Project IDCAP: Improve Digital Competence in Adult People

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

Kaip apsaugoti savo prietaisą?

Kompetencijos sritis : prietaisų apsauga

Įvadas

Šis modulis apima svarbiausias temas, į kurias verta atkreipti dėmesį kasdien dirbant su skaitmeniniais įrenginiais: savo išmaniuoju telefonu, planšetiniu kompiuteriu, nešiojamu kompiuteriu ir staliniu kompiuteriu. Modulio tikslai:

- paaiškinti, kaip apsaugoti įrenginius nuo fizinės prieigos prie kitų asmenų - PIN kodai, slaptažodžio įvedimas, pirštų atspaudai, veido atpažinimas ;
- išmokyti apsaugoti skaitmeninius įrenginius nuo nuotolinio prieigos prie kitų vartotojų - įdiegti ir naudoti antivirusines programas ir programas. Saugus programų ir dokumentų atsisiuntimas į įrenginį
- paaiškinti informacijos apie skaitmeninį įrenginį atsarginių kopijų darymo naudą ir pasiūlyti technines galimybes.

1. Fizinė prietaisų apsauga

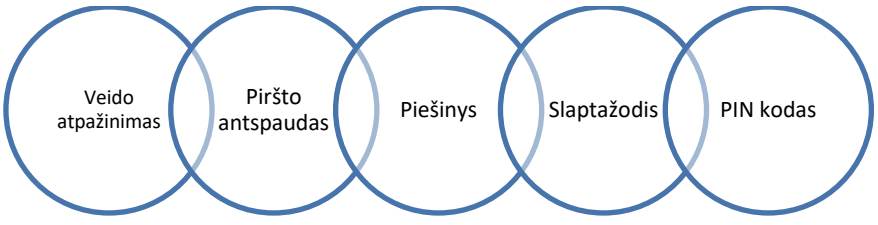
Šiandien daugelis žmonių turi kompiuterį, mobilųjį telefoną ir kai kuriuos kitus prietaisus, kuriuos nori apsaugoti nuo žalos. Grėsmės yra šios: žmogaus fizinis aktyvumas (neryžtingumas, neatsargumas, gedimas, gedimas), kenkėjiška programinė įranga (virusai), įsilaužėliai, gamtos reiškiniai / katastrofos, techniniai gedimai ir t.t. Kaip ir kiekvienas svarbus dalykas, mes norime saugoti duomenis. Savo prietaisą galite apsaugoti įvairiais būdais: užšifruodami savo įrenginį, naudodami PIN kodą, naudodami pirštų atspaudų užraktus, veido atpažinimą, funkciją „suraskite mano įrenginį“, užrakindami ir ištrindami duomenis.

Veiksniai, galintys padidinti jūsų prietaisų fizinę saugą:

- slaptažodžiai / PIN kodai;
- specialūs prietaisai ir programinė įranga ;
- patalpų saugumas;
- tinkamai naudoti įrangą (pagal naudojimo instrukcijas);
- apsauga nuo ugnies ar dregmės.

Naudojant slaptažodžius / PIN kodus ir (arba) specialią programinę įrangą / pirštų atspaudus, prietaiso negalima naudoti vagystės atveju. Yra programų, kuriomis galima sekti pavogtą įrenginį.

Telefono atrakinimo pavyzdžiai:



Informacijos apsauga naudojant išorinę duomenų saugyklą:

- Nukopijuokite į įšorinę duomenų saugyklą arba iš jos (pvz., CD, DVD arba USB atmintinės) tik tam tikroms užduotims atlikti,

- Prijungdami išorinę duomenų saugyklą prie savo kompiuterio, nuskaitykite ją naudodami antivirusinę programą,
- Būkite labai atsargūs, naudodami išorinę duomenų saugyklą, kurią teikia draugai ir pažįstami,
- Be reikalo nelaikykite svarbios ir neskelbtinos informacijos savo įrenginiuose.

2. Šifravimas

Šifravimas yra skaitomos informacijos užšifravimas, kad ją galėtų perskaityti tik tas, kuris turi slaptą kodą arba iššifravimo raktą. Tai būdas paslėpti / užrakinti informaciją, kol nebus įvestas kodas ir informacija vėl paversta skaitomu tekstu. Slaptų duomenų saugumui daugelis naudoja duomenų šifravimą.

