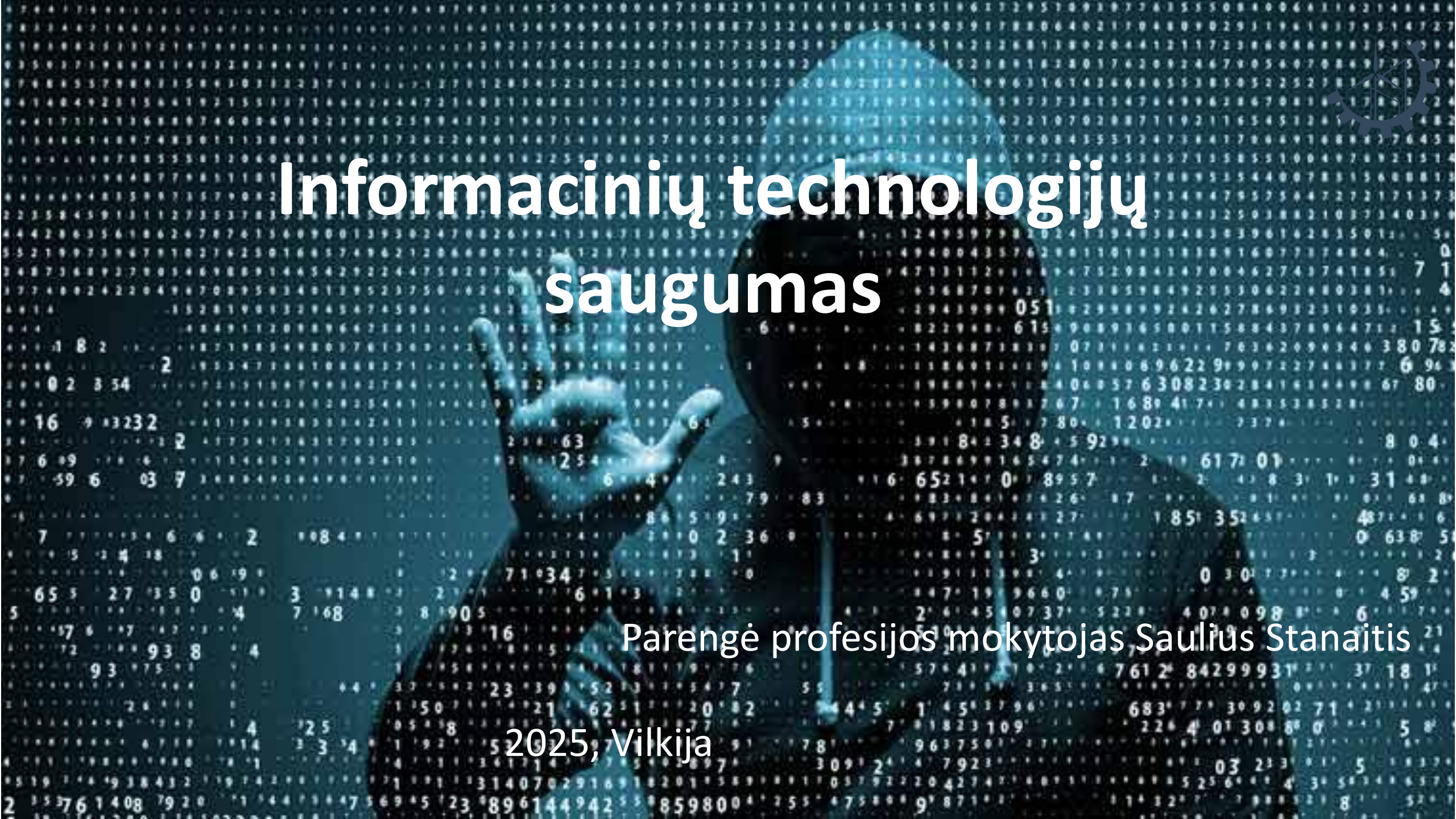


Informacinių technologijų saugumas

Parengė profesijos mokytojas Saulius Stanaitis

2025, Vilkija

Grėsmių vektoriai

80%

didesnių incidentų turi savo „konstrukcijoje“ socialinės manipuliacijos komponentus

SOCIALINĖS MANIPULIACIJOS

Fake news, Phishingas, web atakos

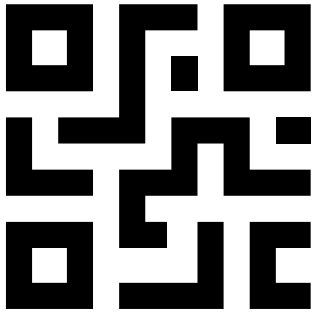
TECHNOLOGINĖS

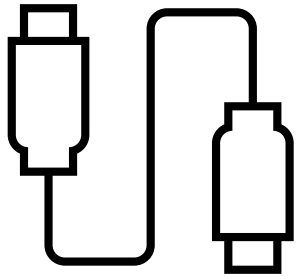
IT grėsmės: virusai, Ransomware, keyloggers, DDoS atakos, kt.

