2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programa

PRISIJUNGUSI LIETUVA

BŪKIME SAUGŪS INTERNETE

MEDŽIAGA MOKYMŲ DALYVIUI

www.prisijungusi.lt

Projektą įgyvendina:

ivpk INFORMACINĖS VISUOMENĖS PLĖTROS KOMITETAS

LANGAS Į ATEITĮ

RYŠIŲ REGULIAVIMO TARNYBA

LIETUVOS NACIONALINĖ MARTYNO MAŽVYDO BIBLIOTEKA

VIDAUS REIKALŲ MINISTERIJA

Mokymus organizuoja: asociacija „Viešieji interneto prieigos taškai“ (VIPT), UAB „Baltijos kompiuterių akademija”, Savivaldybių viešųjų bibliotekų asociacija, VšĮ „Informacinių technologijų institutas“.

2020

ĮVADAS

Ši programa skirta suaugusiems Lietuvos gyventojams, kurie turi pagrindinių skaitmeninių žinių ir įgūdžių, tačiau ribotai naudojasi skaitmeniniais įrenginiais ir technologijomis bei nori tobulinti skaitmeninius įgūdžius, kad galėtų efektyviai naudoti šiuolaikines skaitmenines technologijas kasdieninėje ir profesinėje veikloje.

Skaitmeninių įgūdžių turinčių gyventojų mokymo renginių programa savo turiniu atitinka Europos Komisijos rekomenduojamus skaitmeninių gebėjimų (DigComp 2.1) 1-2 gebėjimų (kompetencijų) lygius. Programa parengta pagal gyventojų skaitmeninio raštingumo žinių ir įgūdžių tobulinimo projekto „Prisijungusi Lietuva: efektyvi, saugi ir atsakinga Lietuvos skaitmeninė bendruomenė“ tikslus, uždavinius ir reikalavimus.

Mokymų programą sudaro penkios pagrindinės dalys:

1. Kodėl svarbu kalbėti apie e. saugą?
2. Pagrindinės e. saugos žinios ir saugus naršymas
3. Saugesnis interneto naudojimas
4. Kompiuterių ir išmaniųjų įrenginių saugumas
5. Rekomendacijos kaip būti saugesniam

Leidinio autorius:

Dr. Renata Danielienė.
VšĮ „Informacinių technologijų universitetas“ vykdančioji direktorė,
VU Kauno fakulteto dėstytoja.

1. KODĖL SVARBU KALBĖTI APIE E. SAUGĄ?

Šiuo metu internetas yra plačiai naudojamas tiek darbe, tiek namuose. Paprastai naudodami internetą įdiegiame papildomas kompiuterį apsaugančias programas ar priemones. Tačiau patys vartotojai dažnai elgiasi neatsakingai, nežinomiems asmenims pateikia per daug asmeninės ar finansinės informacijos, talpina įvairų turinį internete, atsisiunčia nelegalų turinį, diegia nelegalias programas, netinkamai reaguoja į skelbiamas „netikras“ naujienas ir pan.

Pastaruoju metu išmanieji įrenginiai tampa neatsiejama gyvenimo dalimi. Todėl naudojant juos, taip pat būtina imtis įvairių saugumo priemonių, kadangi jie turi panašias funkcijas kaip ir įprasti staliniai ar nešiojamieji kompiuteriai. Naudojant šiuos įrenginius, galima susidurti su tomis pačiomis saugumo problemomis kaip ir kompiuteriuose, prarasti duomenis ir pan. Išmanieji įrenginiai taip pat gali būti apsaugoti nuo virusų ir kitų galimų grėsmių internete kaip ir įprastieji kompiuteriai.

Interneto paslaugos vis plačiau naudojamos kasdieniame mūsų gyvenime bei interneto naudotojų skaičius nuolat sparčiai auga. Vis daugiau žmonių naudoja įvairias paslaugas internete: naudojasi e. valdžios vartų paslaugomis, užsako prekes ir paslaugas internetu, naudojasi e. bankininkyste bei leidžia laisvalaikį internete. Tiek „Facebook“, tiek „Youtube“ yra registruotų po daugiau nei 2 mlrd. aktyvių naudotojų, o didelė dalis iš jų šiose aplinkose naudoja išmaniuosius įrenginius bei praleidžia nemažai laiko.

Interneto naudotojai gauna daug naudingos informacijos ir įvairių paslaugų, tačiau čia slypi ir nemažai grėsmių. Todėl tiek kompiuterių, tiek išmaniųjų įrenginių naudotojai turi žinoti apie galimus pavojus internete ir galimas pasekmes, kai internetu naudojamasi neatsakingai.

Interneto privalumai bei galimos grėsmės

Interneto privalumai	Galimos grėsmės
Interneto portalai, e. paslaugos • Informacijos gausa • Naujienos iš viso pasaulio • Dalinimasis dokumentais ir failais internetu • Prekių įsigijimas ir pardavimas internetu • E. viešosios paslaugos	**Interneto portalai, e. paslaugos** • Asmeninės informacijos išgavimas ir grėsmė privatumui • Netikros svetainės • Nelegali informacija, piratavimas
Paieškos sistemos • Informacija apie viską iš bet kurios pasaulio vietos bet kuriuo paros metu	**Paieškos sistemos** • Nepatikima informacija, kadangi informaciją internete, ypač tinklaraščiuose ir socialiniuose tinkluose, gali skelbti bet kas. • Netinkamas turinys tam tikroms žmonių grupėms (netikra tapatybė, psichologinė žala, rasizmas, religinės sektos, viliojimai ką nors nusipirkti ar atskleisti asmeninę informaciją, informacija apie narkotikus, smurtą ir t. t.).
Laisvalaikio praleidimas	**Laisvalaikis** • Priklausomybė nuo technologijų
Virtualus bendravimas • Naujų kontaktų paieška • Bendravimas e. paštu • Tiesioginio bendravimo priemonės („Skype“, „Messenger“, „Viber“, „Whats up“) • Socialiniai tinklai	**Virtualus bendravimas** • Galimybė būti kuo nori • Bendravimas su nepažįstamais • Tapatybės slėpimas sukčiavimo ar nusikalstamoms veikloms • Tiesioginio ryšio praradimas
Marketingas, verslo modelis • Reklama • Įsidarbinimo galimybės •	**Marketingas, verslo modelis** • Nepageidaujami laiškai • Nepageidaujama reklama • Finansiniai nuostoliai • Surenkama per daug informacijos, nusikaltėliai gali pasinaudoti realiai veikiančia įmone ir apgaudinėti žmones.
Užsienio kalba • Užsienio kalbų mokymasis ir tobulinimas	**Užsienio kalba** • Kalbos barjeras • Netaisyklinga kalba

