Project IDCAP: Improve Digital Competence in Adult People

Project Number: 2018-1-PL01-KA204-051003

Skaitmeninė tapatybė

1. Įvadas

Kalbant apie skaitmeninę ar internetinę tapatybę, skaitmeninė tapatybė yra informacija, vaizduojanti realų asmenį ar kitą išorės agentą. Išorinis agentas taip pat gali būti atskira mašina, sistema ir (arba) programa. ISO / IEC 24760-1 tapatybę apibrėžia kaip „su subjektu susijusių atributų rinkinį“. Šiais laikais mes kalbame apie tapatybę kaip tam tikrus subjekto, kuris pakeitė terminą „agentas“, atributus. Šiame dokumente bus kalbama tik apie skaitmeninę tapatybę. kaip fizinio asmens tapatybę.

Pateiksime jūsų skaitmeninės tapatybės tvarkymo pagrindus ir kodėl svarbu ją apsaugoti. Toliau pamatysime daugiau informacijos apie tai, kaip valdyti ir internetinę sąskaitą bei kokie yra pagrindiniai proceso veiksmai. Toliau pateiksime saugumo ir privatumo internete pagrindus. Galiausiai trumpai aptarsime skaitmeninio pėdsako ir internetinės tapatybės problemas.

2. Skaitmeninės tapatybės valdymas

Skaitmeninės tapatybės valdymas remiamas principais, daugiau ar mažiau žinomais mechanizmais, kurie buvo sukurti ne skaitmeninei tapatybei. Tai gali pasirodyti sudėtinga, tačiau pagalvokite apie savo asmens tapatybės kortelę. Paprašant gauti asmens tapatybės kortelę, ją išduodanti institucija patvirtina jūsų gimtadienį, mokesčių kodą, piliečio numerį (jei jis yra), padaro naują nuotrauką ir t.t. Skaitmeniniame pasaulyje jūsų skaitmeninė tapatybė gali būti tokia pat paprasta kaip jūsų. vartotojo vardas ir slaptažodis arba jis gali būti daug sudėtingesnis, kad garantuotumėte, jog tos pačios tapatybės savininkas esate jūs, tik jūs. Šie lygiai gali apimti atskirą elektroninį parašą, „atsitiktinio“ tam tikro skaitmeninio kodo generavimo ženklą, SMS patvirtinimą arba kodą, siunčiamą į tam tikrą mobilųjį telefoną (kuris, kaip žinoma, registruotas konkrečiam asmeniui), balso atpažinimą, atsakymą į konkretų klausimą (pvz., koks buvo jūsų pirmojo augintinio vardas?), pirštų atspaudų patvirtinimo ir daugelio kitų. Visi šie lygiai yra skirti garantuoti, kad tik konkrečiam asmeniui leidžiama atlikti kai kuriuos veiksmus skaitmeniniame pasaulyje.

Daugeliui vartotojų sunku suprasti tuos lygius, jie yra painūs ir varginantys. Žmonės gali būti teisūs, tačiau, kita vertus, reikėtų suprasti, kad skaitmeninis pasaulis yra tiesioginis fizinio pasaulio vaizdas ir niekas nenorėtų, kad jų „skaitmeniniai“ pinigai nutekėtų iš jų „tikrosios“ banko sąskaitos. Įstaigos, ypač bankai, teikia įvairius saugumo lygius, ne erzinti vartotojus, o siekdamos apsaugoti jų tapatybę ir užtikrinti operacijų teisę. Tuo pačiu metu vis daugiau paslaugų teikiama per jūsų mobilųjį telefoną. Jie apima platų asortimentą, ir tik keletą iš jų pateiksime kaip iliustraciją. Galvokite apie jas kaip apie paslaugas, kurios daro tiesioginę įtaką jūsų „tikrajai“ banko sąskaitai. Kai kurios iš šių paslaugų teikiamos naudojant

išmaniuosius telefonus (atsižvelgiant į jūsų gyvenamąją šalį):

- Mokėstis už automobilio stovėjimą (SMS žinutė)
- Sąskaitos apmokėjimas prekybos centre
- Namų sąskaitų apmokėjimas
- Tiesioginis pinigų pervedimas per tam skirtą banko įgaliotą programą

3D patvirtintas jūsų VISA arba Master Card mokėjimas - pateikę kortelės numerį, galiojimo laiką ir saugos kodą, ši sistema siunčia SMS žinutes su 6 skaitmenų kodu į iš anksto patikrintą mobilųjį telefoną, kuris pridės dar vieną jūsų kortelės operacijų apsaugos sluoksnį.

