Digitālo prasmju uzlabošana pieaugušajiem

Projekta Nr.: 2018-1-PL01-KA204-051003

Kā aizsargāt personas datus?

Kompetence: Personas datu un privātuma aizsardzība

Ievads

Modulis aptver galvenās tēmas personas datu un privātuma aizsardzības jomā.

Moduļa mērķi ir:

- aplūkot drošības principus digitālajā vidē un informēt par iespējamiem draudiem - informācijas zagšanu, viltus e-pastiem u.c.;
- iepazīstināt ar tehnoloģiju izmantošanas drošības pamatprincipiem - kādi noteikumi jāievēro, lietojot internetu publiski pieejamos Wi-Fi tīklos, kas ir drošs savienojums, un kādi ir nedroši e-pasta pielikumi?
- izskaidrot drošu paroļu izmantošanu - kādi principi jāievēro, veidojot paroles? Kā droši lietot paroles ikdienā?

1. Ievads drošībai digitālajā vidē

1.1. Datora drošība

Datora drošība nozīmē, ka mūsu dators ir pasargāts no neautorizētas piekļuves, izmantošanas, publiskošanas, pieejamības traucēšanas, pārveidošanas vai iznīcināšanas. Ir svarīgi apzināties, ka informācija, kas saglabāta datorā un publicēta internetā, var ietekmēt gan personisko labsajūtu, gan veselību un pat dzīvību. Mūsdienās ir ļoti daudz draudu tehnoloģiju pasaulē - draudi privātumam, paroles uzzināšana vai uzlaušana, personīgas informācijas izpaušana, vīrusi, kaitīgu failu augšupielāde, lejupielāde un sūtīšana, kā arī ļaundari, kas vēlas kaitēt mūsu ierīcei.

Internetā mums ir pieejami sociālie tīkli, tiešsaistes sarunas (biežāk sauktas par “čatiem”), forumi, īpašas sarunu programmas (piemēram, Skype), spēles u. c. Ja netiek ievērotas nepieciešamās drošības normas, cilvēki ar sliktiem nodomiem var uzzināt ne tikai jums zināmas privātas lietas, bet arī izmantot jūsu identitāti (uzdoties par jums).

Datorvīrusi ir kļuvuši par "klasisku vērtību". Tiek izmantotas dažādas metodes, piemēram, lietotājs saņem e-pasta vēstuli ar saiti uz kādu populāru interneta vietni, piemēram, Youtube vai Facebook ar vilinošu filmu vai attēlu. Mēģinot to skatīties, jau pēc viena peles klikšķa lietotāja nepilnīgi aizsargātais dators tiek inficēts.

E-pasta pielikumi ir īpaši bīstami, jo tie var saturēt vīrusus un citu ļaunprātīgu programmatūru. Atverot pielikumu e-pastā, datorā automātiski var tikt instalēta ļaunprātīga programma un jūs to pat nepamanīsiet. Šādas ļaunprātīgas programmatūras var ietekmēt datora failus, nozagt paroles vai izspiegot jūs, tāpēc ir jābūt īpaši piesardzīgiem, saņemot vēstules ar pielikumiem no nezināmiem adresātiem.

Ieteikumi, kā cīnīties ar nevēlamiem pielikumiem e-pastā:

Ieteikums	Paskaidrojums
Nekad neatveriet aizdomīgus e-pasta pielikumus	Arī tad, ja saņemat vēstuli no pazīstama cilvēka, nav garantēts, ka šis cilvēks tiešām to ir sūtījis. Ļaunprātīgas programmas var automātiski nosūtīt vēstuli, kas satur vīrusus. Šis ir viens no veidiem, kā izplatās vīrusi. Saņemot vēstuli ar pielikumu, vislabāk ir pajautāt pašam sūtītājam, lai pārliecinātos, ka šo vēstuli tiešām viņš ir sūtījis.
Atjauniniet antivīrusa programmu	Vīrusi var izplatīties ļoti ātri. Ja antivīrusa programma nav atjaunota, tā nevar aizsargāt datoru no vīrusiem.
Atstājiet ieslēgtu datora ugunsmūri (Firewall)	Datora ugunsmūris palīdz novērst cilvēku vai ļaunprātīgu programmu piekļuvi datoram caur internetu.
Ja iespējams, pirms e-pastu pielikumu lejupielādes, pārbaudiet, vai tie nesatur vīrusus	Daudzu tiešsaistes e-pastu sniedzēji automātiski pārbauda pielikumus pirms to lejupielādes. Gadījumos, kad lejupielādējot pielikumus, dators piedāvā pārbaudīt, vai tie nesatur vīrusus, veiciet šo pārbaudi paši.

1.2. Datu drošība - pikšķerēšana

Pikšķerēšana ir kibernozieguma veids, kurā apvienots sociālās inženierijas un tehnisko instrumentu kopums, lai izvēlētajam upurim nozagtu sensitīva, personīga un finansiāla rakstura informāciju. Uzbrucējs cenšas izlikties par īstu organizāciju, uzticamu iestādi vai zināmu personu.

Visbiežāk pikšķerēšanas upuri tiek aicināti klikšķināt uz e-pastiem, ar šādiem tematiem:

- ✓ Oficiāls paziņojums par datu noplūdi
- ✓ UPS piegādes paziņojums 1ZBE312TYI00015011B23
- ✓ IT atgādinājums: Jūsu paroles derīguma termiņš beigsies pēc mazāk kā 24 h
- ✓ Nepieciešama tūlītēja paroles maiņa
- ✓ Lūdzu, izlasiet svarīgu paziņojumu no administratora

Kā atpazīt pikšķerēšanu:

Pārāk labi, lai būtu patiesība. Šīs ir ziņas, vēstules, zvani, kuros informācija vēsta, ka esat vinnējis loterijā vai nejaušas izvēles gadījumā esat privileģēts saņemt kādu balvu vai pakalpojumu.

Ātrais piedāvājums. Frāzes: "pēdējā iespēja", "vēl tikai 1 stunda", "tikai šodien" u.tml. liecina par pikšķerēšanas gadījumu. Krāpnieki izmanto manipulāciju, kas rada sajūtu, ka ir jāsteidzas. Ja tiek saņemts šāda veida ziņojumus, tad ieteicams pārbaudīt informācijas patiesumu, vēršoties tieši pie attiecīgās kompānijas, uzņēmuma vai pakalpojumu sniedzēja.

