Digitālo prasmju uzlabošana pieaugušajiem

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

Kā aizsargāt digitālās ierīces?

Kompetence: Ierīču aizsardzība

Ievads 3
1. Ierīču fiziskā drošība 4
2. Šifrēšana 5
3. PIN kods/zīmējums 6
4. Pirkstu nospiedums 6
5. Sejas atpazīšana 7
6. Telefona atrašana 8
7. Droša mobilo lietotņu izmantošana 8
8. Slēgšana (lock) un nodzēšana (wipe) 10
9. Vīrusi un antivīruss 10
10. Licencētas un nelicencētas programmas 12
11. Lejupielādes 13
12. Pārlūkprogrammas 13
13. Datu rezerves kopija 15
14. Sakņota ierīce 18
Kopsavilkums 19
Izmantotās informācijas avoti 20

Ievads

Modulis aptver svarīgākās tēmas, kurām jāpievērš uzmanība, ikdienā strādājot ar digitālajām ierīcēm: viedtālruni, planšetdatoru, portatīvo datoru un stacionāro datoru.

Moduļa mērķi ir:

- izskaidrot metodes, kā aizsargāt ierīces no citu cilvēku fiziskas piekļuves - PIN, paroles ievadīšana, pirkstu nospiedumu slēdzene, sejas atpazīšana;
- iemācīt, kā aizsargāt digitālās ierīces no citu lietotāju attālinātas piekļuves - pretvīrusu programmu un lietojumprogrammu instalēšana un lietošana, droša programmu un dokumentu lejupielāde ierīcē;
- izskaidrot ieguvumus no informācijas dublēšanas digitālajā ierīcē un informēt par iespējām, kā veidot datu rezerves kopijas.

1. Ierīču fiziskā drošība

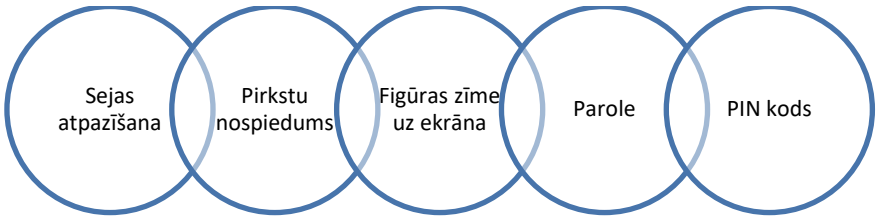
Mūsdienās daudziem cilvēkiem ir dators, mobilais tālrunis un kāda cita ierīce, kuru viņi vēlas pasargāt no kaitējuma. Draudi ierīcēm ir vairāki: cilvēka fiziskās darbības (pārgalvība, neuzmanība, kļūmes, darbības traucējumi), ļaunprātīga programmatūra (vīrusi), hakeri, dabas parādības / katastrofas, tehniskas kļūmes u.t.t. Ierīces aizsardzībai ir daudz veidu: ierīces šifrēšana, PIN koda izmantošana, pirkstu nospiedumu slēdzenes, sejas atpazīšana, funkcija "atrast manu ierīci", bloķēšana un datu dzēšana.

Faktori, kas var uzlabot ierīču fizisko drošību:

- paroles / PIN kodi;
- speciālas ierīces un programmatūra;
- telpu drošība;
- pareiza aprīkojuma izmantošana (saskaņā ar lietošanas instrukcijām);
- aizsargāšana no iespējas aizdegties vai samirkt.

Lietojot paroles/PIN kodus un/vai speciālu programmatūru, ierīces zādzības gadījumā tā nav izmantojama. Ir pieejamas programmas, ar kuru palīdzību nozagtu ierīci var izsekot.

Piemēri tālruņa atslēgšanas veidiem:



Informācijas aizsardzība, lietojot ārējos datu nesējus:

- Datņu kopēšanu uz/no ārējiem informācijas nesējiem (piemēram, disketēm, CD vai DVD diskiem, vai USB zibatmiņām) veiciet vienīgi konkrētu uzdevumu izpildei,

- Pievienojot datoram ārējo datu nesēju to noskanējiet ar antivīrusu programmu,
- Ar īpašu piesardzību lietojiet ārējos datu nesējus, kurus iedevuši draugi un paziņas,
- Bez vajadzības ierīcēs neglabājiet svarīgu un aizsargājumu informāciju.

