



Funded by the
Erasmus+ Programme
of the European Union

Kibernetinių atakų atpažinimas ir apsauga

Prevencinės priemonės

Safeguarding against Phishing in the age of 4th Industrial Revolution

www.cyberphish.eu

This project has been funded with support from the European Commission.

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



Mokymosi tikslai



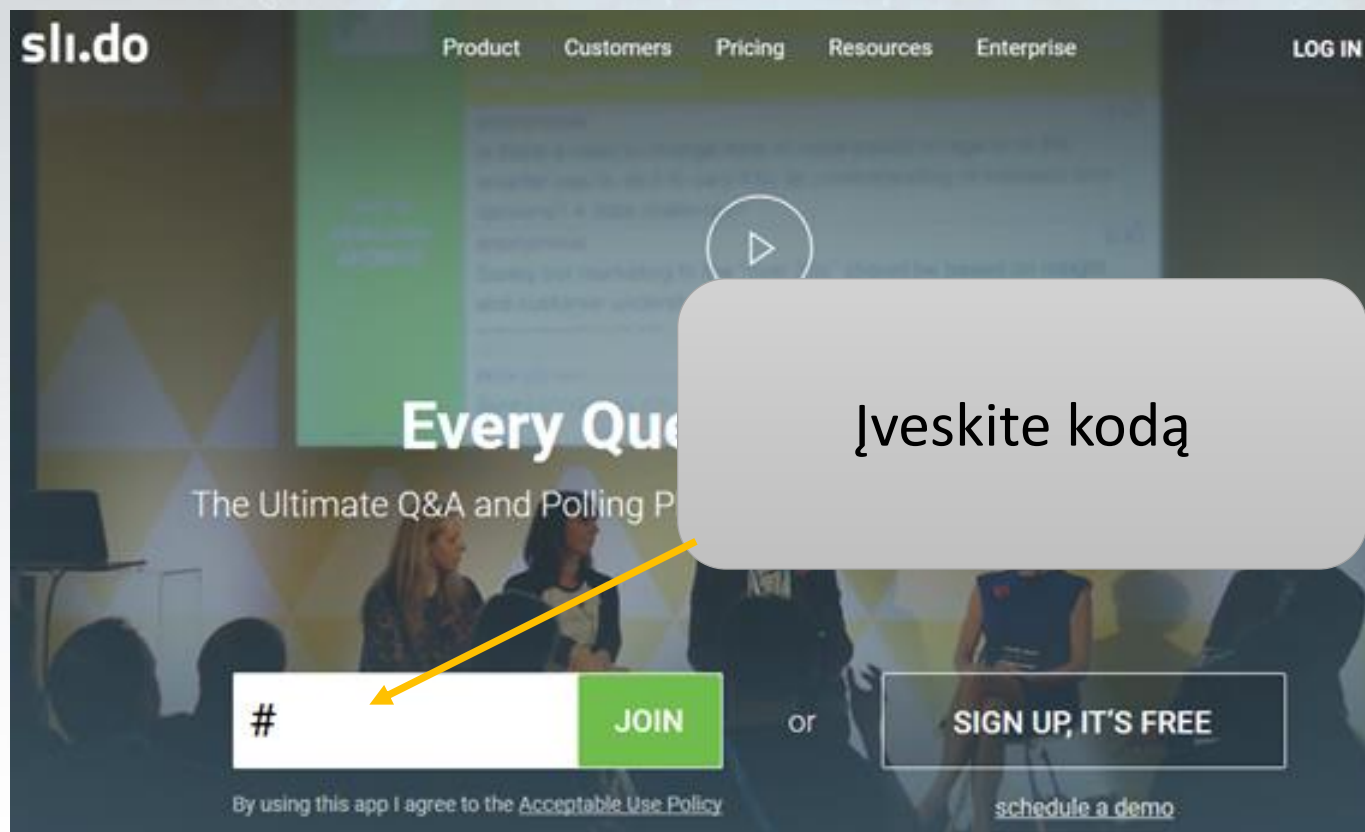
Kibernetinė higiena internete
Kibernetinė higiena darbo vietoje
Speciali įranga ir technologijos

Studento darbo krūvis



Paskaita	2 val.
Garso ir vaizdo medžiaga	1 val.
Panaudojimo atvejai	0,5 val.
Papildomi skaitiniai	1,5 val.
Pasiruošimas atsiskaitymui	1 val.

Praktinė užduotis: pateikite kuo daugiau būdvardžių, susijusių su internetu ir skaitmeninių prietaisų saugumu sli.do aplinkoje.



The screenshot shows the sli.do website. At the top, there is a navigation bar with links: Product, Customers, Pricing, Resources, Enterprise, and a LOG IN button. The main content area features a large video player with a play button icon. Below the video, the text "Every Question" is visible, followed by "The Ultimate Q&A and Polling Platform". A semi-transparent grey box with rounded corners is overlaid on the right side of the page, containing the text "Įveskite kodą" (Enter code). Below this box, there is a white input field with a hash symbol (#) and a green "JOIN" button. A yellow arrow points from the "Įveskite kodą" text to the input field. To the right of the input field, there is a link "or SIGN UP, IT'S FREE" and a link "schedule a demo". At the bottom, there is a small text: "By using this app I agree to the [Acceptable Use Policy](#)".



USERNAME:

Administrator

PASSWORD:

•••••

LOGIN

Kibernetinė higiena internete

Skaitmeninis pēdsakas

- Saugoma informacija apie bet kokius naudotojo veiksmus: aplankytas svetainės, peržiūrėtus profilius ar nuotraukas, užpildytas formos, registraciją pažinčių svetainėje, įdiegtas programėles ir t. t.
- **Aktyvus pėdsakas** – informacija, kurią savanoriškai ir sąmoningai įkeliamo ir paliekame (nuotraukos, įrašai, komentarai).
- **Pasyvus pėdsakas** – informacija, kurią paliekame nesąmoningai, dažnai net nežinodami ar nesuprasdami (IP adresai, paieškos istorija, geografinės padėties duomenys).



Asmeninė informacija

Asmeninė informacija – tai informacija, apibrėžianti ryšį tarp konkrečios informacijos ir asmens.*



* Malinauskaitė-van de Castel, Inga. Duomenų subjektų teisės virtualiuose socialiniuose tinkluose: daktaro disertacija – Vilnius, 2017.

Kas yra asmeniniai duomenys?

- Asmens kontaktiniai duomenys (t. y. vardas, pavardė, namų adresas, mobiliojo telefono numeris)
- Biometriniai duomenys
- Asmens kodas
- Asmens tapatybės kortelės arba paso numeris
- Asmens pajamos
- Slaptažodžiai
- Finansiniai duomenys
- Klientų duomenys
- Intelektiniai duomenys be savininkų leidimo



Kas yra viešieji duomenys?