Interneto privalumai	Galimos grėsmės
Kiti privalumai • Informacijos publikavimas apie save • Darbo galimybės neišeinant iš namų •	**Kitos galimos grėsmės** • Patyčios, priekabiavimas • Darbo galimybių praradimas kaip padarinys (reputacijos sugadinimas – prieš tai paskelbtos informacijos internete) • Virusai • Nusikalstama veikla internete

Interneto naudotojai patys turi būti atsargūs, turėti bent pagrindines žinias, kaip būti saugesniam internete.

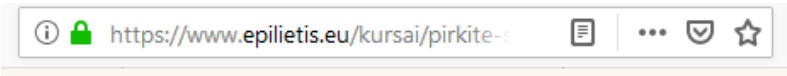
2. PAGRINDINĖS E. SAUGOS ŽINIOS IR SAUGUS NARŠYMAS

Jungiantis prie įvairių svetainių ar portalų reiktų būti atidiems ir atkreipti dėmesį į keletą svarbių dalykų, siekiant apsisaugoti, kad asmeniniai ar finansiniai duomenys nebūtų pavogti, perduoti tretiesiems asmenims ar pan. Pavyzdžiui, jungiantis prie tokių sistemų, kaip e. bankininkystės, e. prekybos, e. pašto svetainių, reikia atkreipti dėmesį ar naršyklės adreso juostoje yra spynelės piktograma ir ar svetainės adresas prasideda „https“.

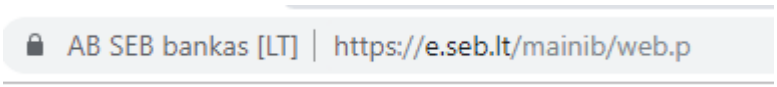
„https“ – užtikrina privatų ir saugų ryšį tarp kliento ir serverio (persiunčiamų duomenų šifravimu bei dešifravimu t.y. naudojant šį protokolą persiunčiama informacija yra užšifruojama). „https“ protokolas naudojamas vykdant finansines operacijas, atsiskaitant už prekes ar paslaugas internetu, jungiantis prie įvairių sistemų, pavyzdžiui, e. pašto ar paslaugų tiekėjo aplinkos, ir pan., kai persiunčiami asmens, bankiniai ir kt. duomenys. Naudojant šį protokolą, svetainės adresas prasideda „https://“, pavyzdžiui, https://adresas.lt.

Taip pat svarbu atkreipti dėmesį į svetainės adreso juostoje esančią spynelės piktogramą, kuri nurodo, kad prisijungimas yra šifruotas ir saugus. Šifravimas užtikrinamas pagal svetainės pateikiamą dokumentą, vadinamą sertifikatu. Kai svetainė naudoja „https“ protokolą, interneto naršyklės (pavyzdžiui, *Internet Explorer*, *Mozilla Firefox*) svetainės adreso juostoje paprastai yra rodoma spynelės piktograma ( ).

Mozilla Firefox“ lango pavyzdys:



„Google Chrome“ lango pavyzdys:



Paspaudus ant spynelės parodoma, ar ryšys yra saugus, ir pateikiama informacija apie svetainės sertifikatą, kur nurodoma informacija, kam sertifikatas buvo išduotas, galiojimo laikas ir kita informacija.

Socialinė inžinerija

Socialinė inžinerija – tai psichologinių manipuliacijų naudojimas siekiant, kad kiti žmonės atliktų tam tikrus veiksmus, arba siekiant išgauti konfidencialią informaciją naudojant įvairias technikas.

Socialinės inžinerijos taikymo sritys:

- Įvairaus tipo kritinių duomenų vagystės,
- Pramoninis šnipinėjimas,
- Finansinės machinacijos,
- Sukčiavimas,
- Šantažas,
- Informacijos rinkimas.

Internetinė tapatybė

Internetinė arba skaitmeninė tapatybė – tai asmenybės „atspindys“ elektroniniame pasaulyje. Viskas, ką apie save rašome, ką publikuojame, ką aptarinėjame, kaip komentuojame, ką skaitome, yra mūsų skaitmeninės (internetinės) tapatybės dalis. Tai duomenys, kurie pristato asmenybę virtualioje erdvėje.

Galima teigti, kad skaitmeninę tapatybė sudaro:

- socialinių tinklų profiliai,
- tipinė asmens elgsena internete,
- savęs prezentacija skaitmeninėje erdvėje,
- tai, ką asmuo rašo, rodo kitiems,
- tai, ko asmuo ieško elektroninėje erdvėje.

Kas yra asmens duomenys?

Asmens duomenys – bet kuri informacija, susijusi su asmeniu. Asmens tapatybė gali būti tiesiogiai arba netiesiogiai nustatoma pasinaudojant tam tikrais duomenimis, tokiais kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai[1].

