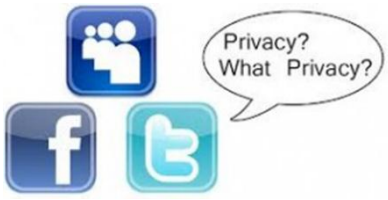
Project IDCAP: Improve Digital Competence in Adult People

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

Kaip apsaugoti mano asmeninius duomenis?

Kompetencijos sritis: Asmens duomenų ir privatumo apsauga



Įvadas

Modulis apima pagrindines temas asmens duomenų ir privatumo apsaugos srityse. Modulio tikslai:

- aptarti saugumo principus skaitmeninėje aplinkoje ir informuoti apie galimas grėsmes - informacijos vagystė, netikri el.laiškai ir kita;
- pristatyti pagrindinius technologijos naudojimo saugumo principus - kokių taisyklių reikia laikytis naudojantis internetu viešai prieinamuose „Wi-Fi“ tinkluose, kas yra saugus ryšys ir kas yra nesaugūs el.pašto priedai?
- paaiškinti saugių slaptažodžių naudojimą - kokiais principais turėtumėte vadovautis kurdami slaptažodžius? Kaip saugiai naudoti slaptažodžius kasdieniame gyvenime?

1.Įvadas į saugą skaitmeninėje aplinkoje

1.1.Kompiuterių saugumas

Kompiuterio saugumas reiškia, kad mūsų kompiuteris yra apsaugotas nuo neteisėtos prieigos, naudojimo, atskleidimo, trikdžių, pakeitimo ar sunaikinimo. Rūpintis savo informacija ir kompiuterio saugumu yra įmanoma ir būtina. Kompiuteryje saugoma ir internete skelbiama informacija gali turėti įtakos asmens gerovei, sveikatai ir netgi gyvybei. Yra daugybė grėsmių - grėsmės privatumui, slaptažodžių nulaužimas ar įsilaužimas, asmeninės informacijos atskleidimas, virusai, kenksmingų failų įkėlimas, atsisiuntimas ir siuntimas, kenksmingi žmonės.

Internete turime prieigą prie socialinių tinklų, internetinių pokalbių, forumų, specialių pokalbių programų (pvz., „Skype“), žaidimų ir dar daugiau. Jei nesilaikoma būtinų saugumo standartų, blogus ketinimus turintys žmonės gali ne tik sužinoti apie jūsų asmeninius duomenis, bet ir naudoti jūsų tapatybę (apsimesti jumis).

Kompiuteriniai virusai tapo „klasikine vertybe“. Taikomi įvairūs metodai, pavyzdžiui, vartotojas gauna el.laišką su nuoroda į populiarų tinklalapį, pavyzdžiui, Youtube ar Facebook, su viliojančiu filmu ar vaizdu. Bandydami jį užkrėsti vartotojo kompiuterį, kuriame nėra gynybos, vos vienu pelės paspaudimu.

El.pašto priedai yra ypač pavojingi, nes juose gali būti virusų ir kitos kenksmingos programinės įrangos. Atidarę el. Laiško priedą, kompiuteryje galite automatiškai įdiegti kenkėjiškas programas ir to net nepastebėsite. Tokia kenkėjiška programa gali paveikti kompiuterio failus, pavogti slaptažodžius ar šnipinėti jus, todėl turėtumėte būti ypač atsargūs, gaudami pranešimus su priedais iš nežinomų gavėjų.

Patarimai, kaip tvarkyti nepageidaujamus el.pašto priedus:

Patarimas	Paaiškinimas
Niekada neatidarykite įtartinų el. pašto priedų	Net jei gavote el.laišką iš pažįstamo asmens, nėra garantijos, kad asmuo iš tikrųjų jį išsiuntė. Kenkėjiška programa gali automatiškai siųsti jums pranešimus, kuriuose yra virusų. Gavus el.laišką su priedu, geriausia paprašyti paties siuntėjo, kad jis įsitikintų, jog išsiuntė el.laišką.
Atnaujinkite antivirusinę programą	Jei antivirusinė programa nėra atnaujinta, ji negali apsaugoti jūsų kompiuterio nuo virusų.
Palikite įjungtą kompiuterio užkardą	Kompiuterio užkarda neleidžia žmonėms ar kenkėjiškoms programoms prieiti prie jūsų kompiuterio per internetą.
Jei įmanoma, prieš atsisiųsdami el. pašto priedus patikrinkite, ar nėra virusų	Daugelis internetinių el.pašto paslaugų teikėjų prieš atsisiųsdami automatiškai patikrina priedus. Jei jūsų kompiuteris ragina atsisiųsti priedus patikrinti, ar nėra virusų, tai padarykite patys.

1.2.Duomenų saugumas – sukčiavimas

Sukčiavimas yra elektroninių nusikaltimų rūšis, apimanti socialinės inžinerijos ir techninių priemonių rinkinį, siekiant iš aukos pavogti neskelbtiną, asmeninę ir

finansinę informaciją. Užpuolikas bando apsimesti tikra organizacija, patikima institucija ar žinomu asmeniu.

Sukčiavimo aukos raginamos spustelėti el.laiškus šiomis temomis:

- ✓ Oficialus pranešimas apie duomenų nutekėjimą
- ✓ UPS pristatymo pranešimas 1ZBE312TYI00015011B23
- ✓ IT priminimas: slaptažodžio galiojimas pasibaigs per mažiau nei 24 val.
- ✓ Jūs turite nedelsdami pakeisti slaptažodį
- ✓ Perskaitykite svarbų administratoriaus pranešimą

Kaip atpažinti sukčiavimą:

Per gerai, kad būtų tiesa. Tai yra žinutės, laiškai, skambučiai, informuojantys, kad laimėjote loteriją ar atsitiktinai buvote pasirinktas gauti prizą ar paslaugą.