- Viešieji duomenys gali būti:
 - Įmonės kodas
 - Įmonės el. paštas, pvz., info@company.com
 - Nuasmeninti duomenys
 - Slapyvardis
 - Hobiai
 - Gamtos nuotraukos
 - Tinklaraščiai
 - ...



Kodėl svarbu neskelbti asmens duomenų

- Tapatybės vagystė
- Kibernetiniai nusikaltimai (vagystės, šantažas, priekabiavimas)
- Galima žala reputacijai:
 - bet kas internete gali pasiekti laisvai prieinamus duomenis;
 - Paskelbti duomenys gali būti panaudoti prieš asmenį.
- Kuo daugiau informacijos skelbiama internete, tuo lengviau sukčiai gali pavogti asmens tapatybę, panaudoti duomenis



Patikrinkite, kokia informacija apie jus yra prieinama

- Naudodami paieškos sistemą atlikite paiešką internete apie save ir pažiūrėkite, kokią informaciją galite rasti.
- Atlikite paiešką apie save skirtingose paieškos sistemose:
 - Google
 - Bing
 - DuckDuckGo
- Naudokite kabutes ir kitus simbolius atlikdami paiešką, pavyzdžiui:
 - “Vardas Pavardė” – gausite informaciją apie šį asmenį.
 - “Vardas Pavardė@” – gausite su šiuo asmeniu susijusius el. pašto adresus.
 - “Vardas Pavardė” filetype: PDF – gausite PDF dokumentus, kuriame minimas šis asmuo.

Nuotraukų skelbimas

- Ar pagalvojote:
 - Kas turi prieigą prie jūsų nuotraukų?
 - Ar nuotraukoje yra kitų žmonių?
 - Ar nuotraukoje saugoma GPS informacija apie vietą?
- Naudodamiesi paieškos sistema galite pabandyti rasti nuotraukų su jumis.



Nuotraukų ir vaizdo įrašų bendrinimas

- Gerbkite kitų žmonių privatumą.
- Jei norite pasidalyti nuotrauka ar vaizdo įrašu su pažįstamais žmonėmis, derėtų paprašyti leidimo.
- Neplatinkite kitų žmonių vaikų nuotraukų be jų tėvų sutikimo.
- Reklaminėje medžiagoje nenaudokite žmonių nuotraukų, jei jie nedavė sutikimo.
- Nepažįstamus žmones fotografuokite tik viešoje vietoje. Jei asmuo aiškiai pareiškė, kad nenori būti fotografuojamas, jo fotografuoti negalima.
- Nesidalykite nuotraukomis ir vaizdo įrašais keršto ar pasityčiojimo tikslais.
- Nesidalykite smurto, neapykantos ar įžeidžiančiomis nuotraukomis ir vaizdo įrašais, net jei norite pasmerkti smurtą ar neapykantą.
- Nesidalykite nuotraukomis ir vaizdo įrašais, kuriuose jūs arba jūsų draugai ar giminaičiai užfiksuoti pažeidžiantys taisykles, besielgiantys netinkamai ar net pažeidžiantys įstatymus.

Nuotraukų ir vaizdo įrašų bendrinimas

- Jei radote savo ar artimųjų nuotrauką ir nenorite, kad ja būtų dalijamasi, galite imtis šių priemonių:
 - susisiekit su tuo, kas bendrino ir paprašykite ją pašalinti;
 - susisiekit su socialinio tinklo administratoriumi ir paprašykite pašalinti nuotrauką, paaiškindami situaciją;
 - jei pirmiau nurodyti veiksmai nepadėjo, kreipkitės į Asmens duomenų apsaugos inspekciją.

Draugai socialiniuose tinkluose

Išmintingai atsirinkite vartotojus, kuriuos priimate į draugus socialiniuose tinkluose.



Būkite atsargūs, neskelbkite bet kokios jus identifikuojančios informacijos

- Viskas, ką pateikiate internete, gali būti visam laikui.
- Informacija gali būti prieinama archyvuose, pvz., <https://web.archive.org>.
- Kiti žmonės gali:
 - išsaugoti informaciją savo įrenginiuose;
 - atspausdinti ar
 - pakartotinai paskelbti informaciją internete.

Stebėkite, kokia informacija apie jus skelbiama internete

- Galite stebėti, ar tinklalapiuose, tinklaraščiuose, moksliniuose tyrimuose, forumuose, „Youtube“ neskelbiama nauja informacija apie naudotoją, naudodamiesi pokyčių aptikimo ir pranešimo paslaugomis, pvz., [Google Alerts](#).
- „Google“ perspėjimų sistemoje galima pateikti raktinius žodžius.
- Kai randami nauji rezultatai, naudotojas gauna pranešimą el. paštu arba bet kuriuo metu gali peržiūrėti rezultatus www.google.com/alerts.



Prašymas pašalinti asmeninę informaciją iš „Google“ paslaugų

- Galite pranešti pateikdami išsamią informaciją, kad turinys apie jus būtų pašalintas iš „Google“ paslaugų.
- Galite prašyti pašalinti turinį iš tokių „Google“ paslaugų.

- ☐  Google Search
- ☐  Blogger/Blogspot
- ☐  Google Maps and related products
- ☐  Google Play: Apps
- ☐  YouTube
- ☐  Google Images
- ☐  A Google Ad
- ☐  Drive and Docs
- ☐  Google Photos and Picasa Web Albums
- ☐  Google Shopping
- ☐ See more products

Patikrinkite, ar jūsų duomenų saugumas nebuvo pažeistas

- Naudodami internetinius įrankius, pvz., [Have I Been Pwned?](https://haveibeenpwned.com/) galite patikrinti, ar jūsų el. paštas arba telefonas nepatyrė duomenų saugumo pažeidimo.
- Taip pat galite patikrinti, ar jūsų slaptažodis nebuvo pažeistas <https://haveibeenpwned.com/Passwords>. Pažeistų slaptažodžių galima ieškoti internete ir bet kas gali juos atsisiųsti.

';--have i been pwned?