Aizslēptas saites ar citiem atslēgvārdiem. Daudzi krāpnieki izmanto vienkāršus atslēgvārdus, frāzes, uz kurām noklikšķinot jūs nonāksiet krāpniekam vēlamā vietnē. Šīs saites bieži vien slēpj pilnīgi citu vietni salīdzinājumā ar to, ko domājat. Ļoti labs veids kā pārliecināties par to, ko atvērsiet patiesībā ir, noklikšķiniet uz saites LABO peles taustiņu un izvēlieties opciju *Inspect* – pārbaudīt, izpētīt. Aplūkojiet, ar kādu saiti ir sasaistīta attiecīgā saite vai atslēgvārds. Ko tā slēpj? Ir jābūt vērīgam, jo ar pareizrakstības neprecizitātēm bieži vien tiek veidotas neīstās saites.

Dīvaini pielikumi. Ja jūs negaidāt kādu konkrētu informāciju, nekādā gadījumā nevajag skatīties, vērt vaļā pielikumus. Viena no kibernozieguma metodēm ir it kā nevainīgam ziņojumam pielikt klāt failu, kas var saturēt ļaunprogrammatūru. Ieteicams pārbaudīt sūtītāju, vēstules mērķi pirms atveriet to. Vienīgais drošais formāts, ko drīkst atvērt .txt fails.

Kā izvairīties no pikšķerēšanas:

Ieteikums	Paskaidrojums
Esiet modrs	Vienmēr uzmanīgi lasiet e-pastus gan no draugiem, gan nepazīstamiem cilvēkiem.
Esiet uzmanīgs dažādos komunikācijas kanālos	Pievērsiet uzmanību dažāda veida komunikācijai – e-pastiem, reklāmām, telefona zvaniem u.c., kur tiek lūgta finansiāla satura informācija.
Klikšķiniet apdomīgi	Izvairieties klikšķināt uz "iespējot saturu", kas ļauj iespējot papildu sasaisti starp dažādiem dokumentiem.
Neklikšķiniet uz aizdomīgām saitēm	Izvairieties klikšķināt uz saitēm e-pastos, ziņojumu apmaiņas lietojumprogrammās vai reklāmās. Izpētiet tās katru atsevišķi, izmantojot visus iespējamos resursus.
Pārbaudiet sūtītāja uzticamību	Esiet drošs, ka e-pasts ir sūtīts no uzticama avota.

Ja esat kļuvis par pikšķerēšanas upuri:

1) Nomainiet paroles savām aplikācijām un tiešsaistes kontiem, izmantojot citu telefonu vai datoru.

2) Skenējiet savu datoru, lai atklātu vīrusus un noteiktu, vai datoram nav uzstādīta ļaunprātīga programmatūra.

3) Ziņojiet par datu zādzību policijai un saglabājiet iesnieguma kopiju.

4) Ziņojiet savai organizācijai/ bankai vai kompetentajai iestādei.

1.3. Datora lietotāja drošība – sociālajos tīklos publicētā informācija

Datora lietotāja drošības jēdzienu iespējams aplūkot divējādi. Ir iespējams runāt par datora iespējām apdraudēt tā lietotāja veselību, piemēram, par kaut nelielu, bet tomēr iespējamību, ka kaitējumu nodara strāvas trieciens. Taču visbiežāk apdraudējumu personai var izraisīt paša neapdomīgi publicēta informācija.

Bieži netiek pievērsta uzmanība tam, cik daudz un dažādi draudi ir iespējami sociālajos tīklos.

Sociālie tīkli ir mūsdienu ikdienas svarīga sastāvdaļa – tos lieto, lai:

- Komunicētu;
- Iegūtu informāciju;
- Ievietotu savu informāciju, dalītos ar to u.c.

Sociālo tīklu draudu veidus var iedalīt divos veidos - **tehnoloģiskajos** un **organizatoriskajos** draudos.

Tehnoloģisko draudi ir saistīti ar dažādām tehnoloģijām un to izmantošanu sociālo tīklu lietošanā. **Organizatoriskie draudi** ir saistīti ar paša lietotāja – cilvēka – uzvedību internetā, darbībām un aktivitātēm, ko viņš veic. Organizatoriskā drauda uzbrukuma izraisītājs parasti ir kāds cits sociālā tīkla lietotājs.

Visbiežāk sastopamie draudi sociālajos tīklos ir:

- ✓ dažādas ļaundabīgas programmatūras jeb vīrusi;
- ✓ piksķerēšanas (phising) uzbrukumi - pikšķerēšanas ziņas vai vēstules, kas ietver saites uz mājas lapām, kas ir inficētas ar ļaundabīgu programmatūru;
- ✓ spam e-pastu sūtīšana;
- ✓ slēptie klikšķi, kas liek lietotājam uzklikšķināt uz kaut ko citu, nekā lietotājs sākotnēji domā;
- ✓ dažāda veida viltotie profili – daļa no tiem ir daļēji automatizēti vai pilnībā automatizēti, kā arī daļa ir cilvēku veidotie;

- ✓ izvedumu uzbrukums (inference attacks) ir datu un informācijas ieguves tehnika, kurā tiek analizēti pieejamie dati, lai iegūtu papildus informāciju par upuri. Sociālajos tīklos tie tiek izmantoti, lai minētu un noteiktu lietotāja personīgu informāciju, ar kuru lietotājs nav izvēlējies dalīties, kā, piemēram, reliģisko nostāju un seksuālo orientāciju. Uzbrukums sociālajā tīklā tiek veikts, izmantojot tajā atrodamo upura un viņa draugu profilos pieejamo informāciju;
- ✓ kibermobings - emocionāla pazemošana, izmantojot mūsdienu tehnoloģijas. Izstumšana, pazemošana, sekstings, uzmākšanās, piedauzīgu attēlu sūtīšana, ņirgāšanās, melošana par savu identitāti, lai uzzinātu personīgu informāciju, piekļūšana citu informācijai, izsekošana u.c.

Lai izvairītos no draudiem, var tikt izmantoti dažādi sociālo tīklu piedāvātie risinājumi:

- autentifikācijas mehānismi,
- lietotāju bloķēšana,
- lietotāju personīgie uzstādījumi,
- opcija “ziņot par lietotāju”.

