

BŪKIME SAUGŪS INTERNETE

LUKAS MISIUKEVIČIUS

LUKAS.MISIUKEVICIUS@KNF.VU.LT

2022, Kaunas

DUOMENŲ APSAUGA

Šiandien didelė dalis kasdienio gyvenimo vyksta elektroninėje erdvėje. Čia užsukame rasti informacijos, apsipirkti, užsisakyti įvairių paslaugų ir, aišku, pabendrauti, susipažinti su įdomiais žmonėmis. Internetu, taip pat kaip ir įprastiniame pasaulyje reikia elgtis atsargiai ir protingai, mokėti apsaugoti savo duomenis ir privatumą, skirti tikrą informaciją nuo apgaulės.

Šiandien susipažinsime su duomenų ir privatumo apsauga internete, išmoksime sudaryti saugius slaptažodžius, susipažinsime su pagrindiniais žingsniais, kuriuos reikia turėti galvoje naudojantis internetu.

DISKUSIJA

Kokiomis veiklomis dažniausiai užsiimate internete?

Kaip dažnai jaučiatės kad esate saugūs ir pilnai savimi pasitikite?



POPULIARŪS MITAI

„Stipraus slaptažodžio užtenka apsaugoti informaciją“

„Nusikaltėlius domina ir jų taikiniai tampa tik verslo įmonės arba turtingi fiziniai asmenys“

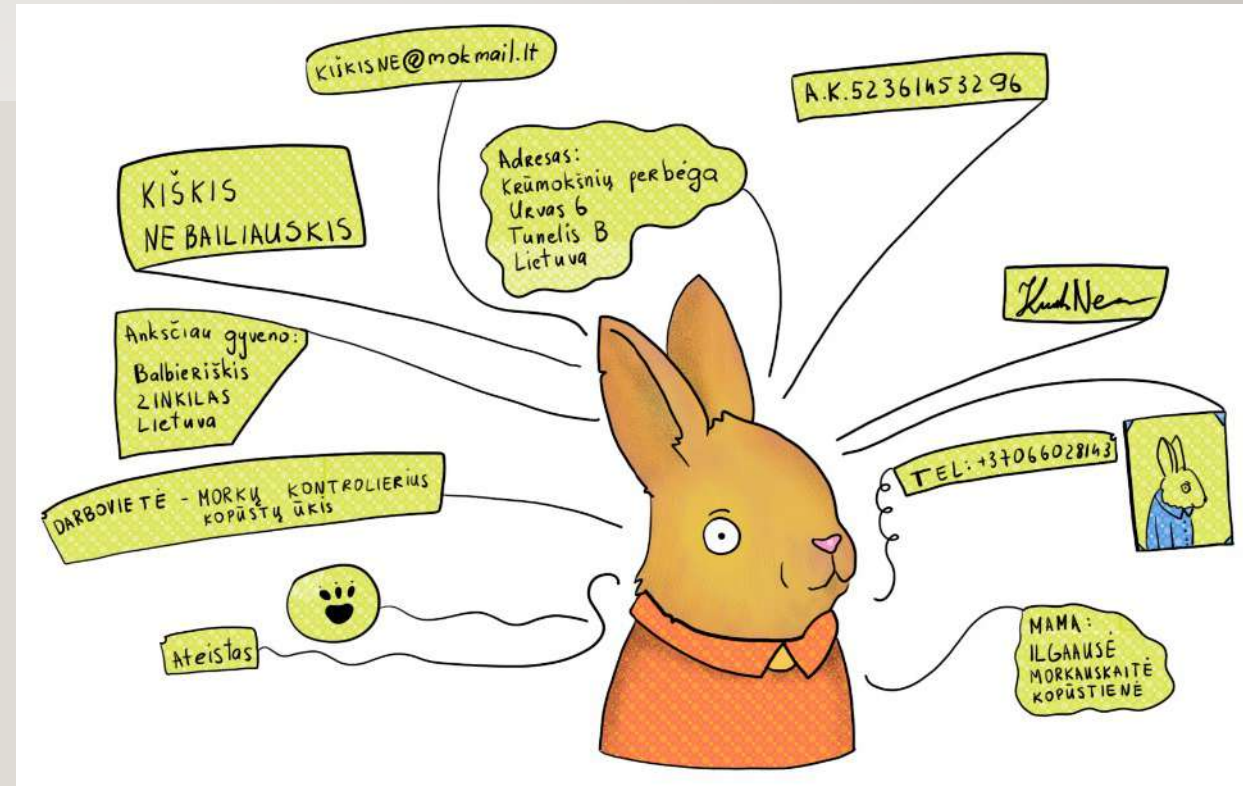
„Programinė įranga (antivirusinė, ugniasienė) patikimai apsaugo kompiuterį nuo įsilaužimų“



ASMENS DUOMENYS

Asmens duomenys – tai bet kuri informacija apie žmogų, iš kurios galima jį pažinti ar nustatyti jo tapatybę.

- Vardas, pavardė, asmens kodas, pilietybė
- Gyvenamosios vietos adresas
- Išsilavinimas, pajamos, turto duomenys
- Susijusių šeimos narių duomenys
- Ir kita...

