Projekts “IDCAP”: Digitālo prasmju uzlabošana pieaugušajiem

Projekta numurs: 2018-1-PL01-KA204-051003

# Digitālā identitāte

# Ievads

Digitālās vai interneta identitātes kontekstā digitālā identitāte ir informācija, kas attiecas uz reālu personu vai citu ārēju aģentu. Ārējais aģents var būt arī konkrēta ierīce, sistēma un/vai lietotne. Standartā ISO/IEC 24760-1 identitāte definēta kā “ar juridisku vai fizisku personu saistītu īpašību kopums”[1]. Mūsdienās ar identitāti saprotam noteiktas īpašības, piemītošas juridiskai vai fiziskai personai, kas aizstāj agrāko apzīmējumu “aģents”. Šajā dokumentā minētā digitālā identitāte attiecas tikai uz fiziskas personas identitāti.

Šajā pamācībā aplūkosim digitālās identitātes pārvaldības pamatus un kāpēc ir svarīgi aizsargāt digitālo identitāti. Pēc tam detalizēti izskatīsim, kā pārvaldīt interneta kontu un kādi ir šī procesa galvenie soļi. Tālāk sniegsim pamatinformāciju par drošību un privātumu internetā. Nobeigumā sniegsim īsu informāciju par digitālo pēdas nospiedumu un tiešsaistes identitātes problēmām.

[1] ISO/IEC 24760-1: A framework for identity management - Part 1: Terminology and concepts". ISO. 2011.

# 1. Digitālās identitātes pārvaldība

Digitālās identitātes pārvaldības principi balstās uz vairāk vai mazāk zināmiem mehānismiem, kas izstrādāti nedigitālās identitātes pārvaldībai. Lai arī tas varētu šķist sarežģīti, padomājiet par savu personas apliecību. Kad vēlaties saņemt personas apliecību, tās izdevējiestāde no citām iestādēm saņem apstiprinājumu par jūsu dzimšanas datumu, nodokļu maksātāja numuru, pilsoņa numuru (ja piemērojams), uzņem jūsu fotoattēlu utt. Digitālajā pasaulē jūsu identitāti var veidot vien lietotājvārds un parole, vai arī tai var būt papildu sarežģītības pakāpes, kuru mērķis ir nodrošināt, ka konkrētās identitātes īpašnieks esat jūs, un tikai jūs. Šīs pakāpes var ietvert atsevišķu e-parakstu, marķieri, lai izveidotu "nejauši izvēlētu" ciparu kodu, SMS apstiprinājumu vai koda nosūtīšanu uz konkrētu mobilā tālruņa numuru (kas reģistrēts konkrētas personas vārdā), balss identifikāciju, atbildi uz konkrētu jautājumu (piemēram: kāds bija jūsu pirmā mājdzīvnieka vārds?) pirkstu nospieduma nolasīšanu un citas metodes. Visas šīs pakāpes tiek īstenotas, lai tikai konkrētajai personai būtu piekļuve zināmām darbībām digitālajā pasaulē.

Daudziem šīs pakāpes šķiet grūti uztveramas, mulsinošas un kaitinošas. Varbūt viņiem ir taisnība, tomēr jāsaprot, ka digitālā pasaule ir fiziskās pasaules tiešs atspoguļojums, un neviens nevēlētos, lai viņu "digitālā" nauda pazustu no viņu "reālā" bankas konta. Iestādes un it sevišķi bankas izmanto vairākus drošības līmeņus nevis, lai kaitinātu lietotājus, bet lai pasargātu to identitāti un nodrošinātu to tiesības veikt darbības un darījumus. Paralēli tam, arvien vairāk pakalpojumu piedāvā veikt, izmantojot mobilo tālruni. Ir aptvertas tik daudzas jomas, ka šeit kā piemēru minēsim vien dažas no tām. Uztveriet tos kā pakalpojumus, kas tieši ietekmē jūsu "reālo" bankas kontu.

