

(Ne)bezpečný online svět

Michal Kučera



- 10+ let v IT
- Product Owner & Senior Lecturer
- Microsoft Certified Trainer
- michalkucera.com
- [Instagram](#), [LinkedIn](#), [Twitter](#)

Michal Kučera

Lektor kurzů bezpečnosti

Social Engineering

Modus Operandi

- Vyvolat strach
 - Máme vaše video, fotky,...
- Donutit uživatele jednat pod časovým tlakem
 - Máte jen pět minut, jinak...
 - Pokud nepošlete Bitcoinů do 24 hodin, pošleme ...
- S cílem donutit uživatele k akci, než se zamyslí

Phishing

Phishing

- Útok na uživatele s cílem získat citlivé údaje
 - jméno a heslo
 - 2FA
 - číslo platební karty
- Útočník se vydává za autoritu
 - Banka
 - Poskytovatel služeb (e-mail, e-shop,...)
- Cílený phishing je označován jako *spear-phishing*
 - Konkrétní osoba, společnost

Phishing: e-mail

NETFLIX

Update current billing information

Hi,

Unfortunately, we cannot authorize our payment for next billing cycle of your subscription, Netflix was unable to receive a payment because the financial institution rejected the monthly charge.

To resolve this issue, Please update your payment information by pressing the button below.

Update Payment

Obviously we'd love to have you back. If you change your mind, simply restart your membership and update your payment to enjoy all the best TV shows & movies without interruption.

(Spear)Phishing: e-mail

FWD: 1129832412442 || Azure AD connector blog update



Herman Maier <v-hemaie@support.microsoftonline.ml>
To: Michal Kučera



↩ Reply

↩ Reply All

→ Forward



Sun 2/9/2020 2:33 PM



Podpora

Hi Michal,

My name is Herman and I am assisting on the case regarding STC blog project. From the case it seems that there was a problem with application link.

During my remote session with Mr. Hruban we modified the AAD link but to complete the solution everyone needs to regrant permissions to blog app. Then we will finish the task and everyone who did not regrant will be unable to log in.

Please use this link to regrant (grant) permissions: https://login.microsoftonline.com/45ab8ba3-4ca1-45bd-95d7-18658bb01287/oauth2/authorize?client_id=52f095c0-3135-4f2b-a270-87c816665059

Thank You

With Best Regards,

Herman Maier

Senior Support Engineer || Azure Identity

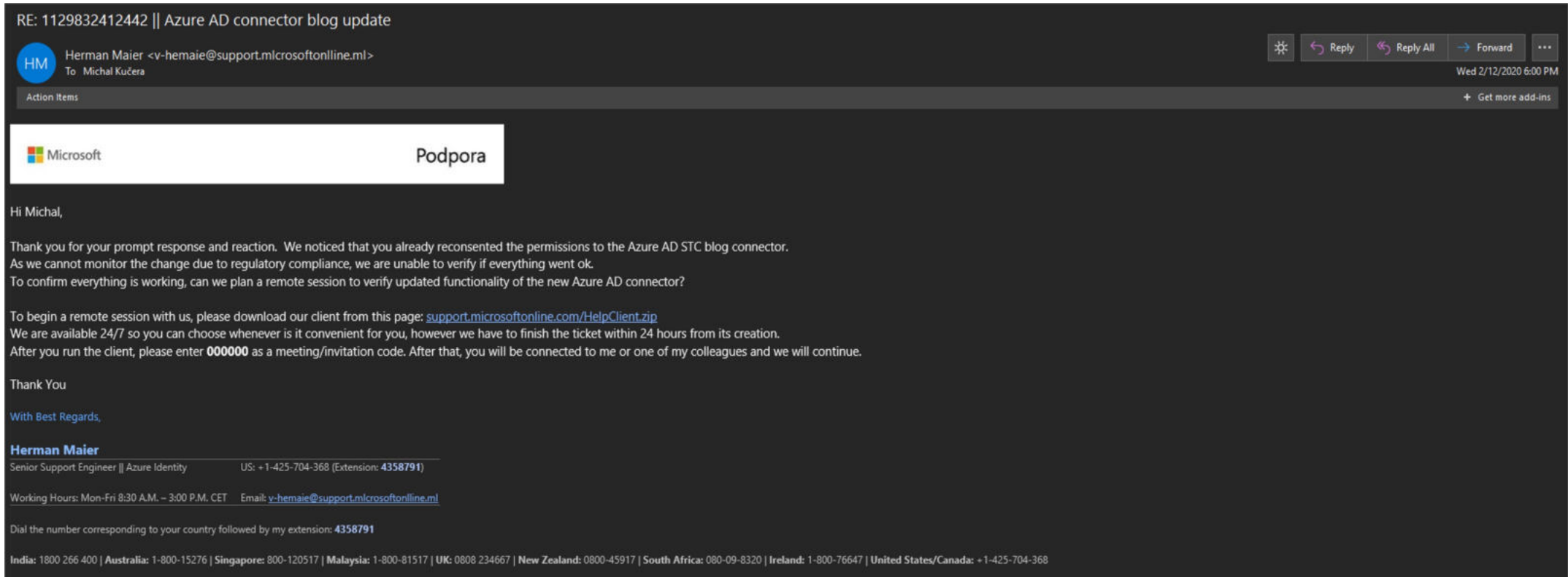
US: +1-425-704-368 (Extension: **4358791**)