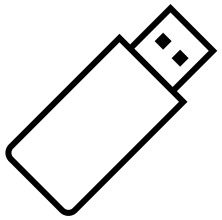
FIZINĖS GRĖSMĖS

Fizinės infrastruktūros problemos

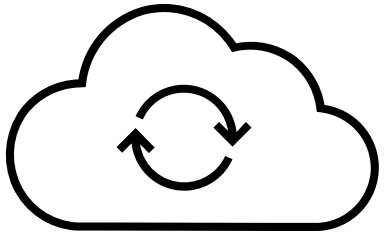
Fizinės grėsmės

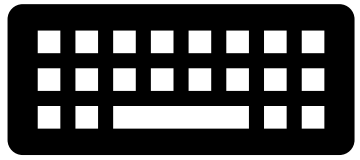


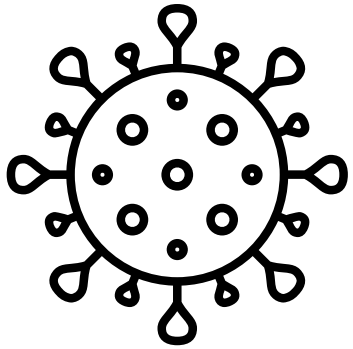


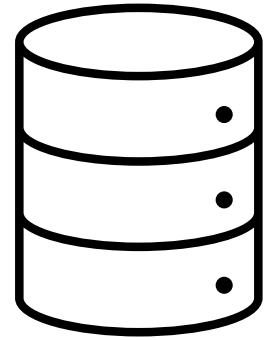


Technologinės grėsmės

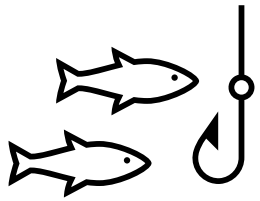


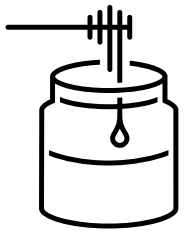


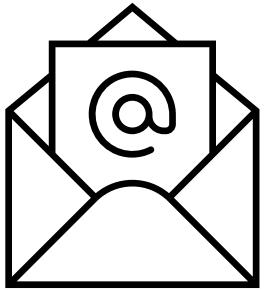


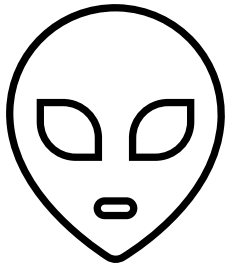


Socialinė inžinerija









Žmogiškoji socialinė inžinerija

- Impersonavimas
  - Apsimetimas kažkuo
  - Arba akis į akį, arba naudojant skaitmeninius komunikacijos kanalus
  - Tapatybės pasisavinimas
- Slaptas klausymasis ir žiūrėjimas į ekraną/klaviatūrą
- Rausimasis po šiukšles
- Atvirkštinė socialinė inžinerija
- Sekimas iš paskos ir patekimas į patalpą neturint tam teisės

Kompiuterinė socialinė inžinerija

Phishingas - atakos vykdomas elektroniniu paštu

Smishingas - atakos vykdomas SMS žinutėmis

Vishingas – atakos vykdomas gyvais skambučiais

Pharmingas – atakos vykdomas duomenų peradresavimu

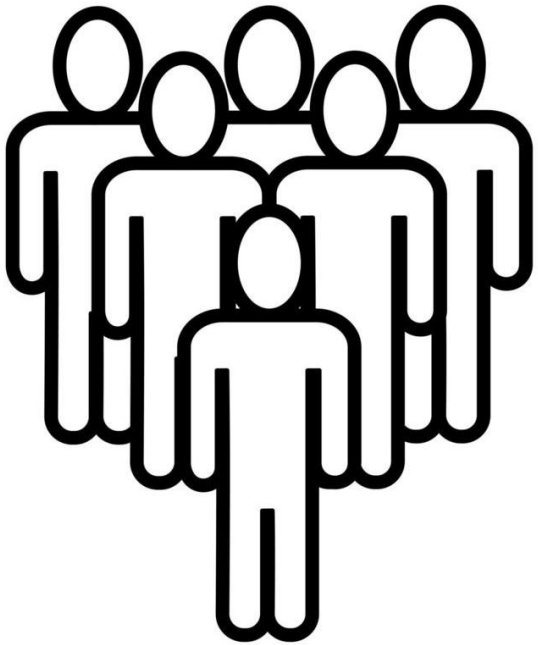
Kodėl mes užkimbam?

Panagrinėkime šešis Arizonos valstijos universiteto psichologijos ir rinkodaros profesoriaus, knygos "Įtaka: įtikinėjimo menas" autoriaus. **R. Cialdinio principus:**

1**. Grįžtamumas**. Kaip žmonės, mes linkę grąžinti paslaugas, apmokėti skolas ir elgtis su kitais taip, kaip šie elgiasi su mumis. Pagal grįžtamumo logiką, tai gali įpareigoti mus daryti išimtis ar nuolaidas tiems žmonėms, kurie pasiūlė mums kažką patrauklaus.

2. Nuoseklumas. R. Cialdini teigia, jog mes turime gilų troškimą būti nuosekliais. To pasėkoje, kai įsipareigojame kažkam, siekiame tai įgyvendinti pilnu pajėgumu.

3. Socialinis patvirtinimas. Principas remiasi „saugumo skaičiuose“ jausmu. Tarkim, jūs būsite labiau linkęs dirbti vėliau, jei tą darys kiti jūsų komandos nariai. Didesnė tikimybė, kad įdėsite arbatpinigių, jeigu ten jau bus pinigų. Norėsite vakarieniauti restorane, jei jis užimtas. Jeigu kiti žmonės daro kažką, vadinasi tas kažkas yra patikimas.