Stebėkite duomenų saugumo pažeidimą

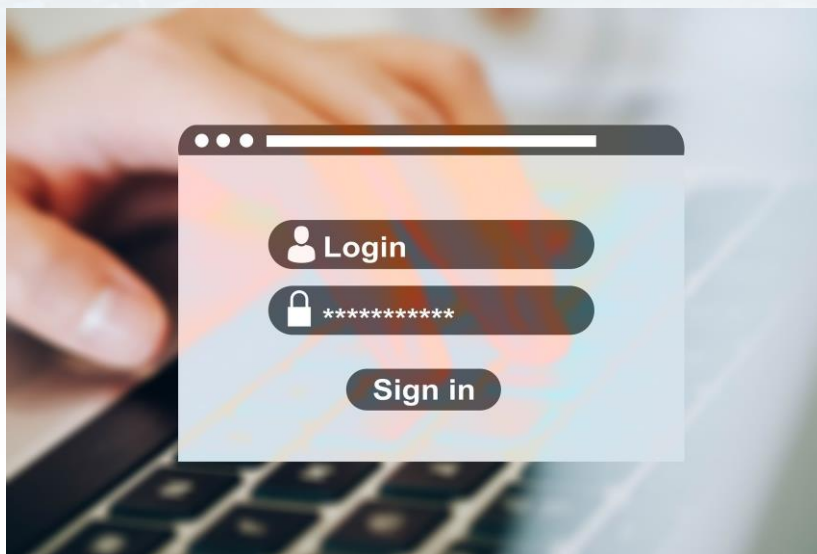
- Galite užsiregistruoti specialiuose portaluose, kurie informuoja, jei buvo pažeista naudotojo paskyra, pvz., <https://monitor.firefox.com>.



Daugiau informacijos: www.cnet.com/tech/services-and-software/firefox-monitor-shows-if-your-personal-information-was-lost-in-a-hack
<https://www.online-tech-tips.com/computer-tips/what-is-firefox-monitor-and-how-it-protects-your-login-details/>

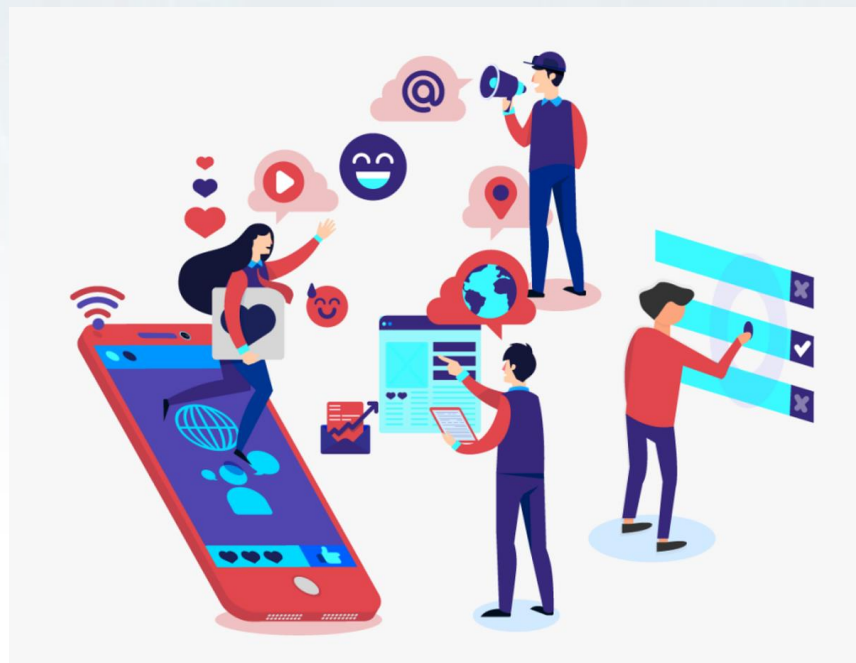
Veiksmai, jei buvo pažeistas jūsų paskyros saugumas

- Jei buvo pažeistas jūsų paskyros saugumas, tai reiškia, kad jūsų el. pašto adresas ir slaptažodis gali būti kibernetinių nusikaltėlių rankose. Tokiu atveju imkitės šių veiksmų:
 - nedelsdami pakeiskite pažeistos paskyros slaptažodį;
 - pakeiskite kitų paskyrų slaptažodį, jei naudojote tą patį slaptažodį;
 - įjunkite dviejų veiksmų autentifikavimą, jei yra galimybė.



Venkite dalytis asmenine informacija

- Atsargiai vertinkite pateikiamos informacijos kiekį, nes paprastai žmonės socialiniuose tinkluose linkę pateikti daugiau informacijos.
- Neskelbkite savo planų, namų adresų, finansinės informacijos.
- Nustatykite paskyros saugumo nustatymus ir tvarkykite, kas gali matyti jūsų pranešimus ir kitą informaciją.



Skirtingiems tikslams naudokite skirtingus el. pašto adresus

- El. paštas asmeniniam gyvenimui, pvz., vardas.pavarde@gmail.com.
- El. paštas verslo tikslais, pvz., vardas.pavarde@imones-pavadinimas.com.
- El. paštas registracijoms:
 - galite susikurti paskyrą registracijai nemokamuose el. pašto paslaugų portaluose;
 - galite naudoti laikino el. pašto paslaugą, pvz., [Guerrilla Mail](#), [Mailinator](#).

Nepasitikėk, tiesiog tikrink

- Būkite atsargūs, spausdami nuorodas, gautas draugų žinutėse.
- Netikėkite, kad žinutė tikrai yra nuo to, kas ją siunčia.
- SKAITYKITE prieš ką nors spustelėdami, kad atsisiųstumėte arba įdiegtumėte nemokamas programas.





Skaitmeninių įrenginių higiena

Skaitmeninių įrenginių saugumas

- Naudotojai, naudodamiesi kompiuteriais ir išmaniaisiais įrenginiais, turi elgtis atsakingai ir naudoti tinkamas saugumo priemones, nes išmaniųjų įrenginių funkcijos panašios į stalinių ar nešiojamųjų kompiuterių.
- Naudojant šiuos įrenginius gali kilti tokių pačių saugumo problemų kaip ir naudojant kompiuterius, gali būti prarasti duomenys ir pan.
- Išmaniuosius įrenginius, kaip ir kompiuterius, taip pat galima apsaugoti nuo virusų ir kitų galimų interneto grėsmių.