Jūs turite galimybę užšifruoti ir įrenginiuose saugomus duomenis, ir siunčiamus duomenis. Yra keli šifravimo metodai. Pavyzdžiui, FDE yra visas disko šifravimas, naudojamas šifruoti visą jūsų sistemos diską. Tai reiškia, kad visa informacija, ne tik dalis, yra paslėpta.

Siunčiamų duomenų apsaugai naudojamas HTTPS internetinis šifravimas. Tai reiškia, kad informacija yra užšifruota pakeliui iš naršyklės į pagrindinį puslapį. El. Laiškai ir kitos komunikacijos programos taip pat siūlo šifravimo metodus, kuriuos turite nustatyti patys. Sėkmingo šifravimo raktas yra tai, kad jūsų raktas / slaptažodis būtų saugus ir būtų labai sudėtingas - kiek įmanoma ilgesnis ir kitaip saugus. Galite naudoti slaptažodžių tvarkytuvę slaptažodžiams atsiminti.

Šifravimas gali veikti, jei jūsų įrenginys yra saugus. Svarbiausia yra įsitikinti, kad įrenginys nėra bekompromisis, jame nėra virusų ar jis nėra pažeistas jokiu kitu būdu. Reguliariai įsitikinkite, kad prietaisas nepasiekiamas nepageidaujamiems asmenims. Atminkite, kad jei norima naudoti programa / programa nesiūlo šifravimo, tada apsvarstykite kitas galimybes. Svarbu naudoti saugias programas / programinę įrangą, kuri jums nekelia pavojaus.

3. PIN kodas/ piešinys

PIN kodas yra specialus apsaugos mechanizmas, kuris naudojamas norint patvirtinti jūsų banko sąskaitą, įrenginį ar bet kokią neskelbtiną informaciją. PIN kodas niekam neturi būti atskleistas. Rekomenduojama jį pakeisti taip pat, kaip keičiant slaptažodį. Turite atsiminti savo PIN kodą. Norėdami apsisaugoti, nemokėkite iš viešų kompiuterių ar iš nepažįstamų įrenginių. Yra programų, kurios gali skaityti viską, ką vartotojas įveda naudodamas klaviatūrą, įskaitant PIN kodus. Todėl PIN kodą naudokite tik asmeniniuose įrenginiuose. Taip pat galimi piešimo tipo PIN kodai, todėl būkite atsargūs, nes žmonės linkę juos kurti per daug paprastai, standartiškai, o įrenginio ekraną reikia reguliariai valyti, kad jo nebūtų galima atsekti tempiant linijas. Įvedant kaištį ar piešinį, patartina, kai rašote, viena ranka uždengti kita ranka ir įsitikinti, kad įrenginio ekranas nėra per šviesus ir aiškiai matomas kitais kampais.

4. Piršto antspaudas

Piršto atspaudo jutiklis galimas keliems įrenginiams. Tai biometrinis prietaisas, padedantis greitai atpažinti asmenį. Jį galima nustatyti beveik visuose išmaniuosiuose įrenginiuose, turinčiuose įmontuotą pirštų atspaudų jutiklį. Pirštų atspaudai gali būti ne tokie saugūs kaip sudėtingas PIN kodas, derinys ar slaptažodis. Yra keletas būdų, kaip fiziškai pašalinti pirštų atspaudus iš savo įrenginio. Atminkite, kad pirštų atspaudus galite pašalinti ir iš kitų kasdienių dalykų. Jei jūsų įrenginys nėra saugus, pirštų atspaudus galima skaityti kaip bet kokią informaciją iš jūsų prietaiso.

Pirštų atspaudų autentifikavimui naudojamas dviejų faktorių autorizacijos procesas. Tai reiškia, kad paprastai naudojamas ir PIN kodas. Jei prietaisai

negali atpažinti / nuskaityti pirštų atspaudų, naudojamas PIN kodas. Taip pat po atnaujinimų ar įjungimo PIN kodas naudojamas saugumo tikslais.