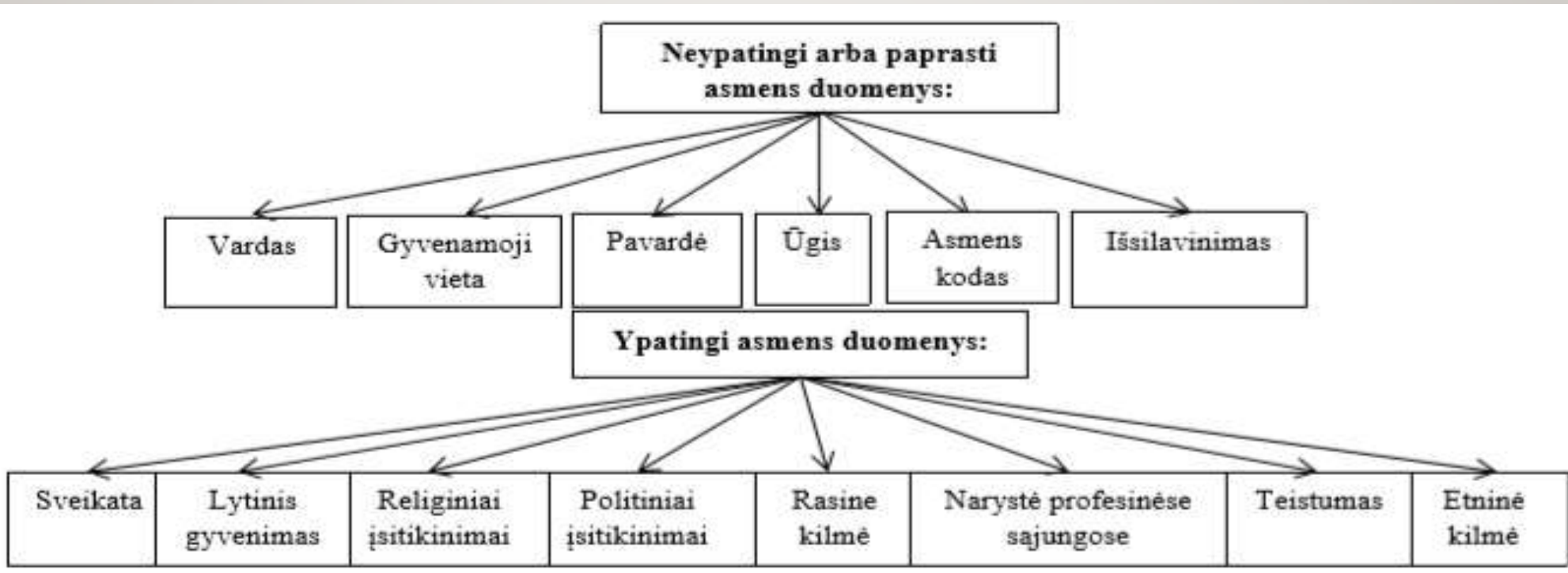


ASMENS DUOMENYS

Savo asmens duomenis pateikiame, kai norime gauti tik mums skirtų paslaugų, apsipirkti internetu, kreiptis į „Sodrą“, banką, įsidarbinti ir panašiai. Nei savo, nei kitų žmonių asmens duomenų negalima skelbti viešai, nei interneto svetainėse, nei socialiniuose tinkluose, nes jais piktam gali pasinaudoti kiti asmenys.

Kitų žmonių nuotraukas, vaizdo įrašus galima viešai skelbti tik turint jų sutikimą. Nepilnamečių nuotraukas skelbti galima tik sutinkant jų tėvams ar globėjams.

YPATINGI ARBA NEYPATINGI ASMENS DUOMENYS



ASMENS DUOMENŲ APSAUGA

Kaip turi būti teikiami ir saugomi asmens duomenys, Europos Sąjungoje nustato Bendrasis duomenų apsaugos reglamentas (BDAR) ir atitinkami šalių apsaugos įstatymai.

Jūsų asmens duomenys gali būti renkami ir tvarkomi tik gavus jūsų sutikimą, kai šie duomenys **būtini** paslaugai teikti ar prekėms pristatyti, švietimo ir sveikatos priežiūros paslaugoms teikti, bei kitais įstatymų numatytais atvejais.

Ar sutinkate, kad organizacija tvarkytų šiuos jūsų asmens duomenis?

☒ Sutinku

Vard. Pavardaitis

☐ Nesutinku

DISKUSIJA

- Ar fizinės parduotuvės darbuotojas gali prašyti jūsų telefono numerio?
- Ar apsiperkinėjant elektroninėje parduotuvėje jums būtina pateikti savo gimimo datą?

ASMENS DUOMENŲ TVARKYMAS

Jūsų asmens duomenys yra jūsų nuosavybė. **Jūs turite teisę:**

- Susipažinti su surinktais jūsų duomenimis
- Reikalauti pataisyti duomenis
- Reikalauti pašalinti duomenis
- Nesutikti, kad jūsų duomenys būtų naudojami
- Reikalauti perkelti duomenis
- Reikalauti būti pamirštiems

PASIKARTOKIME

- Kas yra asmens duomenys?
- Ar galima asmens duomenis skelbti viešai? Kodėl?
- Ar galima prašyti, jog asmens duomenys būtų ištrinti?
- Koks įstatymas atsakingas už asmens duomenų tvarkymą?

KLAUSIMAI?