Uzskaitītie risinājumi var veiksmīgi tikt izmantoti, lai pasargātu lietotāju no viltotajiem profiliem, emocionālās vardarbības, naivās un riska uzvedības.

Dažāda drošību risinājumu kompānijas – AVG, Avira, Kaspersky, Panda, McAfee, Symantec – piedāvā sociālo tīklu lietotājiem Interneta drošības risinājumus. To veidotās programmatūras parasti iekļauj anti-vīrusa programmu un ugunsmūri, reizēm papildus piedāvājot anti-mēstuļošanas un anti-pikšķerēšanas aizsardzību interneta lietotājiem. Šāda programmatūra palīdz sociālo tīklu lietotājiem pasargāt savus personīgos datorus pret tādiem draudiem kā ļaundabīga programmatūra, slēptie klikšķi un pikšķerēšana.

Ieteikumi drošai sociālo tīklu lietošanai

Veids	Piemērs
Publicēšana	Pirms informācijas publicēšanas visu kārtīgi apdomājiet. Viss, ko jūs publicēsiet, visticamāk kādā brīdi kļūs publiski pieejams, un var negatīvi iespaidot jūsu reputāciju un nākotni. Esiet piesardzīgi – arī citi par jums var kaut ko publicēt. Iespējams, jums pat vajadzēs pieprasīt, lai kāds dzēš informāciju, ko par jums ir publicējis.
Privātums	Praktiski visos sociālajos tīklos ir pieejamas papildu privātuma iespējas - uzstādiet tās, kad vien tas ir iespējams. Piemēram, vai mājaslapai tiešām nepieciešams zināt jūsu atrašanās vietu? Papildu privātuma iespējas var būt sarežģītas un tās bieži mainās. Izveidojiet ieradumu regulāri tās pārbaudīt un pārliecināties, vai tās strādā tā, kā jūs esat iedomājies.
Paroles	Aizsargājiet savu sociālo tīklu kontus ar pietiekami garu, unikālu paroli vai paroles frāzi. Paroles frāze ir parole, kas sastāv no vairākiem vārdiem, padarot to viegli iegaumējamu un uzrakstāmu, bet daudz grūtāk uzminamu kibernoziedzniekiem.
Krāpšana	Līdzīgi kā ar e-pastiem, arī sociālo tīklu paziņojumus var izmantot dažādiem krāpšanas mēģinājumiem. Piemēram, ļaundaris var mēģināt izvilināt jūsu paroli vai kredītkartes informāciju. Esiet piesardzīgi attiecībā uz saitēm, ko saņemat.
Saziņa	Nekontaktējieties ar nepazīstamiem un aizdomīgiem cilvēkiem. Viltus profilu izveide ir ļoti vienkārša un daudzi to izmanto, lai melotu par savu identitāti. Šo profilu mērķis ir maldināt, iegūt uzticību un izmantot to pret jums.
Lietošanas noteikumi	Iepazīstieties ar sociālo tīklu lietošanas noteikumiem – jebkas, ko jūs publicējat, var kļūt par sociālo tīklu īpašumu.
Darbs	Ja vēlaties publicēt kaut ko par savu darbu, vispirms noskaidrojiet, vai tas ir pieņemami jūsu darba devējam.

Personalizēta krāpšana

Arvien populārāks kļūst jaunais kibernoziedzības veids – personalizētā krāpšana. Kibernoziedznieki ievāc vai nopērk informāciju par miljoniem cilvēku un izmanto šo informāciju, lai personalizētu uzbrukumus. Jo vairāk jūs zināsiet par šādiem uzbrukumiem, jo vieglāk būs tos atpazīt un apturēt.

E-pasta un telefona krāpniecības nav jaunums, kibernoziedznieki ir centušies apmuļķot cilvēkus gadiem. Kā piemērus var minēt "Jūs esat vinnējuši loterijā" vai slaveno Nigērijas prinča krāpniecību. Taču šajos tradicionālajos uzbrukumos kibernoziedznieki nezina, ar ko viņiem būs darīšana. Viņi vienkārši sagatavo vispārīgu e-pastu un nosūta to miljoniem cilvēku. Tā kā šie krāpnieciskie e-pasti ir tik vispārīgi un vienādi, tos parasti ir viegli atpazīt. Personalizēta krāpniecība ir citāda, kibernoziedznieks vispirms veic izpēti un katram upurim sagatavo tam pielāgotu vēstuli. To dara, ievācot informāciju vai nopērkot datubāzi ar cilvēku vārdiem, parolēm, telefona numuriem un citu informāciju. Šāda informācija ir viegli pieejama, pateicoties daudzajām uzlauztajām tīmekļa vietnēm. Bieži vien tā ir arī brīvi pieejama sociālo tīklu vietnēs un publiski pieejamos valsts iestāžu resursos.

Uzbrukums darbojas šādi: uzbrucēji atrod vai nopērk informāciju par cilvēku lietotājvārdiem un parolēm, kas iegūtas no uzlauztām tīmekļa vietnēm. Tad atrod jūsu e-pasta adresi un ar jums saistītu informāciju šādā datubāzē un nosūta jums (kā arī visiem pārējiem, kas iekļauti šajā datubāzē) e-pastu, kurā norāda ar jums saistītu informāciju, ieskaitot paroli, kuru jūs izmantojāt uzlauztajā tīmekļa vietnē. Kibernoziedznieki uzdod šo paroli par "pierādījumu", ka ir uzlauzuši jūsu datoru vai iekārtu, kas, protams, nav taisnība. Kibernoziedznieki arī apgalvo, ka, uzlaužot iekārtu, pieķēruši jūs vērojam pornogrāfiska rakstura materiālus internetā. E-pastā tiek draudēts, ka, ja nesamaksāsiet izpirkuma maksu, liecības par jūsu apkaunojošajām tiešsaistes aktivitātēm tiks nosūtītas jūsu ģimenei un draugiem.

Atslēga – šajā un gandrīz visos citos šādos gadījumos kibernoziedznieki nav uzlauzuši jūsu iekārtu. Viņi pat nezina, kas jūs esat, nedz arī kādas tīmekļa vietnes apmeklējat. Krāpnieki vienkārši cenšas izmantot dažas viņiem par jums

zināmās lietas, lai jūs iebiedētu un liktu jums noticēt, ka viņi ir uzlauzuši jūsu iekārtu, un panāktu, ka jūs tiem samaksājat. Atcerieties, ka sliktie var izmantot šos pašus paņēmienus arī krāpnieciskos telefona zvanos.