Jei pasirinksite naudoti pirštų atspaudus kaip būdą atrakinti įrenginį, eikite į įrenginio nustatymus ir atlikite atitinkamus veiksmus. Pirmasis nustatymas yra labai svarbus - jūsų pirštai yra nuskaityti. Patartina laikyti telefoną natūralioje padėtyje ir įsitikinti, kad atlikote visus reikalingus veiksmus.

Jį naudojant gali kilti problemų, jei jutiklis yra pažeistas, nešvarus arba nebuvo atliktas reikiamas prietaiso atnaujinimas. Kelios įmonės nori pakeisti savo pirštų atspaudus veido atpažinimo įrankiu.

5. Veido atpažinimas

Veido atpažinimas yra atpažinimo rūšis, kuriai reikalinga kamera. Tai yra galimybė atrakinti įrenginį arba prisijungti prie konkrečių programų, rodant veidą kameroje. Daugelį metų dirbtinio intelekto srityje dirbantys ekspertai pripažįsta, kad veido atpažinimas yra vienas saugiausių būdų prisijungti prie sistemos.

Norėdami nustatyti veido atpažinimą, jums reikia tinkamo prietaiso, fotoaparato ir veido sąrankos - turėsite nuskaityti veidą iš visų pusių, kad jį atpažintų jūsų prietaisas.

Daugeliu atvejų pigaus telefono veido atpažinimo sistemoje naudojama tik į priekį nukreipta kamera ir keletas ne tokių sudėtingų algoritmų - o gal net blykstė, kad būtų galima geriau nufotografuoti. Tačiau įprasta 2D kamera be infraraudonųjų spindulių jutiklio ir taškinis projektorius gali būti lengvai apgauta parodžius nuotrauką.

Jei pasirenkate veido atpažinimą kaip saugos mechanizmą, rekomenduojama naudoti aukštos kokybės prietaisą. Įsitikinkite, kad jis veikia. Ekspertai vis dar tobulina šią sistemą. Jie pripažįsta, kad veido atpažinimas ateityje bus

naudojamas norint patekti į konkrečias svetaines, parduotuvių prekes ir atlikti kitą veiklą.

6.Telefono suradimas

Programos yra skirtos rasti ir valdyti telefoną bet kuriuo metu. Ši funkcija naudojama, jei jūsų telefonas pamestas ar pavogtas. Galite rasti, ištrinti duomenis, peržiūrėti akumuliatoriaus įkrovą ir prisijungti prie „Wi-Fi“ tinklo. Nors atkreipkite dėmesį, kad funkcijos gali skirtis priklausomai nuo operacinės sistemos. Yra tiek integruotos programos, kurios padeda sekti telefono veiklą, tiek yra, kurias galima atsisiųsti atskirai ir įsigyti.

Norėdami naudoti šią funkciją, turite ją įjungti (savo įrenginyje) ir ištirti įrenginio galimybes. Jei norite sužinoti daugiau apie savo įrenginį, naudokite paiešką internete arba pasitarkite su asmeniu, kuris gali jums padėti tai padaryti.

Google“ taip pat yra paslauga, leidžianti nuotoliniu būdu užrakinti, skambinti, atsijungti ir dar daugiau. Jūsų įrenginį galima rasti internetu. Praktika rodo, kad ši funkcija daugiausia naudojama įrenginiui užrakinti ir atsijungti nuo tam tikrų profilių, tačiau ne visada įmanoma fiziškai rasti įrenginį. Yra keletas programų, kurios apmokestina šią funkciją. „Apple“ programa vadinasi „Rasti mano iPhone“, „Microsoft“ programa yra „Mano Windows telefonas“, o „Google“ siūlo „Rasti mano įrenginį“. Tai tik keletas iš daugelio programų.

7.Saugus mobiliųjų programų naudojimas

Svarbu gauti programas mobiliesiems iš saugaus ir patikimo šaltinio. Nusikaltėliai išmoko kurti ir platinti užkrėstas programas mobiliesiems, kurios atrodo kaip tikros. Įdiegę tokią užkrėstą programą, nusikaltėliai gali valdyti jūsų įrenginį.

