GYMNÁZIUM
STREDNÁ ODBORNÁ ŠKOLA
SPOJENÁ ŠKOLA
Kollárova 17 SEČOVCE

Bezpečné prehliadanie webového obsahu

Stredná odborná škola techniky a služieb, Kollárova 17, Sečovce

Riziká

- Bezpečnosť
  - Útoky s cieľom ukradnúť/zneužiť
    - Financie
    - Heslá
    - Identita
    - Zariadenie
- Súkromie
  - Sledovanie aktivity
  - Cielená reklama
- Ovplyvňovanie
  - Hoaxy Falošné správy

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
622,161,052	Data Enrichment Exposure From PDL Customer accounts
593,427,119	Exploit.In accounts
509,458,528	Facebook accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
268,765,495	Wattpad accounts

Snapchat

In January 2014 just one week after Gibson Security detailed vulnerabilities in the service, Snapchat had 4.6 million usernames and phone number exposed. The attack involved brute force enumeration of a large number of phone numbers against the Snapchat API in what appears to be a response to Snapchat's assertion that such an attack was "theoretical". Consequently, the breach enabled individual usernames (which are often used across other services) to be resolved to phone numbers which users usually wish to keep private.

Breach date: 1 January 2014
Date added to HIBP: 2 January 2014
Compromised accounts: 4,609,615
Compromised data: Geographic locations, Phone numbers, Usernames
Permalink

20. marca 2018 13:08 Facebook

Ako Cambridge Analytica zranila Facebook. Najskôr ukradli osobné údaje a potom ovplyvňovali voľby

MIREK TÔDA

TREND Predplatiť

TREND.sk / Správy

Používateľov Facebooku, ktorých dáta boli zneužité, môžu byť 2 miliardy

Tesco

In February 2014, over 2,000 Tesco accounts with usernames, passwords and loyalty card balances appeared on Pastebin. Whilst the source of the breach is not clear, many confirmed the credentials were valid for Tesco and indeed they have a history of poor online security.

Obrana

- Technická
  - Nastavenie prehliadača
  - Používané nástroje
    - Správca hesiel
    - Antimalvér/antivírus
- Používateľská
  - Opatrnosť
  - Precíznosť, dodržiavanie opatrení
  - Kritické myslenie