Greitas pasiūlymas. Frazės: „paskutinis šansas“, „tik 1 valanda“, „tik šiandien“ ir pan. Nurodo sukčiavimo atvejį. Sukčiai naudojasi manipuliacijomis, kurios sukuria skubos jausmą. Gaunant tokio tipo pranešimus, patariama pasitikrinti informacijos teisingumą tiesiogiai su įmone ar paslaugų teikėju.

Paslėptos nuorodos su kitais raktiniais žodžiais. Daugelis sukčių naudoja paprastus raktinius žodžius, frazes, kurios nuves jus į apgaulingą svetainę. Šios nuorodos dažnai slepia visiškai kitokią svetainę, nei jūs manote. Labai geras būdas įsitikinti, ką atidarote, yra paspausti dešinę pelės mygtuką ir pasirinkti parinktį Apžiūrėti. Pažiūrėkite, kokia nuoroda yra susieta su ta nuoroda ar raktiniu žodžiu. Ką jis slepia? Būkite atsargūs, nes rašybos netikslumai dažnai slepia netikras nuorodas.

Keisti priedai. Jei nesitikite jokios konkrečios informacijos, neturėtumėte žiūrėti į el.pašto priedus. Vienas iš elektroninių nusikaltimų būdų yra failo, kuriame gali būti kenkėjiškų programų, pridėjimas prie nekaltos žinutės. Patartina prieš atidarant patikrinti siuntėją, žinutės tikslą. Vienintelis saugus formatas, kurį gali atidaryti .txt failas.

Kaip išvengti sukčiavimo:

Patarimas	Paaiškinimas
Būkite budrūs	Visada atsargiai skaitykite draugų ir nepažįstamų žmonių el.laiškus.
Būkite atsargūs dėl įvairių komunikacijos kanalų	Atkreipkite dėmesį į įvairius bendravimo tipus - el. laiškus, skelbimus, telefono skambučius ir kitas komunikacijos rūšis, kuriose prašoma bet kokios finansinės informacijos.
Spustelėkite atsargiai	Venkite spustelėti „įgalinti turinį“, kuris leidžia įgalinti papildomą susiejimą tarp skirtingų dokumentų.
Nespustelėkite įtartinų nuorodų	Venkite spustelėti saitus el.laiškuose, pranešimų siuntimo programose ar skelbimuose. Naršykite nuorodas atskirai, naudodamiesi visais turimais ištekliais.
Patikrinkite siuntėjo patikimumą	Įsitikinkite, kad el.laiškas yra iš patikimo šaltinio.

Jei esate sukčiavimo auka:

1) Pakeiskite programų ir internetinių paskyrų slaptažodžius naudodami kitą telefoną ar kompiuterį.
2) Patikrinkite, ar kompiuteryje nėra virusų ir nėra kenksmingos programinės įrangos.
3) Pranešti policijai apie duomenų vagystę ir saugoti prašymo kopiją.
4) Praneškite savo organizacijai / bankui arba kompetentingai institucijai.

1.3.Kompiuterių vartotojų sauga – Informacija, paskelbta socialiniuose tinkluose

Yra du būdai, kaip pažvelgti į kompiuterio vartotojo saugumo sąvoką. Galima kalbėti apie kompiuterio potencialą kelti pavojų jo vartotojo sveikatai, pavyzdžiui, apie elektros smūgio galimybę, net ir nedidelį. Vis dėlto labiausiai paplitusi rizika asmeniui yra rizika, kad bus skelbiama pati informacija.

Dažnai trūksta supratimo, kiek įvairių grėsmių kelia socialiniai tinklai.

Socialiniai tinklai yra svarbi šių dienų kasdienio gyvenimo dalis - jie yra naudojami :

- Bendrauti;
- Gauti informacijos;
- Skelbti ir dalintis informacija, t.t.

Yra du socialinių tinklų grėsmių tipai: **technologinės ir organizacinės grėsmės**.

Technologinės grėsmės yra susijusios su įvairiomis technologijomis ir jų naudojimu socialiniuose tinkluose. **Organizacinės grėsmės** yra susijusios su interneto vartotojo elgesiu, paties vartotojo veiksmais ir veikla. Organizacinę grėsmės ataką dažniausiai sukelia kažkas kitas socialiniame tinkle.

Dažniausios grėsmės socialiniuose tinklose yra:

- ✓ įvairių tipų kenkėjiškos programos ar virusai;
- ✓ sukčiavimo išpuoliai - sukčiavimo laiškai arba el.laiškai su nuorodomis į svetaines, kurios užkrėstos kenkėjiškomis programomis;
- ✓ šlamšto siuntimas;
- ✓ paslėpti paspaudimai, dėl kurių vartotojas gali spustelėti ką nors kitą, nei vartotojas iš pradžių ketino;

- ✓ Įvairių tipų suklastoti profiliai - kai kurie iš jų yra pusiau automatiniai arba visiškai automatizuoti, o kiti - žmogaus sukurtį;
- ✓ Išvadų išpuoliai yra duomenų ir informacijos gavybos būdai, kai analizuojami turimi duomenys, siekiant gauti papildomos informacijos apie auką. Socialiniuose tinkluose jie naudojami nurodyti ir identifikuoti vartotojo asmeninę ir neskelbtiną informaciją, kurią vartotojas nepasidalino, pavyzdžiui, religinius įsitikinimus ir seksualinę orientaciją. Išpuolis pagrįstas informacija, pasiekiama aukos ir jo draugų profiliuose.
- ✓ elektroninis mobingas - emocinis pažeminimas naudojant šiuolaikines technologijas. Uždarymas, pažeminimas, seksizmas, priekabiavimas, nemalonių nuotraukų siuntimas, tyčiojimasis, melas apie asmens tapatybę norint gauti asmeninę informaciją, prieiga prie kitų žmonių informacijos, sekimas ir kit.