4. Mėgstamumas. R. Cialdini teigia, jog mes esame labiau paveikiami tų žmonių, kuriuos mėgstame. Mėgstamumas pasireiškia daugeliu formų – tai gali būti žmonės panašūs į mus ar mums žinomi, jie gali mums pasakyti komplimentus, arba mes tiesiog jais pasitikime, žavimės tam tikromis savybėmis.

5. Autoritetas. Jaučiame tam tikrą pagarbą žmonėms kurie užima vadovaujančias ar specialisto pozicijas. Būtent todėl farmacijos produktų reklamose dažnai pasitelkiami gydytojai. Pareigybės ir net statusą pabrėžiantys daiktai – antai automobiliai – gali padaryti mums įtaką bei patikėti tuo, ką sako šiuos daiktus turintys žmonės

6. Stygius bei ribotumas. Anot šio principo, tam tikri dalykai mums yra gerokai patrauklesni, kai priėjimas prie jų yra ribotas, arba jei mes prarandame galimybę juos įsigyti. Tarkim, mes galime įsigyti kažką tuoj pat, jei mums pasakoma, kad tai paskutinė produktų partija, arba, jog specialus pasiūlymas tuoj nebegalios.

Phishingo požymiai

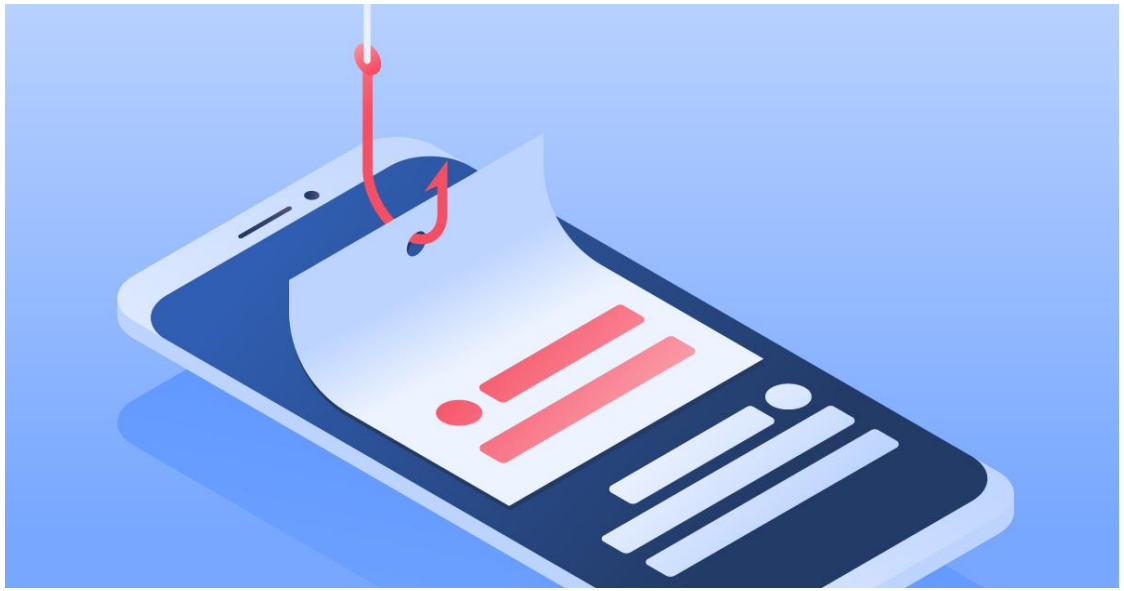
- Jeigu kreipiamasi fraze „Gerb. kliente“ arba „Suinteresuotajam asmeniui“, būkite budrūs;
- Nelogiški minties šuoliai, gramatikos ar rašybos klaidos;
- El. laiško siuntėjo adresas;
- Ar el. laiške nejaučiate skubos;
- Nuorodos nukreipia į kitus puslapius;
- Siunčiamas failas su „įdomia“ informacija;

Kaip apsisaugoti nuo phishingo

- Stabtelėkite ir pagalvokite
- Nespauskite nuorodų
- Užveskite pelytę ant nuorodos
- Paklauskite savęs, ar jau esate bendravę su siuntėju
- Susisiekite su siuntėju kitu kanalu
- Neatsakinėkite į laišką
- Praneškite IT specialistams
- Sugriežtinti elektroninių laiškų filtravimą