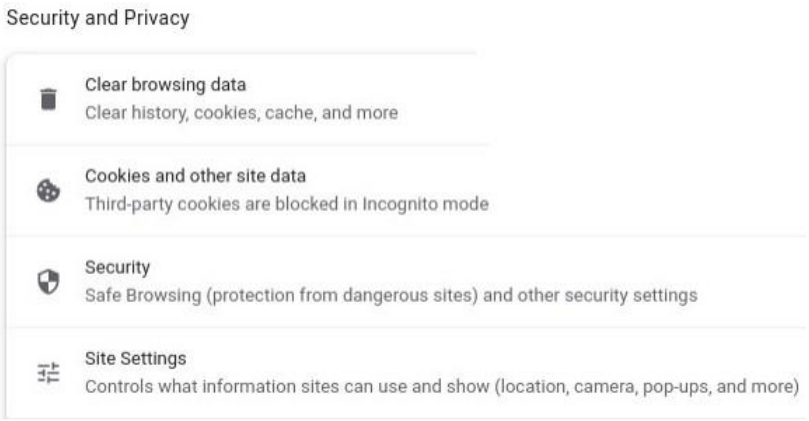
Výber prehliadača

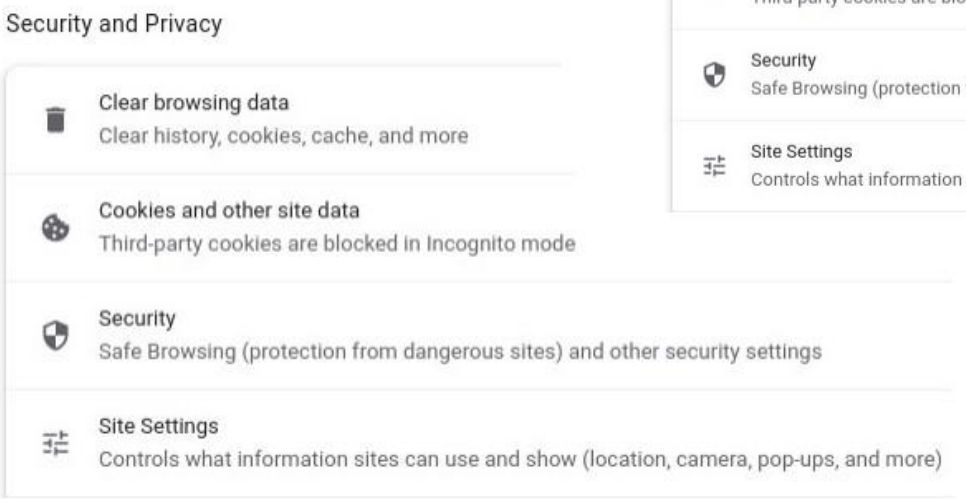
- Požiadavky:
  - *Bezpečný*
  - Aktualizovaný
  - Prispôsobiteľný
  - Funkčný
- *Napr. Chrome, Firefox, opera*

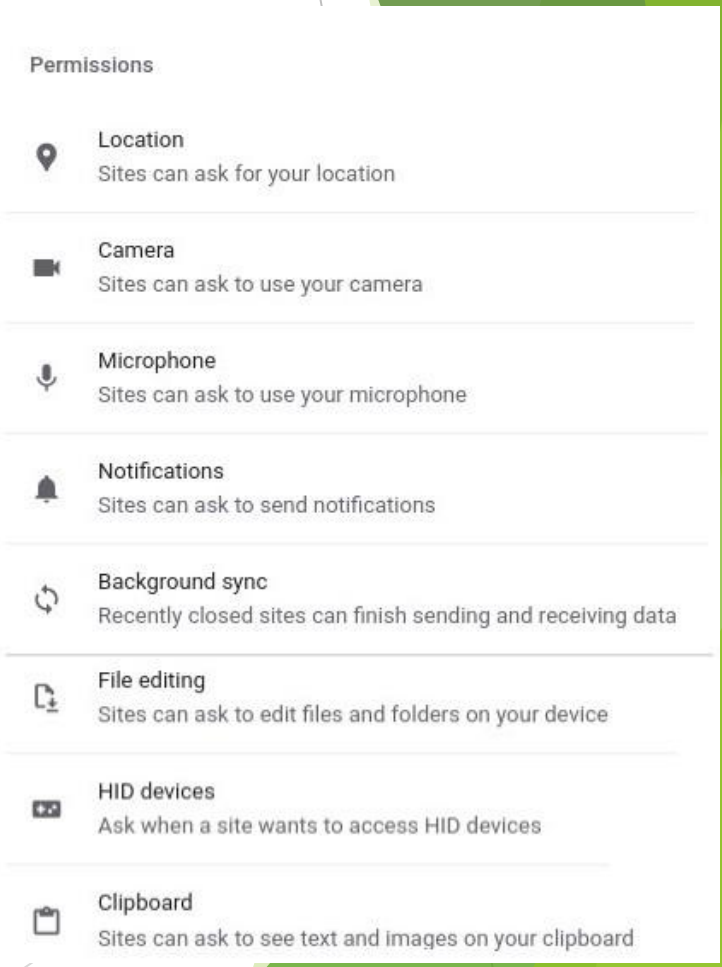
- Zraniteľnosti sú všade
  - Pravidelné opravy
  - (Takmer) všetky aktuálne prehliadače
- Dlhotrvajúca podpora
  - Enterprise, Extended Support

Prispôsobiteľnosť

- Nastavenia
  - Po spustení/Domovská stránka
  - História, záložky
  - Povolenia
  - Bezpečnosť a súkromie