Norint išvengti grėsmių, galima naudoti įvairius socialinių tinklų siūlomus sprendimus:

- autentifikavimo mechanizmus,
- blokuoti vartotojus,
- asmeniniai vartotojų nustatymai,
- parinktis “pranešti vartotojui" .

Išvardyti sprendimai gali būti sėkmingai naudojami siekiant apsaugoti vartotoją nuo suklastotų profilių, emocinės prievartos, naivaus ir rizikingo elgesio.

Įvairios saugos sprendimų kompanijos - AVG, Avira, Kaspersky, Panda, McAfee, Symantec - siūlo interneto saugumo sprendimus socialinių tinklų vartotojams. Jų programinėje įrangoje paprastai yra antivirusinė programa ir užkarda, kartais siūlanti apsaugą nuo šlamšto ir sukčiavimą interneto vartotojams. Tokia programinė įranga padeda socialinio tinklo vartotojams apsaugoti savo asmeninius kompiuterius nuo tokių grėsmių, kaip kenkėjiškos programos, paslėpti paspaudimai ir sukčiavimas.

Saugaus socialinio tinklo patarimai

Tipas	Pavyzdys
Informacijos paskelbimas	Prieš paskelbdami informaciją, gerai pagalvokite. Viskas, ką skelbiate, greičiausiai tam tikru metu taps vieša ir tai gali neigiamai paveikti jūsų reputaciją ir ateitį. Būkite atsargūs - kiti apie jus taip pat gali rašyti. Jums gali tekti paprašyti, kad kažkas ištrintų informaciją, kurią jie paskelbė apie jus.
Privatumas	Praktiškai visuose socialiniuose tinkluose yra papildomų privatumo parinkčių - nustatykite jas visur, kur įmanoma. Pavyzdžiui, ar svetainei iš tikrųjų reikia žinoti jūsų vietą? Reguliariai tikrinkite privatumo parinktis ir įsitikinkite, kad jie veikia taip, kaip jūs manote.
Slaptažodžiai	Apsaugokite savo socialinio tinklo paskyras pakankamai ilgu ir unikaliu slaptažodžiu ar slaptafraze. Slaptažodžio frazė yra slaptažodis, kurį sudaro keli žodžiai, todėl jį lengva atsiminti ir užrašyti, tačiau kibernetiniams nusikaltėliams atspėti yra daug sunkiau.
Sukčiavimas	Kaip ir el. Laiškai, pranešimai socialiniame tinkle gali būti naudojami įvairiems bandymams sukčiauti. Pvz., Kenksmingas asmuo gali bandyti įvesti jūsų slaptažodį ar kredito kortelės informaciją. Būkite atsargūs dėl gaunamų nuorodų.
Kontaktai	Nesikreipkite į nepažįstamus ir įtartinus asmenis. Sukurti netikrus profilius yra labai paprasta, ir daugelis žmonių naudojasi meluodami apie savo tapatybę. Šių profilių tikslas yra apgauti, įgyti jūsų pasitikėjimą ir panaudoti prieš jus.
Naudojimo sąlygos	Susipažinkite su socialinių tinklų terminais - viskas, ką jūs paskelbiate, gali tapti socialinio tinklo ypatybe.
Darbas	Jei norite paskelbti ką nors apie savo darbą, pirmiausia išsiaiškinkite, ar tai priimtina jūsų vadovybei.

Suasmenintas sukčiavimas

Nauja elektroninių nusikaltimų forma - personalizuotas sukčiavimas - tampa vis populiaresnė. Kibernetiniai nusikaltėliai surenka arba perka informaciją apie milijonus žmonių, o paskui naudoja tą informaciją suasmenindami išpuolius. Kuo daugiau žinosite apie tokius išpuolius, tuo lengviau bus juos aptikti ir sustabdyti.

El.pašto ir telefonų sukčiavimai nėra naujiena, kibernetiniai nusikaltėliai metų metus bandė apgauti žmones. Pavyzdžiai: „Jūs laimėjote loteriją“ arba garsioji Nigerijos princo apgaulė. Tačiau vykdant šias tradicines atakas kibernetiniai nusikaltėliai nežino, ką turės veikti. Jie tiesiog sukuria bendrą el.laišką ir išsiunčia jį milijonams žmonių. Kadangi šios apgaulės yra tokios bendros ir vienodos, jas paprastai lengva atpažinti. Individualizuotas sukčiavimas yra skirtingas, pirmiausia tiriami elektroniniai nusikaltimai ir parengiamas kiekvienai aukai tinkamas el.paštas. Jie tai daro rinkdami informaciją arba pirkdami duomenų bazę, kurioje yra žmonių vardai, slaptažodžiai, telefonų numeriai ir kita informacija. Tokia informacija yra lengvai prieinama daugelio nulaužtų svetainių dėka. Ji taip pat dažnai laisvai prieinama socialinių tinklų svetainėse ir viešai prieinamuose valdžios institucijų ištekliuose .

Ataka veikia taip: jie randa arba perka informaciją apie žmonių vardus ir slaptažodžius, gautus iš nulaužtų svetainių, tada tokioje duomenų bazėje randa jūsų el.pašto adresą ir su jumis susijusią informaciją ir siunčia ją jums (kaip ir visiems kitiems šioje duomenų bazėje).) - el.laiškas su informacija apie jus, įskaitant slaptažodį, kurį naudojote nulaužtoje svetainėje. Kibernetiniai nusikaltėliai suteikia jums šį slaptažodį kaip „įrodymą“, kad jūsų kompiuteris ar įrenginys buvo nulaužtas, o tai akivaizdžiai neteisinga. Kibernetiniai nusikaltėliai taip pat tvirtina, kad po įsilaužimo jūs šniukštinėjote pornografinę medžiagą internete. El.laiškas grasina, kad jei nemokėsite išpirkos, jūsų gėdingos internetinės veiklos įrodymai bus išsiųsti jūsų šeimai ir draugams.