Apple įrenginiams atsisiųsite tik iPad ir iPhone programas iš Apple App Store. Šioje parduotuvėje Apple atliko saugos patikrinimus visose mobiliosiose programose prieš jų išleidimą. Apple negali „sugauti“ visų užkrėstų programų, tačiau tokia valdoma aplinka dramatiškai sumažina infekcijos riziką. Jei Apple aptinka užkrėstą programą savo parduotuvėje, ji bus nedelsiant pašalinta iš parduotuvės. „Windows Phone“ laikosi panašaus požiūrio į programų valdymą.

Android suteikia jums galimybę atsisiųsti programą iš bet kurios interneto vietos. Diegdami programas turite būti atsargesni, nes ne visos yra išbandytos. Google palaiko programų parduotuvę - Google Play ir jos programose yra bent pagrindinis saugos patikrinimas. Rekomenduojama naudoti programas tik iš Google Play. Venkite programų iš kitų svetainių, nes gana lengva platinti kenksmingas programas, užkrečiančias jūsų mobilųjį įrenginį. Norėdami gauti daugiau apsaugos, įdiekite antivirusinę programinę įrangą į savo mobilųjį įrenginį.

Leidimai. Įdiegę programą iš patikimo šaltinio, sukonfigūruokite ją pagal savo privatumo nuostatas ir poreikius. Prieš suteikdami leidimą programai, visada pagalvokite - ar norite suteikti jai leidimą ir ar tikrai jums to reikia? Jei leisite programai visada žinoti savo buvimo vietą, galite įgalinti programos kūrėją stebėti jūsų judėjimą ar net parduoti šią informaciją kitiems.

Atnaujinimai. Programos mobiliesiems turi būti reguliariai atnaujinamos. Nusikaltėliai visada ieško programų pažeidžiamumų. Dauguma įrenginių leidžia automatiškai atnaujinti programas. Jei tai neįmanoma, patikrinkite, ar nėra programų atnaujinimų bent kartą per dvi savaites. Galiausiai, kai programa bus atnaujinta, visada peržiūrėkite, kokie pakeitimai daromi programos leidimuose.

8.Užrakinimas, Valymas

Prietaiso užrakinimas yra labai paprastas būdas apsisaugoti nuo pažeidimų ar informacijos atskleidimo. Be to, fiziškai prijungus įrenginį prie darbo stalo, darbo vieta yra linkusi atgrasyti vagis nuo prietaiso įsigijimo. Jį atrakinti gali tik specialus raktas.

Yra įvairių būdų, kurie apsaugo mūsų įrenginį ne tik fiziškai. Vartotojas neturi palikti savo darbo vietos nesaugioje darbo vietoje: laikinai nebūdamas - užrakinti kompiuterį; (**Windows + L**), ilgiau išjungtas - atsijunkite arba išjunkite. Telefonuose ir planšetiniuose kompiuteriuose galite nustatyti, kad įrenginys automatiškai užsiblokuotų po tam tikro sekundžių skaičiaus. Daugelyje įrenginių yra vienas lengvai prieinamas išjungimo mygtukas, palengvinantis procesą.

Neišjungę savo įrenginio, kiti žmonės gali trikdyti jūsų įrenginį. Kai baigsite darbą, saugiau visiškai išjungti įrenginį. Praradę interneto ryšį, įsilaužėliai gali pasiekti įrenginį. Įrenginio įjungimas visada padidina riziką.

Valymas yra veiksmas, dėl kurio standžiojo disko informacija tampa neįskaitoma. Tai reiškia, kad duomenys yra tokie, kokie ištrinti, tačiau juos atkurti galima naudojant tinkamą programą. Kai keičiate įrenginį, standųjį diską, patartina jį kuo daugiau valyti. Tačiau saugiausias būdas yra fiziškai sunaikinti standųjį diską ir įsitikinti, kad failai nėra atkurti.

9.Virusai ir antivirusas

Kibernetinis nusikalstamumas tampa įvaldomas įdiegiant kenkėjiškas programas kompiuteriuose ar įrenginiuose. Tai leidžia nusikaltėliui stebėti jūsų veiklą internete, pavogti slaptažodžius ar failus ir naudoti jūsų sistemą kitiems užpulti.