Working Hours: Mon-Fri 8:30 A.M. – 3:00 P.M. CET Email: v-hemaie@support.microsoftonline.ml

Dial the number corresponding to your country followed by my extension: **4358791**

India: 1800 266 400 | Australia: 1-800-15276 | Singapore: 800-120517 | Malaysia: 1-800-81517 | UK: 0808 234667 | New Zealand: 0800-45917 | South Africa: 080-09-8320 | Ireland: 1-800-76647 | United States/Canada: +1-425-704-368

(Spear)Phishing: e-mail



Phishing: bankovníctví 1/5



Vážený zákazníku,

Platba byla na váš účet zveřejněna dne 12/11/2017.
K uvolnění platby na váš účet je však nutné ověřit platbu.

Zacnete kliknutím a přihlášením do svého účtu [zde](#).

Jsme připraveni vám sloužit lépe.

S pozdravem,
Raiffeisenbank

Podezřelý odkaz ✕

Tento odkaz vede na nedůvěryhodnou stránku. Opravdu chcete pokračovat na stránku greenmarketingzone.com?

[Pokračovat](#) [Zpět](#)

Phishing: bankovníctví 2/5

Banka inspirovaná klienty

[CZ / EN](#) | [Kontakty](#) | [Bezpečnost](#) | [Nápověda](#)

Vstup na účet

Způsob přihlášení

SMS kód

RB klíč

Osobní klíč

Klientské číslo



Zapomněli jste Vaše Klientské číslo? Navštivte jakoukoli pobočku Raiffeisenbank.



Požádejte o autentizační kód kliknutím na tlačítko
POSLAT KÓD

POSLAT KÓD ▶

Upozornění: Autentizační kód bude zaslán na Váš mobilní telefon. V případě potíží nás kontaktujte na NONSTOP infolince 800 900 900 nebo e-mailem na info@rb.cz

Phishing: bankovníctví 3/5



**Raiffeisen
BANK**
Banka inspirovaná klienty

CZ / EN | [Kontakty](#) | [Bezpečnost](#) | [Nápověda](#)

Vstup na účet

Způsob přihlášení

SMS kód

RB klíč

Osobní klíč

Autentizační kód byl zaslán na Váš mobilní telefon

Autentizační kód



kód je ve formátu např. 1234 - 1234 - 123

I-PIN

PŘIHLÁSIT SE ▶

[nebo znovu Poslat kód](#)

V případě potíží nás kontaktujte na NONSTOP infolince 800 900 900 nebo e-mailem na info@rb.cz

Phishing: bankovníctví 4/5





Osobní bankovníctví

CZ

ODHLÁSIT

CERTIFIKAČNÍ KÓD

KROK 3 ZE 3



Certifikační kód byl zaslán na Váš mobilní telefon

Certifikační kód*

[nebo znovu Poslat kód](#)