2. Šifrēšana

Šifrēšana ir process, kurā tiek kodēta lasāmā informācija tā, lai to varētu izlasīt / tā būtu pieejama tikai tai personai, kurai ir slepenais kods vai atšifrēšanas atslēga. Tas ir veids, kā paslēpt / aizslēgt informāciju līdz brīdim, kad tiek ievadīts kods un informācija tiek pārveidota atpakaļ uz lasāmo tekstu. Sensitīvo datu drošībai ļoti daudzi cilvēki izmanto datu šifrēšanu.

Jums ir iespēja šifrēt gan datus, ko uzglabājat savās ierīcēs, gan tos, kurus sūtat. Ir vairākas šifrēšanas metodes. Piemēram, FDE ir pilna diska šifrēšana, ko izmanto, lai nošifrētu visu disku jūsu sistēmā. Tas nozīmē, ka tiek aizslēpta visa informācija nevis tikai kāda daļa.

Lai nosargātu datus, kas tiek sūtīti tiek izmantots HTTPS tiešsaistes šifrēšanas veids. Tas nozīmē, ka informācija tiek šifrēta ceļā no pārlūkprogrammas uz mājas lapu. Arī e-pastiem un citām saziņas programmām tiek piedāvātas šifrēšanas metodes, kas ir jāiestata pašam. Pamatnosacījums, lai šifrēšana būtu veiksmīga, ir turēt atslēgu/paroli drošība un sastādīt to ļoti sarežģītu – pēc iespējas garāku, neuzminamu un visādā citādā ziņā – drošu. Var izmantot paroļu pārvaldnieku, lai atcerētos paroles.

Šifrēšana spēj funkcionēt, ja jūsu ierīce ir drošībā. Primāri ir pārliecināties, ka iekārta nav kompromitēta, tajā nav ļaunprogrammatūras – vīrusi, vai kā citādi tā netiek apdraudēta. Regulāri pārliecinieties, ka iekārtai nav piekļuve trešajai personai. Atcerieties, ja aplikācija/programma, ko vēlaties izmantot, nepiedāvā šifrēšanas iespējas, tad apsveriet citus variantus. Ir svarīgi, izmantot drošas aplikācijas/programmatūras, kuru lietošana jūs neapdraud.

3. PIN kods/zīmējums

PIN kods ir īpašs aizsardzības mehānisms, kas tiek piemērots autorizācijai bankas kontam, ierīcei vai kādai īpaši sensitīvai informācijai. Pin kodu nedrīkst nevienam atklāt. To ieteicams mainīt tāpat kā paroli. PIN kods ir jāzina no galvas. Lai pasargātu sevi, maksājumus ieteicams neveikt no publiski lietojamiem datoriem vai nepazīstamas ierīces. Ir programmas, kas spēj nolasīt visu, ko lietotājs ievada ar tastatūras palīdzību – arī PIN kodus. Tāpēc PIN kodu izmantojiet tikai savā privātajā ierīcē, par kuras drošību esat pārliecināts. Mūsdienās ir pieejami arī **zīmējuma tipa PIN kodi**. Ar tiem jābūt uzmanīgiem, jo cilvēki mēdz tos iestatīt ļoti vienkāršus, standartizētus, kā arī ierīces ekrāns regulāri ir jātīra, lai pēc vilkšanas līnijām, kods nebūtu uzminams. Kad cilvēks ievada PIN kodu vai zīmējumu, ieteicams aizklāt ievades laikā vienu roku ar otru, kā arī pārliecināties, ka ierīces ekrāns nav pārāk gaišs un labi saskatāms no citiem leņķiem.

4. Pirkstu nospiedums

Vairākām ierīcēm ir pieejams pirkstu nospiedumu sensors. Tā ir biometriska ierīce, kas palīdz ātri atpazīt personu. To ir iespējams iestatīt gandrīz visās viedierīcēs, kurās ir iebūvēts pirkstu nospieduma sensors. Pirksta nospiedums var būt mazāk drošs nekā sarežģīts PIN kods, kombinācija vai parole. Tomēr pastāv iespēja fiziski ar dažādām metodēm noņemt pirkstu nospiedumu no jūsu ierīces. Ir jāapzinās, ka noņemt jūsu pirkstu nospiedumu var arī no citām ikdienišķām lietām. Ja ierīce nav drošībā, tad pirkstu nospiedums var tikt nolasīts kā jebkura informācija no jūsu ierīces.

Pirkstu nospieduma autentifikācijas veidam izmanto divu faktoru autorizācijas procesu. Tas nozīmē, ka parasti tiek izmantot arī PIN kods. Ja ierīces nespēj atpazīt/nolasīt pirkstu nospiedumu, tad tiek izmantots PIN kods. Kā arī pēc atjauninājumiem vai ierīces ieslēgšanas, drošības nolūkos, tiek izmantots PIN kods.