Kenkėjiška programinė įranga iš esmės yra kompiuterio programinė įranga, naudojama neteisėtiems tikslams. Šis terminas kilęs iš žodžio „programinė įranga“ ir „kenkėjiška“ derinio. Kibernetiniai nusikaltėliai diegia kenkėjiškas programas kompiuteriuose ar įrenginiuose, kad galėtų juos valdyti. Įdiegę kenkėjišką programinę įrangą nusikaltėlis gali stebėti jūsų veiklą internete,

pavogti slaptažodžius ar failus ir naudoti jūsų sistemą, kad užpultų kitus. Kenkėjiška programa gali užkrėsti bet kurį įrenginį, pradedant „Apple“ kompiuteriais ir baigiant apsaugos kameromis.

Šifravimo virusai yra ypatinga kenkėjiškų programų rūšis, kuri dabar aktyviai plinta internete ir kelia grėsmę aukų dokumentams ir kitiems failams.

Apsaugokite save - sustabdykite kenkėjiškas programas!

Deja, antivirusinės programos negali sustabdyti visos kenksmingos programinės įrangos. Kibernetiniai nusikaltėliai nuolat kuria naują ir modernią programinę įrangą, galinčią išvengti antivirusų. Žinoma, antivirusinių programų kūrėjai taip pat nuolat tobulina savo sprendimus. Kibernetiniai nusikaltėliai išnaudoja jūsų programinės įrangos spragas. Kuo naujesnė / dabartinė programinės įrangos versija, tuo mažesnis jos pažeidžiamumas. Todėl rekomenduojama:

- Atnaujinkite operacines sistemas, programas, naršykles, plėtinius ir kitas programas. Paprasčiausias sprendimas paprastai yra įdiegti automatinius atnaujinimus.

Įprastas būdas, kai kibernetiniai nusikaltėliai užkrečia kompiuterius ir mobiliuosius įrenginius, yra kuriant suklastotą programinę įrangą ar mobiliąsias programas, pateikiant jas internete ir apgaudinėjant žmones savanoriškai jas įdiegiant.

- Atsisiųskite ir įdiekite programas tik iš patikimų internetinių parduotuvių, o studijų programų apžvalgas - venkite tų, kurios mažai naudojamos ar turi tik keletą teigiamų atsiliepimų.
- Ištrinkite programą, kurios jums nebereikia.
- Kibernetiniai nusikaltėliai dažnai manipuliuoja žmonėmis norėdami nustatyti savo kenkėjiškas programas, pavyzdžiui, jie gali atsiųsti jums el. laišką, kuriame yra priedas arba nuoroda tekste, ir gali atrodyti, kad tai atėjo iš jūsų draugo ar jūsų banko. Deja, kai spustelite nuorodą arba atsisiunčiate priedą, jūsų sistemoje yra įdiegta kenkėjiška programa.

- Reguliariai sukurkite atsarginės savo sistemų ir failų kopijas debesyje arba neprisijungę, pavyzdžiui, išoriniame standžiajame diske.

10.Licecijuotos ir Nelicencijuotos Programos

Jei programa turi kainą, ją reikia nusipirkti ir atsisiųsti legaliai. Taip pat turite atkreipti dėmesį į tai, kur atsisiunčiate savo programas. Nedarykite to įtartinose svetainėse - tai gali sukelti pavojų jūsų įrenginiui ir kitai jūsų kompiuterio programinei įrangai. Kompiuterių vartotojai turi atsižvelgti į autorių teisių įstatymus, kurie taikomi knygoms, vaizdo ir muzikos diskams ir kasetėms bei programinei įrangai. Kopijavimas, platinimas ar naudojimasis kompiuterių programomis be autorių teisių savininko leidimo yra vadinamas piratavimu.

Pavyzdžiui, neteisėtas kompiuterių programų naudojimas :

- Įdiegtas vienas legaliai įsigytas programinės įrangos kompaktinis diskas keliuose kompiuteriuose, jei licencija ar sutartis nurodo, kad jis gali būti įdiegtas tik viename kompiuteryje;
- nukopijuotae diegimo ir platinimo programa be autoriaus leidimo;
- programinės įrangos diegimas iš neteisėtai įsigyto disko;
- Neteisėtų kompiuterių programų kopijų atsisiuntimas iš interneto.