Daži no pakalpojumiem, kurus var veikt ar viedtālruņa palīdzību (atkarībā no jūsu dzīvesvietas valsts):

- maksājums par autostāvvietu, nosūtot SMS ziņu;
- samaksa veikalā par iegādātajām precēm;
- dzīvesvietas rēķinu nomaksa;
- tiešs naudas pārskaitījums, izmantojot tam paredzētu bankas apstiprinātu lietotni;

autentificēts 3D maksājums no jūsu *VISA* vai *Master Card* – kad būsiet ievadījis kartes numuru, derīguma termiņu un drošības kodu, sistēma nosūtīs sešu ciparu kodu uz iepriekš apstiprinātu tālruņa numuru, kas sniegs papildus drošības līmeni jūsu darījumiem ar karti;

sauszemes transporta biļetes un lidmašīnu iekāpšanas kartes.
Izmantojot lietotnes “Apple pay” un “Google Wallet”, jūsu tālrunis var veikt jebkuru maksājumu, kas atbalsta NFC vai magnētiskās joslas maksājumus. Tas pat ļauj saņemt maksājumus no dažādām interneta vietnēm, veikaliem un lietotājiem.

Saprotams, kāpēc ir tik svarīgi pareizi pārvaldīt savu digitālo identitāti un kāpēc tā ir aktīvi jāaizsargā.

# 2. Interneta konta pārvaldība

Interneta konts ir daļa no jūsu digitālās identitātes, un visbiežāk tas ir neizbēgams pirmais solis. Parasti tas ir piesaistīts e-pasta pakalpojumiem, piemēram, *Google Gmail*, *Yahoo mail*, *Microsoft email* u.c. Pēc konta izveides jums būs vismaz divi ar to saistīti mainīgie – lietotājvārds un parole. Mūsdienās vairums pakalpojumu sniedzēju prasa, lai katram kontam tiktu pievienots un apstiprināts tālruņa numurs. Tātad jūsu digitālās identitātes kontam ir trīs raksturlielumi: lietotājvārds, parole un tālruņa numurs. Bieži vien

apstiprināšana tiek veikta, nelūdzot jums atļauju, un lai jūs papildus aizsargātu, tiek pievienots ne tikai tālruņa numurs, bet arī unikāls mobilā tālruņa ražošanas numurs *IMEI – International Mobile Equipment Identity* (*Starptautiskā mobilā aprīkojuma identitāte*). Šis numurs, kas tiek piešķirts ražošanas laikā, ir nepieciešams arī, lai autorizētu tālruņa izmantošanu mobilajā tīklā. Šī informācija ir šifrēta un interneta pakalpojumu sniedzēji to uzglabā drošībā, tomēr retos gadījumos tā var tikt nozagta vai ļaunprātīgi izmantota (kā gadījumā ar *Facebook* un *Cambridge Analytica*, kad miljoniem lietotāju datu tika nodoti uzņēmumam, lai sniegtu mērķa reklāmas politisku mērķu sasniegšanai). Daži padomi, kas palīdzēs jums digitālās identitātes veidošanā:

Lietotājvārds – izvēlieties lietotājvārdu, pēc kura esat atpazīstams. Padomājiet, ka, iespējams, izmantosiet šo e-pasta adresi nākotnē, un komiski vārdi ne vienmēr ir pieņemami. Jūsu lietotājvārds būs redzams pirms simbola @, tāpēc no tādiem lietotājvārdiem kā vieglameitene@, stiprinieks@, tavsmurgs@ ne tikai vajadzētu izvairīties, bet tos nevajadzētu lietot vispār. Izvēloties lietotājvārdu, neiekļaujiet tajā savus vai tuvinieka dzimšanas dienas skaitļus.

Parole: Izmantojiet mazo burtu, lielo burtu, ciparu un īpašo rakstzīmju, kā #, $, &, |,~ kombināciju. Pārliecinieties, ka tā ir vismaz 8 rakstzīmes gara un periodiski nomainiet to. Ja piekļūstat savam digitālajam kontam no tālruņa, izmantojiet pirkstu nospiedumu lasītāju vai citu autentifikācijas veidu. Nenoklikšķiniet “atcerēties paroli” savā pārlūkā.
Pat tad, ja tas nav obligāti nepieciešams, pievienojiet kontam savu tālruņa numuru un iestatiet to kā ierīci, ko automātiski izmantot aizmirsto paroļu atjaunošanai. Atveriet sava konta iestatījumus un pievienojiet atgūšanas e-pastu un tālruņa numuru, lai pastiprināti autentificētu savu identitāti. Neizmantojiet to pašu paroli citiem kontiem, piemēram, sociālo tīklu vai spēļu kontiem.