Ja izvēlaties izmantot pirkstu nospiedumu kā ierīces atbloķēšanas metodi, tad dodieties pie ierīces uzstādījumiem un veiciet atbilstošas darbības. Pirmā iestatīšana ir ļoti svarīga – jūsu pirksti tiek noskenēti. Ieteicams ir turēt tālruni dabīgā pozīcijā un pārliecināties, ka izpildāt visus soļus, kas no jums tiek prasīti. Var rasties problēmas ar pirkstu nospieduma izmantošanu, ja sensors ir bojāts, netīrs vai arī nav veikts nepieciešamais ierīces atjauninājums. Vairākas tehnoloģiju kompānijas labāk izvēlas aizstāt pirkstu nospiedumu ar sejas atpazīšanas rīku.

5. Sejas atpazīšana

Sejas atpazīšana ir autentifikācijas veids, kura izmantošanai nepieciešama kamera. Tā ir iespēja atbloķēt ierīci vai pieslēgties konkrētām aplikācijām parādot savu seju kamerā. Eksperti, kas jau ilgus gadus strādā pie mākslīgā intelekta, atzīst, ka sejas atpazīšana ir viens no drošākajiem veidiem, kā pieslēgties sistēmai.

Lai iestatītu sejas atpazīšanas funkciju, nepieciešama šim nolūkam paredzēta ierīce, kamera un sejas iestatīšana – lai ierīce atpazītu jūs, būs nepieciešams seju noskenēt no visām pusēm.

Vairumā gadījumu lēta tālruņa sejas atpazīšanas sistēma izmanto tikai uz priekšu vērsto kameru un dažus ne visai sarežģītus algoritmus — un vēl varbūt arī zibspuldzi, lai uzņemtu labāku foto. Taču parasto 2D kameru bez infrasarkano staru sensora un punktu projektora viegli var piemuļķot, parādot fotogrāfiju.

Ja izvēlaties sejas atpazīšanu kā drošības mehānismu, ieteicams izmantot kvalitatīvu ierīci. Pārliecinieties par tās darbības principiem. Eksperti joprojām strādā pie šīs sistēmas uzlabošanas un atzīst, ka sejas atpazīšana tiks izmantota arī nākotnē, lai piekļūtu konkrētām mājas lapām, iegādātos preces veikalā un veiktu citas darbības.

6. Telefona atrašana

Telefona atrašanas programmas paredzētas, lai jebkurā laikā atrastu savu telefonu, kā arī attālināti to pārvaldītu un redzētu, kas ar to tiek darīts. Šo funkciju izmanto, ja telefons tiek pazaudēts vai ir ticis nozagts. Ir iespēja noteikt telefona atrašanās vietu, dzēst datus, apskatītu baterijas uzlādi un redzēt, kādam Wi-Fi tīklam tas ir pieslēgts. Lai gan jāņem vērā, ka atkarībā no operētājsistēmas, funkcijas var būt atšķirīgas. Ir gan iebūvētas programmas, kas palīdz izsekot telefona darbībai, gan atsevišķi lejupielādējamas un nopērkamas programmas.
Lai izmantotu šo funkciju, tā ir jāieslēdz konkrētajā ierīcē un jāizpēta konkrētās ierīces iespējas to izmantot. Izmantojiet interneta meklētāju, lai uzzinātu visu par tieši jūsu ierīci vai konsultējieties ar cilvēku, kas var palīdzēt noskaidrot šo informāciju.
Arī Google ir pakalpojums, ar kura palīdzību ir iespējams attālināti bloķēt tālruņa darbību, piezvanīt uz to, izrakstīties no Google konta un veikt citas darbības. Ierīces atrašana notiek, izmantojot internetu. Prakse rāda, ka šo funkciju izmanto pārsvarā, lai nobloķētu ierīci un izrakstītos no konkrētiem profiliem, bet ne vienmēr ir iespējams fiziski atrast ierīci. Ir vairākas programmas, kurām tieši šī funkcija paredz maksu. Apple kompānijas programma ir “Find My iPhone”, Microsoft programma - “My Windows Phone” un Google piedāvā “Find My Device”. Tās ir tikai dažas no daudzām programmām.

7. Droša mobilo lietotņu izmantošana

Pirmais solis ir lietotņu iegūšana no droša un uzticama avota. Noziedznieki ir iemācījušies radīt un izplatīt inficētas mobilās lietotnes, kas izskatās kā īstas. Ja jūs instalējat šādu inficētu mobilo lietotni, noziedznieki var pārņemt kontroli pār jūsu iekārtu.