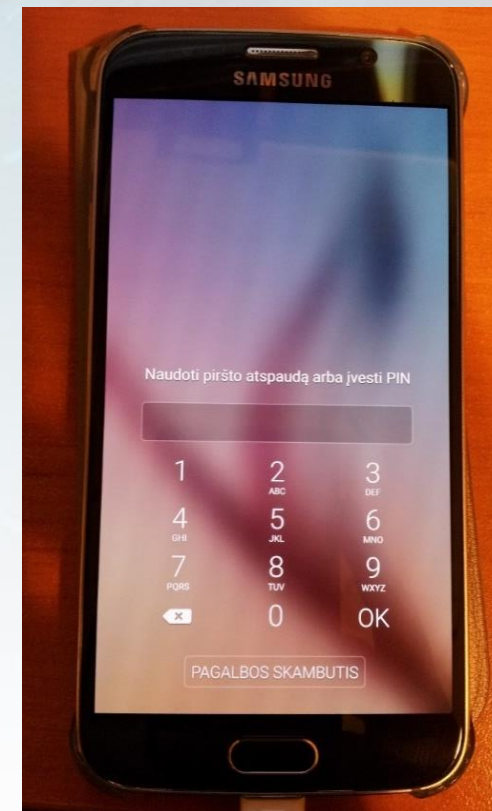
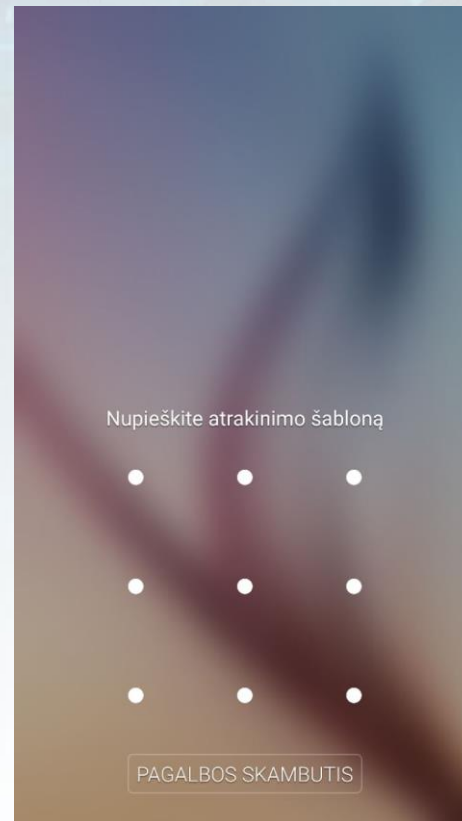


*Naudokite prisijungimo vardus ir slaptažodžius,
jungdamiesi prie skaitmeninių įrenginių*



Suaktyvinkite PIN kodo ar kitos saugios prisijungimo funkcijos naudojimą

- Mobiliuosiuose įrenginiuose rekomenduojama kiekvieną kartą prieš pradedant naudotis įrenginiu aktyvuoti PIN kodą, kad pašaliniai asmenys negalėtų naršyti jūsų įrenginyje, peržiūrėti jūsų asmeninių duomenų, nuotraukų ir pan.
- Kai kuriuose įrenginiuose yra kitų saugaus prisijungimo funkcijų, pvz., pirštų atspaudų nuskaitymo, akių nuskaitymo.
- Įjunkite automatinio užrakinimo funkciją baigus darbą su prietaisu.



Privatus naršymas

- Išjunkite trečiųjų šalių slapukus.
- Naudokite privataus naršymo režimą.
- Naudokite naršyklės papildinius (angl. *plug-in*), pvz. [HTTPS Everywhere](#).
- Naudokite virtualaus privataus tinklo VPN sprendimus, jei reikia paslėpti srautą.
- Patikrinkite, ką „Google“ žino apie jus <https://myactivity.google.com/myactivity>.

Slaptažodžių tvarkymo gairės

- Nesidalykite savo vartotojo vardais ir slaptažodžiais su kitais asmenimis, net su kolegomis.
- Niekada nelaikykite slaptažodžių užrašuose, atmintinėse ar failuose kompiuteryje ar mobiliajame įrenginyje.
- Nenaudokite slaptažodžių, sudarytų iš vardų, adresų, telefono numerių ir kitų lengvai atspėjamų žodžių.
- Skirtingoms paskyroms naudokite skirtingus slaptažodžius.
- Periodiškai keiskite slaptažodžius, kad užtikrintumėte didesnę saugumą.
- Slaptažodžiams apsaugoti naudokite slaptažodžių tvarkykles, pvz., [Firefox](#), [Lockwise](#), [NordPass](#), [KeePass](#).

Patikrinkite slaptažodžio sudėtingumą

The Password Meter

www.passwordmeter.com

safest9

Test Your Password	
Password:	●●●●●●●●
Hide:	☒
Score:	23%
Complexity:	Weak

MyPassword!5SafeAndStrong

Test Your Password	
Password:	●●●●●●●●●●●●●●●●
Hide:	☐
Score:	100%
Complexity:	Very Strong

Patarimai paliekant darbo vietą

- Baigę darbą atsijunkite nuo informacinių sistemų.
- Naršyklės uždarymas nebūtinai reiškia, kad atsijungėte.
- Užrakinkite skaitmeninį prietaisą, net jei trumpam jį paliekate. Jei paliksite neužrakintą įrenginį, kiti asmenys gali:
 - prieiti prie jūsų informacijos be jūsų leidimo;
 - prieiti prie konfidencialių duomenų;
 - išsiųsti laiškus iš jūsų paskyros;
 - ištrinti jūsų failus;
 - atlikti kitą kenkėjišką veiklą.

Jei naudojate kito asmens įrenginį

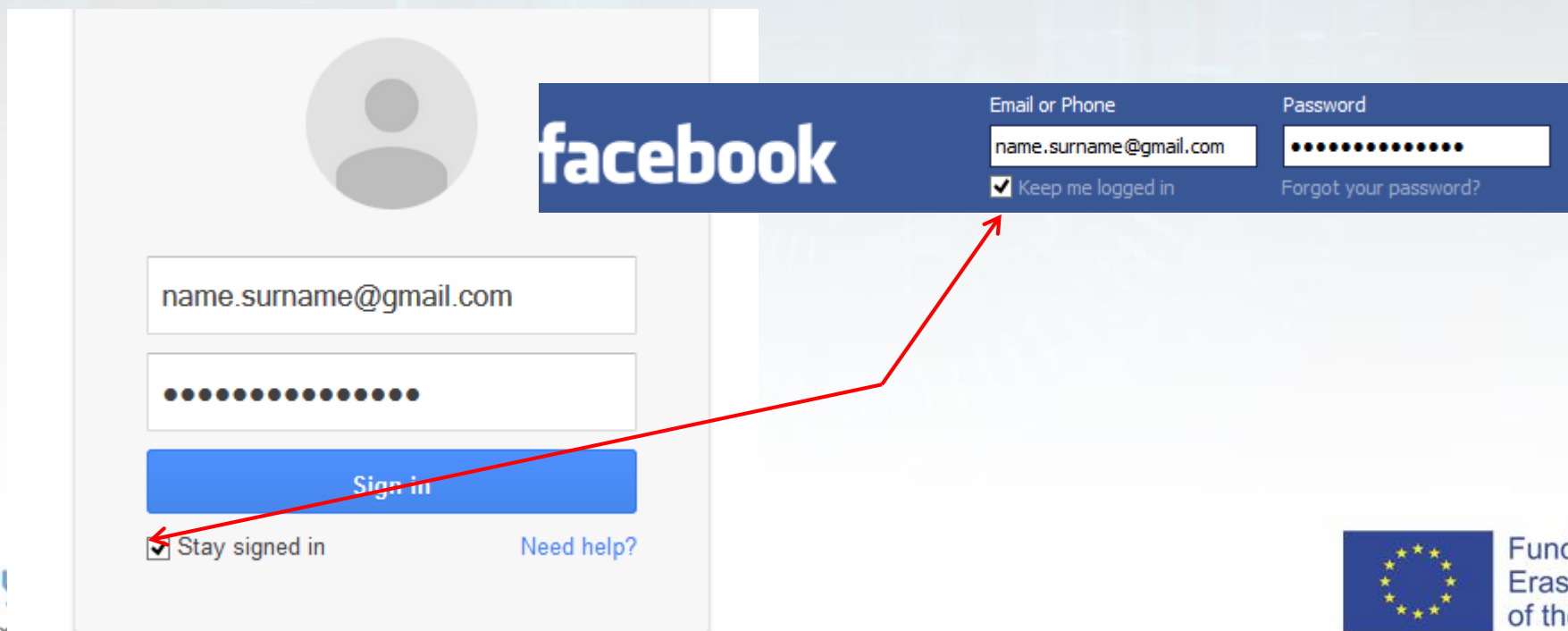
- Jei naudojotės svetimu įrenginiu ir įtariate, kad vykdoma neįprasta veikla, pakeiskite paslaugos, kuria naudojotės, slaptažodį iš patikimo kompiuterio ir tinklo.
- Slaptažodžiams įvesti naudokite virtualią klaviatūrą.
- Atsijunkite iš svetainių, kuriose reikia autorizacijos.
- Neišsaugokite savo prisijungimo informacijos.
- Ištrinkite naršyklės „istoriją“ ir atsisiųstus failus.