Svarbiausia, kad šiuo ir beveik visais tokiais atvejais kibernetiniai nusikaltėliai nebuvo įsilaužę į jūsų įrenginį. Jie net nežino, kas jūs esate ar kokiose svetainėse lankotės. Sukčiai tiesiog bando panaudoti kai kuriuos iš jūsų žinomus dalykus, kad įbaugintų jus ir priverstų jus patikėti, kad jie įsilaužė į jūsų mašiną, ir priversti jus sumokėti. Atminkite, kad jie gali naudoti tas pačias metodikas apgaulingiems telefono skambučiams.

Ką daryti? Pripažinkite, kad tokie el.laiškai ir telefono skambučiai yra apgaulingi. Natūralu, kad bijote, kai kas nors turi jūsų asmeninę informaciją. Bet atminkite, kad siuntėjas meluoja! Puolimas yra automatizuotos masinės kampanijos dalis, o ne bandymas jus užpulti. Šiais laikais nusikaltėliams tampa vis lengviau susirasti ar nusipirkti asmeninės informacijos, todėl ateityje pasiruoškite asmeniškesniems išpuoliams.

Kaip atpažinti išpuolį:

- Visada būkite įtarūs, kai gausite labai skubų el.laišką, pranešimą ar telefono skambutį. Kai kas nors naudoja emocijas, tokias kaip baimė ar skubumas, jie bando jus priversti skubėti.
- Bet kuris asmuo, prašantis mokėjimo „BitCoin“ kriptovaliuta, dovanų kortelėmis ar kitomis neatsekiamomis mokėjimo priemonėmis.
- Jei gaunate įtartiną el.laišką, atlikite „Google“ paiešką ir patikrinkite, ar kas nors nepranešė apie panašų išpuolį.

Visada stenkitės naudoti ilgus unikalius slaptažodžius kiekvienai savo internetinei paskyrai. Negalite atsiminti visų slaptažodžių? Naudokite slaptažodžių tvarkytuvę. Be to, kai įmanoma, naudokite dviejų pakopų autentifikavimą.

1.4.Skaitmeniniai pėdsakai

Skaitmeninis pėdsakas yra informacija, kurią sąmoningai ar nesąmoningai paliekame virtualioje aplinkoje - vaizdinė, garso ir rašytinė informacija. Taip pat yra tam tikros informacijos, kurią sukuria ne patys tėvai, o tėvai, draugai, darbas

ir pan. Šiandien neturėti skaitmeninio pėdsako gali būti neįmanoma, tačiau buvimas per daug aktyvus socialiniuose tinkluose taip pat gali sukelti neigiamų padarinių.

Skaitmeninis pėdsakas pagrįstas jūsų veikla internete: apsipirkimo įpročiais, laikmenomis, įrenginių naudojimu, jūsų pasirinktomis platformomis.

2.Pagrindiniai saugaus technologijų naudojimo principai

2.1.Interneto ryšys

Norėdami, kad kiti žmonės nenaudotų kažkieno autentifikavimo duomenų, tokių kaip vartotojo vardas ir slaptažodis, **turite įsitikinti, kad naršote saugiai!**

Interneto naršyklė kaupia informaciją apie jūsų lankomus tinklalapius vartotojo kietajame diske, kurią galima suskirstyti į tris tipus:

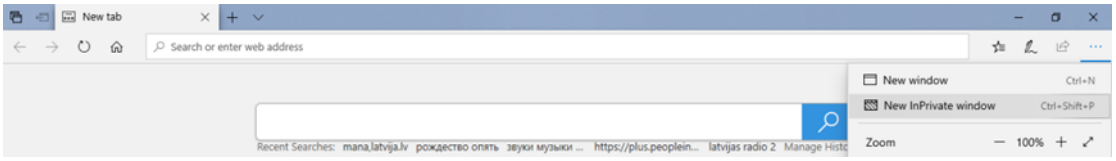
a) Jūsų lankomų puslapių sąrašas arba lankomų puslapių istorija.
b) Informacija, esanti tinklalapiuose, kuri paprastai saugoma vadinamojoje talpykloje. Paprastai tai yra aplankas, vadinamas Temporary Internet Files.
c) Slapukai - maži tekstiniai failai. Šie failai įrašo, slaptažodžius, aplankytų puslapių sąrašus ir datas, kada jie buvo peržiūrėti. Naršyklės perduoda šią informaciją atgal į interneto serverius. Paprastai, kai atidarote svetainę savo naršyklėje, jums suteikiama galimybė sutikti / atsisakyti slapukų naudojimo. Rekomenduojama sutikti su slapukų naudojimu svetainėse, kuriose planuojate grįžti dar kartą.

Kai naudojate viešą kompiuterį, atminkite, kad kiti žmonės galės peržiūrėti klientų aplankytų svetainių naršyklių istoriją, taip pat atsisiųstus failus. Norint išvengti nemalonių situacijų, rekomenduojama išvalyti naršyklės istoriją

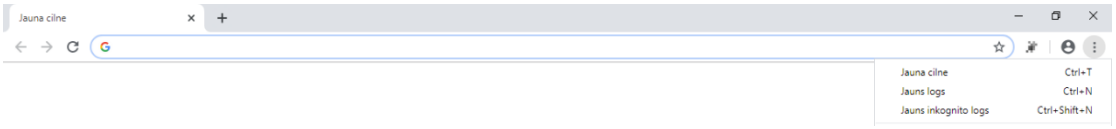
Ctrl + H ir slapukus. Daugelyje naršyklių tai galite padaryti paspausdami klaviatūros klavišus **Ctrl + Shift + Delete**.

Jei nenorite, kad naršyklė įrašytų jūsų veiklos istoriją ir vartotojo vardus bei slaptažodžius, rekomenduojame naudoti asmeninį naršymą. Asmeninis naršymas kiekvienoje naršyklėje gali turėti skirtingą pavadinimą, tačiau jo esmė yra vienoda visose naršyklėse. Žemiau pateiktuose vaizduose yra keletas pavyzdžių, kaip atidaryti privatų naršymo langą.