Ko darīt? Atpazīstiet šādus e-pastus un telefona zvanus kā krāpnieciskus. Tas ir dabiski just bailes, ja kāds ir ieguvis jūsu personīgo informāciju. Taču atcerieties, sūtītājs melo! Uzbrukums ir daļa no automatizētas masveida kampaņas, nevis mēģinājums uzbrukt tieši jums. Mūsdienās kriminālnoziedzniekiem kļūst arvien vieglāk atrast vai nopirkt personīga rakstura informāciju, līdz ar ko gatavojieties lielākam personalizēto uzbrukumu apjomam nākotnē.

Pazīmes, pēc kurām atpazīt uzbrukumu:

- Vienmēr esiet aizdomu pilns, kad saņemat ļoti steidzinošu e-pastu, ziņu vai telefona zvanu. Ja kāds izmanto tādas emocijas kā bailes vai steidzamību, viņš cenšas panākt, lai jūs steigā kļūdītos.
- Ja kāds pieprasa maksājumu *BitCoin* kriptovalūtā, dāvanu kartēs vai citos neizsekojamos maksājumu līdzekļos.
- Ja saņemat aizdomīgu e-pastu, veiciet meklēšanu Google, lai noskaidrotu, vai citi nav ziņojuši par līdzīgu uzbrukumu.

Vienmēr centieties izmantot garas, unikālas paroles katram jūsu tiešsaistes kontam. Nevarat atcerēties visas paroles? Izmantojiet paroļu pārvaldnieku. Papildus tam, izmantojiet divu pakāpju autentifikāciju, kad vien tas ir iespējams.

1.4. Digitālās pēdas

Digitālā pēda ir informācija, ko apzināti vai neapzināti atstājam virtuālajā vidē – vizuāla, audio un arī rakstiskā informācija. Ir arī daļa informācijas, kas nav paša radīta, bet gan vecāku, draugu, darba vietas u.c. Katram ir jādomā par savas digitālās pēdas veidošanu. Tādas neesamība mūsdienās var arī kaitēt, bet pārlieku aktīva sociālo tīklu dzīve, var arī radīt negatīvas sekas nākotnei.

Digitālā pēda tiek veidota, ņemot vērā jūsu aktivitāti globālajā tīmeklī: iepirkšanās paradumus, medijus, ierīču izmantošanu, izvēlētās platformas.

2. Tehnoloģiju rīku lietošanas drošības pamatprincipi

2.1. Interneta savienojums

Lai citas personas nevarētu izmantot jūsu pieejas autentifikācijas datus, **nepieciešams parūpēties par drošu interneta pārlūkošanu!**

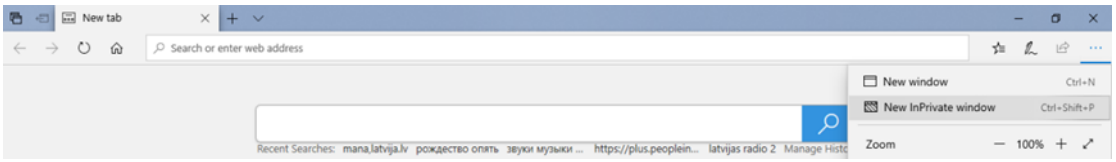
Pārlūkošanas laikā interneta pārlūkprogramma lietotāja cietajā diskā saglabā informāciju par apmeklētajām tīmekļa lappusēm, ko var iedalīt trīs veidos:

a) Apmeklēto lappušu adrešu saraksts jeb pārlūkošanas vēsture (History).
b) Tīmekļa lappusēs esošā informācija, ko parasti saglabā tā saucamajā kešatmiņā (Cachememory). Parasti tā ir mape ar nosaukumu *Temporary Internet Files*.
c) Sīkdatnes (cookies) – mazas teksta datnes. Šajās datnēs ieraksta, piemēram, paroles, apmeklēto lappušu sarakstu un to skatīšanas datumus. Pārlūkprogrammas šo informāciju pārsūta atpakaļ interneta serveriem. Ieteicams akceptēt sīkdatnes tīmekļa vietnēs, kuras plānojat apmeklēt atkārtoti.

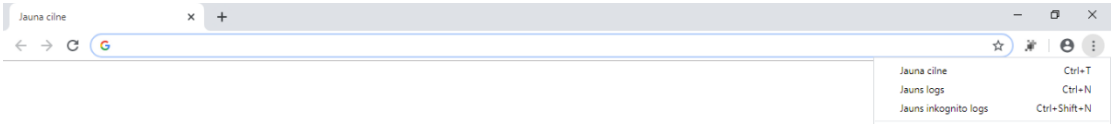
Izmantojot publiski pieejamu datoru, jārēķinās, ka citi cilvēki varēs aplūkot pārlūkprogrammas vēsturē klienta apmeklētās vietnes, kā arī lejupielādētās datnes. Lai izvairītos no nepatīkamām situācijām, ieteicams dzēst pārlūkprogrammas vēsturi **Ctrl+H** un sīkdatnes. Daudzās pārlūkprogrammās to var veikt, vienlaikus nospiežot tastatūras taustiņus **Ctrl+Shift+Delete**.

Ja nevēlaties, ka pārlūkprogrammā tiek pierakstīta darbību vēsture un lietotājvārdi un paroles, ieteicams izmantot **privāto pārlūkošanu**. Katrā pārlūkprogrammā privātajai pārlūkošanai var būt cits nosaukums, bet tā būtība visās pārlūkprogrammās ir vienāda. Tālāk redzamajos attēlos parādīti daži piemēri, kā atvērt privātās pārlūkošanas logu.

Microsoft Edge



Google Chrome



Atcerieties, ka jāsargā dati par savu identitāti, paroles un drošības kodi. Ar šiem datiem svešas personas var veikt nelikumīgas darbības.