Siūloma nemokamai atsisiųsti programinę įrangą ir kitų tipų failus (tekstus, vaizdus ir kt.) Internetu. Jų leidėjai ne visada turi teises platinti juos naudoti kitiems. Todėl prieš atsisiųsdami turite įsitikinti, kad jums leista kopijuoti.

11. Atsisiuntimas

Atsisiuntimas yra failų saugojimo iš tinklo serverio į saugojimo įrenginį procesas. Atsisiųsti failus reikia, jei vartotojas nori gauti tinklalapyje siūlomus failus, tokius kaip dokumentai, paveikslėliai, muzika, vaizdo įrašai ir programinė įranga.

Norėdami išsaugoti failą ar atvaizdą kompiuteryje ar įrenginyje, atsisiųskite jį. Failas bus išsaugotas numatytoje atsisiuntimo vietoje.

Galite atsisiųsti įvairių tipų failus:

Tipas	**Formatas**	**Pavyzdys**
Tekstas	Docx, txt	Kopsavilkums.docx
Paveikslas	Jpg. Gif, png.	IMG0034.jpg
Audio	Mp3, wma	Voice.mp3
Video	Avi, mpg, mpeg	Ceplis.avi
Programa	Exe	Skype.exe
Archivas	Zip, rar	Arhivs.zip

Failo atsisiuntimo parinktį galima nurodyti skirtingais būdais, tačiau paprastai tai apibūdina nuoroda arba mygtukas Atsisiųsti.

12.Naršyklės

Naršyklė yra programa tinklalapiams peržiūrėti. Norėdami peržiūrėti tinklalapį, jis pirmiausia atsisiunčiamas arba perduodamas iš visuotinio žiniatinklio serverio į vartotojo kompiuterį, prieš jį atidarant.

Norint naudotis interneto paslaugomis, jums reikalingi:

- programuojamas įrenginys su tinklo ryšio galimybe;
- interneto paslaugų teikėjas (IPT), užtikrinantis, kad įrenginį būtų galima prijungti prie interneto (gali prireikti papildomos aparatūros);
- Interneto naršyklė.

Keletas naršyklių pavyzdžių:

Atidaryti bet kurį puslapį nėra saugu, nes yra rizika, kad jame yra virusų, kurie taip pat gali atidaryti apgaulingus puslapius, kurie klastoja informaciją.

Yra ženklų, pagal kuriuos galima manyti, kad internetinis puslapis yra saugus. Adreso juostoje rodomos dvi paprasčiausios funkcijos, nurodančios puslapio saugumą:

- https prieš adresą (nurodo, kad informacija į kompiuterį perduodama užšifruota forma);
- Paprastai užrakinamas „užrakto“ simbolis (užrakto simbolis gali skirtis įvairiose interneto naršyklėse).

Puslapio atsisiuntimas sustabdomas, jei:

- atsisiuntimas atidėtas;
- atsisiuntimo metu nustato, kad trūksta puslapio reikalingos informacijos.

Puslapis turi būti atnaujintas, jei:

- Puslapis neįkeltas. Pvz., Kai kurių vaizdų puslapyje yra kvadratų su raudonais kryžiais arba nėra visos informacijos;
- Vartotojas kurį laiką nežiūrėjo puslapio ir per tą laiką pasikeitė puslapio informacija (puslapis neatnaujinamas automatiškai).

13. Duomenų kopijos

Svarbu saugoti duomenis ne tik kompiuteryje, bet ir kitoje vietoje. Tokiu atveju visada įmanoma atkurti svarbius duomenis, jei kyla kokių nors problemų su kompiuteriu.

Duomenys, paprastai saugomi kompiuteryje:

- nuotraukos;
- darbo dokumentai;
- svarbios programos, programinė įranga;
- vaizdo, garso projektai;
- el.-pašto archyvas ir draugų laiškai.

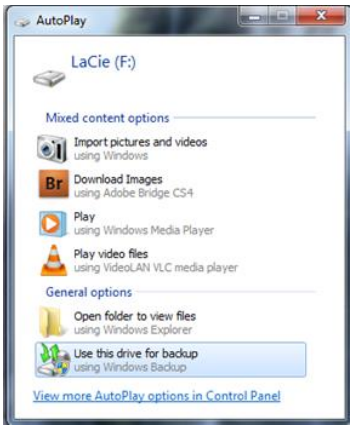
Jei manote, kad jums nereikia duomenų kopijų, atminkite, kad yra daug būdų, kaip galite pamesti svarbius dokumentus.