Apple ierīcēm – iPad un iPhone mobilās lietotnes lejupielādējat tikai no Apple Aplikāciju veikala (App Store). Šajā veikalā Apple ir veicis drošības pārbaudes visām mobilajām lietotnēm pirms to publiskošanas. Apple nevar "izķert" visas inficētās aplikācijas, taču šāda pārvaldīta vide būtiski samazina inficēšanās risku. Ja Apple atrod inficētu lietotni savā veikalā, tā nekavējoties tiek izņemta no veikala. Windows Phone izmanto līdzīgu pieeju aplikāciju pārvaldīšanā.

Android dod jums izvēles iespējas lejupielādēt mobilo lietotni no jebkuras vietas internetā. Taču jums ir jābūt piesardzīgākiem attiecībā uz šādām lietotnēm, ko jūs instalējat, jo ne visas tās ir pārbaudītas. Google uztur mobilo lietotņu veikalu – Google Play un lietotnēm tajā ir veikta vismaz pamata drošības pārbaude. Tādēļ ieteicams izmantot lietotnes tikai no Google Play. Izvairieties no lietotnēm citās tīmekļa vietnēs, jo ir salīdzinoši vienkārši izplatīt ļaundabīgas lietotnes, tā inficējot jūsu mobilo iekārtu. Kā papildu aizsardzību, ja tas ir iespējams, instalējiet mobilajā ierīcē antivīrusa programmatūru.

Atļaujas. Kad esat instalējis mobilo lietotni no uzticama avota, konfigurējiet to atbilstoši savām privātuma vēlmēm un vajadzībām. Pirms dodiet mobilai lietotnei kādu atļauju – vienmēr apsveriet, vai jūs vēlaties šo atļauju dot un vai aplikācijai tā tiešām ir nepieciešama. Ja jūs atļaujat lietotnei vienmēr zināt jūsu atrašanās vietu, jūs varat dot iespēju aplikācijas izstrādātājam izsekot jūsu kustību vai pat pārdot šo informāciju citiem.

Lietotņu atjaunināšana. Mobilās lietotnes ir regulāri jāatjaunina. Noziedznieki vienmēr meklē ievainojamības lietotnēs. Vairums iekārtu dod iespēju atjaunināt lietotnes automātiski. Ja tas nav iespējams, pārbaudiet lietotņu atjauninājumus vismaz reizi divās nedēļās. Visbeidzot, kad lietotne ir atjaunota, vienmēr pārskatiet izmaiņas lietotnes atļaujās.

8. Slēgšana (lock) un nodzēšana (wipe)

Ierīces aizbloķēšana jeb slēgšana (lock) ir ļoti vienkāršs veids, kā pasargāt sevi no pēkšņiem kaitējumiem vai informācijas atklāšanas, nodošanas citai personai. Arī fiziska ierīces pieslēgšana galdam, darba vietai mēdz atturēt zagļus no ierīces iegūšanas. Tikai ar īpašu atslēgu ierīci var atslēgt.

Ir arī dažādi veidi, kas var mūsu ierīci pasargāt ne tikai fiziski. Lietotājs nedrīkst atstāt darba vietu ar nenoslēgtu darbstaciju: īslaicīgai prombūtnei - **Lock Computer; (Windows+L),** ilgākam laikam **– Log off** vai **Shut down.** Telefoniem un planšetdatoriem ieteicams uzlikt automātisko ierīces bloķēšanu pēc konkrēta sekunžu skaita. Pārsvarā ierīcēm ir viena, ērti pieejama slēgšanas poga, kas atvieglo šo procesu.

Ierīces neaizslēgšana var provocēt kāda cita cilvēka nelabvēlīgu darbību ar jūsu ierīci. Kad esiet beidzis darbu, drošāk ir ierīci pilnībā izslēgt. Zaudējot savienojumu ar internetu, tai nevar piekļūt nelabvēļi. Turot ierīci visu laiku ieslēgtu, risks pieaug.

Wipe jeb nodzēšanas funkcija ir darbība, kas cietā diska informāciju padara nenolasāmu. Tas nozīmē, ka dati ir kā izdzēsti, bet ar piemērotas programmas palīdzību, ir iespējams tos atgūt. Ja tiek mainīta ierīce, cietais disks, tad ieteicams ir tos maksimāli iztīrīt. Tomēr visdrošākais veids ir arī fiziska cietā diska iznīcināšana, lai būtu droši, ka faili netiks atjaunoti.

9. Vīrusi un antivīruss

Kibernoziedznieki iegūst rīcības brīvību, uzstādot ļaunprogrammatūru datoros vai ierīcēs. Tādā veidā ir iespējams noziedzniekam novērot jūsu tiešsaistes aktivitātes, nozagt paroles vai failus, kā arī izmantot jūsu sistēmu, lai uzbruktu citiem.