Lietojot internetu, ieteicams ievērot šādus pamatnoteikumus:

- Nedodiet citām personām savu personas apliecību (eID karti) ar PIN kodiem vai internetbanku piekļuves līdzekļus;
- Neievietojiet internetā un nesūtiet dokumentu kopijas (pasi, personas apliecību (eID karti), autovadītāja apliecību) pa e-pastu, izmantojot saziņas lietotnes vai sociālos tīklus;
- Nepārsūtiet paroles un citu privātu informāciju e-pasta vēstulēs vai saziņas lietotņu (WhatsApp, Viber, Messenger u.c.) un sociālo tīklu (Facebook, Twitter u.c.) ziņojumos;
- Saņemot e-pasta vēstules ar aizdomīgu saturu, neatveriet tai pievienotos failus;
- Neatklājiet citiem internetā un sociālajos tīklos pārāk daudz par savu dzīvi, jo īpaši par finansiālo situāciju, jauniegūtajām lietām, izbraukšanu no mājām u.tml.;
- Rūpīgi pārdomājiet, kādas fotogrāfijas publicēt internetā, un kā to publiskošana kādu dienu var ietekmēt personas dzīvi, piemēram, attiecības ar draugiem, radiniekiem, kolēģiem, esošajiem vai nākamajiem darba devējiem;
- Saņemot e-pastu no valsts iestādes vai bankas ar pieprasījumu nosūtīt iestādei savus personas datus, nekādā gadījumā to nedariet, jo iestāde nekad nejautās datus e-pastā;

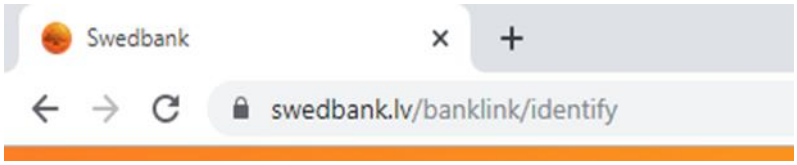
- Pieslēdzoties e-pakalpojumiem, pārliecinieties, ka citi cilvēki nevar redzēt ievadītos piekļuves datus un e-pakalpojuma rezultātā iegūto informāciju;
- Datorā, kurš ir pieslēgts pie interneta, noteikti ir jābūt instalētai antivīrusu programmai;
- Datoru uz nakti ir atslēdziet, lai ne tikai ietaupītu elektrību, bet arī samazinātu risku, ka dators tiek uzlauzts un izmantots nelikumīgi.

2.2. Drošs savienojums – lapas ar drošības sertifikātiem

Ar drošību (security) saprot datoru tīklos un datoru sistēmās glabājamo datu aizsardzību pret to bojāšanu, zaudēšanu vai nesankcionētu piekļuvi. Mūsdienās datortīklu un it īpaši interneta straujā pieejamība liek šai problēmai pievērst arvien lielāku uzmanību. Galvenā drošības problēma datortīklos ir to aizsardzība pret nesankcionētu izmantošanu, piemēram, veicot elektroniskos maksājumus, pastāv iespēja, ka dati tiks nozagti un ļaunprātīgi izmantoti.

Lai datus vai ziņojuma saturu nodrošinātu pret nesankcionētu izmantošanu, lieto **šifrēšanu** (encryption). Šifrēšana ir datu un ziņojumu apstrādes process, ko veic datu sagatavotājs vai ziņojuma nosūtītājs. Lai šādus datus vai ziņojuma saturu varētu izmantot, jāveic tā atšifrēšana. Datu šifrēšanai un atšifrēšanai lieto šifrēšanas atslēgu (encryption key).

Tīmekļa vietnes, ar kurām notiek šifrēta ziņojuma apmaiņa, sauc par **drošām tīmekļa vietnēm (secure website)**.



Drošu savienojumu parasti raksturo ikona

Riski, kas saistīti ar tiešsaistes aktivitātēm:

- netīša personīgas informācijas izpaušana. Lai izmantotu tīmekļa vietnēs piedāvātos pakalpojumus, bieži nepieciešams reģistrēties, norādot par savu personīgo informāciju, piemēram, vārdu, uzvārdu, dzimšanas

datumu, adresi. Pirms sniegt šīs ziņas, būtu jāpārliecinās, ka vietne ir uzticama un droša;

- uzmākšanās vai iebiedēšana, izplatot ļaunprātīgas baumas vai apmelojumus vai nosūtot draudu ziņojumus;
- potenciāla varmācība. Lietojot sociālos tīklus un nodibinot jaunus kontaktus, pastāv iespēja iepazīties ar potenciālu varmāku, ļaundari u. tml. Tāpēc jāpadomā, kādu informāciju sniegt par sevi, kritiski jānovērtē izteiktie piedāvājumi.

Gadījumos, kad nākas saskarties ar krāpšanos, uzmākšanos, emocionālu pazemošanu informējiet tiesībsargājošās institūcijas, piemēram, policiju.

Bērnu drošība internetā

Lai pasargātu bērnus no nelabvēlīgas ietekmes, lietojot globālo tīmekli, ieteicams veikt šādus pasākumus:

- novietot datoru telpā, kurā ir iespējams sekot bērna darbībām tīmeklī;
- izveidot bērniem lietotāju kontus ar ierobežotām datora lietotāja tiesībām;
- ierobežot globālā tīmekļa pārlūkošanu, ieslēdzot filtrus, kas aizliedz apmeklēt tīmekļa vietnes ar bērniem kaitīgu saturu (narkotikas, pornogrāfija, naida kurināšana, ieroči u. tml.);
- ierobežot spēļu ar kaitīgu ietekmi lietošanu, aizliedzot spēles par noteiktām tēmām;
- ierobežot datora lietošanas laiku, nosakot datora lietošanas grafiku;
- piemēram: **User Accounts and Family Safety**.

2.3. Wi-fi izmantošana

Ja jūsu dators, planšetdators vai viedtālrunis atbalsta WiFi, varat izmantot internetu, ierīcei nepievienojot papildu vadu, kas ierobežo jūsu atrašanās vietu.

WiFi var izmantot gan mājās, gam ārpus tām. Ja WiFi vēlaties izmantot ārpus mājas, savās ierīcēs bieži varat redzēt dažādus WiFi tīklus. Apdzīvotās vietās, iespējams, redzēsiet vairākus WiFi tīklus, bet ne visiem varēsiet piekļūt, jo tīkls var būt aizsargāts ar paroli.

Daudzās vietās, piemeram, kafejnīcās, veikalos, parkos jums ir iespēja izmantot bezmaksas publisko WiFi. Vislabākais veids, kā droši lietot publiskos WiFi pieslēgumus kādā iestādē vai citā sabiedriskā vietā, ir konkrētā iestādē uzzināt paroli un lietot bezmaksas pieslēgumu caur šifrēto pieeju. Publiski pieejamais WiFi tīkls joprojām ir viens no visbiežāk lietotajiem veidiem, kā nelikumīgi pieslēgties jūsu mobīljai ierīcei un piekļūt jūsu personiskajiem datiem.