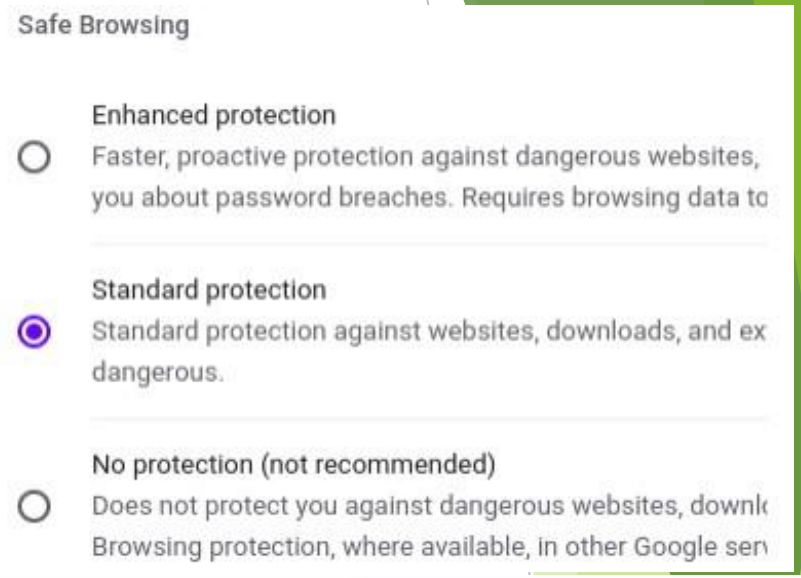






Čo nastaviť?

- Bezpečnosť
  - Pokročilá alebo štandardná ochrana
  - Zabezpečené spojenia (HTTPS) a DNS
- Blokovanie
  - Sledovanie a reklamy
    - Nastavenie prehliadača alebo doplnok
  - Cookies tretích strán
- Povolenia
  - Zakázať/Skontrolovať editovanie súborov a prístup do schránky



Prečo šifrovať?

- HTTPS
  - Inak celý obsah je čitateľný (napr. WiFi)
    - Aj prihlasovacie údaje

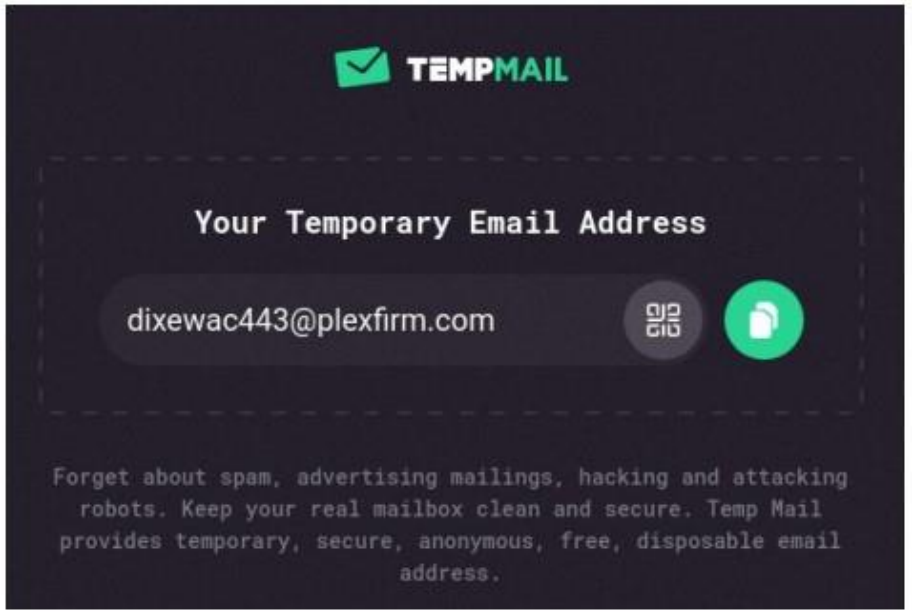
```
POST /user.php HTTP/1.1
Host: dsl.sk
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
Origin: http://dsl.sk
DNT: 1
Connection: keep-alive
Referer: http://dsl.sk/user.php?action=login
Cookie: PHPSESSID=kgjnad5gd87bmobt8rh04idm25
Upgrade-Insecure-Requests: 1

action=login&save=true&url=&login=ibawareness&password=SilneHesloAleNesifrovane&submit=Prihl%E1si%9D
```