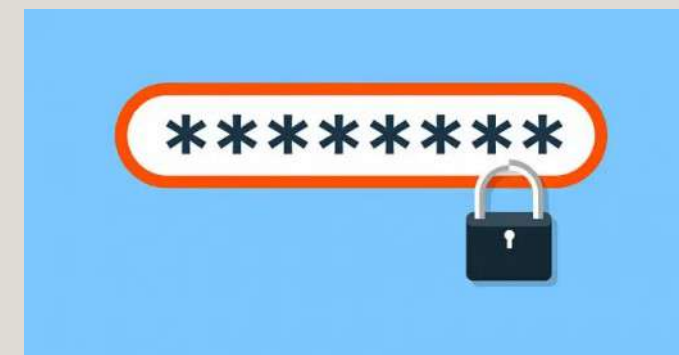
SKAITMENINĖ TAPATYBĖ

Skaitmeninė tapatybė – informacija, iš kurios skaitmeninėje erdvėje galima atpažinti prisijungusį vartotoją. Tai gali būti vartotojo asmens duomenys, jo prisijungimų prie svetainių duomenys, slaptyvardžiai ir panašiai. Skaitmeninė tapatybė gali būti pavogta, suklastota, pavyzdžiui, prisijungus prie svetimos elektroninio pašto paskyros siųsti laiškus jūsų vardu ar juos skaityti, todėl reikia rūpestingai ją saugoti.

Prie įvairių svetainių, elektroninių parduotuvių vartotojai jungiasi pateikdami savo **vartotojo vardą** ir tik jiems žinomą **slaptažodį**. Ten, kur reikia didesnio saugumo, naudojamas elektroninis arba mobilusis parašas, kitos saugios priemonės.

SLAPTAŽODŽIAI

Slaptažodis – tai pagrindinė autentifikavimo priemonė, skirta tam, kad tik įgalioti asmenys galėtų pasiekti jiems skirtą informaciją. Kad ir kaip būtų sunku atsiminti visus slaptažodžius ir skaičių kombinacijas, reikia nepamiršti, jog būtent jie saugo jūsų asmeninius duomenis nuo pašalinių asmenų. Kuo slaptažodis ilgesnis ir sudėtingesnis, tuo jis tampa stipresnis, todėl natūralu, kad jį sunkiau atspėti.



SUDĖTINGAS SLAPTAŽODIS

- Slaptažodis netrumpesnis nei 12 simbolių
- Naudojamos didžiosios raidės, mažosios raidės, skaitmenys bei specialieji simboliai
- Slaptažodis turi būti unikalus ir daugiau niekur kitur nenaudojamas

<u>REITINGAS</u>	<u>SLAPTAŽODIS</u>	<u>LAIKAS IKI NULAUŽIMO</u>
1	123456	< 1 Sekundę
2	kilobaitas	6 Dienos
3	123456789	< 1 Sekundę
4	lopas123	4 Sekundžių
5	labas123	9 Sekundžių
6	123123	< 1 Sekundę
7	Matttt24	2 Valandos
8	nesakysiu	7 Sekundžių
9	samsung	< 1 Sekundę
10	kompas	5 Sekundžių
11	kaktusas	1 Minutė
12	qwerty	< 1 Sekundę
13	lietuva	3 Sekundžių
14	slaptazodis	4 Mėnesiai
15	katinas	8 Sekundžių

Top 15 dažniausiai naudotų slaptažodžių Lietuvoje 2023 m.

SUDĖTINGAS SLAPTAŽODIS

<https://www.passwordmonster.com>



DISKUSIJA

- Kaip įsiminti sunkius slaptažodžius?

SUDĖTINGAS SLAPTAŽODIS

- Neatskleiskite slaptažodžių niekam – nei policijai, nei banko darbuotojams, nei savo artimiesiems.
- Įsiminkite slaptažodžius, neužsirašykite jų, nesiųskite laiškuose.

Niekas niekada neturi teisės jūsų prašyti atskleisti savo slaptažodžius ar kitus prisijungimo duomenis. Nei „Sodros“, nei banko, nei policijos, nei kitų įstaigų darbuotojai.

Įsiminti slaptažodžius bus paprasta, jei juos susiesite su kokiomis nors frazėmis.

Pl6anperE!

Plaukia 6 antelės per Ežerėlį!

SUDĖTINGAS SLAPTAŽODIS

Yra nemokamų programų, kurios padeda sukurti, įsiminti ir įvesti slaptažodžius.

Ieškokite internete, pavyzdžiui „LastPass“, „NordPass“ ir panašiai.

Jos kiekvienos registracijos metu jums sukurs sunkų ir unikalų slaptažodį, kurį išsisaugos ir jums nereikės jo įsiminti. Jums tereikės įsiminti vieną stiprų slaptažodį, kad galėtumėte prisijungti prie šios programos.

UjHR^g^96c@0

Customize your password

Password Length

12

☐ Easy to say

☐ Easy to read

☒ All characters

☒ Uppercase

☒ Lowercase

☒ Numbers

☒ Symbols

UjHR^g^96c@0

Very Strong

12 characters containing: Lower case Upper case Numbers Symbols

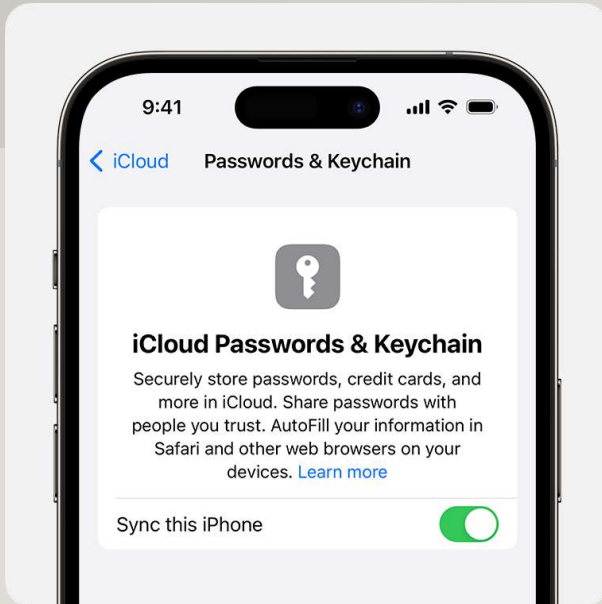
Time to crack your password:
292 million years