Apsisaugokite nuo žiūrėjimo per petį (angl. Shoulder surfing)

- Kai dirbate su skaitmeniniu įrenginiu, pavyzdžiui, kompiuteriu, nešiojamuoju kompiuteriu, išmaniuoju telefonu, kas nors gali paslapčia stebėti, ką naudotojas daro ekrane, kokią informaciją ar slaptažodžius įveda, kad gautų informaciją ir panaudotų ją kenkėjiškiems veiksams.
- Norėdami apsisaugoti nuo žiūrėjimo per petį:
 - susiraskite vietą, kur galėtumėte sėdėti arba stovėti nugarą į sieną;
 - visada stebėkite aplinką, ne tik žmones, bet ir vaizdo kameras, kurios gali filmuoti jūsų veiksmus.

Prisijungimas ir atsijungimas

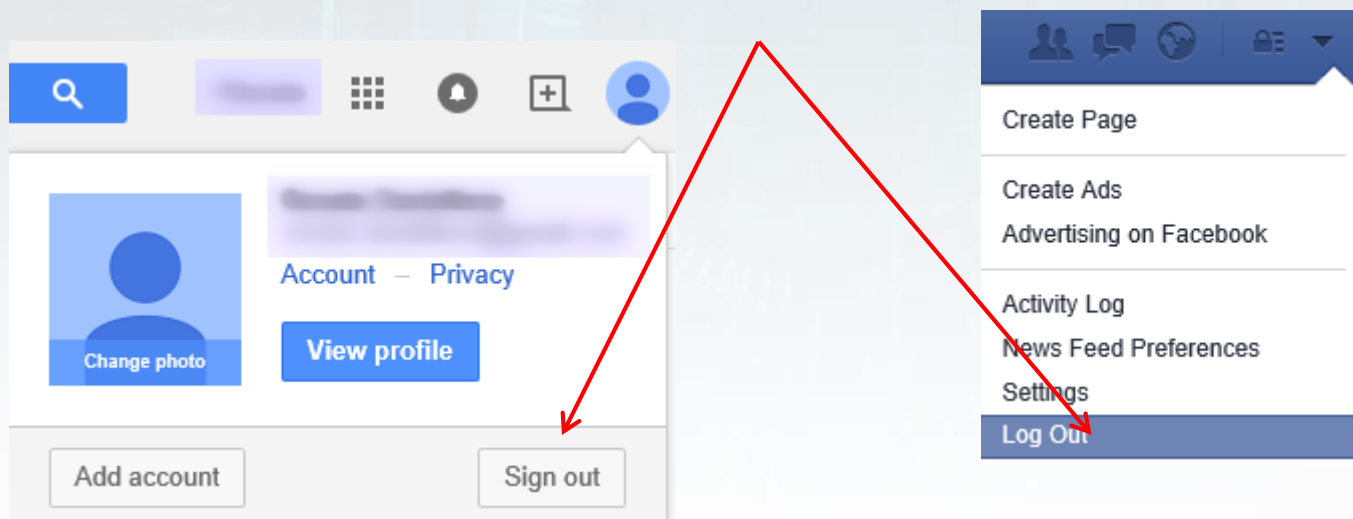
- Naudodamiesi viešuoju kompiuteriu (arba svetimu įrenginiu) panaikinkite žymimąjį langelį „Keep me logged in“ arba „Stay signed in“.
- Neleiskite žiniatinklio naršyklei įsiminti slaptažodžio ir automatiškai prisijungti.



The image shows a screenshot of the Facebook login page. On the left, there is a large login form with a placeholder profile picture, a text input field containing 'name.surname@gmail.com', a password input field with dots, a blue 'Sign in' button, and a checkbox labeled 'Stay signed in' which is checked. To the right of this form is a smaller, dark blue version of the login interface. It features the Facebook logo, a text input field with 'name.surname@gmail.com', a password input field with dots, a checked checkbox labeled 'Keep me logged in', and a link that says 'Forgot your password?'. A red arrow originates from the 'Stay signed in' checkbox in the larger form and points to the 'Keep me logged in' checkbox in the smaller form.

Prisijungimas ir atsijungimas

- naudodamiesi viešuoju kompiuteriu (arba svetimu įrenginiu) atsijunkite nuo paskyrų ir programėlių.



Nuotolinis atjungimas nuo sistemų

- Galite atsijungti nuotoliniu būdu, jei pamiršote atsijungti nuo savo paskyrų, dirbdami su viešuoju ar svetimu kompiuteriu, arba jei pametėte savo skaitmeninį įrenginį.
- Reikia patikrinti, ar paslauga teikia nuotolinio atsijungimo funkciją, pavyzdžiui, „Google“, „Facebook“, „Dropbox“, „Netflix“, „Microsoft“, „Instagram“, „Amazon“ ir kt.