 ZPĚT

POTVRDIT 

 800 900 900
Tuzemské

 +420 412 446 400
Mezinárodní

 info@rb.cz
Odpovíme do 24 hodin

Poslední přihlášení 07.04.2020 08:09:49
© 2020 Raiffeisenbank

Phishing: bankovníctví 5/5

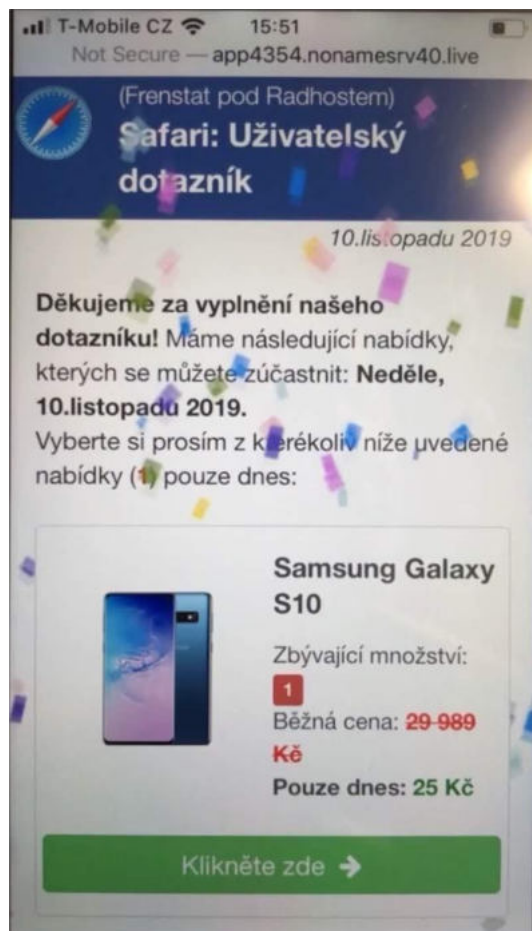
Omlouváme se, požadovaná stránka neexistuje

Uvedenou stránku se nám nepodařilo najít. Je možné, že byla odstraněna, přejmenována nebo není dočasně dostupná.

Zkuste použít jednu z uvedených možností:

- Zkontrolujte, zda máte správnou adresu.
- Zkuste začít znovu z úvodní stránky.
- Vraťte se zpět na předchozí stránku.
- Využít vyhledávání v pravém horním rohu stránky.

Phishing: reklama



Phishing: obchod, banka



(Ceska Sporitelna) Vazeny
kliente, Vase internetove
bankovnictvi bylo zablokovano.
Pro odblokovani pokračujte na
<https://csas-george.best/csas>
([CSAS.CZ](https://csas-george.best/csas))

Phishing: česká pošta



Česká pošta, s.p. @Ceska_posta_sp · 31 m



VAROVÁNÍ !!

V posledních hodinách se objevují sms, že Váš balíček je k dispozici.

Přiložen je odkaz bit tečka ly lomeno CeskaPosta.

Po rozkliknutí je adresát přesměrován na stránku s doménou .ru, kde platební brána žádá údaje k platební kartě.

Jedná se o podvod! Na nic neklikejte!