Ļaunatūra būtībā ir datora programmatūra, ko izmanto pretlikumīgiem nolūkiem. Termins radies savienojot vārdus „programmatūra" un „ļaundabīgs". Kibernoziedznieki uzstāda ļaunatūru datoros vai ierīcēs, lai iegūtu pār tām kontroli. Pēc uzstādīšanas ļaunatūra dod iespēju noziedzniekam novērot jūsu tiešsaistes aktivitātes, nozagt paroles vai failus, kā arī izmantot jūsu sistēmu, lai uzbruktu citiem. Ļaunatūra var inficēt praktiski jebkuru ierīci, sākot no Apple datoriem līdz drošības kamerām.

Šifrējošie vīrusi ir īpaša veida ļaunatūra, kas šobrīd aktīvi izplatās internetā, apdraudot upuru dokumentus un citus failus.

Aizsargājiet sevi – apturiet ļaunatūru!

Diemžēl antivīrusa programmas nespēj apturēt visu ļaunarūru. Kibernoziedznieki nepārtraukti izstrādā jaunu un sarežģītāku programmatūru, kas var izvairīties no antivīrusiem. Protams, antivīrusu izstrādātāji nepārtraukti uzlabo arī savus risinājumus. Kibernoziedznieki izmanto ievainojamības jūsu programmatūrā. Jo jaunāka/aktuālāka programmatūras versija jums ir, jo tai ir mazāk ievainojamību. Tāpēc ieteicams:

- regulāri atjaunināt jūsu operētājsistēmas, lietotnes, pārlūkus, to paplašinājumus un citas programmas. Vienkāršākais risinājums parasti ir uzlikt automātisku atjauninājumu uzstādīšanu.

Izplatīts veids, kā kibernoziedznieki inficē datorus un mobilās ierīces, ir izstrādājot viltotas datorprogrammas vai mobilās lietotnes, publiskojot tās internetā un apmānot cilvēkus, lai tie savās ierīcēs brīvprātīgi uzstādītu šos viltojumus.

- Lejupielādējiet un uzstādiet programmas tikai no uzticamiem tiešsaistes veikaliem, turklāt izpētiet atsauksmes par programmām un izvairieties no tām, kas ir maz izmantotas, vai kurām ir tikai dažas pozitīvas atsauksmes.
- Izdzēsiet lietotni vai programmu, kas jums vairs nav nepieciešama.
- Kibernoziedznieki bieži manipulē ar cilvēkiem, lai tie paši uzstādītu ļaunatūru, piemēram, tie var nosūtīt jums e-pastu, kas satur pielikumu vai saiti tekstā, un, iespējams, izskatās kā nācis no jūsu drauga vai bankas.

Diemžēl, kad jūs noklikšķināt uz saites vai lejupielādējat pielikumu, jūsu sistēmā tiek uzstādīta ļaunatūra.

- Regulāri veidojiet rezerves kopijas jūsu sistēmām un failiem, vai nu mākonī, vai bezsaistē, piemēram, uz ārējā cietā diska.

10. Licencētas un nelicencētas programmas

Ja programmai ir noteikta maksa, tad tā ir jāiegādājas un lejupielāde jāveic likumīgā ceļā. Arī programmu lejupielādes vietai ir jāpievērš uzmanība. Nedrīkst to darīt aizdomīgās vietnēs – tas var apdraudēt ierīci un citu programmatūru datorā. Datoru lietotājiem jāievēro autortiesību likuma normas, kas attiecas uz grāmatām, video un mūzikas diskiem un kasetēm, kā arī programmatūru. Datorprogrammu kopēšanu, izplatīšanu vai izmantošanu bez autortiesību īpašnieka atļaujas sauc par datorprogrammu pirātismu.

Nelegāla datorprogrammu izmantošana ir, piemēram:

- Viena legāli iegādāta programmatūras kompaktdiska instalēšana uz vairākiem datoriem, ja licencē vai līgumā ir norādīts, ka to atļauts instalēt tikai uz viena datora;
- Programmas kopēšana instalēšanai un izplatīšanai bez autora atļaujas;
- Programmatūras instalēšana no nelegāli iegādāta diska;
- Nelegālas datorprogrammu kopijas lejupielāde no interneta.

Internetā lejupielādei bez maksas tiek piedāvāta gan programmatūra, gan cita veida datnes (teksti, attēli u.c.). Ne vienmēr to publicētājiem ir tiesības tos izplatīt lietošanai citiem. Tāpēc pirms lejupielādes nepieciešams pārliecināties, vai to kopēšana ir legāla.