Microsoft Edge



Google Chrome



Nepamirškite saugoti savo tapatybės, slaptažodžių ir saugos kodų. Šiais duomenimis gali naudotis pašaliniai asmenys.

Naudojant internetą rekomenduojamos šios pagrindinės gairės:

- neduokite savo asmens tapatybės kortelės, PIN kodų ir kitų prieigos duomenų kitiems asmenims;
- Neskelbkite internete ir nesiųskite dokumentų kopijų (paso, asmens tapatybės kortelės, vairuotojo pažymėjimo) el. Paštu, ryšių programomis ar socialiniais tinklais;
- Neperduokite slaptažodžių ir kitos asmeninės informacijos el. Laiškuose ar pranešimuose iš ryšių programų („WhatsApp“, „Viber“, „Messenger“ ir kt.) Ir socialinių tinklų („Facebook“, „Twitter“ ir kt.);
- Neatidarykite priedų, kai gaunate įtartinus el.laiškus;

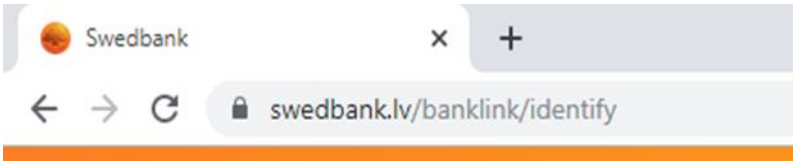
- Per daug nepasakokite kitiems apie savo gyvenimą internete ir socialiniuose tinkluose, ypač apie savo finansinę padėtį, naujus dalykus, palikimą namuose ir pan .;
- Gerai pagalvokite, kokias nuotraukas skelbti internete ir kaip jų paskelbimas vieną dieną gali paveikti žmogaus gyvenimą, pvz., santykius su draugais, giminaičiais, kolegomis, dabartiniais ar būsimaisiais darbdaviais;
- Gavę el.laišką iš valdžios institucijos ar banko, kuriame prašoma atsiųsti savo asmens duomenis institucijai, niekada neturėtumėte to daryti, nes institucija niekada neprašys duomenų el.laiško forma;
- Prisijungdami prie el.paslaugų įsitikinkite, kad kiti žmonės nemato jūsų įvestų prieigos duomenų ir informacijos, gautos naudojantis el.paslauga;
- Įsitikinkite, kad kompiuteryje yra įdiegta antivirusinė programa, prijungta prie interneto;
- Išjunkite kompiuterį per naktį, kad ne tik taupytumėte elektrą, bet ir sumažintumėte kompiuterio įsilaužimo ir neteisėto naudojimo pavojų.

2.2.Saugus ryšys – tinklalapiai su saugos sertifikatais

Saugumas reiškia kompiuterių tinkluose ir kompiuterinėse sistemose saugomų duomenų apsaugą nuo pažeidimų, praradimo ar nesankcionuotos prieigos. Šiais laikais, atsižvelgiant į greitą kompiuterinių tinklų, ypač interneto, prieinamumą, reikia vis labiau spręsti šią problemą. Pagrindinė kompiuterių tinklų saugumo problema yra jų apsauga nuo neteisėto naudojimo, pavyzdžiui, atliekant elektroninius mokėjimus, yra tikimybė, kad duomenys bus pavogti ir netinkamai naudojami.

Šifravimas naudojamas duomenų ar pranešimų turiniui apsaugoti nuo neteisėto naudojimo. Šifravimas yra duomenų ir pranešimų apdorojimo procesas, kurį inicijuoja arba siunčia siuntėjas. Norint naudoti tokius duomenis ar pranešimo turinį, jie turi būti iššifruoti. Šifravimo raktas naudojamas duomenims užšifruoti ir iššifruoti.

Svetainės, kurios keičiasi užšifruotais pranešimais, vadinamos saugiomis svetainėmis.



Saugų ryšį paprastai žymi piktograma 

Su internetine veikla susijusi rizika:

- netyčinis asmeninės informacijos atskleidimas. Norėdami naudotis interneto svetainėse siūlomomis paslaugomis, dažnai turite pasirašyti su savo asmenine informacija, pavyzdžiui, vardu, gimimo data, adresu. Prieš pateikdami šią informaciją įsitikinkite, kad svetainė yra patikima ir saugi;
- priekabiavimas ar bauginimas skleidžiant kenksmingus gandus arba siunčiant grasinimų pranešimus;
- galimas smurtas. Naudodamiesi socialiniais tinklais, tokiais kaip Facebook.com, ir užmezgdami naujus kontaktus, galite sutikti potencialų priekabiautoją, patyčias ir pan., Todėl būtina apgalvoti, kokią informaciją pateikti apie save, ir kritiškai įvertinti pateiktus pasiūlymus.
- Sukčiavimo, priekabiavimo ir emocinio pažeminimo atvejais informuokite teisėsaugos institucijas, tokias kaip policija.

Vaikų saugumas internete

Norint apsaugoti vaikus nuo neigiamos įtakos naudojantis internetu, rekomenduojamos šios priemonės:

- Padėkite kompiuterį kambaryje, kur galima stebėti vaiko veiklą internete;
- Kurkite vaiko abonementus su ribotomis kompiuterio vartotojo teisėmis;
- Apribokite naršymą įjungdami filtrus, draudžiančius patekti į svetaines, kuriose yra neigiamo turinio (narkotikų, pornografijos, neapykantos kalbų, ginklų ir kt.);

- Apribokitei žalingų žaidimų naudojimą, uždraudžiant žaidimus tam tikromis temomis;
- Apribokite kompiuterio naudojimą nustatydami kompiuterio naudojimo grafiką;
- Pavyzdžiui: **Vartotojo abonementai ir šeimos sauga**.