# 3. Drošības apsvērumi un privātums

Daži serveri un lietotnes ievāc daudz informācijas par to izmantošanu, un šī informācija, iespējams, var tikt piesaistīta fiziskai personai un viņa/viņas digitālajiem paradumiem internetā. ES līmenī VDAR (Vispārīgā datu aizsardzības regula) mēģina to novērst, tomēr lietotājiem joprojām iesaka būt piesardzīgiem attiecībā uz to, kur un ar kādu saturu tie dalās, un kādas darbības veic internetā, it sevišķi sociālajos tīklos.

Jūsu foto un video materiālu apstrādei ir pieejami neskaitāmi rīki, un sociālie tīkli bieži vien piedāvā arī pareizrakstības pārbaudi angļu valodā rakstītam tekstam. Digitālajiem fotoattēliem (un video) var pievienot dažādus filtrus, mainīt krāsu piesātinājumu, kontrastu u.c. Varat izmantot jūsu ierīcē piedāvātos vai instalēt sev tīkamākos. Atcerieties, ka vairumam tiešsaistes bezmaksas apstrādes rīku ir ierobežojumi, un jums ir jāveic maksājums, lai gūtu piekļuvi visām funkcijām. Izmantojot šīs programmas, bieži vien jūsu foto vai video tiks pievienots uzraksts, ka materiāls veidots, izmantojot šo programmatūru, un tas ne vienmēr ir patīkami. Eksperimentējiet un pārbaudiet dažādus rīkus, līdz atrodat to, kas atbilst jūsu vajadzībām.

Kā norādīts ESAO 2016. gadā veiktajā pētījumā[2]

[2] DIGITĀLĀS DROŠĪBAS UN PRIVĀTUMA RISKA PĀRVALDĪBA, ESAO DIGITĀLĀS EKONOMIKAS DOKUMENTI Nr. 254, https://www.oecd-ilibrary.org/docserver/5jlwt49ccklt-en.pdf?expires=1591780736&id=id&accname=guest&checksum=AF002079529F4DE263769B3FBEB40035

: *“Veicot darbības, kuru pamatā ir digitālā vide, nav iespējams pilnībā novērst digitālās drošības risku. Tomēr risku var pārvaldīt, tas ir, samazināt līdz pieņemamam līmenim, ņemot vērā attiecīgās intereses un ieguvumus, kā arī kontekstu.”* Tomēr pastāv samērā saprotami un diezgan vienkārši soļi, ko indivīds vai organizācija var veikt, lai sasniegtu apmierinošu digitālās drošības un privātuma aizsardzības līmeni. Tie ietver, bet neaprobežojas ar

stingrām parolēm, striktu interneta piekļuves politiku, saprātīgu rīcību pārlūkojot internetu, izglītošanu un apmācību kā galvenajiem stūrakmeņiem, kā arī politikas izstrādi par personas datiem un to aizsardzību. Papildus minētajam, ES ir izvirzījusi augstākos personas datu un privātuma aizsardzības standartus pasaulē.

Indivīds var ievērot vienkāršus soļus, lai mazinātu privātuma pārkāpuma iespēju. Vienmēr rūpīgi jāizlasa vietnes, interneta pakalpojuma, ziņu un sociālo tīklu platformas sīkdatņu politika. Ja nevēlaties, lai jūs izseko (dažas vietnes vāc datus par jūsu pārlūkošanas paradumiem, cik bieži apmeklējat konkrētu vietni, uz kādām reklāmām noklikšķināt, kādu informāciju meklējat internetā utt.), varat izmantot privātu pārlūka logu, ko piedāvā gandrīz visi interneta pārlūki, kā *Google Chrome*, *Mozilla Firefox*, *Microsoft Internet Explorer* u.c.