2.4. E-pastiem pievienotie faili, iekļautās saites un Spam ziņas

Nevēlamus e-pastus vai uzbāzīgas reklāmu vēstules sauc par mēstulēm (spam un junk). Mēstuļu sūtītāji vienlaikus var viegli un lēti aizsūtīt e-pasta vēstuli vairākiem tūkstošiem cilvēku. Šādas vēstules ir anonīmas.

Ieteikumi, kā cīnīties pret mēstulēm:

a) **Izmantot mēstuļu bloķētāju.** Mēstuļu bloķētājs var ievērojami samazināt ienākošo mēstuļu skaitu. Lielākajai daļai e-pasta sniedzēju, piemēram, Google Gmail ir automātisks mēstuļu bloķētājs. Ja nepieciešams, var izmantot arī papildu programmas, kas bloķē mēstuļu saņemšanu. Tomēr arī šajā gadījumā pastāv varbūtība tās saņemt.

b) **Neatbildēt uz mēstulēm.** Saņemot interesantu mēstuli, Jums var rasties kārdinājums atbildēt uz to vai noklikšķināt uz saites, lai atteiktos no turpmākās vēstuļu saņemšanas. Atteikties var tikai no likumīgiem e-pastiem, kurus esat abonējis. Atbildot uz mēstuli vai noklikšķinot uz kādas saites, jūs nemanot paziņojat, ka šī e-pasta adrese darbojas un turpmāk uz šo adresi tiks sūtītas jaunas mēstules.

c) **Deaktivizēt attēlus.** E-pasta vēstule var saturēt attēlus, kurus mēstuļu izplatītājs var izsekot. Atverot mēstuli un atļaujot lejupielādēt attēlus tajā, jūs norādāt, ka esat gatavs saņemt jaunas mēstules.

d) **Deaktivizēt ziņojumu priekšstatījuma rūti.** Noklikšķinot uz vēstules, tā automātiski tiek attēlota priekšstatījuma rūtī. Mēstules apskatīšana var izraisīt nākamo mēstuļu saņemšanu.

e) **Regulāri pārbaudīt mēstuļu mapi.** Dažreiz mēstuļu bloķētāji bloķē ne tikai mēstules, bet arī likumīgus e-pastus. Tādēļ pēc iespējas biežāk

jāpārbauda mēstuļu mapīte, lai nepalaistu garām svarīgu vēstuli. Pārbaudiet e-pasta programmas iestatījumus, kas nosaka, kuru vēstuļu saņemšana tiks atļauta, un kuras tiks bloķētas.

☑	Izveidojiet vairākas e-pasta adreses, kuras izmantot dažādiem mērķiem.
☑	Publiskajos tīklos neizpaudiet savas privāto e-pasta adresi.
☑	Neveidojiet īsas e-pasta adreses. Daudzi mēstuļu sūtītāji sūta vēstules uz nejauši izdomātiem e-pastiem. Jo īsāka adrese, jo vieglāk to atklāt.
☑	Ja vēlaties ielikt sludinājumu internetā, izveidojiet jaunu, šim nolūkam paredzētu e-pasta adresi.
☑	Ja nepieciešams paziņot e-pasta adresi atklātībā, tad dariet to mazāk saprotamā formā, piemēram, vārds.uzvārds@pasts.lv rakstiet kā vārds-uzvārds-et-pasts-punkts-lv.
☑	Nelietojiet privāto e-pasta adresi, reģistrējoties publiskajos tīklos
☑	Neriskējiet izmantot iespēju “atteikties no šī pakalpojuma”, jo bieži vien tas tikai veicinās jaunu mēstuļu saņemšanu.
☑	Nomainiet privāto adresi, ja tā tika atklāta un tajā ienāk daudz mēstuļu.

2.5. Drošas paroles

Jūsu izvēlētās paroles ir svarīgākais un primārais “vairogs” jūsu kontu aizsardzībai. Izmantojiet vienkāršu, bet drošu veidu, kā izveidot un uzglabāt visas jūsu paroles.

Soļi, kā vienkāršot paroles:

1. *Paroļu frāzes*

Paroļu svarīgākā īpašība – tām jābūt garām, jo vairāk simbolu ir parolē, jo labāk. Tās sauc par paroļu frāzēm, kas ir drošu paroļu veids, kurā izmanto īsus teikumus vai gadījuma vārdus:

- *Laiks stiprai melnai kafijai!*
- *Pazudis-gliemezis-lien-pludmale*

Abas paroles ir drošas, ar vairāk kā 20 simboliem, abas paroles ir viegli atcerēties un vienkārši uzrakstīt, bet grūti uzlauzt. Jūs saskarsieties ar tīmekļa vietnēm vai situācijām, kurās tiks prasīts parolē izmantot simbolus, ciparus vai lielos burtus, un arī tādas paroles var veidot. Bet atcerieties, ka galvenais parolē ir garums!

2. *Paroļu pārvaldnieki*

Jums nepieciešama unikāla parole katram jūsu kontam. Ja izmantojat vienu paroli vairākiem kontiem, jūs pakļaujat sevi lielam riskam. Viss, kas kiberuzbrucējam ir nepieciešams, ir uzlauzt jūsu izmantoto tīmekļa vietni, nozagt visas paroles, ieskaitot jūsējo, un tad izmantot jūsu paroli, lai autorizētos visos citos jūsu kontos. Tas notiek biežāk nekā jūs to iedomājaties. To iespējams pārbaudīt www.haveibeenpwned.com, cik daudzas vietnes, kuras izmantojat, ir tikušas uzlauztas, un, iespējams, jūsu paroles kompromitētas. Tādos gadījumos viens no risinājumiem ir izmantot paroļu pārvaldnieku.

Paroļu pārvaldnieks ir speciāla datorprogramma, kas glabā visas jūsu paroles drošā, šifrētā veidā. Jums jāatceras tikai viena parole - jūsu paroļu pārvaldniekam.