STIPRUS SLAPTAŽODIS

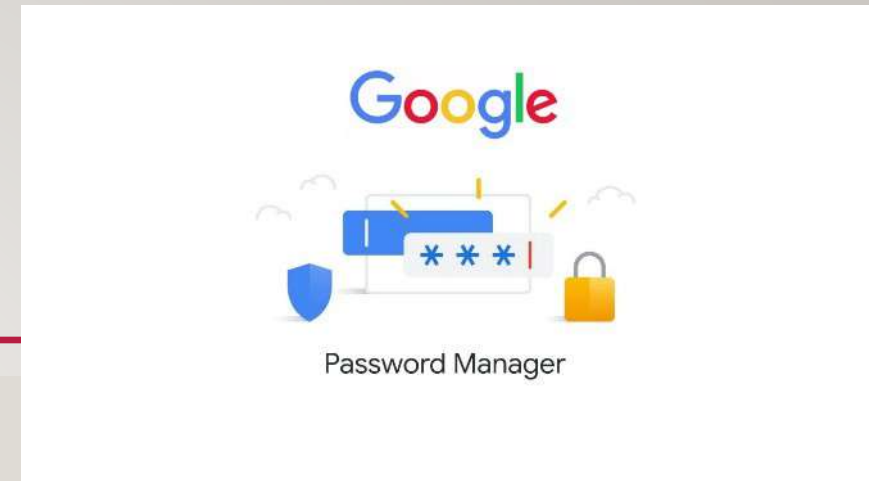
PATARIMAI

- Keiskite slaptažodį kartą ar kelis metuose – tokiu būdu apsisaugome nuo to, jei slaptažodžius sužinojo pašaliniai
- Nesijunkite prie svarbių paskyrų naudodamiesi svetimus ar viešus kompiuterius, o jeigu teko prisijungti, iškart pakeiskite slaptažodį per savo asmeninį kompiuterį

SLAPTAŽODŽIŲ TVARKYKLĖS



- [LastPass](#)
- [NordPass](#)
- [Google Password Manager](#)
- [iCloud Keychain](#)



DISKUSIJA

- Kokie yra papildomi apsaugos būdai?