Pavyzdžiui:

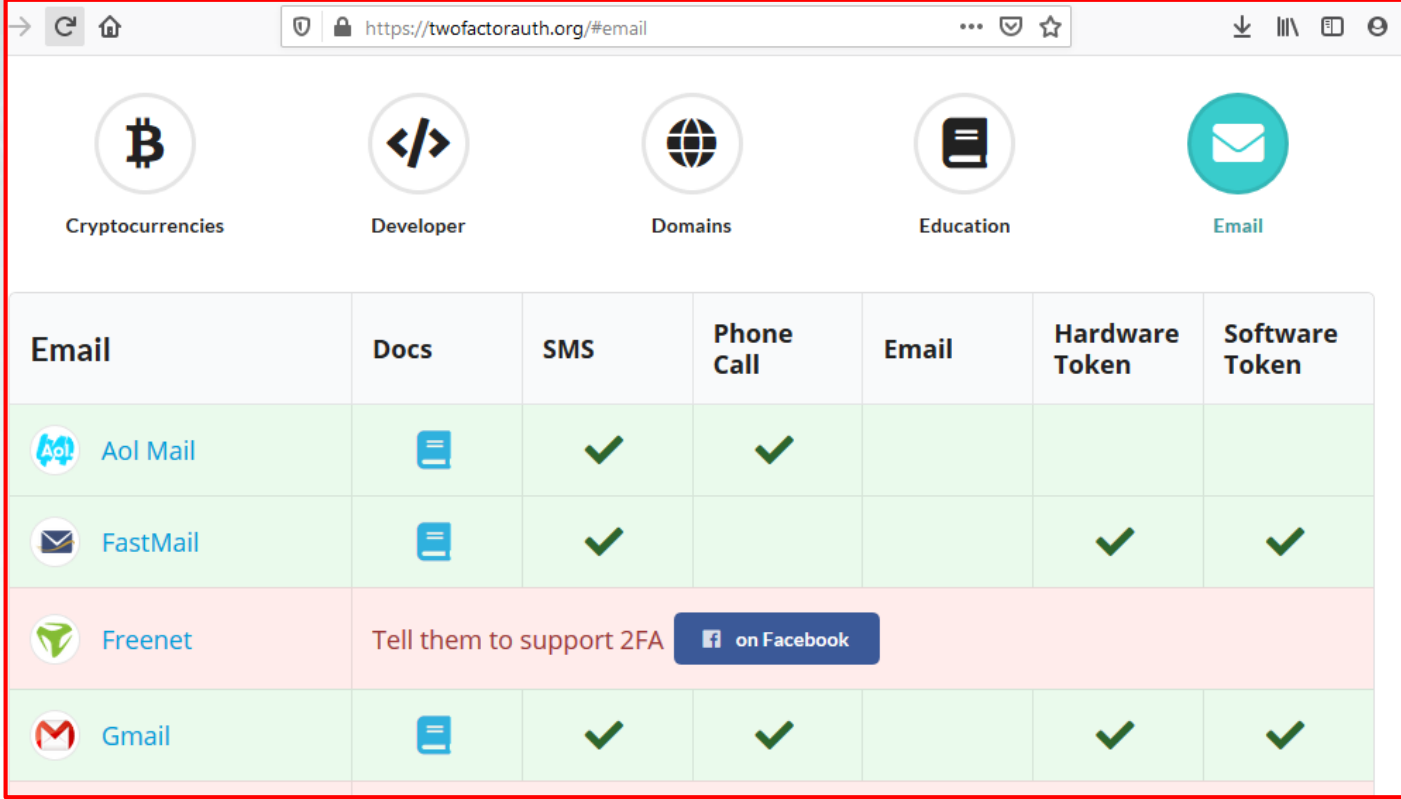
atsijungimas nuo Gmail <https://support.google.com/mail/answer/8154?hl=lt&co=GENIE.Platform%3DDesktop>

atsijungimas nuo Netflix <https://help.netflix.com/en/node/18>

atsijungimas nuo Dropbox <https://help.dropbox.com/accounts-billing/settings-sign-in/device-list-remote-sign-out>

Dviejų veiksmų autentifikacija

- Rekomenduojama įjungti dviejų veiksmų autentifikavimą, jei paslaugų teikėjas tokį palaiko.
- Patikrinkite, kuriose svetainėse palaikomas dviejų veiksmų autentifikavimas, pvz.
<https://twofactorauth.org>.



The screenshot shows the website <https://twofactorauth.org/#email>. At the top, there are five category icons: Cryptocurrencies (Bitcoin), Developer (code icon), Domains (globe), Education (book), and Email (envelope). Below these is a table with columns: Email, Docs, SMS, Phone Call, Email, Hardware Token, and Software Token. The table lists several email services and their 2FA support status.

Email	Docs	SMS	Phone Call	Email	Hardware Token	Software Token
Aol Mail		✓	✓			
FastMail		✓			✓	✓
Freenet	Tell them to support 2FA on Facebook					
Gmail		✓	✓		✓	✓



Technologiniai klausimai

Įdiekite legalią programinę įrangą ir programėles tik iš patikimų šaltinių

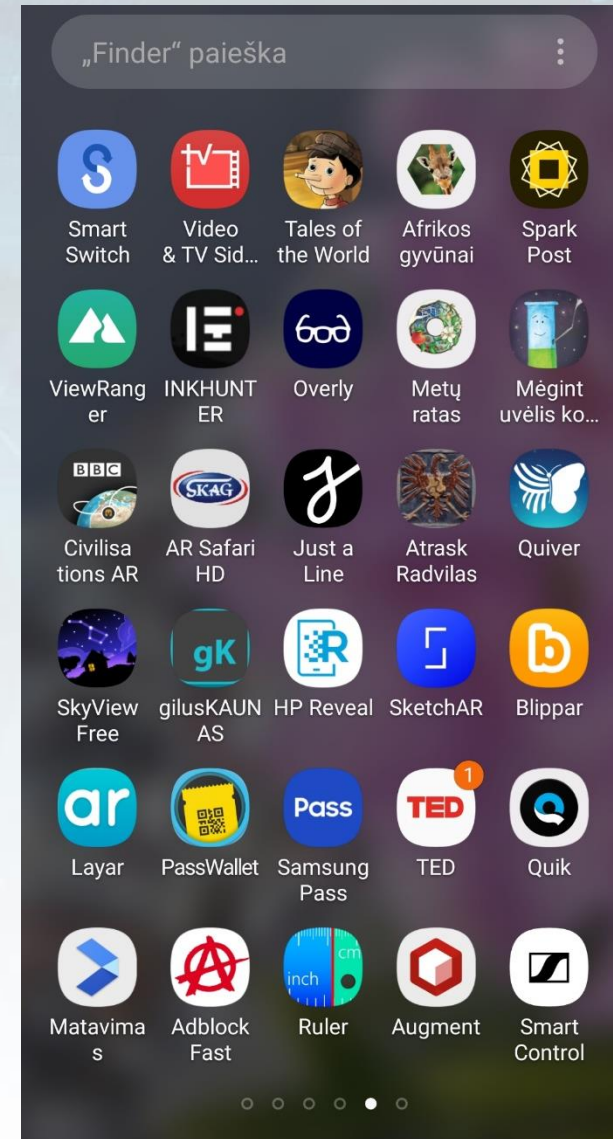
- Įdiekite tik legalią programinę įrangą ir programėles
- Nediekite nepatikimos programinės įrangos
- Įdiekite programėles tik iš patikimų šaltinių, pvz.:
 - Google Play
 - Apple App Store
 - Microsoft Store
 -