15



268



431



Phishing: česká pošta

Seznam dodávek a/nebo sbírek

Česká pošta Vám umožňuje kdykoliv sledovat zásilky Vašich balíků

Rychlý balík: Váš balíček je odestán do 24 hodin

Česká pošta

Zadejte správně následující informace a klikněte na tlačítko níže

*Tvoje jméno

*. telefonní číslo

*Číslo karty

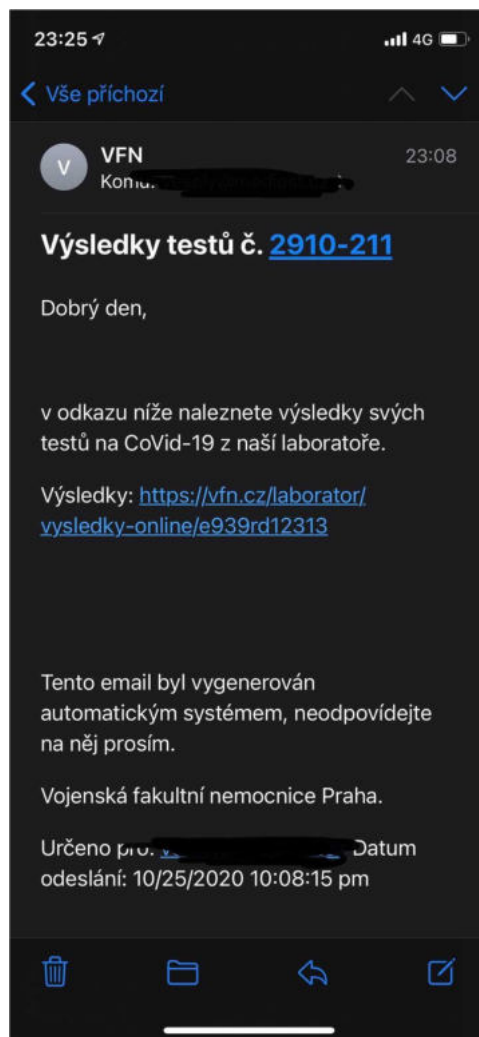
Expiry Month

Year

CVV

[pokračovat](#)

Phishing: test na COVID





Stav: Nové / Málo používané

Množství: 1

Cena: **1000 Kč**

Adresa: Kopernikova 1267, 735 53 Dolni Lutyne

Název: Svoboda

Příjmení: Tereza



Kupující již objednávku zaplatil.

Po obdržení peněz na vaši kartu odešlete zboží kupujícímu dle zadaných údajů nebo k rukám kurýra, který vás bude do 12 hodin kontaktovat.

Po odeslání položky poskytněte kupujícímu sledovací číslo! Položka musí být odeslána do 3 dnů od obdržení peněz

Sada knih Deník maleho poseroutky - 1. az 7. díl
1000 Kč

Získat prostředky



 **Provádějte platby bezpečně**

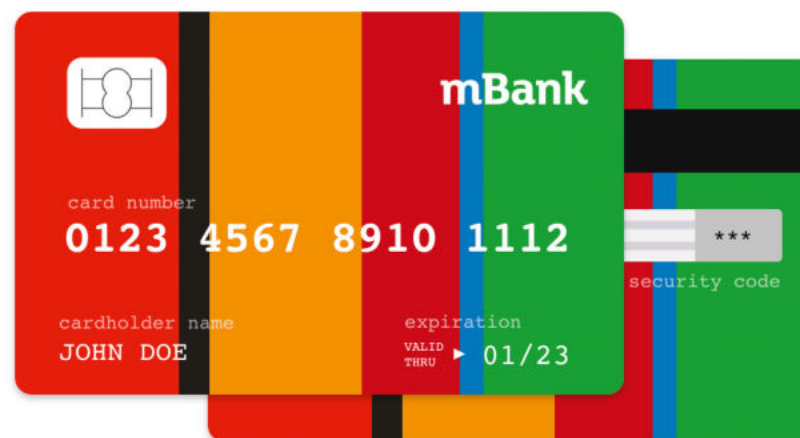
Kliknutím na tlačítko „Získat prostředky“ souhlasíte s podmínkami používání online služby „Bezpečná nabídka“.



@ Bazoš.sk



Zadání bankovní karty



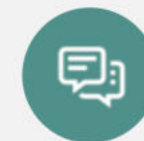
Jméno a příjmení držitele karty

Číslo karty

Datum ukončení platnosti (mm/yy)

CVC/CVV

Další





Přihlaste se na webovou stránku transakce

Individuální i firemní klienti

Rodné číslo s lomítkem nebo cestovní pas série a číslo

Vaše heslo

Zadejte jméno své matky za svobodna

PIN aplikace

Datum narození

Pokračovat





Zadaná data se ověřují

Může to trvat několik minut,
prosím nezavírejte stránku, dokud nebude stahování dokončeno



Pokračovat



mBank varuje!