- DNS
  - *Preklad domén na IP adresy*
  - Inak vidno, aké stránky navštevujeme

Destination	Protocol	Length	Info
8.8.4.4	DNS	77	Standard query 0x4bc7 A dsl.sk OPT
8.8.4.4	DNS	77	Standard query 0x4bbd AAAA dsl.sk OPT

Emaily

- Bez emailu to nejde...
  - Registrácie
  - Prístup k informáciám
    - Články, dokumenty
    - Stiahnutie súboru
    - Zľavové kódy
  - => Spam, zber informácií
- Jednorázové emaily
  - https://temp-mail.org/
  - https://anonbox.net/
- Špecifické emailové adresy
  - Vhodné pre registráciu
  - Pre každú službu zvlášť

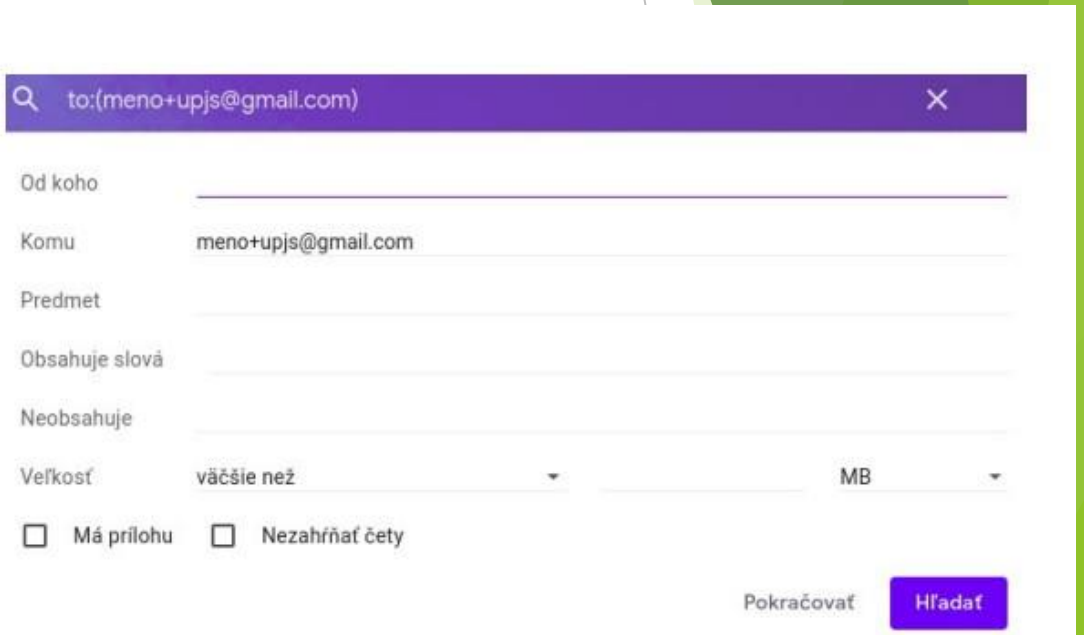


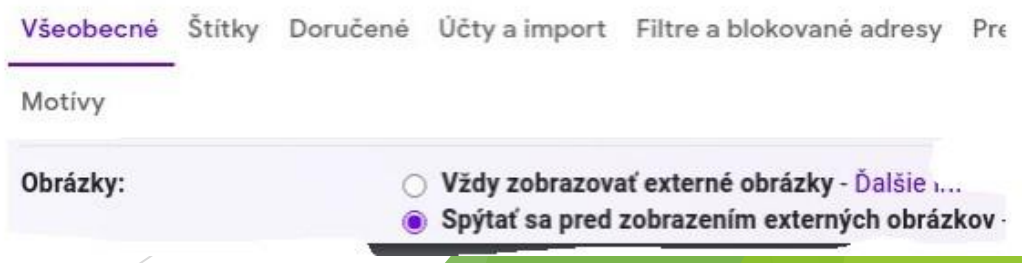
Registrácie

- Prihlásiť sa cez Google/FaceBook
  - Závislosť na danej službe
  - Čo ak?
    - Už nebude zadarmo
    - Využívanie bude podmienené poskytnutím ďalších údajov
    - Prestane existovať
    - Niekto získa prístup ku Vášmu mailu? (mobil s mailom)
- Meno (email) + heslo
  - Potrebné emaily
    - Spam
  - Potrebné heslá