Smishingas, telefoniniai sukčiai

Bankas“ ne visada yra bankas

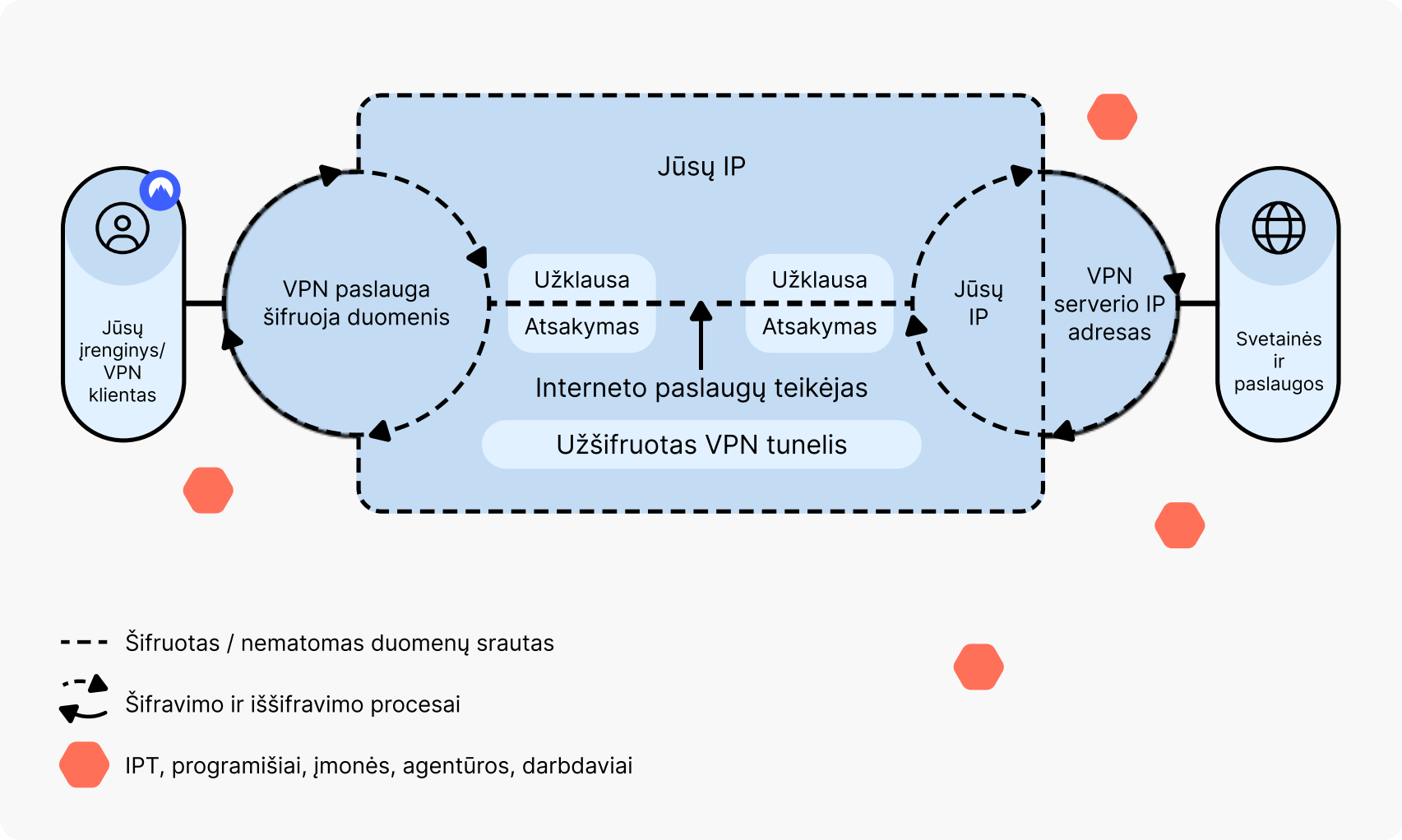


Nebandykite gudrauti ir apgauti sukčiaus !!!!!

Pharmingas

- Standartiniai maršrutizatoriaus nustatymai
- Patikimas interneto tiekėjas
- VPN naudojimas
- https internetiniai puslapiai
- Pasiūlymai, kurie „per geri“, kad būtų tiesa
- Naudokite antivirusinę programinę įrangą

VPN reiškia „virtualų privatų tinklą“ – tai paslauga, apsauganti jūsų interneto ryšį ir privatumą internete. VPN sukuria jūsų duomenims skirtą šifruotą tunelį, apsaugo jūsų internetinę tapatybę paslėpdamas jūsų IP adresą ir leidžia saugiai naudotis viešomis „Wi-Fi“ saitvietėmis.




http://www

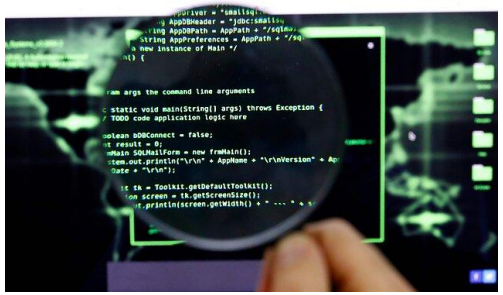

https://
http://


https://ww


SSL Certificate
https://ww

Sąlygos būtinos sėkmingai socialinės inžinerijos atakai

Žinoti atakos tikslą



Žinoti atakos objektą

Nusistatyti atakai trūkstamos informacijos poreikį

STEBĖTI

SURINKTI trūkstamą informaciją

Netikri profiliai

Netikras profilis, dažnai vadinamas „fake account“ arba „hony profile“ sukurta naudojant fiktyvią ar klaidinančią informaciją. Šie profiliai nėra susieti su tikrais asmenimis, bet yra sukurti įvairiems tikslams, kurie gali būti nuo nekenksmingų iki kenkėjiškų.