Google Play

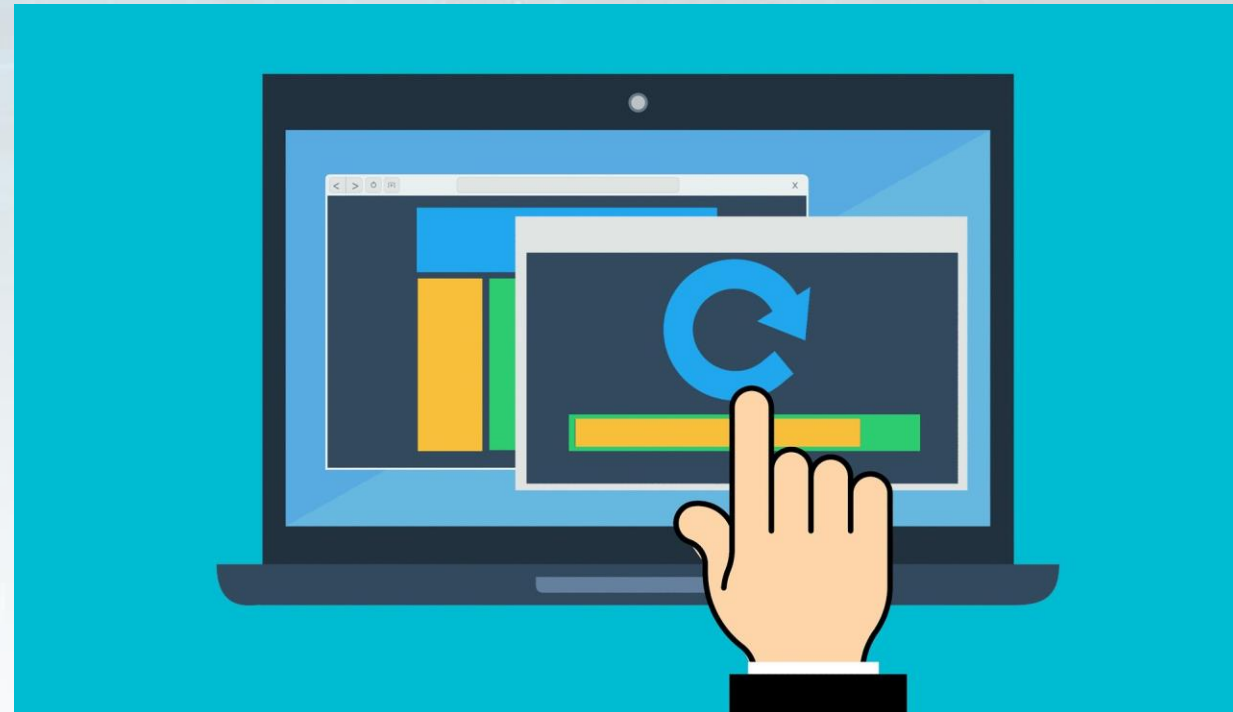
Klausimas

- Ar žinote visų jūsų įrenginyje esančių programėlių paskirtį?



Atnaujinkite programinę įrangą

- Užtikrinkite, kad visi reikalingi naujinimai ir pataisos būtų reguliariai diegiami įrenginiuose, programose ir informacinėse sistemose.
- Įgalinkite automatinius operacinės sistemos ir programinės įrangos atnaujinimus.



Naudokite antivirusines ir interneto apsaugos priemones

- Dauguma antivirusinės programinės įrangos yra komercinės ir mokamos.
- Asmeniniam naudojimui yra keletas nemokamų antivirusinių programų, pavyzdžiui:
 - Avira Free Antivirus
 - AVG
 - Avast
 - Bitdefender Antivirus Free Edition
 - Windows Defender

Naudokite šlamšto (angl. spam) ir el. pašto filtrus

- Šlamšto filtrai analizuoja, aptinka ir sustabdo nepageidaujamus ar pavojingus el. laiškus. Šlamšto filtrai gali analizuoti el. laiškus pagal skirtingus kriterijus:
 - Antraštės filtras
 - Turinio filtras
 - Juodojo sąrašo filtras
 - Taisyklėmis pagrįstas filtras
- Šlamšto filtras apsaugo serverius nuo perkrovos ir neleidžia darbuotojams gauti nepageidaujamų laiškų į savo el. paštą.
- Turėtumėte žinoti, kad nepageidaujamų laiškų filtras visiškai neapsaugo nuo nepageidaujamų ir apgaulingų laiškų.

Naudokite sistemos šifravimo funkciją

- Sistemos šifravimo funkcija užšifruoja visus telefone ar planšetiniame kompiuteryje esančius duomenis, įskaitant programų duomenis, atsisiųstus failus ir visa kita.
- Kiekvieną kartą įjungę telefoną turėsite įvesti PIN kodą arba slaptažodį.



Kurkite atsarginę duomenų kopiją

- Kurdami atsargines duomenų kopijas apsisaugosite, jei sugestų kompiuteris, nutrūktų elektros energijos tiekimas ar kiltų įtampos svyravimai, pvz., žaibo atveju.
- Atsarginėms kopijoms naudokite išorinį kietąjį diską arba kitą laikmeną.
- Atsarginės kopijos gali būti saugomos:
 - išoriniuose saugojimo įrenginiuose;
 - internetiniuose diskuose, kaip „Dropbox“, „Apple iCloud“, „Google Diskas“ ir kt.



Tapatybės apsaugos priemonė

- Naudokite įspėjamuosius ženklus, kad buvo pažeisti jūsų duomenys arba buvo įsilaužta į jūsų paskyrą, pvz. [Canarytokens](#).
- „Canarytokens“ – tai nemokamas įrankis, kuris padeda sužinoti, kad buvo pažeistas jūsų duomenų saugumas, nes užpuolikai praneša apie save.
- „Canary“ įspėjamasis ženklas (angl. token) – tai failas, URL, API raktas ar kitas išteklius, kurio prieiga stebima. Kai prie ištekliaus prieinama, įjungiamas perspėjimas, kuriuo objekto savininkui pranešama apie minėtą prieigą.