Špecifické emailové adresy

- Jedna schránka, mnoho emailových aliasov
  - meno@email.org
  - meno+hocico@email.org
- Gmail aj ProtonMail
  - meno@gmail.com
  - meno+hocico@gmail.com
  - meno@protonmail.com
  - meno+hocico@protonmail.com
- Filtrovanie
  - Triedenie do adresárov, aplikovanie štítkov
  - Spam? Zablokovať celý alias





Jeden email na všetko?

- Veľa spamu
- Výrazná digitálna stopa
- Prepojenie všetkých identít
- Únik jednej identity môže viesť ku kompromitácii druhej
  - Recyklácia hesiel
  - Sociálne inžinierstvo
    - Na Vás
    - Na poskytovateľa služby

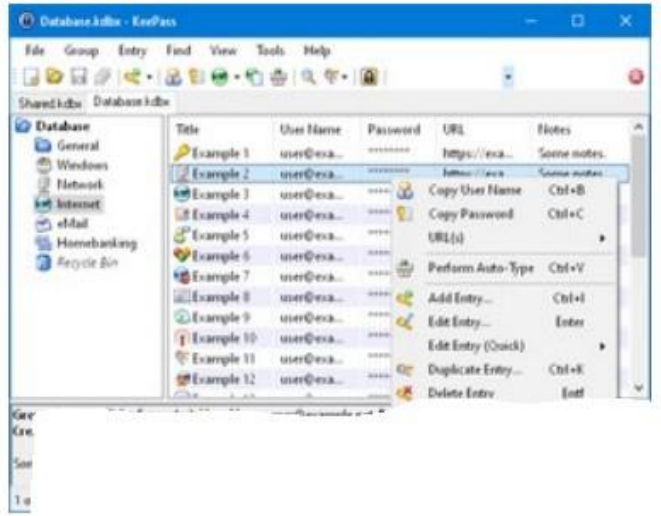
Časté chyby

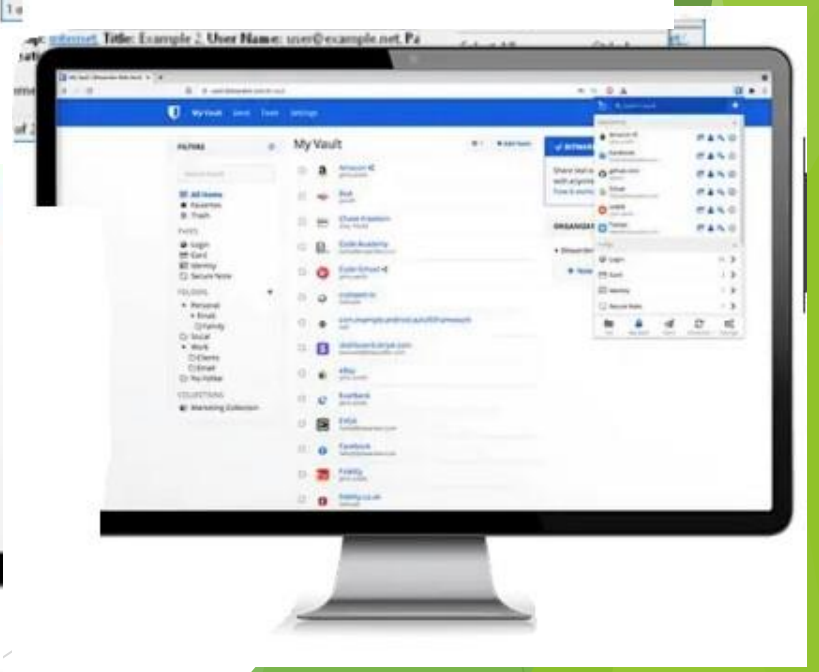
- Slabé heslá
  - Heslo/password
  - Milujemta/iloveyou
  - Pustmadnu/letmein
  - Nbusr123
  - Uhádnuteľné heslá
    - Dátumy narodenia
    - Mená, slová
    - Filmy, piesne, ...