Ransomware
– išpirkos reikalaujančios atakos

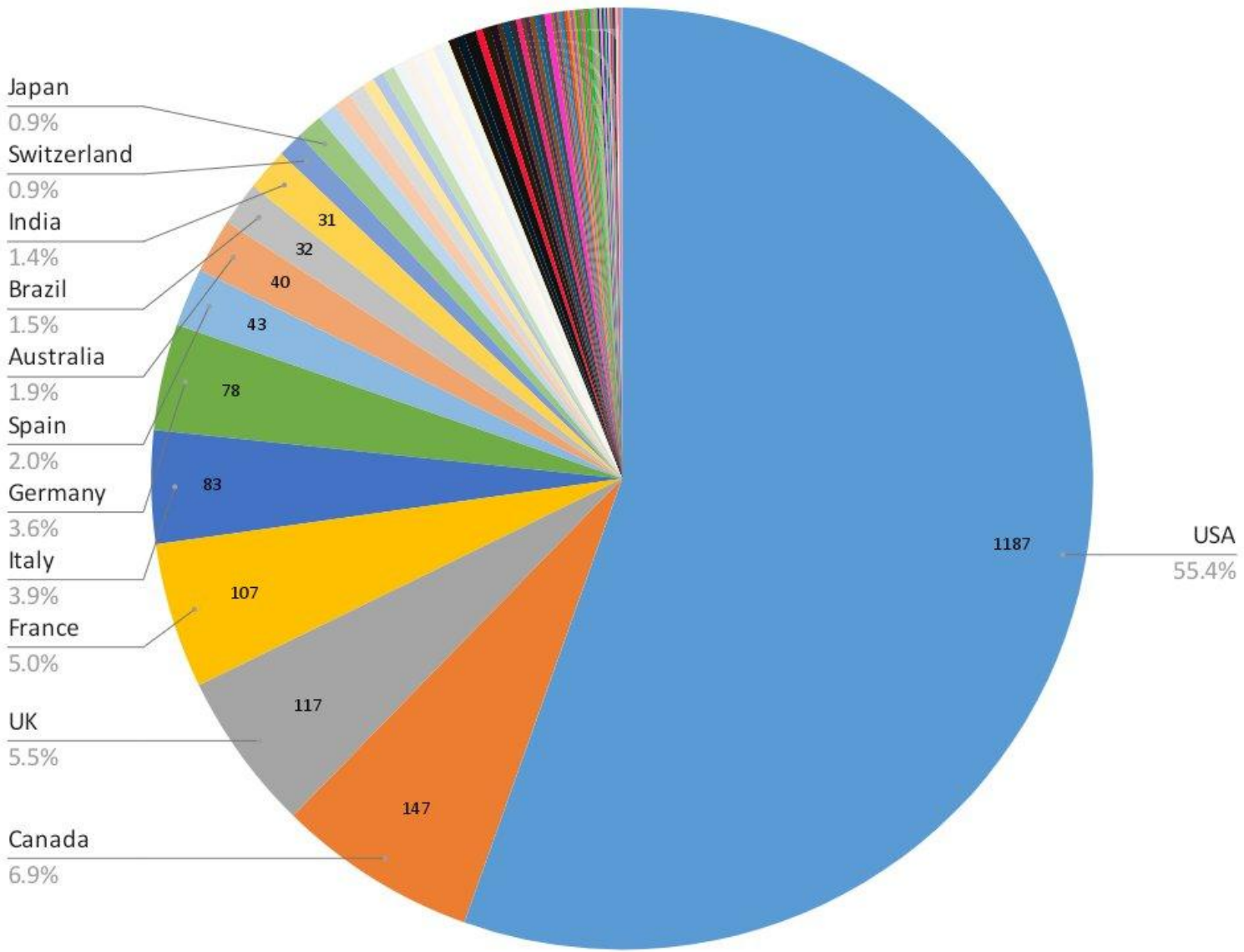
Apibūdinimas

Ransomware atakos nukreiptos į asmenis, įmones, vyriausybines organizacijas ir svarbią infrastruktūrą. Užpuolikai gali pasirinkti taikinius pagal suvokiamą gebėjimą sumokėti išpirką.

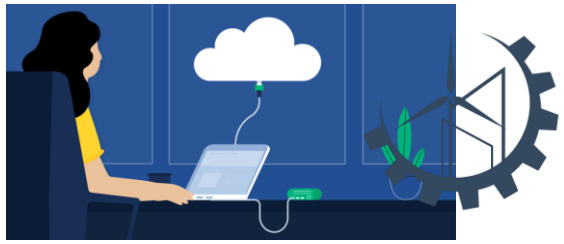
Kenkėjiška programinė įranga - nusikaltėliai reikalauja iš aukos sumokėti išpirką

Pristatymo būdai - gali būti platinamas įvairiais būdais, įskaitant kenkėjiškus el. pašto priedus, užkrėstas svetaines, pažeistą programinės įrangos atsisiuntimą ir net per tinklo pažeidžiamumą.

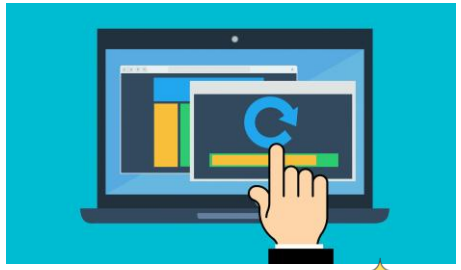
Statistics on countries affected by darkweb ransomware



Apsauga nuo ransomware



Atsarginės kopijos + kopijų saugojimo + testavimas



Programinės įrangos atnaujinimai (Update and Patch)

Elektroninio pašto serverio nustatymai

Mokymai

Tinklo, aplinkų atskyrimas

Draudimas

LIETUVOS DRAUDIMAS

Higiena

Tvarkyti failus ir programas: Periodiškai peržiūrėkite savo failų sistemą ir programas, ištrindami nereikalingus failus ir programų versijas. Tai ne tik atidarys vietą diske, bet ir pagerins bendrą sistemos veiklą.