2.3.Bevielis internetas

Jei jūsų kompiuteris, planšetinis kompiuteris ar išmanusis telefonas palaiko „WiFi“ (belaidį internetą), galite naudotis internetu neprisijungdami prie įrenginio papildomo laido.

„WiFi“ galima naudoti tiek namuose, tiek už jo ribų. Jei norite naudoti „WiFi“ ne savo namuose, įrenginiuose dažnai galite pamatyti skirtingus „WiFi“ tinklus, tačiau ne visi turės prieigą, nes tinklas gali būti apsaugotas slaptažodžiu.

Daugelyje vietų, pavyzdžiui, kavinėse, parduotuvėse, parkuose, galite naudotis nemokamu viešuoju belaidžiu internetu. Geriausias būdas saugiai naudotis viešaisiais „Wi-Fi“ ryšiais viešoje vietoje yra sužinoti slaptažodį ir naudotis nemokamu ryšiu per šifruotą prieigą. Viešai prieinamas „WiFi“ vis dar yra vienas iš dažniausiai naudojamų būdų neteisėtai prisijungti prie savo mobiliojo prietaiso ir pasiekti savo asmeninius duomenis.

2.4.El.pašto priedai, įtrauktos nuorodos ir šlamšto žinutės

Nepageidaujamas paštas yra šlamštas. Šlamšto platintojai gali lengvai ir nebrangiai siųsti el.laiškus tūkstančiams žmonių tuo pačiu metu. Tokie laiškai yra anonimiški.

Kaip kovoti su šlamštu:

a) **Naudokite šlamšto blokatorių**. Šlamšto blokavimas gali žymiai sumažinti gaunamą šlamštą. Daugelis el. Pašto paslaugų teikėjų, tokių kaip „Google Gmail“, turi automatinį šlamšto blokavimą. Jei reikia, taip

pat gali būti naudojamos papildomos programos, blokuojančios šlamštą. Tačiau ir šiuo atveju yra tikimybė juos gauti.

b) **Nereaguokite į šlamštą**. Jei gausite įdomų šlamšto pranešimą, jums gali kilti pagunda į jį atsakyti arba spustelėkite nuorodą, kad atsisakytumėte gauti daugiau el. Laiškų. Atsakydami į šlamštą ar spustelėdami nuorodą, jūs nesąmoningai teigiate, kad šis el. Pašto adresas veikia, ir ateityje šiuo adresu bus išsiųstas naujas šlamštas.

c) **Išjunkite vaizdus**. El.laiške gali būti vaizdų, kuriuos gali stebėti šiukšlintojas. Kai atidarote šlamštą ir leidžiate į jį atsisiųsti vaizdus, jūs nurodote, kad esate pasirengęs priimti naują šlamštą.

d) **Išjunkite pranešimų rodymo sritį**. Spustelėjus raidę, ji automatiškai parodoma pateikimo srityje. Peržiūrėję šlamštą, galite sulaukti daugiau šlamšto.

e) **Reguliariai tikrinkite šlamšto aplanką**. Kartais šlamšto blokatoriai blokuoja ne tik šlamštą, bet ir teisėtus el.laiškus. Todėl turėtumėte kuo dažniau tikrinti šlamšto aplanką, kad nepraleistumėte svarbaus pranešimo. Patikrinkite el. Pašto kliento nustatymus, kuriems el.laiškai bus leidžiami, o kurie bus blokuojami.

✍	Sukurkite kelis el.pašto adresus, kad juos galėtumėte naudoti skirtingais tikslais.
✍	Neatskleiskite savo asmeninio el.pašto adreso viešuose tinkluose.
✍	Nekurkite trumpų el.pašto adresų. Daugelis šlamšto platintojų siunčia el.laiškus į atsitiktinius el.paštus. Kuo trumpesnis adresas, tuo lengviau jį atrasti.
✍	Jei norite patalpinti skelbimą internete, sukurkite naują el.pašto adresą šiuo tikslu.
✍	Jei jums reikia atskleisti savo el.pašto adresą, darykite tai mažiau suprantama forma, pvz., Vardas.vardas@mail.com rašykite kaip vardas-pavardė-el.paštas-dot-com.
✍	Nenaudokite savo asmeninio el.pašto adreso, kai prisiregistruojate į

	viešuosius tinklus.
✍	Nerizikuokite naudodami parinktį „atsisakyti prenumeratos“, nes tai dažnai tik paskatins atsiųsti daugiau šlamšto.
✍	Pakeiskite savo asmeninį el.pašto adresą, jei jis buvo rastas ir jame yra daug šlamšto.

2.5.Saugūs slaptažodžiai

Pasirinkti slaptažodžiai yra pats svarbiausias skydas apsaugant paskyras. Norėdami sukurti ir saugoti visus savo slaptažodžius, naudokite paprastą, bet saugų būdą.

Slaptažodžių supapratinimo veiksmai:

1. *Slaptažodžio frazės*

Svarbiausia slaptažodžių savybė yra ta, kad jie turi būti pakankamai ilgi, kuo daugiau slaptažodžio ženklų yra, tuo geriau. Tai vadinamos slaptažodžių frazėmis, saugaus slaptažodžio, naudojančio trumpus sakinius ar atsitiktinius žodžius, rūšimi:

- *Time for strong black coffee!. (Laikas stipriai juodai kavavai!)*
- *missing-snail-crawl-beach (palūdimys be sraigių)*

Abu slaptažodžiai yra saugūs, juose yra daugiau nei 20 ženklų. Juos lengva atsiminti, paprasta rašyti, bet sunku nulaužti. Jūs susidursite su internetinėmis svetainėmis ar situacijomis, kai slaptažodžiui reikia naudoti simbolius, skaičius ar didžiąsias raides. Bet atminkite, kad slaptažodžio raktas yra ilgis!