- Recyklácia hesiel
  - Rovnaké heslá na viacerých účtoch
  - 2-3 rôzne heslá, ktoré sa opakujú v závislosti od „dôležitosti“ služby
  - Strata/zabudnutie hesla → reset cez email + ľahké kontrolné otázky

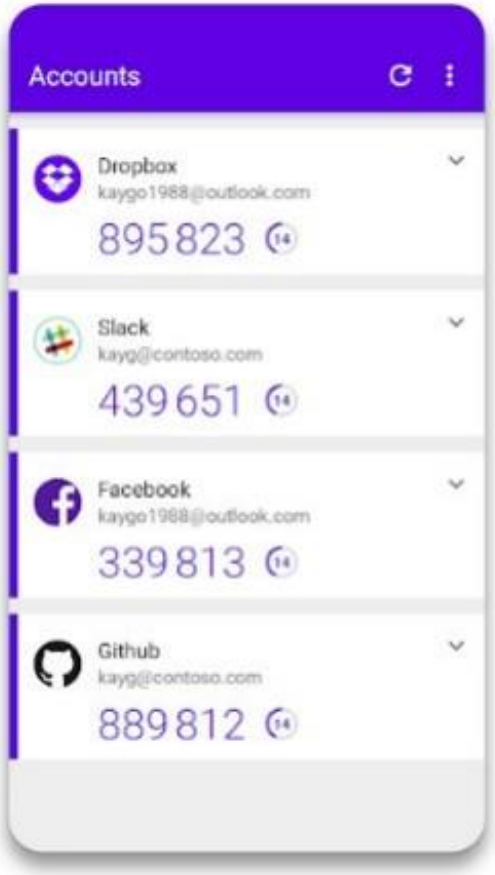
Správcovia hesiel

- Jedno supersilné heslo
  - Ostatné heslé bezpečne uložené
  - Ľahko sa generujú nové bezpečné heslá
  - Možnosť bezpečnej kontroly uniknutých hesiel
  - KeePass (offline), Bitwarden (online)
- Použitie
  - Copy-Paste hesla do prehliadača
  - Alebo priamo doplní správca hesiel
    - Doplnok do prehliadača
    - Iba na správnej stránke
- Na čo si dať pozor?
  - Zabudnutie hlavného hesla
  - Strata zašifrovanej databázy
  - Phishingové stránky





Faktory:
niečo som (biometria),
niečo viem (heslo),
niečo mám (zariadenie).



2FA= + ***_

2FA= +

Druhý faktor

	1	2	3	4	5	6
A	1234	5678	9012	2412	0000	1234
B	0000	1234	5678	9012	2412	0000
C	3333	0000	1234	5678	9012	3333
D	9012	3333	9999	1234	5678	9012
E	9999	5678	3333	1234	3333	5678
F	5678	9999	9999	0000	9999	5678

- Grid karta ani SMS nestačí
  - Možnosť skopírovania karty, málo kombinácií
  - SMS má veľa zraniteľností
- Autentikátor
  - Aplikácia, ktorá generuje kódy
- Bezpečnostný kľúč
  - FIDO2, WebAuthN protokol
  - Odolné voči phishingu
  - Yubikey (25-80 Eur), Key-ID (8 Eur)
- Na čo si dať pozor?
  - Phishingové stránky
  - Strata druhého faktora
  - Strata druhého faktora
    - SMS,Email,kontrolnéotázky,záložnékódy