DVIEJŲ ŽINGSNIŲ AUTENTIFIKAVIMAS

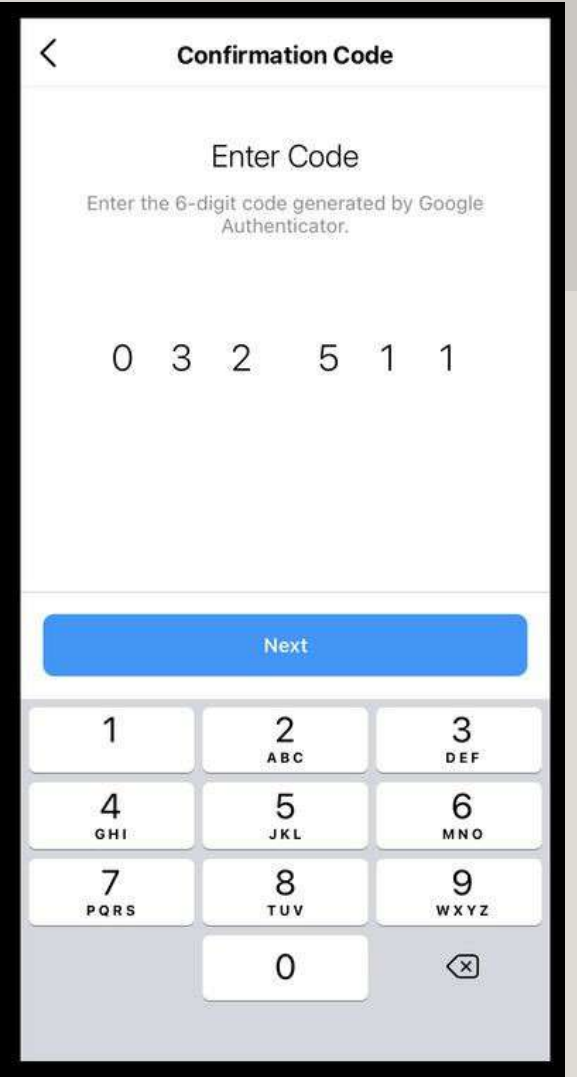
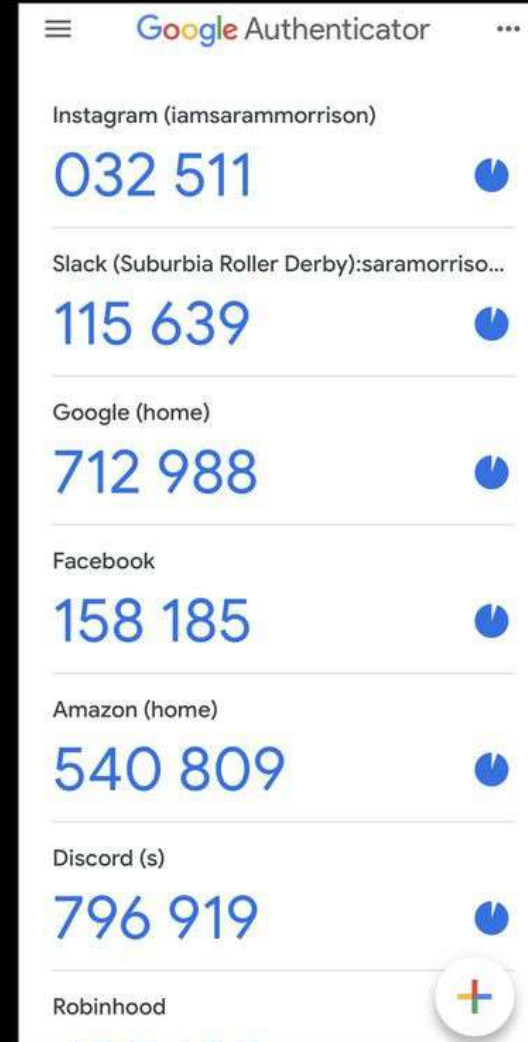
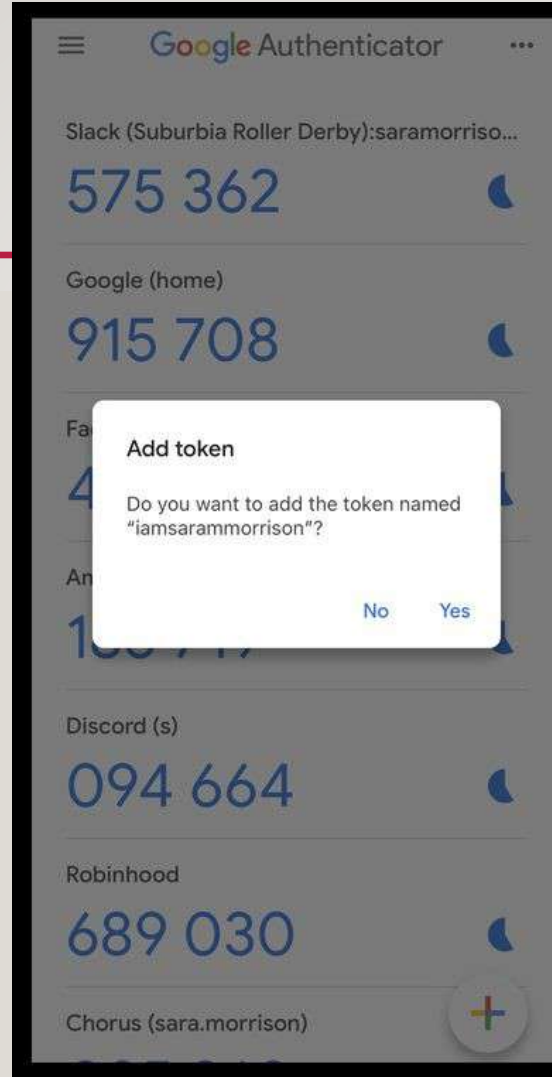
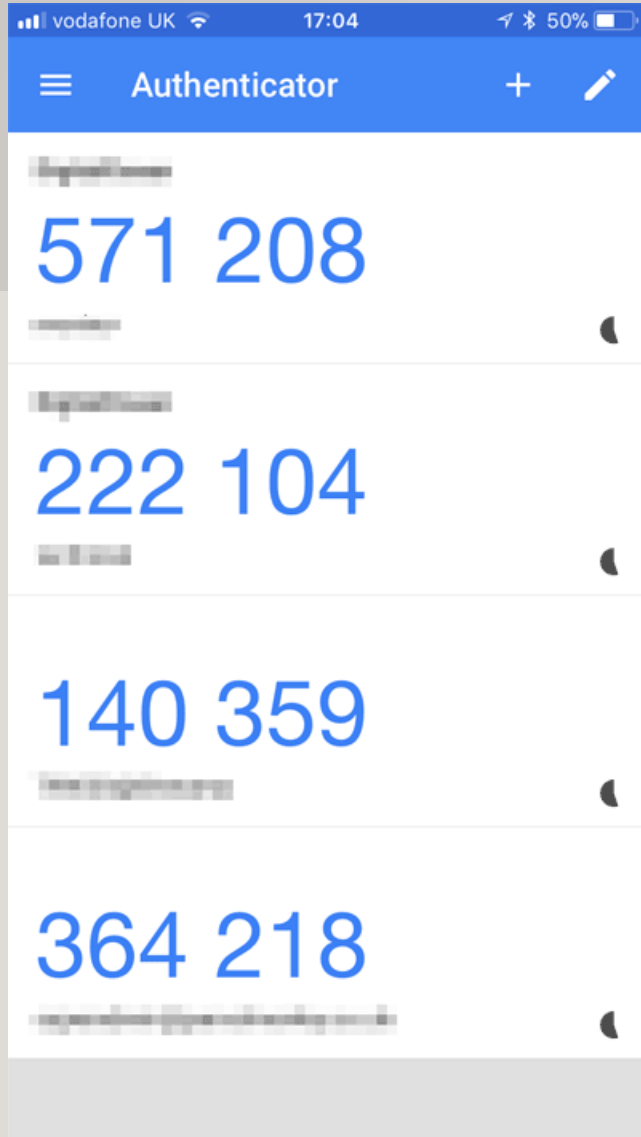
Dviejų žingsnių autentifikavimas – tai prisijungimo procesas, kuris reikalauja ne tik prisijungimo vardo ir slaptažodžio, bet kartu ir papildomo autentifikacijos būdo.