Paroļu pārvaldnieks pēcāk automātiski sameklē jūsu paroles atbilstošajām vietnēm, kad jums tas ir nepieciešams, un autentificē jūs. Tiem ir vēl arī citas funkcijas, piemēram, iespēja saglabāt jūsu atbildes uz drošības jautājumiem, brīdināt jūs, ja izmantojat paroli atkārtoti, paroļu ģeneratora funkcija, kas ļaus jums veidot un izmatot drošas paroles, un daudzas citas iespējas. Lielākā daļa paroļu pārvaldnieku arī droši sinhronizējas starp virkni dažādu ierīču, tā ka jums ir vienkārša un droša piekļuve jūsu parolēm, neatkarīgi no tā, kādu sistēmu jūs izmantojat.

Pierakstiet sava paroļu pārvaldnieka paroli uz papīra un noglabājiet to drošā vietā savās mājās. Daži paroļu pārvaldnieki pat ļauj izdrukāt paroļu pārvaldnieka atgūšanas rīku. Tādejādi, ja jūs aizmirsīsiet sava paroļu pārvaldnieka paroli, jums būs rezerves plāns. Arī kādā ārkārtas dzīves situācijā, kad tas nepieciešams, jūsu tuvinieks varēs jūsu vārdā iegūt informāciju.

3. *Divu faktoru autentifikācija*

Divu soļu verifikācija (bieži saukta arī par divu faktoru autentifikāciju vai daudzfaktoru autentifikāciju) sniedz papildus drošības līmeni. Tā pieprasa divas lietas, kad veicat pierakstīšanos savos kontos, jūsu paroli un ciparu kodu, kurš tiktu uzģenerēts jūsu viedierīcē vai atsūtīts uz jūsu telefonu. Šis process nodrošina to, ka pat tad, ja kiberuzbrucēji ir ieguvuši jūsu paroles, tie nevar piekļūt jūsu kontiem. Divu faktoru autentifikācija ir vienkārši uzstādāma, un parasti jums to jāizmanto tikai vienreiz, kad veicat autorizāciju no jaunas iekārtas. Iespējojiet to, kad vien iespējams, it īpaši saviem svarīgākajiem kontiem, tādiem kā jūsu banka vai e-pasts. Kā piemēru var minēt banku izdoto kodu kalkulatoru un jūsu paša izdomāta parole. Ja jūs izmantojat paroļu pārvaldnieku, iesakām to aizsargāt gan ar drošu paroļu frāzi, gan ar divu faktoru autentifikāciju.

Divpakāpju autentifikācija

Vienkāršoti divpakāpju autentifikācija nozīmē to, ka papildus tam, ka jūs ievadāt kaut ko, ko jūs zināt (paroli), jūs to apstiprināt ar kaut ko, kas jums ir (piemēram, kodu no mobilā tālruņa). Pastāv arī trīs pakāpju autorizācija, kur piekļuve papildus jāapstiprina ar kaut ko, kas ir tieši jums – piemēram, pirksta nospiedums. Divpakāpju autentifikācijas priekšrocība ir tāda, ka, lai uzlauztu jūsu kontu, ļaundarim nepieciešams arī piekļūt jūsu mobilajai ierīcei.

3. Paroļu izmantošana

3.1. Paroles: drošības pirmais solis

Ir divu veidu paroles: drošas un nedrošas. Vairākums cilvēku izmanto nedrošas paroles- paroles, kuras ir īsas, viegli iegaumējamas, satur personīgo informāciju (piemēram, vārdu, uzvārdu, dzimšanas gadu, nozīmīgu datumu, mājdzīvnieku vārdus, ģimenes locekļu vārdus) vai pat viena un tā pati parole tiek izmantota vairākiem kontiem.

Ļaundari jeb tā saucamie hakeri bieži vien izmanto paroles atklāšanas programmatūras, kuras pārbauda lielu skaitu paroļu, līdz atrod īsto. Nedrošas paroles var ļoti ātri atklāt. Dažādu paroļu izveide samazina iespēju, ka noziedznieki atklās jūsu paroli un nozags personīgo un finanšu informāciju.

Lai nosargātu savus datus, pastāv droša darba pamatprincipi, kas jāievēro, izmantojot paroli:

- Ievadot paroli, uzmaniet, lai citi cilvēki neredz pirkstu kustību uz tastatūras vai viedtālruņa ekrāna;
- Mainiet paroli ik pēc 3 mēnešiem;
- Uzmanieties, lai netiktu saglabāta automātiskā piekļuve kontam. Vienmēr izmantojiet pogu **"Iziet", "Atslēgties"** vai **"Beigt darbu".**
- Izvairoties no paroļu izmantošanas brīvpiekļuves interneta vietās.

3.2. Drošas paroles izveides principi

Veidojot lietotāja kontu sociālajos tīklos, izmantojot internetbanku vai kādu citu pašapkalpošanās portālu, ir jāreģistrējas, norādot lietotājvārdu, paroli un citus datus.

Apgalvojums	**Paskaidrojums**
Nekad neizmantojiet personīgo informāciju	Kā paroli neizmantojiet vārdu, dzimšanas dienu vai ģimenes locekļu vārdus. Personīgā informācija bieži vien ir publiski pieejama, tāpēc paroli var ļoti ātri uzminēt.
Izmantojiet garākas paroles	Parolei jāsastāv vismaz no sešām rakstzīmēm. Lai padarītu paroli vēl drošāku, paroles sastādīšanā var izmantot 12 un vairāk rakstzīmes.
Izvairieties no paroļu pierakstīšanas blociņā vai tālrunī	Ja tomēr vēlaties paroli pierakstīt, glabājiet to drošā vietā un nerādiet nevienam. Ieteicams paroles šifrēt un pierakstīt nevis pašu paroli, bet dot tikai sev saprotamu mājienu uz šo paroli.
Izmantojiet nejauši izvēlētas paroles	Nejauši izvēlētas paroles ir visdrošākās. Tā vietā, lai domātu savas paroles, var izmantot paroļu ģeneratorus. Nejauši izvēlētas paroles ir grūtāk atcerēties, jo tās izveido ierīces.