2. Slaptažodžio tvarkytojai

Kiekvienai paskyrai reikalingas unikalus slaptažodis. Jei kelioms paskyroms naudojate tą patį slaptažodį, jūs rizikuojate. Viskas, kas reikalinga kibernetiniam užpuolikui, yra įsilaužti į jūsų naudojamą svetainę, pavogti visus slaptažodžius, įskaitant jūsų, tada naudoti slaptažodį prisijungimui prie visų kitų savo paskyrų. Tai atsitinka dažniau, nei jūs galite įsivaizduoti. Galima patikrinti www.haveibeenpwned.com., kiek jūsų naudojamų svetainių buvo nulaužta ir ar jūsų slaptažodžiai galėjo būti pažeisti. Tokiais atvejais vienas iš būdų yra slaptažodžio tvarkyklės naudojimas. **Password Manager yra speciali kompiuterinė programa, ji saugiai ir užšifruoja visus jūsų slaptažodžius**. Turite atsiminti tik vieną slaptažodį - savo slaptažodžių tvarkyklės.

Tada „Password Manager“ automatiškai nuskaito jūsų slaptažodžius į atitinkamas svetaines, ir atpažįsta jus. Jie taip pat turi kitų funkcijų, tokių kaip galimybė išsaugoti jūsų atsakymus į saugos klausimus, įspėti, jei dar kartą naudojate slaptažodį, slaptažodžių generatoriaus funkcija, leidžianti jums sukurti ir naudoti saugius slaptažodžius, ir daugybė kitų. Daugelis slaptažodžių tvarkytojų taip pat saugiai sinchronizuoja įvairius įrenginius, todėl jūs turite lengvą ir saugią prieigą prie savo slaptažodžių, nesvarbu, kokią sistemą naudojate.

Užrašykite slaptažodžių tvarkyklės slaptažodį ant popieriaus ir laikykite saugioje vietoje namuose. Kai kurie slaptažodžių tvarkytojai netgi leidžia spausdinti slaptažodžių tvarkyklės atkūrimo įrankį. Tokiu būdu, jei pamiršite slaptažodį tvarkyklės slaptažodį, turėsite atsarginį planą. Be to, esant kritinei situacijai, jūsų patikimi žmonės galės gauti informacijos jūsų vardu.

3. *Dviejų veiksnių autentifikavimas*

Dviejų etapų tikrinimas (dažnai vadinamas dviejų faktorių autentifikavimu arba kelių faktorių autentifikavimu) suteikia papildomą saugumo lygį. Kai prisijungiate prie savo sąskaitų, jums reikia dviejų dalykų: slaptažodžio ir skaitmeninio kodo, kuris bus sugeneruotas jūsų išmaniajame įrenginyje arba išsiųstas į telefoną. Šis procesas užtikrina, kad net jei kibernetiniai užpuolikai būtų gavę jūsų

slaptažodžius, jie negalėtų pasiekti jūsų paskyrų. Dviejų veiksnių autentifikavimą lengva nustatyti ir paprastai jį reikia naudoti tik vieną kartą, kai suteikiate prieigą iš naujo įrenginio. Jei naudojate slaptažodžių tvarkyklę, rekomenduojama ją apsaugoti tiek saugaus slaptažodžio fraze, tiek dviejų faktorių autentifikavimu.

Supaprastinta **dviejų pakopų autentifikacija** reiškia, kad jūs ne tik įvesite slaptažodį, bet ir patvirtinate jį turėdami, pavyzdžiui, kodą iš mobiliojo telefono. Taip pat yra trijų etapų įgaliojimas, kai turite patvirtinti prieigą naudodamiesi tuo, kas jums tinka, pavyzdžiui, pirštų atspaudu. Dviejų žingsnių autentifikavimo pranašumas yra tas, kad įsilaužėliui taip pat reikia prieigos prie jūsų mobiliojo prietaiso, kad jis įsilaužtų į jūsų sąskaitą.

3.Slaptažodžių naudojimas

3.1.Slaptažodžiai: pirmasis saugumo žingsnis

Yra du slaptažodžių tipai: saugus ir nesaugus. Daugelis žmonių naudoja nesaugius slaptažodžius - trumpus, lengvai įsimenamus slaptažodžius, kuriuose yra asmeninės informacijos (pvz., Vardas, pavardė, gimimo metai, svarbi data, augintinių vardai, pavardės) arba net tas pats slaptažodis naudojamas kelioms paskyroms.

Piratai dažnai naudoja slaptažodžių paieškos programinę įrangą, kuri patikrina daugelį slaptažodžių, kol randa tinkamą. Netikimi slaptažodžiai gali būti randami labai greitai. Sukūrę saugius slaptažodžius, sumažėja tikimybė, kad nusikaltėliai atskleis jūsų slaptažodį ir pavogs asmeninę bei finansinę informaciją.

Norint apsaugoti jūsų duomenis, yra pagrindiniai saugumo principai, kurių reikia laikytis naudojant slaptažodį:

- Įvesdami slaptažodį, saugokitės, kad kiti žmonės nematytų jūsų pirštų judesių jūsų išmaniojo telefono klaviatūroje ar ekrane;
- Keiskite slaptažodį kas 3 mėnesius;

- Būkite atsargūs ir neišsaugokite automatinės prieigos prie sąskaitos. Visada naudokite mygtukus Išeiti, Atsijungti arba Baigti darbą;
- Venkite slaptažodžių laisvos prieigos interneto svetainėse.

3.2.Saugaus slaptažodžio kūrimo principai

Kurdami vartotojo abonementą socialiniuose tinkluose, naudodamiesi interneto banku ar kitu savitarnos portalu, turite užsiregistruoti naudodami savo vartotojo vardą, slaptažodį ir kitą informaciją.