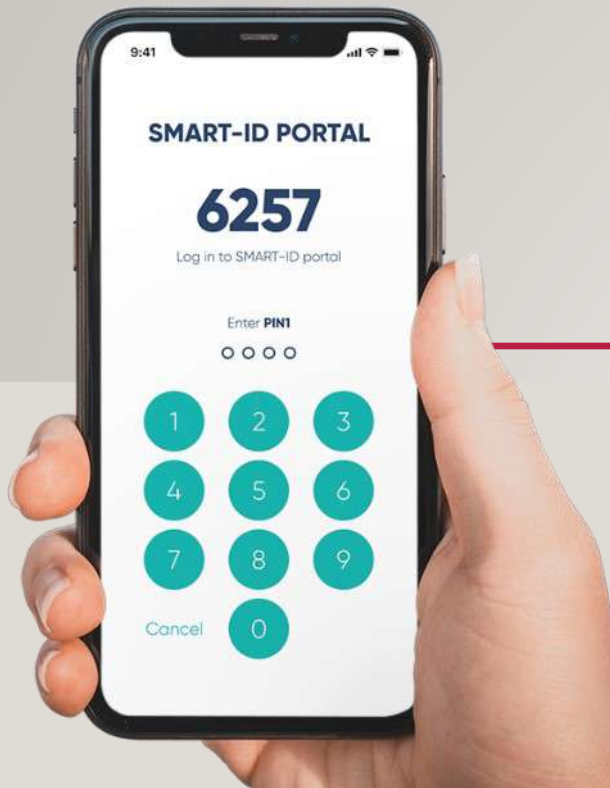
Egzistuoja trys pagrindiniai autentifikacijos būdai:

- Tai, ką jūs žinote: slaptažodis, PIN, paskyros numeris ar bet kokia kita skaitmenų ar raidžių seka
- Tai, ką jūs turite: USB saugos raktas, telefonas ar bet kokia kita technologija kurią galite turėti fiziškai
- Tai, kuo esate: jūsų pirštų antspaudas, akies, veido atvaizdas arba tiesiog – biometriniai duomeys

DVIEJŲ ŽINGSNIŲ AUTENTIFIKAVIMAS

Norint naudoti dviejų žingsnių autentifikaciją, būtina naudoti bent 2 iš 3 anksčiau paminėtų autentifikavimo būdų. Prisijungimui prie sistemų rekomenduojama visada naudoti dviejų žingsnių autentifikaciją, jeigu toks funkcionalumas įgalintas. Tai ženkliai padidins jūsų duomenų saugumą.





PASIKARTOKIME

- Kas yra skaitmeninė tapatybė ir kodėl ją reikia saugoti?
- Koks slaptažodis yra stiprus, o koks silpnas?
- Kaip įsiminti sunkius slaptažodžius?
- Kam galima atskleisti savo slaptažodžius?
- Kokie gali būtų dviejų žingsnių autentifikacijos būdai?

KLAUSIMAI?



SAUGUS ELGESYS INTERNETE

Kaip ir realiame pasaulyje, internete susiduriame su įvairiausiais žmonėmis, tik interneto anonimiškumas sudaro didesnes galimybes apsimesti kitu asmeniu, skleisti netikrą informaciją, išvilioti duomenis, gundo elgtis neetiškai. Todėl labai svarbu saugiai elgti internete, sugebėti laiku atpažinti netikrą informaciją bei įtartina elgesį.



SOCIALINIAI TINKLAI

Socialiniuose tinkluose žmonės bendrauja, buriasi į bendruomenes, dalijasi informacija lygiai taip pat, kaip ir realiame gyvenime. Užsiregistravę socialinių tinklų vartotojai gali įkelti nuotraukas ar vaizdo įrašus, skelbti informaciją apie pomėgius ar rašyti savo tinklaraštį, vertinti ir komentuoti kitų vartotojų įrašus, jungtis į interesų grupes. Visa tai sukuria bendrumo su kitais žmonėmis ir jų pripažinimo pojūtį.



DISKUSIJA

- Ar naudojate socialinius tinklus?
- Kodėl?

SOCIALINIAI TINKLAI

Socialiniu tinklu „Facebook“ Lietuvoje naudojasi daugiau nei 2,1 milijono šalies gyventojų ([šaltinis](#)). Tai populiariausias socialinis tinklas mūsų šalyje, kurį mėgsta vyresni asmenys. Facebook'o vartotojai savo paskyrose gali pateikti nemažai informacijos apie save – ne tik vardą ir pavardę, bet ir daugiau gyvenimo faktų – gimtąjį miestą, adresą, mokyklą, kurią baigė, darbovietę ir pan. Kokią papildomą informaciją skelbti – tai vartotojo asmeninis pasirinkimas. Nuotrauka taip pat yra nebūtina.

Tokios plačios galimybės, kai jos netinkamai naudojamos, be abejo, gali sukelti įvairias grėsmes. Jūsų paskyroje skelbiama informacija gali patekti ne tiems asmenims, kuriems yra skirta.

SOCIALINIAI TINKLAI

Facebook'e kitus vartotojus galima priimti į draugus, ir tada ne tik su jais keisitės informacija, bet ir su jums nepažįstamais šių draugų draugais, tarp kurių gali pasitaikyti ir visai niekam nežinomų ar suklastotų paskyrų vartotojų. Lygiai tas pats atsitiktų ir jei jūs priimtumėte į draugus kokį nors nepažįstamąjį.