Vieši duomenys gali būti vardas, pseudonimas, lytis, hobis ir pan., tačiau internete neturėtų būti viešinama:

- Asmens kontaktiniai duomenys,
- Biometriniai duomenys,
- Asmens kodas,
- Asmens pajamos,
- Slaptažodžiai,
- …

Tapatybės vagystė

Tapatybės vagystė – tai tokia vagystė, kai pasinaudojama kito asmens tapatybę identifikuojančiais duomenimis, tokiais kaip asmens kodas, kredito kortelės duomenys, paso ar valstybinio socialinio draudimo pažymėjimo duomenys.

Dažniausiai naudojamos priemonės siekiant pavogti prisijungimo prie banko duomenis:

- Duomenų vagystė („phishing“),
- Šnipinėjimo programos,
- Virusai,
- Trojanai,
- Klavišų paspaudimų įrašikliai („keyloggers“).

Tipinė tapatybės vagystės ataka

Skambučiai:

- Skambina apsimetę saugumo, banko ar kitų institucijų darbuotojais,
- Skambina dėl artimojo nelaimės,
- ...

E. laiškai, socialiniai tinklai ir netikros svetainės:

- Siunčia e. laiškus su netikromis nuorodomis ir priedais su virusu,
- Siunčia artimiesiems e. laiškus iš kitų pašto tiekėjų sukurtų adresų, pvz. žinodami Vardaitis@gmail.com, sukuria Vardaitis@yahoo.com,
- Sukuria analogišką socialinio tinklo paskyrą jūsų vardu,
- ...

Virusai, šnipinėjimo programos ir pan.

Reiktų būti atidiems, kai kas nors jūsų prašo:

- Pateikti asmeninę informaciją nežinomam šaltiniui;
- Patvirtinti sąskaitos informaciją, kitaip grasinama užblokuoti jūsų sąskaitą;
- Parduoti daiktą, kai siūloma suma yra gerokai didesnė už daikto vertę;
- Tiesiogiai aukoti pinigų sumas;
- Reaguoti nedelsiant.

Taip pat būkite atsargūs ir atitinkamai reaguokite, kai:

- E. paštu gaunate sąskaitą Zip formatu iš nežinomų siuntėjų;
- E. laiške yra nuoroda, kurią siūlo paspausti;
- Su jumis susisiekia kreditorius dėl jums nežinomos skolos;
- Su jumis susisiekia „banko“ ar „kredito kompanijos“ darbuotojai dėl įtartinų sandorių, kurie „atliekami“ per jūsų sąskaitą;
- E. laiške yra gramatinių klaidų, laiško siuntėjas nežinomas;
- ...

[1] https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=-rwipzqom4&documentId=TAIS.106090&category=TAD

Nepageidaujami laiškai

Dažnai e. pašto naudotojai gauna iš nežinomų siuntėjų laiškus, kurių nelaukė ir nesitikėjo. Tai būna įvairiausio turinio laiškai – prekių ir paslaugų reklamos, komerciniai pasiūlymai, beprasmiai laiškai ir pan. Tokie laiškai lietuvių kalba vadinami elektroniniu šlamštu, brukalu, nepageidaujamais laiškais, o anglų kalba – *spam*, *junk mail*.

Nepageidaujamais laiškais gali būti platinamas kenkėjiško pobūdžio šlamštas, kai su elektroninio pašto laiškais gavėjus pasiekia ir kompiuterių virusai, interneto kirminai ir kita kenkėjiška programinė įranga, siekiama išgauti asmens duomenis.

Daugiau informacijos rasite žemiau pateiktame sąraše (paspaudus nuorodą, bus atveriamas vaizdo įrašas arba svetainė):

- Kaip atpažinti manipuliacijas
- Istorijos, susijusios su tapatybės vagystėmis
- Kaip atskirti, kad vaistus internetu siūlo sukčiai?
- Kaip apsisaugoti nuo finansinių nusikaltimų internete
- Kaip išvengti socialinių tinklų profilių vagysčių?
- Dažniausiai pasitaikančios sukčiavimo schemos
- Greito uždarbio spąstai internete
- Paslaptingas draugas
- Duomenų vagystės („phishing“)
- Kaip atpažinti duomenų išviliojimo (angl. phishing) e. laiškus
- Grandininiai e. laiškai
- Apgaulingos SMS žinutės
- Kritinis mąstymas apie turinį internete
- Saugesnis apsipirkimas internetu

3. SAUGESNIS INTERNETO NAUDOJIMAS

Asmens duomenų saugojimas skaitmeniniame įrenginyje

Naršant internete (ne privačiame interneto naršyklės režime), kiekviena naršyklė fiksuoja darbo istoriją (žurnalą). Naršyklės žurnale yra fiksuojami:

- Aplankytų tinklapių adresai;
- Prisijungimo vardai ir slaptažodžiai;
- Kiti aplankytų tinklapių duomenys (slapukai).

Be to, atsisiųsti iš interneto dokumentai, paveikslėliai ir kiti failai taip pat saugomi skaitmeniniame įrenginyje.

Kas yra slapukas?

Slapukas (angl. *cookies*) – tai tekstinis duomenų rinkinys, kuris yra perduodamas iš interneto tinklalapio į lankytojo kompiuterio laikmeną ir saugomas tekstiniame faile, norint rinkti informaciją apie svetainės naudojimą. Naudojant slapuką, atsimenama tam tikra informacija, tokia kaip prisijungimo prie svetainės duomenys, svetainės kalba ir pan.