No drošības viedokļa nekad nevajadzētu izmantot tās pašas paroles dažādām interneta lietotnēm kā e-pasts, sociālo tīklu platformas un vietnes, kurām nepieciešams pieteikties. Nodrošiniet, ka parole ir pietiekami sarežģīta ar desmit vai vairāk rakstzīmēm, iekļaujot tajā ciparus, lielos un mazos burtus, kā arī īpašās rakstzīmes (&, #, $, ^ u.c.) Nesaglabājiet paroles pārlūkā, bet centieties tās atcerieties vai veidojiet paroles pēc noteikta, paša veidota principa. Piemērs:

*#MansUzvārds4VietnesNosaukums~mAns_vārds$.*

Lai gan šī parole var šķist sarežģīta, svarīgākais ir iegaumēt principu. Ja iespējams, pievienojiet tālruņa numuru kā alternatīvu autentifikācijas veidu, lai varētu atjaunot aizmirstu vai nozagtu paroli. Tas radīs papildu personīgās

aizsardzības līmeni, kas samazinās risku, ka jūsu interneta dati var tikt ļaunprātīgi izmantoti.

# 4. Digitālais pēdas nospiedums

Digitālais pēdas nospiedums apzīmē konkrēta interneta lietotāja unikālās izsekojamās digitālās darbības. Izmanto arī citus terminus, piemēram, digitālā ēna, interneta pēdas nospiedums, kiberēna utt. Lai gan parasti šo terminu attiecina uz fizisku personu, to var attiecināt arī uz organizācijām, uzņēmumiem, korporācijām, digitālo pakalpojumu vietnēm u.c. Pastāv divu veidu digitālais pēdas nospiedums – aktīvais un pasīvais.

Pasīvais digitālais pēdas nospiedums attiecas uz datiem, kas ievākti, personai nezinot. Tas nenozīmē, ka tas tiek slēpts no lietotāja. Aktīvais digitālais pēdas nospiedums ir informācija, ko lietotājs pats no brīvas gribas kopīgo par sevi, visbiežāk, sociālajos tīklos vai citās vietnēs. Informācija par lietotāju var tikt apzināti vai neapzināti atklāta, un tādā gadījumā to aktīvi vai pasīvi ievāc trešās personas. Piemēram, ja savā sociālo tīklu profilā atkļāti norādīsiet savu e-pasta adresi, tālruņa numuru, dzīvesvietas adresi, darba vietu, jūsu uzņēmuma interneta adresi u.c., datorprogrammai vai fiziskai personai būs ļoti viegli ievākt samērā daudz informācijas par jums. Gadījumā, ja notiks datu drošības pārkāpums, iespējams, pieejama kļūs arī jūsu bankas konta vai nodokļu informācija.

Ir veikti vairāki pētījumi, kas liecina, ka aptuveni 70 procenti no visām cilvēku darbībām internetā tiek veiktas apzināti. Tomēr aptuveni 30 procenti cilvēka digitālā pēdas nospieduma ir tāds, ko viņš pats nekad apzināti nepublicētu. Tas atklāj diezgan daudz informācijas par iepirkšanās paradumiem internetā, vaļaspriekiem un citām personīgās dzīves niansēm, kas tiek tālāk analizēta. Lai gan nav nekas slikts analizēt klientus vispārīgi lielās datu bāzēs, veicot to

pašu ar indivīdiem, šādas analīzes var būt pamats identitātes zādzībai, kriminālām darbībām un privātuma pārkāpšanai.

Lai arī digitālais pēdas nospiedums nav tas pats, kas digitālā identitāte vai digitālais ID, tā saturs un aprakstošie dati (saukti arī par metadatiem) spēcīgi ietekmē privātumu, uzticēšanos internetam un digitālo reputāciju. Interneta pēdas nospiedumu uzņēmumi var izmantot, pieņemot darbā jaunus darbiniekus, tiesību aizsardzības iestādes – vācot datus par konkrētiem indivīdiem, kad tas nav iespējams citādi, mārketinga speciālisti – lai uzzinātu, kādi produkti interesē lietotāju(-us), vai lai palielinātu to interesi par konkrētu produktu vai pakalpojumu. Sociālie tīkli ir to galvenais avots šādas informācijas ieguvei. Dažkārt sociālās platformas var ievākt datus no lietotāja ierīces, lietotājam par to nezinot, izmantojot dažādus mobilā tālruņa vai citu lietotāja ierīču sensorus. Piemēram, *Facebook* un *Google* ievāc daudz informācijas par lietotāju, kuru kombinējot var izdarīt detalizētus secinājumus par lietotāja personību, interesēm, politiskajiem uzskatiem, iepirkšanās paradumiem, interesēm u.c.