SOCIALINIAI TINKLAI

- Prieš skelbdami bet kokią informaciją, gerai pagalvokite
- Apribokite ratą vartotojų, kurie mato jūsų informaciją
- Nepriimkite į savo draugus nepažįstamųjų
- Pasitikrinkite, kokią informaciją kiti vartotojai mato jūsų paskyroje

Patarimai kaip naudoti facebook ir kokius privatumo nustatymus pakeisti - [čia](#)



Išvykome atostogų
savaitei, bute liko tik
kaktusas!

KAS NEGERAI ŠIOJE
NUOTRAUKOJE?



Kaip supratote, labai neatsargu skelbti tokią informaciją, kuria galėtų pasinaudoti piktavaliai. Spauldoje dažnai pasirodo pranešimų apie vagystes pasinaudojus informacija, aptikta socialiniuose tinkluose

SOCIALINIAI TINKLAI

Nepilnamečiui klaipėdiečiui socialiniame tinkle paskelbus apie išvykimą iš buto, vagys įsibrovė į jo tėvo butą ir pavogė nemažai daiktų.

SOCIALINIAI TINKLAI

Internete galioja tos pačios bendravimo taisyklės, kaip ir realiame gyvenime. Pašnekovą reikia gerbti, tuomet galime tikėtis ir atsakomosios pagarbos.

Pagrindinės bendravimo taisyklės:

- Gerbkite kitus
- Elkitės etiškai
- Taupykite kitų žmonių laiką
- Valdykite savo jausmus, nesivelkite į ginčus ir jų nekurstykite
- Nepiktnaudžiaukite savo teisėmis ir būkite atlidūs suklydusiems

SOCIALINIAI TINKLAI

Pavyzdžiui, gavus įžeidžiančia žinutę, nereikėtų skatinti konflikto – geriausia būtų į ją neatsakyti ir viešai nereaguoti. Kiekviename socialiniame tinkle yra galimybė patiems užblokuoti nepatinkamus vartotojus.

PASIKARTOKIME

- Kaip reikia elgtis su savo duomenimis socialiniuose tinkluose?
- Ar galima nustatyti kokią informaciją, kas matys jūsų skelbiamą informaciją?
- Ar galima priimti nepažįstamus žmones į draugus?

KLAUSIMAI



SUKČIAI IR MELAGINGA INFORMACIJA

Dažnai atrodo, kad melaginga informacija, melagingos naujienos internetu plinta dar greičiau nei tikros žinios. Kai kuriose svetainėse, ypač socialiniuose tinkluose susidaro tarsi informaciniai burbulai, kuriuose vartotojai keičiasi netikra informacija ir neįsileidžia tikrovės.

Ypač daug melagienų pasklinda svarbių valstybės ar pasaulio politinių įvykių metu – prieš rinkimus, referendumus, tarptautinių sutarčių sudarymo išvakarėse. Taip dažniausiai priešiškos valstybės stengiasi viena ar kita kryptimi paveikti kitų valstybių viešąją ar atskirų piliečių nuomonę.



12 KRITINIO MĄSTYMO PATARIMŲ

1 Įvertinkite informacijos aplinką

- Kas konkrečiai paskelbė informaciją?
- Ar tai patikima žiniasklaidos priemonė?
- Kokios rūšies informacija vyrauja šioje žiniasklaidos priemonėje?
- Naujienų, mokslo, skandalų, humoro?
- Ar jums žinoma patikima spauda cituoja šią žiniasklaidos priemonę?

2 Įvertinkite informacijos autorių

- Ar nurodytas informacijos autorius?
- Ar tai realus asmuo?
- Ką dar jis yra paskelbęs?
- Kur šis autorius skelbia informaciją, ar tai patikima žiniasklaida?
- Ar kiti šio autoriaus tekstai yra panašaus stiliaus ir turinio?

3 Įvertinkite informacijos šaltinius

- Ar nurodyta, iš kur gauta informacija?
- Ar tikrai yra tokie asmenys arba šaltiniai?
- Ar patikimi cituojami asmenys?
- Ką dar jie yra paskelbę šia tema?
- Ar patikimi cituojami šaltiniai?
- Kokiomis temomis informacija juose skelbiama?

4 Pasitikrinkite kituose informacijos šaltiniuose

- Ar šią informaciją skelbia kiti, žinomi ir patikimi kanalai?
- Ar informacija skirtinguose šaltiniuose iš esmės sutampa, nėra pakeista ar iškraipyta?
- Ar labai nesiskiria informacijos paskelbimo data skirtinguose šaltiniuose?

5 Neplatinkite nepatikimos informacijos

- Pagalvokite prieš persiųdami ar skelbdami kitų asmenų informaciją.
- Neplatinkite apgaulingų laiškų, paramos prašymų, įspėjimų apie virusus ir pan.
- Neplatinkite žinučių, kuriose prašoma jas persiųsti kitiems.

6 Nepasiduokite spaudimui

- Ypač kritiškai vertinkite raginimus skubiai ką nors daryti.
- Nepasiduokite gąsdinimui.
- Prieš spausdami nuorodas, pateikdami informaciją, – pagalvokite.
- Nepateikite bet kam svarbių duomenų.
- Net banko darbuotojai neturi teisės reikalauti slaptažodžių.
- Jei kilo įtarimas, paskambinkite į banką.