Slapukai paspartina darbą ir yra naudingi, pavyzdžiui, vieną kartą įrašius prisijungimo prie svetainės duomenis (vartotojo vardą ir slaptažodį), kitą kartą nereikia prisiminti slaptažodžio, kadangi jis įrašomas automatiškai, tik įrašius vartotojo vardą. Slapukai taip pat paspartina darbą, kadangi yra įrašomas įvairių pildomų formų laukelių turinys, pavyzdžiui, svetainės formos laukelyje pradėjus rašyti vardą pasiūloma iš karto užpildyti anksčiau įrašytą vardą ir pan.

Naršant svetainėse dažnai naudotojo yra klausiama, ar išsaugoti prisijungimo duomenis, tuomet galima sutikti arba atmesti. Nereikia sutikti saugoti prisijungimo duomenis jungiantis prie svetainių naudojant viešuosius kompiuterius arba skaitmeninius įrenginius, kuriais naudojasi kiti asmenys.

> **Naršydami prie kitų asmenų ar viešųjų skaitmeninių įrenginių neleiskite** naršyklei įsiminti jūsų įvedamų prisijungimo vardų ir slaptažodžių.

Failai ir dokumentai, kurie įrašomi skaitmeniniame įrenginyje

Dažnai į savo skaitmeninius įrenginius atsisiunčiame failų ir dokumentų iš svetainių, o taip pat įvairių dokumentų, kurie būna prisegti prie e. laiškų. Reikia atkreipti dėmesį, kad dažniausiai tokie failai yra saugomi atsisiunčiamų failų aplankuose.

Jei dirbama prie viešųjų kompiuterių arba skaitmeninių įrenginių, kuriais naudojasi kiti asmenys, reiktų tokius failus ir dokumentus pašalinti baigus darbą, kad kiti asmenys negalėtų jų peržiūrėti.

Reiktų pasirūpinti, kad dokumentai ir failai būtų pašalinami ir iš šiukšlinės (kompiuteriuose), į kurią patenka pašalinti failai (jei nenustatyta kitaip). Šiukšlinę paprastai galima rasti darbalaukyje. Norint patikrinti, ar šiukšlinėje nėra jūsų failų, reikia ją atverti ir, jei jūsų failai yra, juos pašalinti dar kartą.

Naršymo istorija

Naršyklės naršymo istorija pildoma automatiškai (jei nepakeisti naršyklės nustatymai), todėl bet kada galima pamatyti, kada buvo aplankyti tam tikri puslapiai, o taip pat sužinoti, kokius puslapius lankoma daugiausiai.

Taupant vietą diske arba dėl kitų sumetimų, galima išvalyti laikinuosius interneto failus, naršymo žurnalą (istoriją), įsimintus formų duomenis ar slapukus.

Privatus naršymo režimas

Privataus naršymo režime neįsimenama tokia informacija:

- Aplankytos svetainės: adresai nebus įrašyti į naršymo istoriją;
- Formų ir paieškos įrašai: teksto laukeliuose ir paieškos juostoje rašomi žodžiai nebus išsaugomi į automatinį sąrašą;
- Slaptažodžiai: naujai įvesti slaptažodžiai nebus įsimenami;
- Atsiuntimų įrašai: atsiuntimuose neliks atsiųstų failų pavadinimų;
- Slapukai: slapukai saugo lankytų svetainių nuostatas, prisijungimo duomenis. Slapukus gali panaudoti trečiosios šalys sekti jūsų veiksmams internete;
- Nebus kuriami laikinieji failai.

Privatų naršymo režimą galima rasti visose šiuolaikinėse naršyklėse, tik gali būti skirtingas pavadinimas ir skirtinga piktograma.

Naršyklė		Privataus režimo lango atidarymas	Piktograma
„MS Internet Explorer“		Įrankiai > „InPrivate“ naršymas.	
„Firefox“		Failas > Naujas privataus naršymo langas.	
„Google Chrome“		Dešinėje viršutinėje lango dalyje paspaudus trijų taškų ⋮ mygtuką, reikia pasirinkti **Naujas nežinomas langas**.	
„Opera“		Kairėje viršutinėje lango dalyje, paspaudus Opera  mygtuką, reikia pasirinkti **Naujas asmeninis puslapis**.	

Saugus atsijungimas nuo svetainių

Baigus darbą įvairiuose portaluose, tokiuose kaip e. bankininkystės tinklalapiai, e. parduotuvės, e. valdžios vartai, e. paštas, socialinių tinklų svetainės, prieš uždarant naršyklės langą reikia išsiregistruoti (t. y. atsijungti nuo svetainės, angl. *log off*).

Būkite atsargūs, kai viešose vietose (oro uostuose, viešbučiuose) bandote prisijungti prie nežinomų (privačių) belaidžių tinklų. Rekomenduojama atsijungti nuo belaidžio tinklo viešose vietose, kai internetu nebesinaudojama.

Prisijungimo prie įvairių sistemų ypatumai

Jungiantis prie įvairių sistemų reikia imtis kompleksinių apsaugos priemonių. Slaptažodžiai turi būti sukurti ir saugomi laikantis tam tikrų rekomendacijų, esant galimybei, jungtis prie sistemų naudojant kelių faktorių autentifikaciją ir pan.

Socialinės paskyros nustatymai

Vis daugiau žmonių naudojasi socialiniais tinklais, tokiais kaip „Facebook“, „Twitter“, „LinkedIn“ ir pan. Šie tinklai leidžia naudotojams skelbti informaciją apie save, taip pat bendrauti su draugais ir kolegomis. Tačiau tam tikra šiuose tinkluose pateikiama informacija turėtų likti konfidenciali ir neskelbiama. Socialinius tinklus aptarnaujančios kompanijos renka gan daug duomenų apie jų naudotojus, norėdamos individualizuoti teikiamas paslaugas.