Apgalvojums	Paskaidrojums
Neizmantojiet vienādas paroles vairākiem kontiem	Ja kāds atklās viena konta paroli, arī pārējo kontu paroles būs neaizsargātas.
Neizmantojiet vārdus, kurus var atrast apkārtējā vidē	Piemēram, parole *skolotajs1* būs nedroša parole
Parolēs iekļaujiet ciparus, simbolus, kā arī mazos un lielos burtus	Lai izveidotu drošu paroli, burtus var aizvietot ar dažādiem simboliem, piemēram, par pamatu ņemot vārdu *skolotājs* un aizstājot burtus “o” un ”a”, varat izveidot šādu drošu paroli *Sk0lot@js!*

3.3. Situācija un praktiskais uzdevums

Pilsonis Bērziņš, vīrietis labākajos gados, beidzot nolēmis sākt izmantot elektroniskos pakalpojumus un ir gatavs piereģistrēties Ceļu satiksmes drošības direkcijas (CSDD) mājas lapā, lai turpmāk varētu informāciju par sevi un savu auto uzzināt attālināti.

Lai izveidotu jeb aktivizētu savu CSDD kontu, pirmajā reizē ieejot mājas lapā ir jāpiereģistrējas ar savu e-pastu, pašam jāizdomā un jāievada parole. Pēc konta pirmreizējās izveides, turpmāk piekļuve savam CSDD kontam jau notiek gan ar izveidoto pieeju, gan ar savas internetbankas piekļuvi.

Situācijas virsuzdevums - pilsonim Bērziņam, atrodoties savā viesistabā pie sava datora, izdomāt jaunizveidotajam CSDD kontam paroli, lai neviens to nevarētu uzminēt.

Kopējā aina - pilsonis Bērziņš savā lauku mājā, viesistabā sēd pie galda un ir atvēris portatīvo datoru. Fonā- stūra dīvāns, uz kura laiski vienā galā guļ ruds persiešu runcis, vārdā Rūdis, dīvāna otrā galā sēd Bērziņa kundze un tamborē rudens cepuri. Saimniekam pie kājām guļ melns suns, vārdā Poga. Kaut kur fonā silti čurkst kamīns, virs kura karājās Bērziņa medību trofeja, aļņa galva ar ragiem. Par cik, tā ir viesistaba, tad vienu sienu aizņem grāmatu plaukts, no kura var ieraudzīt dažādus, atpazīstamus rakstnieku darbus, bet uz dažu grāmatu vākiem

var redzēt to ģīmetnes. Piemēram, Rainis, Jaunsudrabiņš, Brigadere, Šekspīrs, Dostojevskis, Čehovs utt. Pie citas sienas ir Bērziņu ģimenes kopbilde, kurā var redzēt pieaugušos bērnus un pat dažus mazbērnus. Tur pat ir Bērziņa un viņa sievas pagājušovasar bildēta kopbilde pie Niagāras ūdenskrituma. Nedaudz tālāk, pie sienas no kāda plaukta istabā nokarājusies efeja, uz palodzes aug līdakaste. Vienvārdsakot, kārtīga latvieša viesistaba lauku mājā, kurā ir visa ģimenes vēsture.

1) Katrs no Bērziņu ģimenes mājas atslēgas objektiem (elementiem) var tikt aplūkots kā sliktais vai **labais** paroles piemērs:

- Kaķis Rūdis: Rudis/ **RuD!$**
- Sievas hobijs: tamboresana/ **T@m80r3$@n@**
- Istabas augs Līdakaste: lidakaste/**etsakadil**
- Medību Trofeja: Trofeja/ **Tr0f3j@**
- Suns Poga: Poga/ **50g@**
- Mazdēls12: Mazdels12/ **M@zd3l$12**
- Sieva Rozālija: Rozalija/ **R0z@l!j@**
- Čehovs: Cehovs/ **C3h0v$**
- Dostojevskis: Dostojevskis/**D0$t0j3v$k!$**
- Anna Brigadere: Brigadere/**8r!g@d3r3**

Kopsavilkums

Šajā modulī tika aplūkotas trīs svarīgas tēmas, kas saistītas ar personas datu un privātuma aizsardzību. Piemēram, datora drošības pamati un datu aizsardzības pamatprincipi. Lai izvairītos no pikšķerēšanas, izglītojamie tika iepazīstināti ar veidiem, kā kibernoziedznieki rīkojas, lai zagtu informāciju. Ņemot vērā to, ka mūsdienās viena no lielākajām personas datu aizsardzības problēmām ir pārāk personīgas informācijas ievietošana dažādos sociālajos tīklos, modulis ietvēra arī drošības vadlīnijas par šo tēmu.

Lai droši izmantotu digitālās ierīces ārpus mājas, modulī tika apskatītas interneta savienojumu tēmas, kā arī droša Wi-Fi lietošanas pamatprincipi. Tika arī izskaidrotas nedroša e-pasta un surogātpasta pazīmes un sniegti padomi, kā pareizi un droši lietot paroles.

Moduļa noslēguma sadaļā apskatīti paroļu izveides piemēri un aprakstīta situācija - kā tiek izveidotas paroles, kāda veida paroles ir drošas lietošanai, un no kurām ir jāizvairās?

Izmantotie informācijas avoti

- *Drošība internetā.* (n.d.). Mana.latvija.lv. https://mana.latvija.lv/drosiba/
- *E-rīki jeb ceļvedis e-pakalpojumu lietošanā*. (n.d.). Mana.latvija.lv. https://mana.latvija.lv/e-riki/
- *Esiet sveicināti Mācību e-vidē!* (n.d.). [Mācību e-vide]. Macibas.mana.latvija.lv. https://macibas.mana.latvija.lv/
- Pieslēdzies, Latvija! (n.d.). *Esiet sveicināti datorskolā! Mācies pats*. [Tiešsaistes kurss]. Tet.lv. https://www.tet.lv/piesledzies-latvija/materiali/start/
- SEB. (n.d.). *SEB privātpersonām*. Seb.lv. https://www.seb.lv/private
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Esidross.lv. https://www.esidross.lv/
- Valsts reģionālās attīstības aģentūra. (n.d.). *Valsts pārvaldes pakalpojumu portāls.* Latvija.lv. https://www.latvija.lv/
- *Mana Latvija.lv. Dari digitāli!* (n.d.). Mana.latvija.lv. https://mana.latvija.lv/
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Cert.lv. https://www.cert.lv/lv
- Uzdevumi.lv. (n.d.). Uzdevumi.lv. https://www.uzdevumi.lv/
- Latvijas Drošāka interneta centrs. (n.d.). Drossinternets.lv. www.Drossinternets.lv
- Draudzīgs internets. (n.d.). *Interneta Drosības ABC*. Draudzigsinternets.lv. www.draudzigsinternets.lv