11. Lejupielādes

Par lejupielādi (download) sauc procesu, kura laikā datnes no tīkla servera tiek ierakstītas datu glabāšanas ierīcē. Datņu lejupielāde ir nepieciešama, ja lietotājs vēlas iegūt tīmekļa vietnē piedāvātas datnes, piemēram, dokumentus, attēlus, mūziku, video un programmatūru.

Lai saglabātu savā datorā vai ierīcē kādu failu vai attēlu, to jālejupielādē. Fails tiks saglabāts lejupielāžu noklusējuma atrašanās vietā.

Ir iespējams lejupielādēt dažādus datņu veidus:

Veids	**Formāts**	**Piemērs**
Teksts	Docx, txt	Kopsavilkums.docx
Attēls	Jpg. Gif, png.	IMG0034.jpg
Skaņas	Mp3, wma	Voice.mp3
Video	Avi, mpg, mpeg	Ceplis.avi
Programmatūras	Exe	Skype.exe
Arhīvs	Zip, rar	Arhivs.zip

Datņu lejupielādes iespēju var norādīt dažādi, bet parasti to raksturo saite vai poga *Lejupielādēt (Download)*.

12. Pārlūkprogrammas

Pārlūkprogramma ir lietotne, kas paredzēta interneta lappušu skatīšanai. Lai tīmekļa lappusi apskatītu, tā vispirms tiek lejupielādēta jeb pārsūtīta no globālā tīmekļa servera lietotāja datorā un tikai tad atvērta.

Lai varētu izmantot interneta pakalpojumus, nepieciešams:

- Programmvadāma ierīce ar iespēju pieslēgties tīklam;

- Interneta pakalpojumu sniedzējs (IPS), kas nodrošina, ka ar konkrēto ierīci var pieslēgties internetam (var būt neieciešama papildus aparatūra);
- Interneta pārlūkprogramma.

Daži pārlūkprogrammu piemēri:

Jebkuru interneta lapu atvērt nav droši, jo pastāv riski, ka lapa satur vīrusus. Šādā veidā iespējams atvērt arī krāpnieciskas lapas, kas izkrāpj informāciju par cilvēku.

Pastāv pazīmes, pēc kurām var novērtēt, ka tīmekļa lapa ir droša. Divas vienkāršākās pazīmes, kas liecina par lapas drošumu tiek attēlotas adrešu joslā:

- **https** pirms adreses (norāda, ka informācija uz datoru tiek pārraidīta šifrētā veidā);
- parasti aizslēgtas "atslēdziņas" simbols (dažādās interneta pārlūkprogrammās atslēdziņas simbols var atšķirties).

Lapas lejupielāde tiek apturēta, ja:

- Lejupielāde ir ieilgusi;
- Lejupielādes laikā konstatē, ka konkrētajā lapā vajadzīgās informācijas nav.

Lapu nepieciešams atsvaidzināt (refresh), ja:

- Lapas ielāde nav bijusi veiksmīga. Piemēram, uz lapas dažu attēlu vietā ir kvadrātiņi ar sarkanu krustu vai nav pienākusi visa informācija;
- Lietotājs kādu laiku nav aplūkojis lappusi un informācija šajā laikā lappusē ir mainījusies (lapa neatjaunojas automātiski).

13. Datu rezerves kopija

Datu rezerves kopijas veidošana ietver sevī datu glabāšanu ne tikai uz datora, bet arī kādā citā vietā. Šādā gadījumā, ja rodas kādas problēmas ar datoru, vienmēr ir iespējams svarīgos datus atjaunot no to rezerves kopijām.

Dati, kuri parasti tiek glabāti datorā:

- fotogrāfijas;
- darba dokumenti;
- svarīgas programmas, programmatūra;
- video, audio projekti;
- e-pasta sarakstes arhīvs un draugu e-pasti.

Ja domājat, ka jums nav nepieciešamas rezerves kopijas, atcerieties, ka ir daudz veidu, kā jūs varat pazaudēt sev svarīgus dokumentus.