- Paprasčiausias būdas prarasti visus duomenis yra pamesti kompiuterį arba, jei jis pavogtas (tai daugiau taikoma nešiojamiesiems kompiuteriams).
- Yra galimybė netyčia ištrinti duomenis ar nukopijuoti juos į svarbius dokumentus.
- Jūsų kompiuteris gali būti užkrėstas, o kenkėjiška programa gali sugadinti tam tikrus duomenis ar net sugadinti kietąjį diską.
- Gali būti tam tikrų techninių problemų (įskaitant standžiojo disko sugadinimą - nieko nėra amžino), dėl kurio gali būti prarasti kai kurie duomenys.

Duomenų kopijavimas.

Į Windows kompiuterį:

- **Įsigykite išorinį saugojimo įrenginį**. Tai gali būti bet koks USB atmintinis arba išorinis standusis diskas. Pageidautina įsigyti įrenginį, kuriame yra bent dvigubai daugiau vietos nei jūsų kompiuterio atmintyje.
- Kai pirmą kartą prijungiate išorinį atminties įrenginį prie savo kompiuterio, jis siūlo galimybę jį naudoti kaip duomenų saugojimo vietą. Jei ši parinktis nerodoma, tiesiog įveskite programos pavadinimą paieškos lange „Atsarginė kopija“.



- Atsidarys šis langas, kuriame turėsite spustelėti „Nustatyti atsarginę kopiją“. Tada turėsite pasirinkti, kuriame išoriniame diske norite sukurti atsarginę duomenų kopiją. Galų gale turėsite spustelėti „Išsaugoti nustatymus ir vykdyti atsarginę kopiją“.
- Atlikę šiuos veiksmus, „Windows“ padarys pirmą jūsų duomenų atsarginę kopiją (svarbiausia yra neišimti išorinio saugojimo disko!). Žemiau galite pasirinkti „Keisti tvarkaraštį“ ir pasirodys šis vaizdas. Paveikslėlyje parodyta, kad jums suteikiama galimybė pasirinkti tvarkaraštį, kada duomenų kopijos bus atkurtos. Jums siūloma galimybė tai padaryti kartą per dieną, savaitę ir mėnesį. Svarbiausia atsiminti, kad įrenginys, kurio atsarginę kopiją sukuriate, turi būti prijungtas prie kompiuterio pasirinktu laiku ir dieną.

Duomenų kopijavimas į „Mac OS“ kompiuterį.

Tai beveik tas pats, kas naudojant „Windows“ kompiuterį. Įdėję išorinį saugojimo diską, galėsite naudoti jį kaip atsarginę vietą. Jūs turite jį pasirinkti arba eiti per Sistemos nuostatos -> Laiko mašina. Tada pasirinkite reikiamą išorinio saugojimo diską ir pasidarykite jame esančių duomenų kopiją.

Duomenų kopijavimas mobiliajame telefone.

Labai patogus kontaktų ir kalendoriaus atsarginių kopijų kūrimo būdas yra „Google“ paskyra („Gmail“ el. Paštas). Paskyros ir sinchronizavimo nustatymais galite bet kada įjungti atsarginės kopijos funkciją. „Google“ paskyra turėtų būti rodoma šalia jūsų paskyrų, jei ją pasiekėte iš savo telefono. Tokio adresatų

kopijavimo pranašumas yra tas, kad keičiant telefonus duomenys bus automatiškai nukopijuoti į naują įrenginį. Internete galite peržiūrėti informaciją apie savo kontaktus kairėje, spustelėdami „Gmail“. Be „Google“ teikiamų galimybių, yra ir kitų tipų programinės įrangos, siūlančios atsargines kopijas. Viena galimybė yra paprasčiausiai nukopijuoti svarbius duomenis prijungiant telefoną prie kompiuterio. Taip pat internete galite rasti atskirų programų, kurios teikia atsargines kopijas. Jei ieškote sau tinkančio, svarbu įsitikinti, kad jis tinka jūsų kompiuterio operacinei sistemai.