Perkant bilietus į sausumos arba oro transportą su “Apple pay” arba “Google wallet” programomis, jūsų telefonas tampa visų mokėjimų palaikančių NFC ar magnetinius mokėjimus pinigine. Tai netgi leidžia jums gauti mokėjimus iš įvairių interneto svetainių, parduotuvių ir vartotojų.

Suprantama, kodėl taip svarbu tinkamai valdyti savo skaitmeninę tapatybę ir kodėl reikia ją energingai saugoti.

3. Internetinės sąskaitos tvarkymas

Kaip jūsų skaitmeninės tapatybės dalis, jūsų internetinė sąskaita yra pirmas ir daugeliu atvejų neišvengiamas žingsnis. Paprastai jis yra prijungtas prie el.pašto paslaugų, tokių kaip Google, Gmail, Yahoo, Microsoft el. paštas ir kt. Sukūrę tokią sąskaitą, prie jos turite pridėti bent du kintamuosius: savo vartotojo vardą ir slaptažodį. Šiandien dauguma teikiamų paslaugų reikalauja, kad kiekvienoje konkrečioje sąskaitoje būtų pridėtas ir patvirtintas mobiliojo telefono numeris. Taigi skaitmeninės tapatybės

abonementas turi 3 atributus - vartotojo vardą, slaptažodį ir mobiliojo telefono numerį. Daugeliu atvejų šis patikrinimas jūsų neprašant ir siekiant

dar labiau apsaugoti jus prideda ne tik telefono numerį, bet ir unikalų mobiliųjų telefonų gamybos numerį, vadinamą IMEI - tarptautine mobiliosios įrangos tapatybe. Šis numeris, priskirtas gamybos metu, reikalingas tam, kad būtų leista naudoti mobilųjį telefoną ir mobiliuoju tinklu. Tą informaciją užšifruoja ir saugo interneto paslaugų teikėjai, tačiau retais atvejais ji vis dar gali būti pavogta ar neteisėtai panaudota (pvz., Facebook ir Cambridge Analytica atveju, kai milijonai vartotojų duomenų įmonei buvo pateikti siekiant daryti tikslinę reklamą politiniais tikslais). Čia yra keletas patarimų, kurie padės sukurti jūsų skaitmeninę tapatybę:

Vartotojo vardas: pasirinkite vartotojo vardą, kuris aiškiai atspindi jus. Pagalvokite, kad galbūt ateityje naudosite šį konkretų el.pašto adresą, o juokingi vardai ne visada yra gerai priimami. Jūsų vartotojo vardas liks prieš jūsų @ el.pašto ženklą, todėl tokių vardų kaip „easygirl @“, „toughguy @“, „nightnightre @“ reikia vengti, Kai pasirenkate savo vartotojo vardą, neįtraukite tokių skaičių kaip jūsų gimtadienis ar jūsų artimųjų gimtadieniai.

Slaptažodis: naudokite mažųjų, didžiųjų raidžių, skaičių ir spec. simbolių, tokių kaip #, $, &, |, ~, derinį. Padarykite jį bent iš 8 ženklų ir dažnai keiskite slaptažodį. Jei prie savo skaitmeninės sąskaitos prisijungiate naudodamiesi mobiliuoju telefonu, naudokite pirštų atspaudus ar kitą tapatybės nustatymo formą. “Nepriminkite” savo paskyros slaptažodžio. naršyklėje.

Net jei neprivalote, pridėkite mobilųjį telefoną prie savo paskyros ir nustatykite jį kaip numatytąjį įrenginį atkurti pamirštus slaptažodžius. Peržiūrėkite savo paskyros nustatymus ir nustatykite atkūrimo el.pašto adresą bei telefono numerį, kad dar geriau patvirtintumėte savo tapatybę.

Nenaudokite to paties slaptažodžio kitose paskyrose, tokiose kaip socialiniuose tinkluose ar žaidimuose.