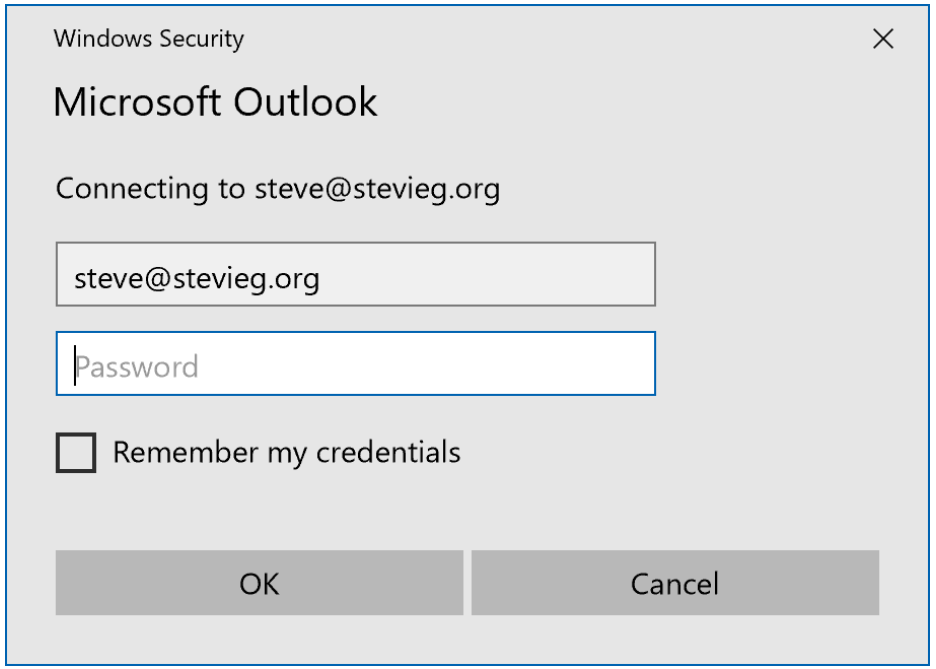
Atnaujinimai: Užtikrinkite, kad visos operacinės sistemos ir programas būtų atnaujintos iki naujausių versijų. Dažni atnaujinimai ne tik gerina saugumą, bet ir pagerina programas, taip sumažindami galimybę pasitaikyti klaidoms ir sutrikimams.

Antivirusinės programos: Įdiekite patikimą antivirusinę programą ir reguliariai atnaujinkite jos virusų duomenų bazę. Tai padės apsaugoti jūsų kompiuterį nuo kenkėjiškų programų ir virusų.

Disko tvarkymas: Periodiškai vykdykite disko defragmentaciją ir tikrinkite disko būklę. Tai gali pagerinti sistemos veikimą ir padidinti disko efektyvumą.

Autentifikavimas, autorizavimas ir apskaita

Autentifikavimas: tai pradinis AAA proceso žingsnis. Autentifikavimo metu sistema patikrina vartotojo ar įrenginio, bandančio pasiekti tinklą arba konkretų išteklį, tapatybę. Autentifikavimo metodai gali apimti vartotojo vardus ir slaptažodžius, skaitmeninius sertifikatus, QR kodus, smart korteles, biometrinius duomenis (pirštų atspaudus, veido atpažinimą) ir žetonais pagrįstas sistemas



Autorizacija: sėkmingai atpažinus vartotoją arba įrenginį, kitas veiksmas yra autorizacija. Leidimas nustato, kokius veiksmus autentifikuotam subjektui leidžiama atlikti tinkle arba konkrečiuose šaltiniuose. Tai apima leidimų ir prieigos lygių nustatymą pagal vartotojo vaidmenį arba atributus.

Apskaita: apskaitos fazė apima visų autentifikuoto vartotojo ar įrenginio atliktų veiksmų ir veiksmų sekimą ir registravimą. Šie duomenys yra labai svarbūs tikrinant, stebint ir generuojant tinklo naudojimo ir saugos įvykių ataskaitas.