Dejte si pozor na podvodníky, kteří tvrdí, že jsou zaměstnanci bank nebo investiční poradci v oblasti kryptoměn! - více

Telefonický Phishing (Vishing)

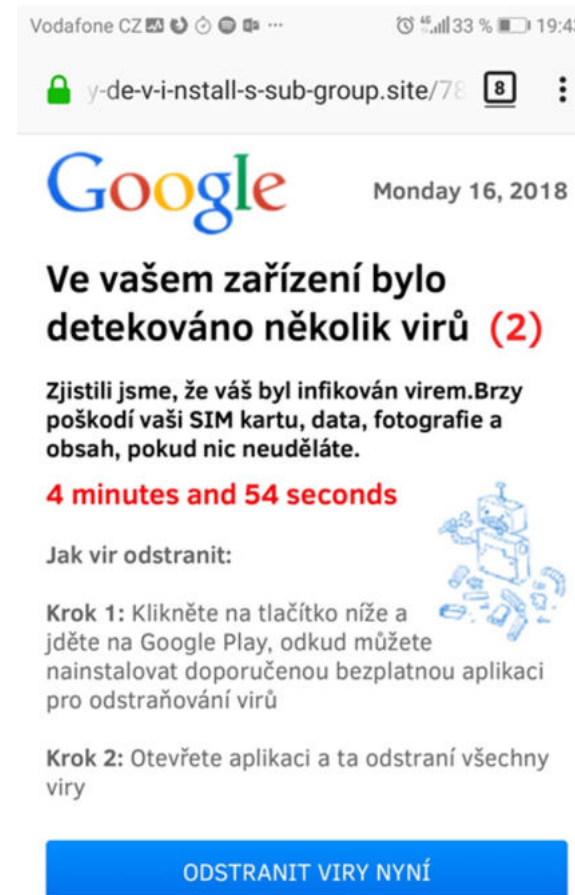
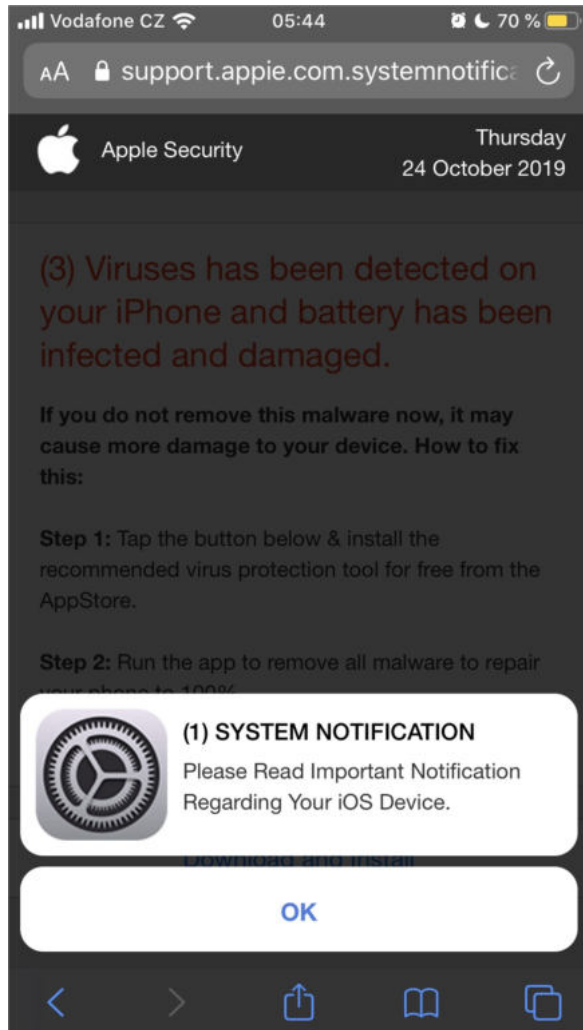