# 5. Tiešsaistes identitāte

Tiešsaistes identitāte ir identitāte, ko lietotājs apzināti izveido internetā, visbiežāk ar mērķi spēlēt spēles. Lietotāji var izvēlēties sevi attēlot ar avatāriem (ikonu lieluma grafiku), nevis ar īstu fotoattēlu. Lietotāji var arī izmantot pseidonīmus sava īstā vārda vietā. Tiešsaistes identitāti var noteikt arī, balstoties uz lietotāja saistību ar konkrētu cilvēku grupu internetā. Tiešsaistes identitāte tiek saistīta ar faktisko lietotāju, veicot tādas autorizācijas procedūras kā reģistrācija vai pieslēgšanās (lietotājvārds un parole), kā arī izmantojot konkrētas iekārtas vai ierīces IP adresi. Šādas vietnes nereti instalē izsekošanas sīkdatnes, kas var tālāk noteikt lietotāja tiešsaistes uzvedību un saistīt to ar reālo personu. Tā kā spēles visbiežāk,

lai gan ne vienmēr, tiek piedāvātas gados jaunākai mērķauditorijai, kas nepievērš īpašu uzmanību piesardzībai internetā, svarīgi, lai par digitālās un tiešsaistes identitātes jēdzieniem un digitālais pēdas nospiedumu pēc iespējas skaidrāk tiktu informēti visi interneta lietotāji.

Tiešsaistes identitātē var ietilpt jebkas, sākot no jūsu e-pasta akreditācijas datiem (lietotājvārds un parole) līdz sociālo tīklu kontam, izvēlētajam vārdam forumos vai pircēja profilam noteiktā vietnē. Tas ietver arī jūsu pārlūka vēsturi, IP adresi, veikto meklēšanu utt. Cilvēki un organizācijas var būt ieinteresēti jūsu tiešsaistes identitātē pilnīgi likumīgu vai nelikumīgu iemeslu dēļ (hakeri). Dažiem uzņēmumiem jūsu pārlūka un meklēšanas vēsture ir nepieciešama, lai piedāvātu piemeklētas reklāmas produktiem un pakalpojumiem, balstoties uz jūsu vajadzībām un interesēm. Savukārt citiem var būt nelikumīgs nolūks nozagt jūsu datus, kredītkartes numuru utt.

Pastāv vairāki veidi, kā pasargāt savu tiešsaistes identitāti, piemēram, izmantojot stingras paroles, sociālajos tīklos nepublicējot pārāk daudz personīgās informācijas, izmantojot pārlūku inkognito režīmā, izmantojot virtuālus privātos tīklus, šifrējot savu komunikāciju u.c. Jo lielāku uzmanību pievērsīsiet savai tiešsaistes identitātei, jo pasargātāks būsiet.

# Kopsavilkums

Esam iepazīstinājuši jūs ar digitālās identitātes un interneta konta pamatjēdzieniem un informāciju. Balstoties uz šiem pamatjēdzieniem, aprakstījām lietotāju privātuma un drošības jautājumus. Nobeigumā sniedzām ieskatu par digitālo pēdas nospiedumu un tiešsaistes identitāti.

Piedāvājām arī vieglus un saprotamus veidus paroļu veidošanai, autentifikācijai, digitālās identitātes radīšanai, privātuma uzturēšanai un interneta pārlūkošanai. Ja indivīds vai organizācija ievēros šīs metodes, ievērojami samazināsies

internetā pastāvošie riski. Kā parasti, nav risinājuma, kas spētu aptvert visus iespējamos gadījumus, tāpēc veselais saprāts un īpaša organizatoriskā līmeņa politika ir vislabākie rīki, lai cīnītos pret ļaunprātīgām darbībām internetā un palielinātu uzticēšanos internetam un digitālajām platformām kopumā.
Nobeigumā aplūkojām informāciju gan par to, kas ir tiešsaistes identitāte, gan par veicamajiem soļiem, lai aizsargātu indivīdu no identitātes nelikumīgas izmantošanas.

# Bibliogrāfija:


- 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