Įsilaužėlių tipai

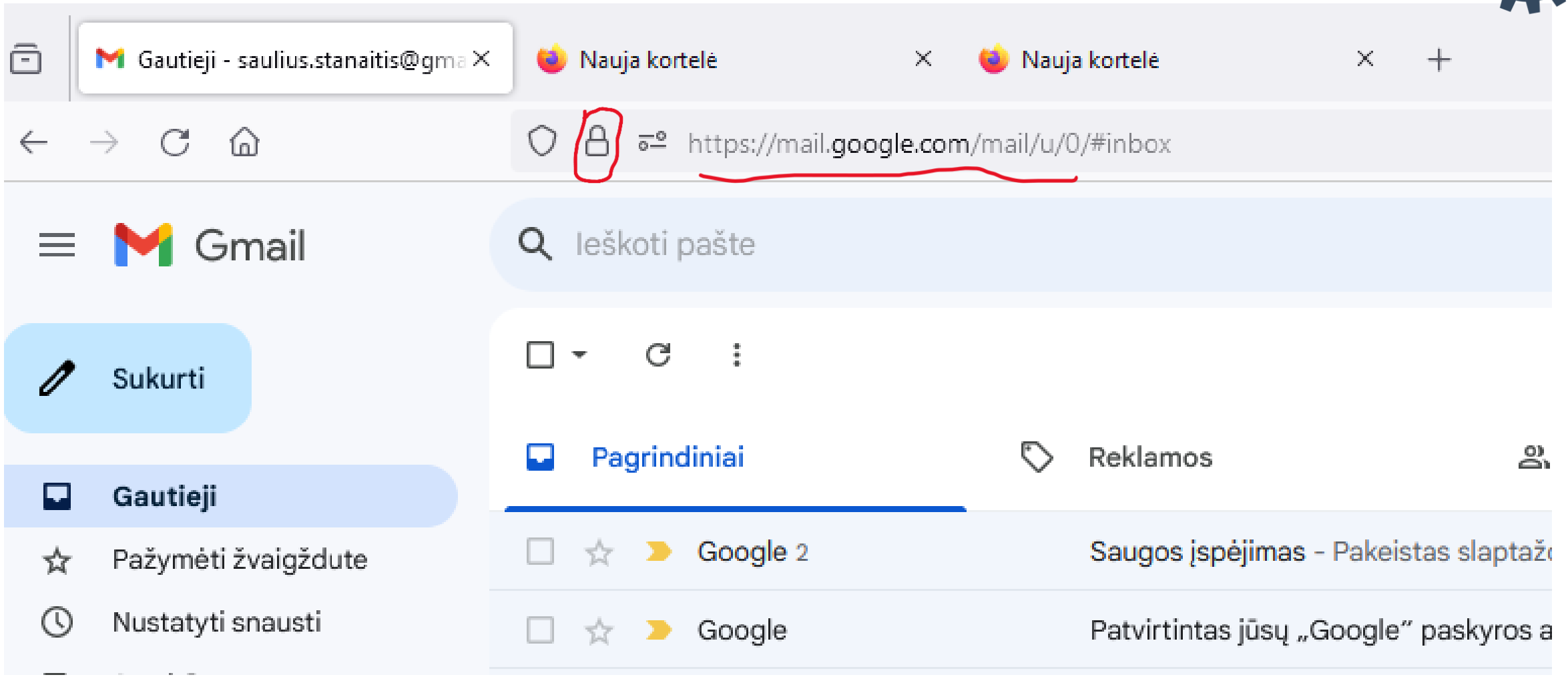
„White Hat“ įsilaužėliai (etiniai įsilaužėliai): „White Hat“ įsilaužėliai yra kibernetinio saugumo profesionalai, kurie savo įsilaužimo įgūdžius naudoja teisėtais ir etiniais tikslais. Organizacijos juos dažnai naudoja siekdamos nustatyti ir pašalinti saugumo spragas, atlikti skverbties testus ir pagerinti bendrą kibernetinį saugumą.

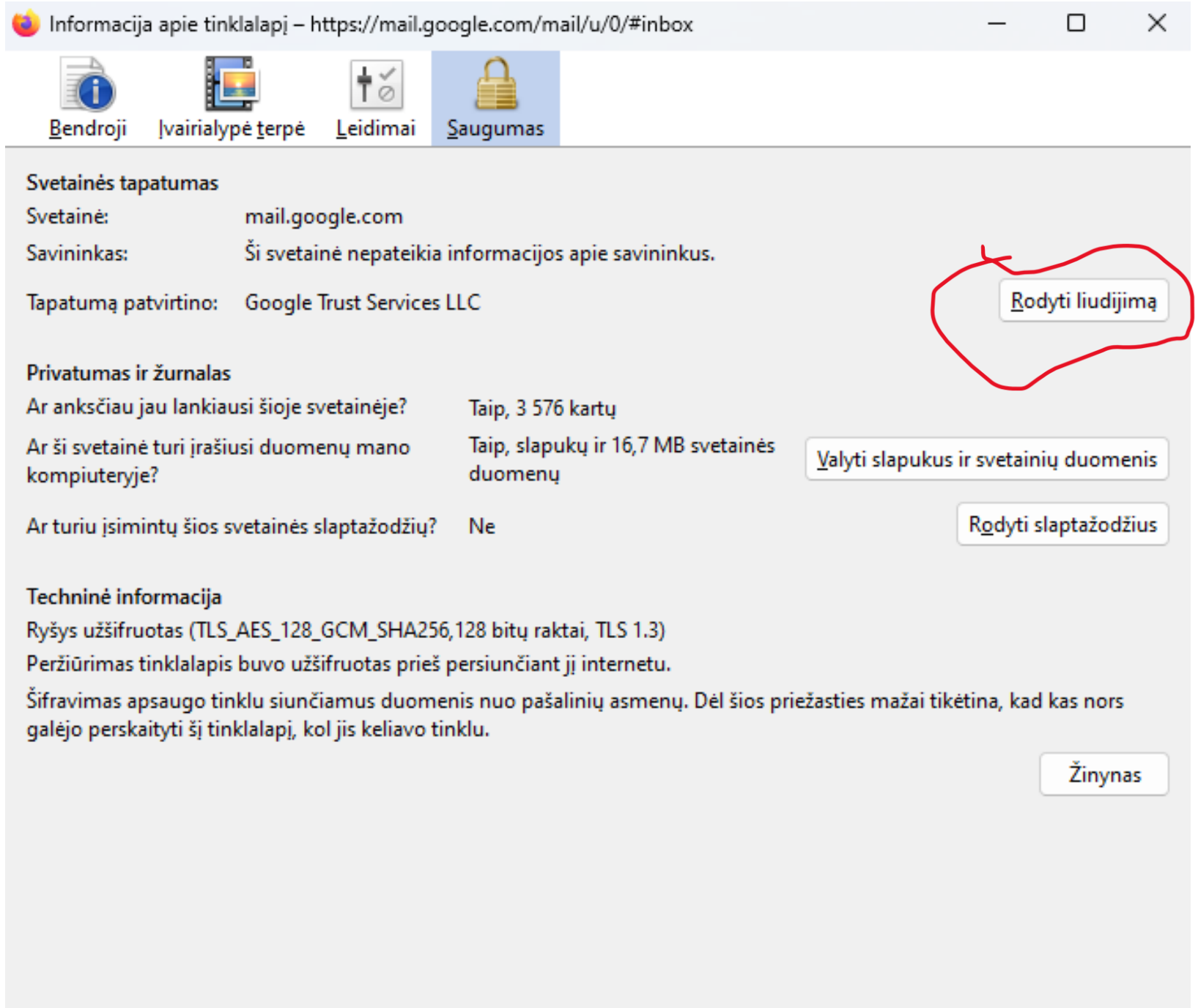
„Black Hat“ įsilaužėliai: „Black Hat“ įsilaužėliai yra piktybiški įsilaužėliai, kurie užsiima neteisėta ir neetiška veikla. Jie išnaudoja saugumo trūkumus siekdami asmeninės naudos, įskaitant duomenų vagystes, finansinį sukčiavimą ir sistemos sutrikimus.