.

4. Saugumo ir privatumo klausimai

Kai kurie serveriai ir programos gali surinkti išsamią informaciją apie tam tikrą naudojimą ir gali būti susieti su fiziniu asmeniu ir jo skaitmeniniais įpročiais internete. ES lygiu bandoma spręsti GDPR (Bendrasis duomenų apsaugos reglamentas), tačiau vis tiek vartotojams rekomenduojama būti atsargiems, ką ir kur jie dalijasi bei daro per internetą ir ypač kai kuriuos socialinius tinklus.

Norėdami apdoroti savo skaitmeninį turinį, yra daugybė nuotraukų ir vaizdo įrašų redaktorių, tuo tarpu paprastai socialinė žiniasklaida teikia rašytinio teksto rašybos tikrinimo galimybes ir anglų kalba. Prie skaitmeninių nuotraukų (ir vaizdo įrašų) galite pridėti įvairių filtrų, pakeisti sodrumą, kontrastą ir tt. Galite naudoti tuos, kurie pateikiami su jūsų prietaisu, arba įdiegti jums labiausiai patinkantį. Atminkite, kad dauguma nemokamų internetinių redaktorių paprastai turi tam tikrų apribojimų ir jūs turite nusipirkti vieną, kad atrakintumėte visas funkcijas. Šios programinės įrangos paslaugos dažnai prideda prie jūsų nuotraukos ar vaizdo įrašo parašytą ženklą, kad medžiaga buvo sukurta naudojant šią programinę įrangą, kuri jums gali nepatikti. Eksperimentuokite ir patikrinkite, kol rasite tai, kas patenkins jūsų poreikius.

Kaip pabrėžta EBPO 2016 m. tyrime: „Vykdant veiklą, kuri remiasi skaitmenine aplinka, neįmanoma visiškai pašalinti skaitmeninio saugumo rizikos. Tačiau rizika gali būti valdoma, tai yra, ją galima sumažinti iki priimtino lygio, atsižvelgiant į svarbius interesus ir naudą bei aplinkybes “. Tačiau yra gana pagrįstų ir gana lengvų žingsnių, kuriuos gali atlikti asmuo

ar organizacija, kad būtų pasiektas patenkinamas skaitmeninio saugumo ir privatumo apsaugos lygis. Tai apima griežtus slaptažodžius, griežtą prieigos prie interneto politiką, sveiką protą naršant internete, švietimą ir mokymą dažniausiai naudojamomis temomis, asmens duomenų ir asmens

duomenų apsaugos politikos nustatymą. Vis dėlto pasakius, kad ES taiko aukščiausius asmens ir privatumo duomenų apsaugos standartus pasaulyje.

Kaip asmenybė, privatumo pažeidimo galimybė yra ribota. Visada reikia atidžiai perskaityti bet kurios svetainės, interneto paslaugų, naujienų ir socialinės žiniasklaidos platformų slapukų politiką. Jei nenorite būti stebimi (tai yra kai kurios svetainės renka duomenis apie jūsų naršymo įpročius, kaip dažnai lankotės tam tikroje svetainėje, kokias reklamas spustelite, kokios informacijos ieškote iš interneto ir pan.), Galite naudoti asmeninį naršymą. langą, kurį siūlo beveik visos naršymo programos, tokios kaip Google Chrome, Mozilla Firefox,„Microsoft, Internet Explorer ir kt.

Saugumo aspektu niekada neturėtų naudoti tų pačių slaptažodžių įvairioms interneto programoms, tokioms kaip el.paštas, socialinės žiniasklaidos platformos ir svetainės, prie kurių reikia prisijungti. Laikykite savo slaptažodį tvirtu, sudarydami 10 ar daugiau simbolių, įskaitant skaičius, didžiąsias ir mažąsias raides bei specialiuosius simbolius, pvz. &, #, $, ^ ir kt. Paprastai neišsaugokite savo slaptažodžių naršyklėje, bet pabandykite juos atsiminti arba sukurti pagal savo suformuluotą taisyklę. Pavyzdžiui:

#MyFamilyName4websiteName~mY_first.name$.