Odkazy, súbory

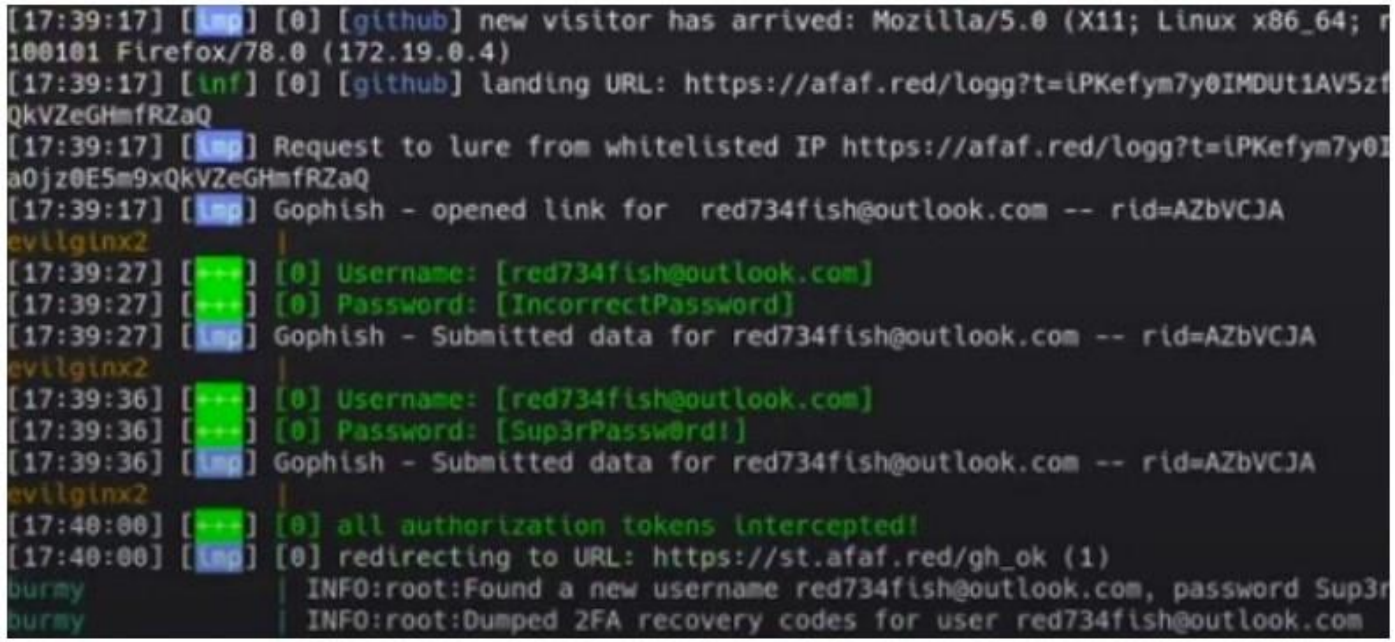
- Zriedkavá kontrola zo strany poskytovateľa
  - Nižšia bezpečnosť ako pri emailoch
  - Väčšia dôvera používateľov
  - Automatické načítanie/sťahovanie
  - „Klikanie“ na mobiloch
    - Bez kontroly, kam odkaz reálne smeruje

- Skracovače URL
  - Tinyurl, bit.ly, goo.gl, ...
  - Zakrývajú skutočnú destináciu
  - Neklikať, prípadne pozrieť si náhľad
    - + na koniec odkazu