Realiame gyvenime bendraudami su kitais žmonėmis save pristatome įvairiai: pasisakome vardą (ir pavardę), kur ir kokį darbą dirbame, kokie mūsų pomėgiai ir pan. Socialiniame tinkle naudotojai taip pat turi asmeninį profilį. Tai asmeninis puslapis, kuriame:

- įrašome savo vardą;
- įkeliame asmeninį atvaizdą;
- aprašome savo pomėgius.

Pateikdami informaciją apie save socialiniame tinkle, turime būti santūrūs ir atsargūs. Ypač patiklūs socialiniuose tinkluose yra jauni žmonės, kurie dažnai nesusimąsto apie asmeninio gyvenimo viešinimo pasekmes, neįžvelgia socialinių tinklų keliamų pavojų.

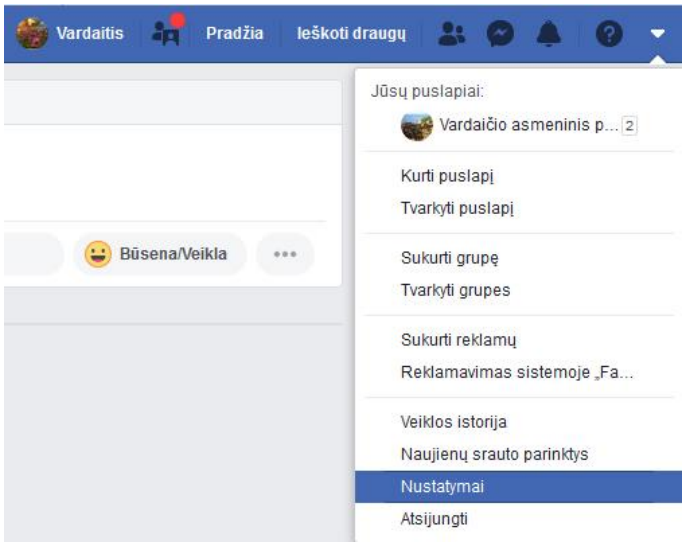
Virtualioje erdvėje dažniausiai susiduriama su asmens tapatybės vagystėmis. Socialinių tinklų ir elektroninio pašto prisijungimo duomenų vagystės pavojingos dėl asmeninės informacijos nutekinimo, sudarančio sąlygas neretai pasitaikančiam svetimų banko sąskaitų atidarymui, prekių įsigijimui, pinigų išėmimui, neva atsitikus nelaimei draugų ir pažįstamų prašymas paskolinti pinigų ir pan.

Asmens tapatybės vagystė internete gali pakenkti ir asmens reputacijai. Piktavalis gali paskleisti tikrovės neatitinkančią informaciją, pasirašydamas kito asmens vardu, arba paskleisti asmeninę informaciją internete.

Atminkite, kad paviešinti jūsų, jūsų artimųjų ar darbdavių duomenys gali būti sukčių panaudoti jiems reikiamos informacijos bazei kurti. Naudotis socialiniais tinklais reikia saikingai ir atsakingai, juose galima viešinti tik naudotojui ir jo artimiesiems neutralią informaciją.

Privatumo nuostatų tvarkymas

„Facebook“ naudotojai gali kontroliuoti, kokią informaciją apie juos gali matyti kiti internetinės bendruomenės nariai. Šie apribojimai yra žinomi kaip „privatumo nuostatos". Kaip pavyzdį panagrinėsime socialinio tinklo „Facebook“ privatumo nuostatų keitimą.



Prisijungus prie savo „Facebook“ paskyros tvarkyti privatumo nuostatas galima spragtelėjus rodyklytės piktogramą, esančią dešinėje viršutinėje lango dalyje ir atsidariusiame meniu pasirinkus **Nustatymai**.

Norėdami nurodyti, kas gali matyti jūsų asmeninę informaciją, kairėje pusėje spragtelkite **Privatumas** ir galėsite, pavyzdžiui, nurodyti, kas matys jūsų įrašus.

Šiame lange rekomenduojama visiems punktams nurodyti, kad stebėti jūsų veiklą ir jus rasti galėtų tik draugai ir draugų draugai.

Daugiau apie socialinių tinklų saugumą skaitykite

- Kibernetinio saugumo centro parengtą medžiagą.
- Rekomenduojami „Facebook“ privatumo nustatymai
- Rekomenduojami „Facebook“ saugumo nustatymai