[Aktivita na doma] Zkuste nenaletět

- Otevřete si Phishing Quiz
- Zadejte požadované údaje a odhalte phishing

Malware

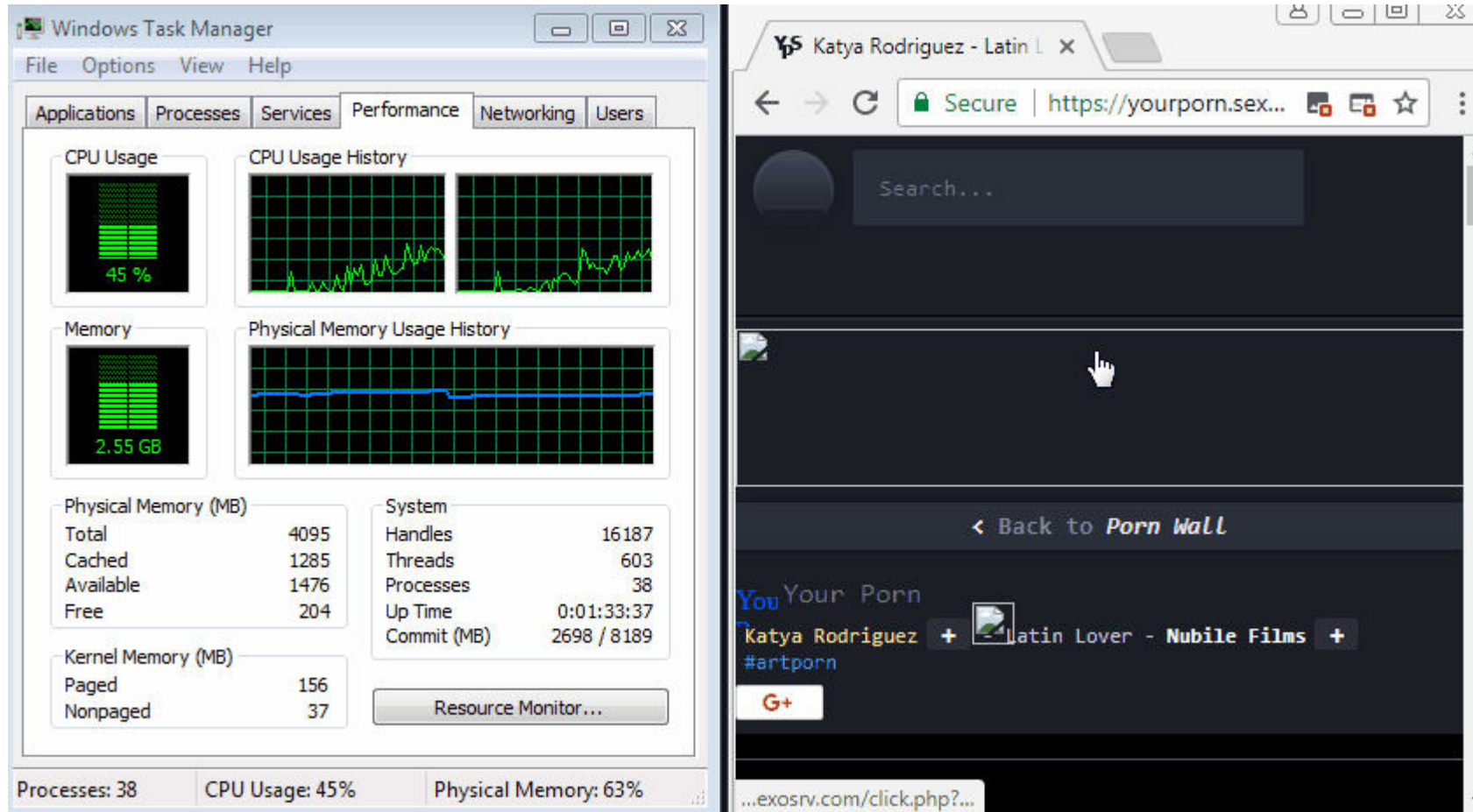
Malware



Malware - ransomware



Malware – cryptojacking



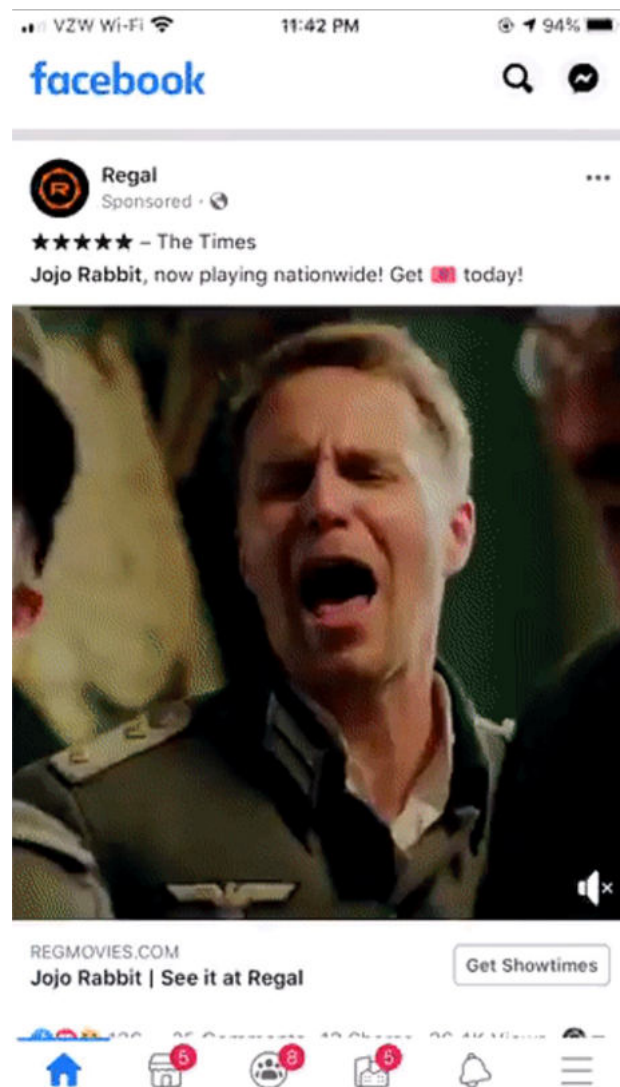