Nors tai gali atrodyti sudėtinga, taisyklę lengva atsiminti. Jei įmanoma, pridėkite savo mobilųjį telefoną kaip alternatyvą autentifikavimui pamiršto ar pavogto slaptažodžio atkūrimui. Tai pridės dar vieną asmeninės

apsaugos sluoksnį, kuris sumažins kenksmingo jūsų internetinių duomenų naudojimo riziką.

5. Skaitmėninis pėdsakas

Skaitmeninis pėdsakas reiškia unikalią atsekamą konkretaus vartotojo skaitmeninę veiklą internete. Šį terminą taip pat galima rasti kaip skaitmeninį šešėlį, interneto pėdsaką, kibernetinį šešėlį ir t.t, nors paprastai terminas yra taikomas fiziniams asmenims, jis taip pat gali būti naudojamas organizacijoms, įmonėms, korporacijoms, skaitmeninių paslaugų svetainėms ir pan. Yra du skaitmeninio pėdsako tipai. - aktyvus ir pasyvus.

Pasyvus skaitmeninis pėdsakas - šis terminas reiškia duomenis, surinktus be asmens žinios. Vartotojas tai nebūtinai gali paslėpti. Aktyvus skaitmeninis pėdsakas yra tas, kuriuo vartotojas sąmoningai dalijasi apie save dažniausiai socialinėje žiniasklaidoje ar įvairiose svetainėse. Informacija apie vartotoją gali būti tyčia ar netyčia palikta, tada šią informaciją aktyviai arba pasyviai renka kitos šalys. Pvz., jei savo socialinės žiniasklaidos profilyje palikote matomą visą savo el.pašto adresą, savo mobiliojo telefono numerį, gyvenamosios vietos adresą, darbo vietą, įmonės interneto adresą ir t.t, tai bus gana lengva kompiuterio programai ar fiziniam asmeniui. surinkti jums labai didelį kiekį informacijos. Kai kuriais atvejais ši informacija taip pat gali apimti jūsų banko sąskaitas ar mokesčių įrašus, jei įvyksta saugumo įrašų pažeidimas.

Buvo atlikta nemažai tyrimų, kurie rodo, kad maždaug 70% visų žmonių skaitmeninio elgesio yra sąmoningi ir už juos atsakingi. Tačiau apie 30%

kiekvieno asmens skaitmeninio pėdsako forma gali būti tokia, kokia niekada nebuvo tyčia atskleista visuomenei. Tai palieka gana daug duomenų pirkimo elgsenos, pirkimo internetu įpročių, pomėgių ir kitų asmeninio gyvenimo sričių analizėms. Nors didelėse duomenų bazėse vykdomos klientų analizės nėra nieko blogo, tokios analizės gali būti tapatybės vagystės, nusikalstamos veiklos ir privatumo pažeidimų pagrindas.

Nors skaitmeninis pėdsakas nėra skaitmeninė tapatybė ar skaitmeninis ID, turinys ir aprašomieji duomenys (dar vadinami meta duomenimis) daro didelę įtaką privatumui, pasitikėjimui internetu ir skaitmeninei reputacijai.

Internetinius pėdsakus įmonės gali naudoti įdarbindamos naujus darbuotojus, teisėsaugos institucijos, rinkdamos duomenis apie konkrečius asmenis, negali būti renkamos kitomis priemonėmis, rinkodaros specialistai ieško, kokio tipo produktai ar paslaugos domina vatotojus. Pagrindinis tokios informacijos šaltinis yra socialiniai tinklai. Kai kuriais atvejais socialinės platformos gali rinkti duomenis iš vartotojo įrenginio, net vartotojui to nežinant, naudojant įvairius jutiklius mobiliuosiuose telefonuose ar kituose vartotojo įrenginiuose. Pavyzdžiui, Facebook ir Google renka daug informacijos apie vartotoją, kuri kartu sudėjus gali gana išsamiai apibūdinti vartotojo asmenybę, pomėgius, politines pažiūras, pirkimo įpročius ir pan.