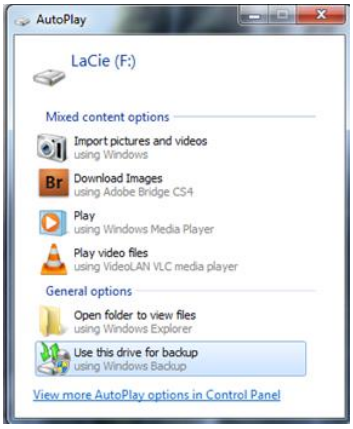
- Vienkāršākais veids, kā pazaudēt visus datus, ir datora nozagšana vai nozaudēšana (tas, protams, attiecas vairāk uz portatīvajiem datoriem).
- Pastāv iespēja nejauši izdzēst datus vai pārkopēt pāri kaut ko citu svarīgiem dokumentiem.
- Dators var tikt inficēts un ļaundabīgā programmatūra var sabojāt konkrētus datus vai pat radīt bojājumus cietajam diskam.
- Var rasties kādas tehniskas problēmas (arī cietais disks var salūzt), kuru dēļ var pazaudēt kādus datus.

Datu rezerves kopiju veidošana.

Datorā ar Windows operētājsistēmu:

- **Iegādājieties ārējās atmiņas ierīci**. Tā var būt jebkurš USB zibatmiņas disks vai ārējais cietais disks. Vēlams iegādāties ierīci ar vismaz divreiz lielāku atmiņas ietilpību nekā jūsu datoram.
- Pirmo reizi pievienojot ārējo atmiņas ierīci pie datora, tā pati piedāvā variantu izmantot to par vietu, kur glabāt datu rezerves kopijas. Ja tāda

opcija neparādās, vienkārši ierakstiet programmu meklēšanas logā „Backup”.



- Tālāk atvērsies logs, kurā jums būs jāuzspiež uz „Set Up Backup” un jāizvēlas, uz kuras ārējās atmiņas diska vēlēsieties veidot datu kopijas. Visbeidzot, būs jānospiež „Save Settings and Run Backup”.
- Pēc šo soļu paveikšanas, Windows izveidos pirmo datu rezervju kopiju (galvenais šajā procesā ir neatvienot ārējo atmiņas disku!). Tālāk varat izvēlēties „Change schedule” un parādīsies šāds attēls. Attēlā redzams, ka tiek piedāvāta iespēja izvēlēties grafiku, kad datu kopijas tiks atjaunotas. Tiek piedāvāta iespēja to darīt reizi dienā, nedēļā un mēnesī. Galvenais atcerēties, ka izvēlētajā laikā un dienā šai ierīcei, uz kā veidojat rezerves datu kopijas, ir jābūt pieslēgtai pie datora.

Datu rezerves kopiju veidošana datorā ar Mac OS operētājsistēmu.

Tas ir paveicams ļoti līdzīgi kā datorā ar Windows operētājsistēmu. Pievienojot ārējo atmiņas disku, parādīsies iespēja izmantot to kā vietu rezerves datu kopiju veidošanai. Izvēlieties to vai arī ejiet caur System Preferences -> Time Machine. Tad jāizvēlas nepieciešamais ārējās atmiņas disks, un uz tā tiks izveidota datu kopija.

Datu rezerves kopiju veidošana mobilajā tālrunī.

Ļoti ērta iespēja, kā veidot kontaktu un kalendāra ierakstu rezerves kopijas, ir ar Google konta (Gmail e-pasta konta) palīdzību. Pie viedtālruņa „Account & Sync Setting” var ieslēgt funkciju, kas ļauj rezerves kopijas veikt jebkurā brīdī. Pie jūsu

kontiem jāparādās Google kontam, ja esat to apmeklējis no sava telefona. Priekšrocība, ja izmantojat šādu kontaktu kopijas veidošanu, ir tāda, ka, mainot telefonus, dati automātiski pārkopēsies uz jauno ierīci. Internetā informāciju par saviem kontaktiem var apskatīt kreisajā pusē, spiežot uz Gmail. Neskaitot Google piedāvātās iespējas, pastāv arī citi veidi un programmatūras, kas piedāvā iespēju veidot rezerves kopijas. Viena no iespējām ir, pieslēdzot telefonu pie datora, vienkārši pārkopēt svarīgos datus. Internetā ir iespējams atrast arī atsevišķas programmas, kas nodrošina rezerves kopiju veidošanu. Ja meklējat sev piemērotu, svarīgi pievērst uzmanību, lai tā būtu derīga jūsu datora operētājsistēmai.

Datu rezerves kopiju veidošana internetā.

Bez maksas šis pakalpojums ir pieejams parasti ar atmiņas ierobežojumiem (aptuveni 5GB-7GB). Šī pakalpojuma izmantošana nodrošina iespēju svarīgākos datus saglabāt internetā, kas nozīmē, ka tiem varēs piekļūt no jebkuras vietas un datora. Pakalpojuma sniedzējs nodrošina šo datu uzglabāšanu šifrētā veidā. Šāda pakalpojuma sniedzēji ir, piemēram, www.mimedia.com un www.backup.comodo.com. Protams, šāda veida datu uzglabāšana ir ērta piekļūšanas ziņā, tomēr netiek arī izslēgtas dažādas drošības problēmas.