Útoky a prevencia

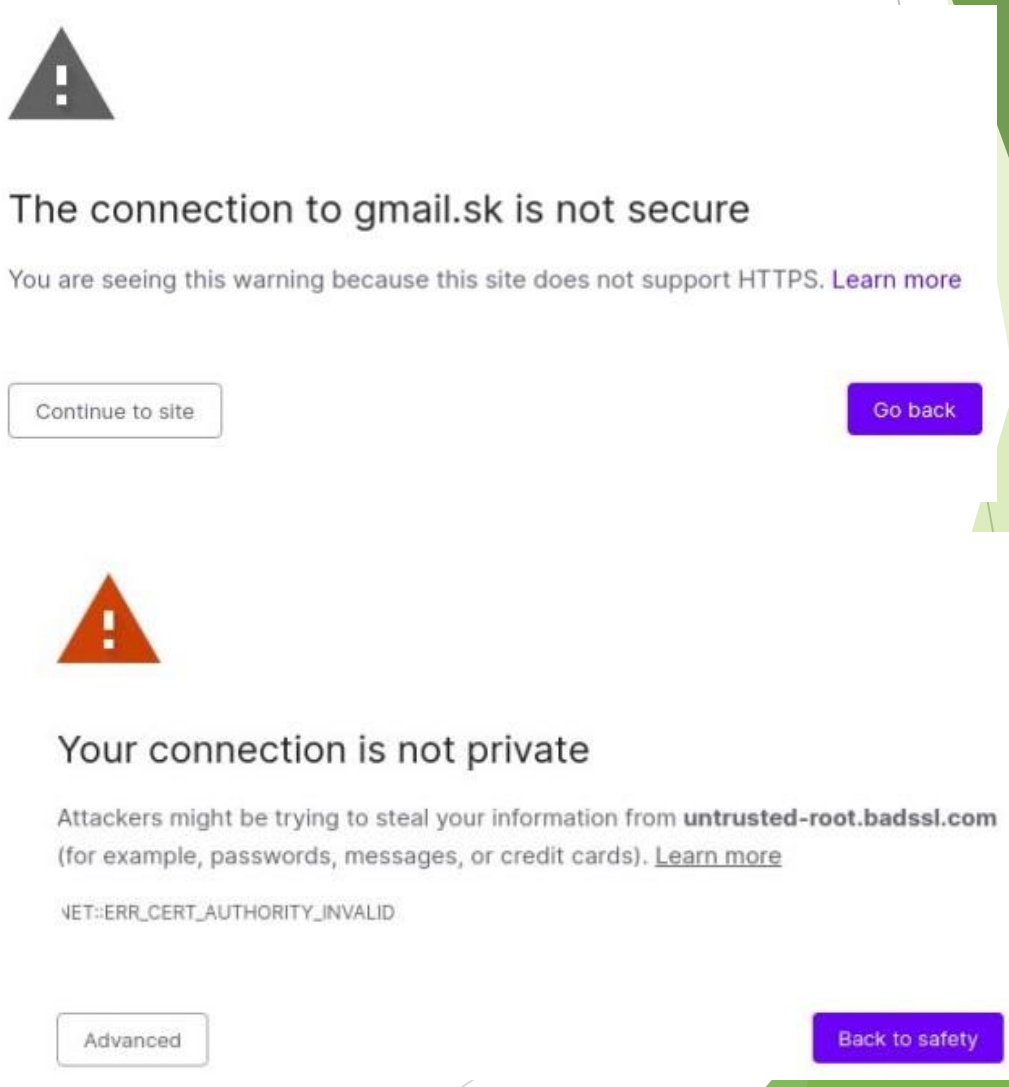
Phishing

- Podvrhnutý odkaz
  - Krádež prihlasovacích údajov
  - Ručné vyplnenie a Copy-Paste hesla



Typosquatting

- Podobné URL
  - Goog1e.com
  - Gmail.sk
  - facebook.com.lang-eu.xyz
  - Skwikipedia.org
- Zdanlivo rovnaké URL
  - IDN homografy
  - Azbuka a latinka
    - CCCP vs SSSR
  - Apple.com
- Rovnaké URL
  - Unesené domény, falošný certifikát
  - *Zmena DNS*



Obrana

- Neklikať na podozrivé odkazy
  - Dôveruj, ale preveruj
    - Náhľady skracovačov URL
    - Nespoliehať sa na zelený zámok (https)
  - Radšej napísať doménu ručne do adresného poľa a preklikať sa
  - Mať dôležité URL v záložkách a klikať iba na ne namiesto tých z mailov
    - Internetbanking
  - Správca hesiel integrovaný v prehliadači/Bitwarden
    - Automatická kontrola správnej domény
  - Bezpečnostný kľúč
    - Yubikey/Key-ID
- Kritické myslenie

Ďakujem za pozornosť!

1.T