„Grey hat“ įsilaužėliai: pilkųjų skrybėlių įsilaužėliai patenka kažkur tarp baltos skrybėlės ir juodos skrybėlės įsilaužėlių. Jie gali nustatyti pažeidžiamumą ir jas išnaudoti neturėdami tinkamo leidimo, tačiau tai daro neturėdami piktų kėslų. Tada pilkosios kepurės įsilaužėliai gali pranešti paveiktoms šalims arba viešai atskleisti pažeidžiamumą.


lib
lib64
lost+fou
sbin

Gmail langas




Informacija apie tinklalapį – https://mail.google.com/mail/u/0/#inbox
Bendroji
Įvairialypė terpė
Leidimai
Saugumas
Svetainės tapatumas
Svetainė: mail.google.com
Savininkas: Ši svetainė nepateikia informacijos apie savininkus.
Tapatumą patvirtino: Google Trust Services LLC
Rodyti liudijimą
Privatumas ir žurnalas
Ar anksčiau jau lankiausi šioje svetainėje? Taip, 3 576 kartų
Ar ši svetainė turi įrašiusi duomenų mano kompiuteryje? Taip, slapukų ir 16,7 MB svetainės duomenų
Valyti slapukus ir svetainių duomenis
Ar turiu įsimintų šios svetainės slaptažodžių? Ne
Rodyti slaptažodžius
Techninė informacija
Ryšys užšifruotas (TLS_AES_128_GCM_SHA256,128 bitų raktai, TLS 1.3)
Peržiūrimas tinklalapis buvo užšifruotas prieš persiunčiant jį internetu.
Šifravimas apsaugo tinklu siunčiamus duomenis nuo pašalinių asmenų. Dėl šios priežasties mažai tikėtina, kad kas nors galėjo perskaityti šį tinklalapį, kol jis keliavo tinklu.
Žinynas

mail.google.com | GTS CA 1C3 | GTS Root R1 | GlobalSign Root CA

Subjekto vardas

Bendrasis vardas	mail.google.com

Išdavėjo vardas

Šalis	US
Įstaiga	Google Trust Services LLC
Bendrasis vardas	GTS CA 1C3

Galiojimas

Ne anksčiau	Mon, 20 Nov 2023 08:09:47 GMT
Ne vėliau	Mon, 12 Feb 2024 08:09:46 GMT

Subjekto alternatyvieji vardai

DNS vardas	mail.google.com
DNS vardas	inbox.google.com

Viešojo rakto informacija

Algoritmas	Elliptic Curve
Rakto dydis	256
Viešoji reikšmė	04:45:7F:67:0C:10:B7:DF:93:09:0A:73:4F:E7:C5:47:90:45:3A:DF:88:11:9D:DA:95:BB:...

Kitkas

Dviejų faktorių autentifikacija

Dviejų faktorių autentifikacija (2FA), kartais vadinama dviejų veiksnių autentifikacija arba dviguba autentifikacija, yra saugumo procesas, kai vartotojo atpažinimui reikalingas daugiau nei vienas tapatybės nustatymo būdas. Šis procesas reikalingas siekiant geriau apsaugoti vartotojų duomenis ir išteklius, kuriais vartotojas siekia pasinaudoti. Daugiau informacijos apie dviejų faktorių autentifikaciją sužinosite peržiūrėję Ryšių reguliavimo tarnybos vaizdo siužetą.

https://www.youtube.com/watch?v=dM5stzG3ANY&t=106s


Dėkoju už dėmesį ir laukiu klausimų