Daugiau informacijos:

<https://canarytokens.org/generate> www.lacework.com/blog/canarytokensandransomwareoperations

Tapatybės apsaugos priemonė

- „Canary“ įspėjamieji ženklai (angl. *token*) gali būti:
 - Žiniatinklio klaida, URL įspėjamasis ženklas (angl. *token*) (perspėjimas, kai aplankomas URL)
 - DNS įspėjamasis ženklas (angl. *token*) (perspėjimas, kai užsakomas „hostname“)
 - Unikalus el. pašto adresas (perspėjimas, kai el. laiškas siunčiamas unikaliu adresu)
 - MS Word, MS Excel, PDF failų įspėjamasis ženklas (angl. *token*) (perspėjimas, kai atidaromas dokumentas)
 - Windows aplankas (perspėjimas, kai atidaromas aplankas)
 - Kita

Išmaniųjų įrenginių saugumas

- Patikrinkite ir sukonfigūruokite visų programų leidimus ir privatumo nustatymus.
- Įgalinkite nuotolinį valdymą ir duomenų naikinimą.
- Kurkite atsarginę mobiliojo prietaiso duomenų kopiją.
- Išjunkite „Bluetooth“, kai nenaudojate.
- Būkite atsargūs peržiūredami telefone esančią informaciją viešose vietose.
- Prieš parduodami prietaisą iš naujo nustatykite gamyklinius nustatymus.

Jrenginio ir tinklo apsauga

- Sunaikinkite nebenaudojamus prietaisus ar atminties korteles.
- Rekomenduojama jungtis tik prie patikimų belaidžių tinklų, apsaugotų slaptažodžiais.
- Užšifruokite USB ir kitas laikmenas.
- Tinkamai ištrinkite dokumentus, kuriuose yra asmeninė informacija.

Kitos rekomendacijos

- Venkite P2P ir platinamų failų dalijimosi.
- Atsisiųskite failus teisėtai.
- Venkite naršyti interneto svetainėse, kurių dar nepažįstate.
- Venkite pasiūlymų, kurie yra pernelyg geri, kad būtų tiesa.

Svarbiausia atsvara kibernetiniams nusikaltėliams: vartotojų informuotumas ir budrumas!

Naudingos nuorodos

What is personal information? | Personal data

<https://www.cloudflare.com/en-gb/learning/privacy/what-is-personal-information/>

Video about how it is easy to get hacked: https://youtu.be/1hpU_Neg1KA

What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More

<https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more>

What is a digital footprint? And how to protect it from hackers <https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint>

How to Protect Your Digital Privacy

<https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy>

How to Remove Personal Information From the Internet

<https://www.lifelock.com/learn-identity-theft-resources-remove-personal-information-from-the-internet.html>

Prevenciniai veiksmai

- Kibernetinė higiena internete
- Skaitmeninių įrenginių higiena
- Technologiniai klausimai



Užduotis

Užpildykite formą:

- vardas, pavardė
- el. pašto adresas
- mokyklos, kurią baigėte, pavadinimas
- jūsų gyvūnų vardai



PATARIMAS: galite naudoti „Google“ formą, tačiau įsitikinkite, kad užduotis yra tiksli, pvz.,

<https://forms.gle/uckbLqBmY2mkFs93A>

Užduotis



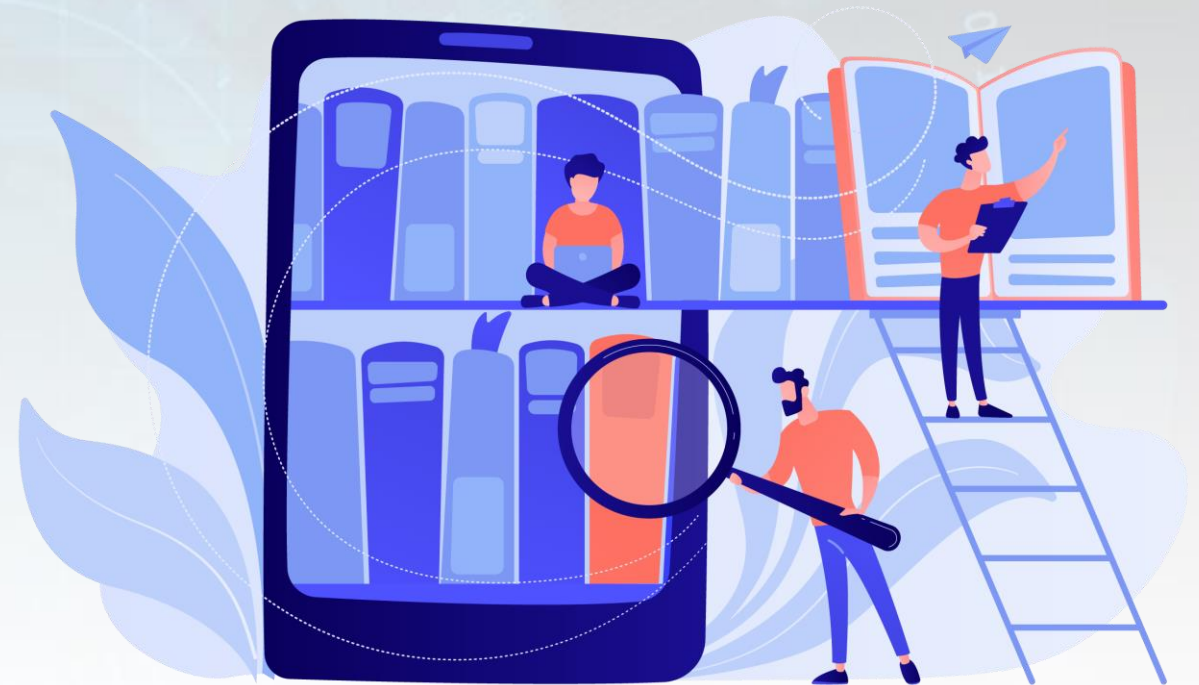
Aptarkite:

- Kokį skaitmeninį pėdsaką paliekate internete?
- Kaip saugote savo asmeninius duomenis?
- Kaip saugote savo skaitmeninius įrenginius?
- Kas yra dviejų veiksnų autentifikavimas ir kur jį naudojate?

Atlikite „Google“ paiešką apie save. Ką radote?

Papildomi skaitiniai

- **European Union. Agency for Network and Information Security** Review of Cyber Hygiene Practices, 2016
- **Gerardus Blokdyk**, Cyber Hygiene Third Edition, 2018
- **Gerardus Blokdyk**, Cyber Hygiene a Complete Guide - 2020 Edition



Trumpi vaizdo įrašai

- Kaip lengva būti „nulažtam“?
 - https://youtu.be/1hpU_Neg1KA
- Kas yra skaitmeninis pėdsakas?
 - <https://youtu.be/CfICOt2uI80>
- Kaip apsaugoti savo duomenis internete
 - <https://youtu.be/XjJZoHOIgu4>
- Kas yra dviejų veiksmų autentifikavimas?
 - <https://youtu.be/mMKo-fG89jQ>
- Mano duomenų saugumas pažeistas. Ką daryti?
 - <https://youtu.be/k5rIMr-u0Jw>
- Mobiliojo saugumo supratimas
 - <https://youtu.be/ahNb6kA0Lms>



Dėkojame!



Pateiktyje naudojamų nuotraukų šaltiniai:

- www.pixabay.com
- asmeninis archyvas
- svetainių ekrano nuotraukos