7 Suabejokite

- Gavote žinutę apie laimėjimą, bet ar toje loterijoje žaidėte?
- Draugas žinute prašo pervesti jam pinigų. Ar tikrai? Paskambinkite paklausti!
- Nepažįstamasis siūlo pasidalyti jo tetos palikimą. Kodėl jums? Kodėl pasidalyti?
- Laimėjote kelionę! Galbūt. Bet kodėl turite dar kažką privalomai pirkti ir mokėti pinigus?

8 Nesidalinkite informacija, kuria galėtų pasinaudoti įsilaužėliai

- Neskelbkite viešai savo ir artimųjų dienotvarkės, planų, pomėgių, bet kokios informacijos, kuri leistų atspėti prisijungimų duomenis ir saugumo klausimus.
- Neišmeskite senų skaitmeninių įrenginių, jei juose buvo laikoma kokia nors informacija.

9 Įvertinkite, ar informacija nėra šališka

- Pirmenybę visada teikite faktams, ne nuomonėms.
- Ar nurodyta, kieno tai nuomonė?
- Ar tai tikras asmuo, ir ar jis turi autoritetą šioje srityje?
- Kas gali nulemti tokią nuomonę: faktai, ar asmeninės priežastys?
- Ar pateikiamus faktus galima patikrinti?

10 Elkitės apgalvotai socialiniuose tinkluose

- Prieš ką nors paskelbdami – pagalvokite dukart.
- Nespauskite nuorodų, reklamų, testų ir pan.
- Nepriimkite į draugus nežinomų asmenų.
- Savo paskyroje nepateikite daugiau savo duomenų, nei būtina. Išjunkite vietos žymes.
- Apribokite savo paskyros matomumą.

11 Nepasitikėkite bet kuo socialiniuose tinkluose

- Venkite netikrų paskyrų. Patikrinkite abejotinų paskyrų draugų sąrašą ir kokio pobūdžio informacija ten skelbiama.
- Net ir gerų draugų pakartota informacija gali būti netikra.
- Nepasiduokite raginimams ką nors skubiai daryti.
- Neskelbkite savo ir kitų privačios informacijos.

12 Būkite atsargus socialiniuose tinkluose

- Neskelbkite itin asmeniškų nuotraukų.
- Venkite neįprastų, keista kalba parašytų žinučių.
- Prieš ką nors spausdami, pagalvokite.
- Žinokite, kad ką nors priimdami į draugus, leidžiate jam matyti ir skelbti informaciją jūsų paskyroje.

SOCIALINĖ INŽINERIJA

Pasitelkdami melagingą informaciją, interneto sukčiai bando manipuliuoti žmonėmis ir priversti juos neatsakingai elgtis. Pavyzdžiui, atskleisti savo slaptažodį, persiųsti slaptą dokumentą ar tiesiog sumokėti pinigų. Norint valdyti žmones, svarbu ne tiek technologijos, kiek žinios apie žmonių psichologiją. Tokie veiksmai bendrai vadinami socialine inžinerija.

Piktadariai dažnai veikia kaip telefoniniai sukčiai – duomenis išgauna naudodami tam tikrus sugalvotus scenarijus ir turėdami pradinių žinių (vardą, pavardę, amžių, adresą ir pan.), apsimesdami kitais asmenimis (banko, socialinės įstaigos atstovais), pasinaudodami smalsumu, noru uždirbti, kitomis žmogiškomis savybėmis.



SOCIALINĖ INŽINERIJA

Internete kartais galite susidurti su ryškiais pranešimais, skelbiančiais, kad laimėjote kokioje nors loterijoje. Tai dažniausiai elektroninių sukčių spąstai, kad susivilioję prizais vartotojai užsuktų į virusais užkrėstas svetaines, įvestų savo asmens duomenis, nurodytų elektroninį paštą ar kitus, ypatingus duomenis. Vėliau ši informacija gali būti panaudota piktavališkiems kėslams.

Elektroniniu paštu taip pat galite gauti panašių pranešimų. Apgaulinguose laiškuose dažnai prašoma pateikti savo duomenis, ar asmeninę informaciją. Nesusigundykite viliojančiais internetiniais laimėjimais ar lengvu uždarbiu. Nekreipkite dėmesio į tokio pobūdžio reklaminius pranešimus, o nepageidaujamus laiškus iškart pašalinkite.



SOCIALINĖ INŽINERIJA

Atminkite, jokie bankai, jokios valstybinės įstaigos niekada nereikalauja slaptažodžių ir kitos konfidencialios informacijos pateikti elektroniniu paštu ar telefonu. Jei kyla įtarimas, paskambinkite tos įstaigos darbuotojams oficialioje jos svetainėje pateiktu numeriu.

DISKUSIJA

- Kaip manote, kodėl gaunate nepageidaujamus laiškus, SMS žinutes ar skambučius?

PASIKARTOKIME

<https://www.prisijungusi.lt/ar-mastote-kritiskai/>

KLAUSIMAI?



ŠALTINIAI

- https://www.nksc.lt/doc/biuletiniai/NKSC_Slaptazodziu_saugumo_biuletenis.pdf
- <https://www.epilietis.eu/temos/tema-1/>
- <https://www.epilietis.eu/temos/tema-2/>
- <https://www.passwordmonster.com>
- <https://www.lastpass.com/features/password-generator>
- <https://www.prisijungusi.lt/ar-mastote-kritiskai/>
- <https://www.prisijungusi.lt/savarankiskas-mokymasis/12-kritinio-mastymo-patarimu/>