Duomenų kopijavimas internete.

Paprastai ši paslauga teikiama nemokamai, turint ribotos atminties (maždaug 5–7 GB). Naudodamiesi šia paslauga galite saugoti savo svarbiausius duomenis internete, tai reiškia, kad galite prieiti prie bet kurios vietos ir iš savo kompiuterio. Paslaugų teikėjas užtikrina, kad šie duomenys būtų saugomi užšifruota forma. Tokių paslaugų teikėjų pavyzdžiai yra www.mimedia.com ir www.backup.comodo.com Žinoma, šio tipo duomenų saugojimas yra patogus prieigos požiūriu, tačiau neatmetamos įvairios saugumo problemos.

Jei prarandate duomenis, juos nesunku atkurti iš atsarginės kopijos. „Windows“ sistemoje įveskite meniu „Pradėti meniu“ atsarginę kopiją ir spustelėkite „Atkurti mano failus“. „Mac“ kompiuteriuose paspauskite „Time Machine“, tada „Enter Time Machine“. Arba tiesiog pasiimkite savo išorinį saugojimo įrenginį, kur sukūrėte atsarginių duomenų kopijas, prijunkite jį prie savo kompiuterio ir nukopijuokite reikalingus failus.

Duomenų kopijų darymo pranašumai.

- **Moralinė nauda** - nereikia jaudintis dėl nieko, kas nutiktų jūsų kompiuteriui; galite būti tikri, kad svarbūs duomenys niekur nebus prarasti!
- **Finansinė nauda** - jei kyla problemų dėl kietojo disko, atkurti šiuos duomenis specialistui gali būti brangu. Jei turite svarbių duomenų atsarginę kopiją, tokių paslaugų jums nereikės.

14. Įsišaknijęs įrenginys

Šaknų įsišaknijimas yra procesas, leidžiantis išmaniųjų telefonų, planšetinių kompiuterių ir kitų įrenginių, kuriuose veikia „Android“ mobiliosios operacinės sistemos, vartotojams įgyti privilegijuotą valdymą (žinomą kaip šakninė prieiga) įvairiuose „Android“ posistemiuose. Šio proceso tikslas yra įveikti apribojimus, kuriuos gamintojai taiko tam tikriems įrenginiams. Taigi įsišaknijimas leidžia jums pakeisti arba pakeisti sistemos programas ir parametrus, paleisti specializuotas programas, kurioms reikia administratoriaus lygio leidimų, arba atlikti kitus veiksmus, kurie nėra prieinami kitam įprastam „Android“ vartotojui. Naudojant „Android“, įsišaknijimas taip pat gali padėti visiškai pašalinti ir pakeisti įrenginio operacinę sistemą, paprastai naujesne dabartinės operacinės sistemos versija.

Santrauka

Mokydamiesi modulio temų, besimokantieji žino, kaip užtikrinti fizinę prietaisų apsaugą, taip pat supranta šifravimo principus. Besimokantieji gali atpažinti ir naudoti skaitmeninių prietaisų apsaugos būdus - veido atpažinimą, slaptažodžio įvedimą, figūros piešimą skaitmeninio įrenginio ekrane ir pirštų atspaudus.

Naudojant aprašytus būdus modulyje, galima rasti pamestą telefoną. Besimokantieji yra informuojami apie įvairius virusams pavojingus prietaisus ir galimybes jų išvengti. Norėdami išlaikyti įrenginių saugumą, vartotojai taip pat turėtų atkreipti dėmesį į atsisiuntimus ir naudoti tik teisėtas ir licencijuotas programas. Pateikę informaciją mokiniai gali įsisavinti antivirusinių programų ir programų naudojimo principus, papasakoti skirtumus tarp interneto naršyklių ir jų naudojimo.

Galiausiai besimokantieji supranta, kaip sukurti atsarginę informacijos kopiją savo skaitmeniniame įrenginyje, taip pat supranta įsišaknijusio įrenginio paskirtį.

Bibliografija

- Pieslēdzies, Latvija! (n.d.). *Esiet sveicināti datorskolā! Mācies pats*. [Online Course]. 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.). [e-learning environment]. 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