Nuotraukų ir vaizdo įrašų platinimas

Pateikiame keletą patarimų platinant nuotraukas ir vaizdo įrašus internete

- Gerbkite kitų žmonių privatumą.
- Jei norite platinti nuotrauką ar įrašą su pažįstamais, geras tonas reikalauja paprašyti leidimo.
- Neplatinkite svetimų vaikų nuotraukų be jų tėvų sutikimo.
- Nenaudokite savo reklaminėje medžiagoje asmenų nuotraukų, jei asmuo nedavė tam sutikimo.
- Nepažįstamuosius fotografuoti galima tik viešoje vietoje.
- Jei asmuo aiškiai išreiškė nenorą, jo fotografuoti negalite.
- Nenaudokite nuotraukų ir vaizdo įrašų platinimo kaip kerštо ar pajuokos įrankio.
- Neplatinkite smurtinių, kurstančių neapykantą, įžeidinėjančių nuotraukų ir vaizdo įrašų. Net tuo atveju, jei norite pasmerkti smurtą ar neapykantą.
- Neplatinkite nuotraukų ir vaizdo įrašų, kur jūs ar jūsų artimieji užfiksuoti nesilaikantys taisyklių, elgiasi nederamai ar net pažeidžia įstatymus.
- Jei radote nuotrauką, kurioje esate užfiksuoti patys arba jūsų artimieji (vaikai, tėvai ir t. t.), ir nenorite, kad ši nuotrauką būtų platinama, imkitės tokių priemonių:
- Kreipkitės į skelbėją ir aiškiai prašykite pašalinti. Kreiptis geriau tomis pačiomis priemonėmis, kur radote nuotrauką (jei radote socialiniame tinkle, kreipkitės to paties socialinio tinklo priemonėmis). Jei nerandate skelbėjo, naudokite kitus jo žinomus kontaktus.
- Kreipkitės į socialinio tinklo administratorių ir prašykite pašalinti nuotrauką, išaiškindami situaciją. Socialiniai tinklai paprastai turi specialias kreipimosi į administraciją formas, kurios skirtos tokiems ir panašiems atvejams.
- Jei aukščiau išvardinti veiksmai nepadėjo, kreipkitės į Asmens duomenų apsaugos inspekciją.
- Jei žinote ar įtariate, kad kas nors iš jūsų atvaizdo gauna komercinės naudos, o jūs nesate tam davę sutikimo, galite susisiekti su skelbėju ir prašyti nuotrauką šalinti. Ši taisyklė negalioja tais atvejais, kai fotografavimosi ar filmavimosi metu buvo sudaryta sutartis, kurioje pažymėta, kad jūsų atvaizdą fotografas gali naudoti reklamos ar komercijos tikslams.

Daugiau informacijos rasite žemiau pateiktame sąraše (paspaudus nuorodą, bus atveriamas vaizdo įrašas arba svetainė):

- Saugesnis internetas: privatumo ir asmens duomenų apsauga
- Prisijungimas naudojant kelis faktorius
- Slapukai
- Suasmeninta reklama
- Rekomenduojami naršyklių nustatymai
- Privatus ir anoniminis naršymo režimas
- Turinio filtravimo programos
- Naudojimasis viešais kompiuteriais
- Saugiau naudokimės viešuoju belaidžiu internetu
- Socialinių tinklų ypatumai
- Facebook paskyros privatumo ir saugumo nustatymai
- Elkimės saugiau socialiniuose tinkluose
- Kaip pašalinti „Facebook“ paskyrą?
- Atsakingas informacijos publikavimas internete
- Atsakingas nuotraukų publikavimas
- Asmeninio pobūdžio nuotraukos ir vaizdo klipai
- Netiketas, e. laiškų etiketas ir atsakingas komentavimas
- Etiško bendravimo principai internete
- Kas yra dviejų faktorių autentifikacija?
- Kaip išvengti grėsmių internete?
- Vaikų apsauga, grėsmės internete
- Lina apie vloginimą ir elgesį internete
- Vaikų privatumas internete (I): Dalintis per daug
- Vaikų privatumas internete (II): Papildymas
- Vaikų privatumas internete (III): Justas
- Vaikų privatumas internete (IV): Darbo pokalbis
- Vaikai: pavojai internete
- Eksperimentas: ko tėvai nežino apie vaikus ir internetą?

4. KOMPIUTERIŲ IR IŠMANIŲJŲ ĮRENGINIŲ SAUGUMAS

Siekiant apsisaugoti nuo įvairių grėsmių, rekomenduojama nuolat atnaujinti savo įrenginių (kompiuterių bei išmaniųjų įrenginių) programas, programėles, kai įrenginys pasiūlo tai padaryti. Rekomenduojama naudoti antivirusinę programą. Taip pat rekomenduojama atlikti programų ir programėlių profilaktiką, pavyzdžiui, pašalinti nenaudojamas, patikrinti ar visos programėlės automatiškai atsisiuntė atnaujinimus ir pan.

Galimos grėsmės

Virusai

Virusas yra kenkėjiška programa, prisijungianti prie vykdomųjų failų arba failų, turinčių vykdomųjų komponentų (pvz., makroprogramų), gaminanti savo kopijas ir jomis užkrečianti kitus failus, galinti pažeisti sistemą, pažeisti arba sunaikinti duomenis, sutrikdyti programų darbą.

Trojanai, Trojos arkliai

Trojanas (Trojos arkliai) į skaitmeninius įrenginius gali patekti nekenksmingų programėlių pavidalu bei iš tikrųjų atlikti kenkėjišką darbą – gali sunaikinti arba sugadinti kompiuteryje esančius duomenis ir programas, rasti ir kam nors išsiųsti neskelbtiną informaciją.

Šnipinėjimo programos

Programa, be asmens žinios renkanti ir kam nors nusiunčianti jo asmeninius duomenis. Šnipinėjimo programa gali pažeisti įvairius privatumo lygius. Naršymo įpročiai paprastai nusiunčiami reklamos kompanijai, kuri ateityje pateikia tuos įpročius atitinkančią reklamą.

Iš kur atsiranda kenkėjiškos programos įrenginiuose?

Pateikiame keletą pavyzdžių, iš kur gali atsirasti kenkėjiškos programos įrenginiuose:

- „Užkrėstų“ programų diegimas įrenginiuose;
- Elektroninis paštas;
- Internetiniai puslapiai, netinkamo turinio svetainės ir pan.;
- Dokumentų apsikeitimo programos (torentai), failų saugyklos ir pan.

„Užkrėsto“ įrenginio požymiai

- Kompiuteris ar skaitmeninis įrenginys veikia lėčiau negu įprasta;
- Programos ar programėlės nuolat „užstringa“, įrenginys nuolat persikrauna;
- Negalima įprastai dirbti su dokumentais ir kitais failais, pvz., negalima atverti, pašalinti dokumentų, gali atsirasti naujų failų ar aplankų ir pan.;

- Neįprastai veikia antivirusinė programa, pvz., yra užboluota, nuolat išsijungia;
- Neįprastai iššokantys langai bei reklamos ar atsiradusios nepageidaujamos programėlės;
- Numatytųjų naršyklės nustatymų pakeitimas be jūsų žinios.

