĄ SUPRANTATE TEISINGAI IR NEREAGUOKITE EMOCIONALIAI

Sukčiavimo užpuolikai bando manipuliuoti aukų emocijomis. Atminkite: jūsų elektroninio pašto adreso negalima išjungti per naktį, taip pat negalima iškart užblokuoti jūsų banko sąskaitos ar telefono numerio. Kaip atpažinti melagingą pranešimą? Atkreipkite dėmesį į gramatinį ir sintaksinį teisingumą, pertvarkytas raides ir laiką, kurį jums suteikiama, kad

sureaguotumėte - kibernetiniai nusikaltėliai dažnai tikisi, kad elgsitės nedelsiant, nes kitaip bus padarytos pasekmės (pvz., Jūsų banko sąskaita bus užblokuota). Jie neklausia - kelia reikalavimus.

5. NEKELKITE SAVO ASMENS TAPATYBĖS DOKUMENTŲ SKENUOČIŲ AR NUOTRAUKŲ Į INETERNETĄ

Elektroniniai nusikaltėliai galės užfiksuoti jūsų nuskaitytus asmens tapatybės dokumentus ir imti paskolą jūsų vardu, palikdami juos mokėti daugelį metų.

6. NAUDOKITE PRIVATUMO NUSTATYMUS, KAI NAUDOJATĖS SOCIALINIAIS TINKLAIS

Negalima dalintis per daug asmeninės informacijos su socialinės žiniasklaidos vartotojais, atminkite, kad viskas, kas rodoma internete, lieka ten amžinai. Gerai pagalvokite prieš pateikdami bet kokią informaciją internete.

7. ŠIFRUOKITE DUOMENIS

EFEKTYVUS DUOMENŲ KODAVIMAS

CLICK HERE!

Galite padaryti internetiniam nusikaltėliui sunkų ar net neįmanomą darbą skaityti jūsų duomenis, net jei jam pavyksta juos pavogti. Galite užšifruoti savo įrenginius (standųjį diską, „Pendrive“ ir visų tipų duomenų laikmenas), failus ir elektroninius laiškus.

8. SUSIKURKITE ATSARGINES KOPIJAS

Kad neprarastumėte svarbios informacijos, reguliariai kurkite atsargines kopijas. Galite naudoti išorinę ir vidinę laikmeną bei tinklo vietą. Norėdami gauti daugiau informacijos, žr. https://support.microsoft.com/pl-pl/help/971759/how-to-back-up-or-transfer-your-data-on-a-windows-based-computer.

9. NESIJUNKITE PRIE VISIEMS PRIEINAMO WI-FI

Prisijungti prie neapsaugoto viešojo „Wi-Fi“ viešosios interneto prieigos taško yra labai rizikinga. Jei atrodo, kad tai neišvengiama, prisiminkite keletą pagrindinių saugos taisyklių: išjunkite duomenų bendrinimą, venkite automatinio prisijungimo prie „Wi-Fi“ tinklo, naudokite VPN, įjunkite užkardą. Norėdami gauti išsamesnės informacijos, kaip išvengti užpuolimo prisijungiant prie viešojo „Wi-Fi“, patikrinkite: https://www.binance.vision/pl/security/why-public-wifi-is-insecure .

10. PRIEŠ JUNGDAMIESI PRIE BANKO PASKYROS, PATIKRINKITE, AR NĖRA UŽRAKTO IKONOS

Kairėje paieškos juostos pusėje yra spynos piktograma. Galite spustelėti, kad būtų rodoma išsami tinklalapio informacija. Čia galite patikrinti, ar jis yra saugus ir ar turi SSL sertifikatą (šifruoja perduodamus duomenis). Jei taip - nereikia jaudintis, perduoti duomenys negali būti naudojami pašaliniams asmenims. Atminkite: spynelė turi būti uždaryta, jei ji atidaryta, svetainė yra neapsaugota.

11. NESISIŲSKITE FAILŲ IŠ PUSLAPIŲ, KURIAIS NEPASITIKITE

Visada atsisiųskite nemokamą programinę įrangą iš gamintojo svetainės. Jei atsisiųsite programą iš svetainės, kuria nepasitikite, yra rizika įdiegti ir kenkėjišką programą.

12. PERSKAITYKITE DUKART PRIEŠ PRIIMDAMI INTERNETU

Neatsargus skaitymas dažnai nesąmoningai dalijasi savo asmens duomenimis su pašaliniais asmenimis arba pasirašo sutartį, kurios iš tikrųjų nenorite pasirašyti. Šlamšto pranešimų

skaičius jūsų pašto dėžutėje atsiranda dėl to, kad automatiškai priimate visus neprivalomus taškus pagal skirtingus reglamentus ir susitarimus. Atminkite, kad priimant serverio ar svetainės taisykles, reikia patikrinti tik privalomus laukus. Jei skaitote nekreipdami ypatingo dėmesio į smulkmenas, taip pat rizikuojate sumokėti pinigus sukčiavimams, kurie bando jus įtikinti, kad užsiregistravę tam tikroje svetainėje turėsite galimybę laimėti naują „iPhone“.

Šių 12 paprastų taisyklių, kaip saugiai naudotis internetu, nesunku laikytis. Tačiau dažnai daugelį jų sulaužome. Mes linkę naudoti tą patį slaptažodį arba leisti jį prisiminti automatiškai. Mes dažnai sutinkame su taisyklėmis jų net nenumalšindami - laukiame programos atsisiuntimo, pirkimo užbaigimo ar naujos paskyros sukūrimo. Norėdami jaustis saugiau internete, turime atsisakyti senų, blogų įpročių ir priimti naujus. Štai kaip tokį procesą apibūdina asmeninio tobulėjimo guru ir motyvacinis kalbėtojas Brianas Tracy:

Geri įpročiai yra jūsų sėkmės ir laimės šaltinis, o analogiškai blogi įpročiai yra atsakingi už daugumą jūsų problemų ir nesėkmių.

Tačiau blogų įpročių taip pat išmokstama, todėl jų galima neišmokti ir pakeisti gerais (B. Tracy: milijono dolerių įpročiai).

Pakeisti senus įpročius niekada nėra lengva, tačiau tikrai verta pasistengti.