Patarimai	**Paaiškinimai**
Niekada nenaudokite asmeninės informacijos	Nenaudokite vardų, gimtadienių ar šeimos vardų kaip slaptažodžių. Asmeninė informacija dažnai yra viešai prieinama, todėl slaptažodį galite atspėti labai greitai.
Naudokite ilgesnius slaptažodžius	Slaptažodis turi būti bent šešių simbolių. Kad slaptažodis būtų saugesnis, įveskite 12 ar daugiau simbolių.
Venkite užsirašyti slaptažodžius knygelėje ar telefone	Jei vis tiek norite užrašyti slaptažodį, laikykite jį saugioje vietoje ir niekam jo nerodykite. Rekomenduojama užšifruoti slaptažodžius, o ne pats užsirašyti.
Naudokite atsitiktinai parinktus slaptažodžius	Patikimiausi yra atsitiktiniai slaptažodžiai. Užuot galvoję apie savo slaptažodžius, galite naudoti slaptažodžių generatorius. Atsitiktinius slaptažodžius sunkiau atsiminti, nes juos sukuria įrenginiai.
Nenaudokite tų pačių slaptažodžių kelioms paskyroms	Jei kas nors atskleidžia vienos paskyros slaptažodį, kitos paskyros slaptažodžiai taip pat bus pažeidžiami.
Nenaudokite žodžių, kuriuos	Pvz., Slaptažodis mokytojas1 bus nesaugus.

Patarimai	Paaiškinimai
galima rasti aplinkoje	
Į slaptažodžius įtraukite skaičius, simbolius ir mažąsias raides.	Norėdami sukurti saugų slaptažodį, galite pakeisti raides skirtingais simboliais, pavyzdžiui, remiantis žodžiu Monday ir pakeisdami raides „o“ ir „a“, galite sukurti šį saugų slaptažodį M0nd @ y!

3.3.Atvejo analizė ir praktinė užduotis

Pagyvenęs ponas Beržinsas nusprendė pradėti naudotis el.paslaugomis, buvo pasirengęs pasirašyti Saugaus eismo automobilių kelių direkcijos (CSDD) svetainėje, kad ateityje galėtų sužinoti apie save ir savo automobilį nuotoliniu būdu.

Norėdami sukurti ar suaktyvinti savo CSDD sąskaitą, pirmą kartą prisijungdami prie svetainės, turite užsiregistruoti el.paštą, susikurti savo slaptažodį ir jį įvesti. Pirmą kartą sukūrus sąskaitą, prieiga prie jūsų CSDD sąskaitos bus tęsiama ir naudojant nustatytą prieigą, ir prieigą prie internetinės bankininkystės.

Susiklosčiusios situacijos uždavinys yra tai, kad ponas Beržinas sugalvotų naujai sukurtos CSDD sąskaitos slaptažodį gyvenamajame kambaryje prie savo kompiuterio, kad niekas jo neatspėtų.

Bendra scena - ponas Beržinas sėdi savo sodybos gyvenamajame kambaryje už atidaryto nešiojamojo kompiuterio. Fone yra sofa, ant kurios miega tingi persų katė vardu Rudis. Ponia Beržina sėdi kitame sofos gale ir mezga skrybėlę. Prie pono Beržinsas kojų guli juodas šuo, vardu Poga. Kažkur fone šiltai dega židinys, virš kurio kabo Beržinų medžioklės trofėjus, briedžio raguota galva. Vieną svetainės sieną užima knygų lentyna, kurioje galite pamatyti atpažįstamus skirtingų rašytojų kūrinius. Kai kurių knygų viršeliuose galite pamatyti jų portretus, pavyzdžiui, Šekspyro, Dostojevskio, Čechovo ir kt. Kitoje

sienoje yra Beržinų šeimos nuotrauka, kurioje galite pamatyti jų suaugusius vaikus ir anūkus. Čia net yra pono Beržino ir jo žmonos nuotrauka, pozuojanti prie Niagaros krioklio. Šiek tiek toliau yra iš lentynos kabančios gebenės, o ant palangės auga kaktusas.

1) Kiekvienas reikšmingas Beržinų šeimos namo objektas (elementas) gali būti vertinamas kaip galimas blogas ar geras slaptažodžio variantas:

- Kate Rudis: *Rudis* / **RuD! $**
- Zmonos hobis: mezgimas /**Mzg*tt*ng**
- augalas: kaktusas / **sutcac**
- Medziokle trofejus: Trophy / **Tr0fhy**
- Suo Poga: Poga / **50s** @
- anukas12: Grandson12 / **An@nds0n**
- zmona Rosalie: Rosalie / **R0s@lie**
- Chekhov: Chekhov / **Ch3kh0v**
- Dostoevsky: Dostoevsky / **D0$t0j3v$ky**

Santrauka

Šiame modulyje buvo trys svarbios temos, susijusios su asmens duomenimis ir privatumo apsauga. Tokie kaip jūsų kompiuterio saugos pagrindai ir pagrindiniai duomenų apsaugos principai. Norėdami išvengti sukčiavimo, besimokantieji buvo supažindinti su elektroninių nusikaltėlių veiksmais, kaip pavogti informaciją. Atsižvelgiant į tai, kad viena iš svarbiausių asmens duomenų apsaugos problemų šiais laikais yra per daug asmeniškos informacijos paskelbimas ir dalijimasis ja įvairiuose socialiniuose tinkluose, šiame modulyje taip pat pateiktos šios temos saugos gairės.

Siekiant saugiai naudotis skaitmeniniais prietaisais ne namuose, šiame modulyje buvo nagrinėjamos interneto jungčių temos ir pagrindiniai saugaus belaidžio interneto naudojimo principai. Taip pat buvo paaiškinti nesaugaus el. pašto ir šlamšto požymiai bei pateikti patarimai, kaip teisingai ir saugiai naudoti slaptažodžius.

Baigiamajame modulio skyriuje apžvelgiami slaptažodžių kūrimo pavyzdžiai ir aprašoma situacija - kaip kuriami slaptažodžiai, į kokius slaptažodžius reikėtų atsižvelgti, o kurių vengti.

Bibliografija

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