Kokių priemonių imtis norint apsisaugoti nuo virusų ir įsilaužimų?

- Naudokite antivirusinę programą;
- Neatidarykite nežinomų siuntėjų e. laiškų priedų;
- Sutikite su operacinės sistemos ir programų atnaujinimu, t. y. neignoruokite jo;
- Nespauskite įtartinų iššokančių langų;
- Nesilankykite svetainėse, kuriose pateikiamas netinkamas turinys ar nelegali informacija;
- Neatidarykite keistų nuorodų, kurios siunčiamos e. laiškais, socialiniais tinklais ar SMS žinutėmis;
- Darykite atsargines failų kopijas, kad esant reikalui būtų galima atstatyti duomenis.
- Diekite tik legalias programas ir programėles;
- Programėles diekite iš patikimų šaltinių, tokių kaip „Google Play“, „Apple Store“, „Windows Store“ ir pan.

Mobiliųjų įrenginių saugumas

Šioje dalyje pateikiame keletą patarimų siekiant apsaugoti mobiliuosius įrenginius.

- **Atidžiai diekite programėles**
  - Diegdami programėles, atidžiai sekite diegimo metu siūlomus parametrus ir prieš spausdami mygtuką „Accept“ („Sutinku“) arba „Install“ („Diegti“) atidžiai perskaitykite, su kuo sutinkate. Atkreipkite dėmesį, ar programėlei tikrai reikės jūsų tam tikros asmeninės informacijos ar prieigos prie tam tikrų programų, ar į įrenginio įtaisų.
- **Atjunkite nenaudojamas ryšių funkcijas**
- **Aktyvuokite PIN kodo ar kitos saugios prisijungimo funkcijos naudojimą**
  - Mobiliuosiuose įrenginiuose rekomenduojama aktyvuoti PIN kodo naudojimą kiekvieną kartą prieš naudojantis įrenginiu, kad nepageidaujami asmenys negalėtų naršyti jūsų įrenginyje, peržiūrėti asmeninių duomenų, nuotraukų ir pan., kai įrenginys paliekamas be priežiūros.
  - Kai kurie įrenginiai turi kitas saugias prisijungimo funkcijas, tokias kaip piršto antspaudo, akių rainelės skenavimas ir pan., kurias galima aktyvuoti.
- **Įjunkite šifravimą**
  - Duomenų šifravimo funkcija leidžia užšifruoti visus duomenis, įskaitant programėlių duomenis, atsisiųstus failus ir kitus duomenis. Ši funkcija ypač naudinga, jei įrenginys prarandamas, kadangi kitas asmuo negalės matyti prarastame įrenginyje esančių duomenų.
- **Darykite atsargines duomenų kopijas**
  - Kurkite atsargines duomenų kopijas, kopijuodami duomenis į išorinius įrenginius. Atsarginių duomenų kūrimas apsaugos jus nuo duomenų praradimo sugedus įrenginiui ar diskui, užkrėtus įrenginį virusu.
- **Galite pažymėti įrenginį policijoje**
- **Vagystės atveju kreipkitės į policiją bei ryšio operatorių**

Greitoji pagalba užkrėstam įrenginiui

- Naudokite skenavimo programas:
  - „Avira Rescue System“
  - „AVG Rescue CD“
  - „Dr.WEB LiveCD“
- Atstatykite gamyklinius įrenginio nustatymus.
- Nepavykus surasti sprendimų, kreipkitės į specialistus.

Slaptažodžiai

Slaptažodžiai yra viena iš labiausiai paplitusių apsaugos priemonių. Jie naudojami prieigai prie skaitmeninių įrenginių, prie juose saugomos svarbios informacijos, prie įvairių sistemų, tokių kaip e. paštas, e. parduotuvės ir pan. Slaptažodžiai kartu su vartotojo vardu leidžia vienareikšmiškai nustatyti vartotojo tapatybę.

Jūsų slaptažodis turi būti sunkiai nuspėjamas. Kuriant slaptažodžius patartina vadovautis keliomis rekomendacijomis:

- slaptažodyje turi būti panaudoti įvairių grupių ženklai:
  - didžiosios raidės (A, B, C, ...),
  - mažosios raidės (a, b, c, ...),
  - skaitmenys (1, 2, 3, ..., 9) ir
  - specialieji simboliai (!, <, @ ...);
- slaptažodis turi būti ne trumpesnis nei aštuoni ženklai (kai kuriose sistemose rekomenduojami ir ilgesni);
- slaptažodis neturi būti prasmingas žodis, pavyzdžiui, jūsų vardas, gimimo data ir pan.
- jei PIN kodas yra 4 skaitmenų derinys, jis taip pat neturi būti lengvai atspėjamas, neturi būti gimimo data ar kitas kitiems žmonėms žinomas skaičius. Kuo ilgesnis PIN kodas, tuo sunkiau jį atspėti.
- nenaudoti atskirų žodžių, ypač asmeniui ką nors reiškiančių, pavyzdžiui, „brangakmenis“ – asmeniui, kuris užsiima juvelyrika.
- nenaudoti artimųjų ar gyvūnų vardų, jų nerašyti su skaičiais, pavyzdžiui, elvyra123.
- nenaudoti skaičių sekų, jei tai nėra PIN kodas.

Negalima naudoti slaptažodžių, sudarytų iš asmenvardžių, adresų, telefono numerių ir kitų nesunkiai atspėjamų žodžių.