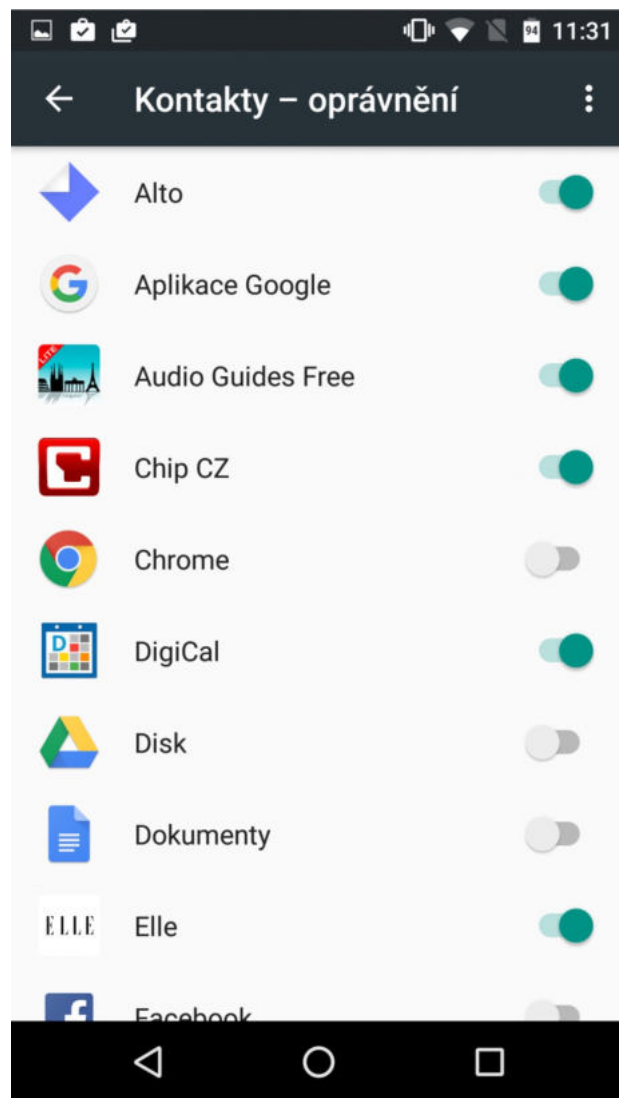
Antivirus

- Pravidlo č. 1 – aktualizujte
- **Základní funkcionality:** ochrana v reálném čase, pravidelná aktualizace virové databáze
- **Prémiové funkce:** Pokročilé webové štíty, správce hesel, rodičovská ochrana, šifrování apod.