Ja radusies situācija, ka dati ir pazuduši, tos atjaunot no rezerves kopijas ir vienkārši. Windows operētājsistēmā „Start Menu" meklēšanā ierakstiet „Backup", un tad spiediet uz „Restore My Files". Mac operētājsistēmas datoros spiediet uz „Time Machine" un tad „Enter Time Machine". Vai arī vienkārši ņemiet savu ārējās atmiņas ierīci, uz kuras līdz šim glabājāt datu rezerves kopijas, pievienojiet to datoram un pārkopējat nepieciešamos failus.

Ieguvumi no rezerves kopiju veidošanas.

- **Morālais ieguvums** - nav lieki jāsatraucas, ka kaut kas var notikt ar datoru; jūs varat būt drošs, ka jūsu svarīgie dati nekur nepazudīs!
- **Finansiālais ieguvums** - ja radušās problēmas ar cieto disku, tad profesionāļu pakalpojumi šo datu atjaunošanai var būt diezgan dārgi. Ja

jums ir rezerves kopija svarīgajiem datiem, šādi pakalpojumi nebūs vajadzīgi.

14. Sakņota ierīce

Sakņošanās ir process, kas viedtālruņu, planšetdatoru un citu ierīču lietotājiem, kas darbojas ar Android mobilo operētājsistēmu, ļauj iegūt priviliģētu kontroli (pazīstamu kā saknes piekļuvi) dažādās Android apakšsistēmās. Šī procesa mērķis ir pārvarēt ierobežojumus, kurus ražotāji uzliek dažām ierīcēm. Tādējādi sakņošanās dod iespēju (vai atļauju) mainīt vai aizstāt sistēmas lietojumprogrammas un iestatījumus, palaist specializētas lietojumprogrammas ("lietotnes"), kurām nepieciešamas administratora līmeņa atļaujas, vai veikt citas darbības, kas parastajam Android lietotājam nav pieejamas. Operētājsistēmā Android sakņošana var arī atvieglot ierīces operētājsistēmas pilnīgu noņemšanu un nomaiņu, parasti ar tās pašreizējās operētājsistēmas jaunāku versiju.

Kopsavilkums

Apgūstot moduļa tēmas, izglītojamie zina, kā nodrošināt ierīču fizisko drošību, kā arī izprot šifrēšanas principus. Izglītojamie spēj atpazīt un izmantot digitālo ierīču aizsardzības tehnikas - sejas atpazīšanu, paroles ievadīšanu, figūru zīmēšanu uz digitālās ierīces ekrāna un pirkstu nospiedumu izmantošanu.

Izmantojot aprakstītos paņēmienus, ir iespējams atrast pazaudētu tālruni. Izglītojamie tiek informēti par dažāda veida vīrusiem, kas apdraud ierīces, un iespējām no tām izvairīties. Lai saglabātu ierīču drošību, lietotājiem jāpievērš uzmanība arī lejupielādēm un jāizmanto tikai licencētas programmas. Pēc sniegtās informācijas izglītojamie var apgūt pretvīrusu programmu un lietojumprogrammu izmantošanas principus, atšķirt dažādas interneta pārlūkprogrammas, kā arī tās izmantot.

Visbeidzot, izglītojamie zina, kā dublēt informāciju savā digitālajā ierīcē, un izprot sakņotās ierīces (rooted device) mērķi.

Izmantotās informācijas avoti

- Pieslēdzies, Latvija! (n.d.). *Esiet sveicināti datorskolā! Mācies pats*. [Tiešsaistes kurss]. Tet.lv. https://www.tet.lv/piesledzies-latvija/materiali/start/
- Swedbank. (n.d.). *Swedbank privātpersonām*. Swedbank.lv. https://www.swedbank.lv/private
- 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/
- *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/
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Cert.lv. https://www.cert.lv/lv
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Esidross.lv. https://www.esidross.lv/
- Uzdevumi.lv. (n.d.). Uzdevumi.lv. https://www.uzdevumi.lv/
- Baltijas Biroju Tehnoloģijas. (n.d.). *Astoņas digitālās prasmes, kas jāmāca bērniem*. Smartboard.lv. https://smartboard.lv/zinas/astonas-digitalas-prasmes-kas-jamaca-berniem/
- Brečko, B., Ferrari, A. (2016) *Patērētāju digitālo kompetenču sistēma*. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC103155/lfna28133lvn.pdf