Negalima niekam atskleisti savo prisijungimo vardo ir slaptažodžio ar PIN kodo. Ne tik įprastiniuose kompiuteriuose, bet ir daugelyje išmaniųjų įrenginių galima sukurti kiekvienam asmeniui atskirą vartotoją, kuris naudotųsi tik jam vienam žinomu slaptažodžiu.

Kuriant slaptažodį, interneto svetainėse galima pasitikrinti slaptažodžių stiprumą ir kiek laiko užtruktų tokio slaptažodžio „atspėjimas“ naudojant specialią įrangą. Pateikiame keletą tokių svetainių pavyzdžių:

- www.passwordmeter.com – čia galima patikrinti slaptažodžio stiprumą (ties laukeliu „Score“ bus rodoma spalvinė juostelė, jei įvedus slaptažodį rodoma žalia spalva, slaptažodis stiprus, jei oranžinė – silpnas);
- https://howsecureismypassword.net – čia galima patikrinti, per kiek laiko slaptažodis galėtų būti „atspėjamas“ naudojant specialią įrangą.

Patarimas: tokiose ir panašiose sistemose nerašykite savo tikrų slaptažodžių. Galite sukurti labai panašų slaptažodį ir patikrinti jo stiprumą.

Deja šios svetainės yra pateikiamos anglų kalba. Norėdami išversti svetainėse pateikiamus tekstus ar terminus, galite naudoti „Google“ automatinės vertyklės paslaugą.

Netinkamų slaptažodžių pavyzdžiai:

- namas25
- Jonas1975
- Margis
- Slaptažodis
- 123456
- 987456
- iloveyou
- saulytė
- qwerty
- 1111

Slaptažodžių tvarkymo rekomendacijos

- Niekam neatskleiskite savo slaptažodžio. Niekada niekam nesakykite savo prisijungimo prie bet kokios sistemos vardo ir slaptažodžio.
- Skirtingose interneto svetainėse naudokite skirtingus slaptažodžius.
- Dėl didesnio saugumo slaptažodžius periodiškai keiskite.
- Niekada nesaugokite prisijungimo prie sistemų duomenų užrašų knygutėse, kompiuterių failuose ar išmaniuosiuose įrenginiuose.
- Naudokite kelias pašto dėžutes skirtingiems tikslams, pavyzdžiui, name.surname@comapny-name.com – darbui, o name.surname@gmail.com – asmeniniam naudojimui.

Daugiau informacijos rasite žemiau pateiktame sąraše (paspaudus nuorodą, bus atveriamas vaizdo įrašas arba svetainė):

- Kenkėjiškos kompiuterinės programos, netinkamas turinys
- Kompiuterių virusai
- Mobilieji virusai
- Išmanusis telefonas: galimybės ir informacijos apsauga kur atsiranda virusai
- Virusų ir šnipinėjimo programų požymiai
- Kaip apsisaugoti nuo galimų virusų ir įsilaužimo
- Antivirusinės nemokamos programos
- Kodėl reikia atnaujinti programinę įrangą?
- Greitoji pagalba apkrėstam kompiuteriui
- Kaip sužinoti ar slaptažodis stiprus?
- Kaip apsaugoti mobiliuosius įrenginius?
- Mobiliųjų įrenginių saugumas

5. REKOMENDACIJOS KAIP BŪTI SAUGESNIAM

Internete elkitės atsakingai

- Venkite P2P programų (pvz., torentų) naudojimo ir failų dalinimosi naudojant šias programas.
- Siųskitės tik legalias programas, muziką, filmus ir kitus legalius dokumentus.
- Aiškinkite vaikams apie e. saugą internete.
- Venkite naršyti puslapiuose, kurių turinys atrodo įtartinas, žinokite, kad programų serijiniai kodai nėra nemokamai skelbiami įtartino turinio svetainėse.
- Venkite sandorių, pagal kuriuos galite lengvai uždirbti ir pan.
- Atsakingai naudokite e. paštą.

Laikykitės organizacinės apsaugos taisyklių

- Jungdami įrenginį prie įmonės ar kitos organizacijos tinklo, laikykitės organizacinės apsaugos taisyklių.
- Atminkite, kad įjungtas įrenginys, paliktas be priežiūros, gali sukelti grėsmę tiek pačiam įrenginiui, tiek tinklui, prie kurio yra prijungtas įrenginys.

Kitos rekomendacijos

- Banke nustatykite finansinių operacijų apribojimus, nuolat stebėkite banko išrašus, ar nėra pirktų pirkinių ar paslaugų, kurių nepirkote ar pavedimų, kurių nedarėte.
- Saugokite asmeninius duomenis, nepublikuokite jų internete, be reikalo neatskleiskite asmeninės informacijos nežinomiems asmenims.

Daugiau informacijos rasite žemiau pateiktame sąraše (paspaudus nuorodą, bus atveriamas vaizdo įrašas arba svetainė):

- Kaip išvengti grėsmių internete?
- Kaip saugiai naudotis programėle „WhatsApp“
- Kaip saugiai naudotis programėle „Viber“
- Kaip saugiai naudotis programėle „Instagram“
- Kaip saugiai naudotis programėle „Facebook Messenger"
- Kaip saugiai naudotis programėle „Snapchat"
- Ką daryti, jei įvyko incidentas?
- Interneto karštoji linija
- Įvykių ar incidentų pranešimas
- Pranešimas apie šlamšto e. laiškus „Gmail“ aplinkoje,
- Asmens e. laiškų blokavimas
- Kaip išjungti „Google“ duomenų rinkimą?
- Ką daryti, jei buvo įsilaužta į pašto dėžutę?
- Ką daryti praradus „Facebook“ paskyrą
- Švaresnis internetas: kaip pranešti apie žalingą turinį internete?