6. Internetinė tapatybė

Internetinė tapatybė - tai tapatybė, kurią vartotojas pasirenka internete, paprastai žaidimų tikslais. Naudotojai gali pasirinkti, kaip save vaizduoti su vaizdais (piktogramos dydžio grafika), o ne su tikromis nuotraukomis. Vartotojai taip pat gali naudoti slapyvardžius vietoj tikrųjų vardų. Internetinę tapatybę netgi gali nulemti vartotojo nuorodos į interneto žmonių grupę. Internetinės tapatybės su realiais vartotojais susiejamos naudojant leidimų suteikimo procedūras, tokias kaip registracija ir prisijungimas (vartotojo

vardas ir slaptažodis), taip pat per konkretų mašinos ar įrenginio IP adresą. Tokiose svetainėse dažnai įdiegiami stebėjimo slapukai, kurie gali padėti nustatyti vartotojo elgesį internete ir susieti jį su realiu asmeniu. Kadangi žaidimai dažnai, bet ne visada, yra skirti jaunesnei auditorijai, kuri nėra tokia atsargi, kad apsaugotų save internete, labai svarbu, kad skaitmeninės tapatybės, internetinės tapatybės ir skaitmeninio pėdsako sąvokos būtų kuo aiškesnės visiems, naudojantiems internetą.

Internetine tapatybe gali būti bet koks dalykas - jūsų el.pašto kredencialai (vartotojo vardas ir slaptažodis) iki socialinės žiniasklaidos paskyros, forumo pavadinimo ar pirkėjo profilio tam tikroje svetainėje. Tai taip pat apima jūsų naršymo istoriją, IP adresą, paieškos veiklą ir kt. Žmonės ir organizacijos gali būti suinteresuoti jūsų internetine tapatybe visiškai legaliais ar neteisėtais tikslais (įsilaužėliai). Kai kurios kompanijos turi žinoti jūsų naršymo ar paieškos istoriją, kad pasiūlytų jums tikslingesnius produktus ar paslaugas, susijusius su jūsų poreikiais ir interesais. Kiti gali būti suinteresuoti neteisėtais tikslais pavogti jūsų duomenis, kreditinės kortelės numerį ir kt.

Yra keletas būdų, kaip apsaugoti savo internetinę tapatybę, pvz., stiprūs slaptažodžiai, ne per daug dalijimasis asmeniniais duomenimis socialiniuose tinkluose, naršyklės inkognito režimo naudojimas, virtualių privačių tinklų naudojimas, jūsų komunikacijos šifravimas ir kt. Kuo daugiau dėmesio skirsite savo internetinėi tapatybėi, tuo labiau busite apsaugotas.

7. Santrauka

Mes pristatėme pagrindines sąvokas ir žinias apie skaitmeninės tapatybės ir internetinės paskyros valdymą. Vadovaudamiesi tomis pagrindinėmis sąvokomis, aprašėme, kas yra saugumo problemos ir vartotojo privatumas. Galiausiai pristatėme, kas yra skaitmeninis pėdsakas ir internetinė tapatybė.

Tai pat pasiūlėme lengvus ir suprantamus slaptažodžių, autentifikavimo, skaitmeninės tapatybės, privatumo ir naršymo internete metodus. Kai asmuo ar organizacija įvykdys šias tezes, tai gali žymiai sumažinti bet kokią internetinę riziką. Tačiau, nėra sprendimų, apimančių visus atvejus, taip pat nėra strategijos organizavimo lygmeniu, kuri padėtų kovoti su kenkėjiškais veiksmais internete ir padidintų pasitikėjimą internetu ir visomis skaitmeninėmis platformomis.

Galiausiai apžvelgėme internetinę tapatybę ir atkreipėme dėmesį į tai, ką ji apima, ir kaip apsisaugoti nuo neteisėto savo tapatybės naudojimo.

Bibliografija:

https://www.zdnet.com/article/identity-management-101-how-digital-identity-works/

https://www.forbes.com/sites/forbestechcouncil/2019/06/07/a-beginners-guide-to-online-privacy-12-important-tips/#5092374e53ed

https://assets.mozilla.net/pdf/IHPbriefs_Online_Privacy_March_2017.pdf

https://www.commonsense.org/education/digital-citizenship/topic/digital-footprint-and-identity

https://www.oecd-ilibrary.org/docserver/5jlwt49ccklt-en.pdf?expires=1591780736&id=id&accname=guest&checksum=AF002079529F4DE263769B3FBEB40035