Obecné tipy & triky

- Nenechávejte přihlášený počítač – win + L
- V základu mějte 2 účty – jeden admin + jeden user
- Zálohujte do cloudu, popř. na externí HDD
- Pokud máte možnost, šifrujte obsah počítače (bitlocker)
- Při recyklaci počítače, minimálně zformátujte disky

Oprávnění aplikací

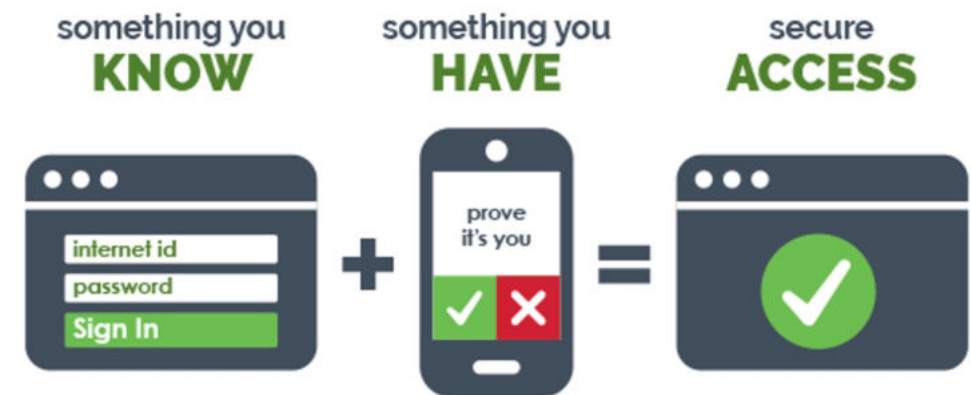
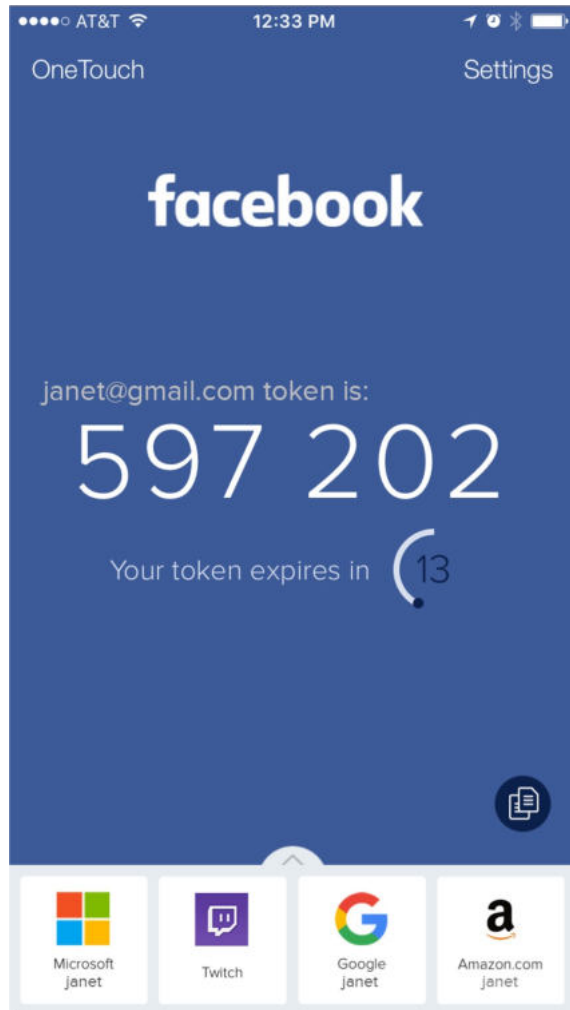


Přihlašování

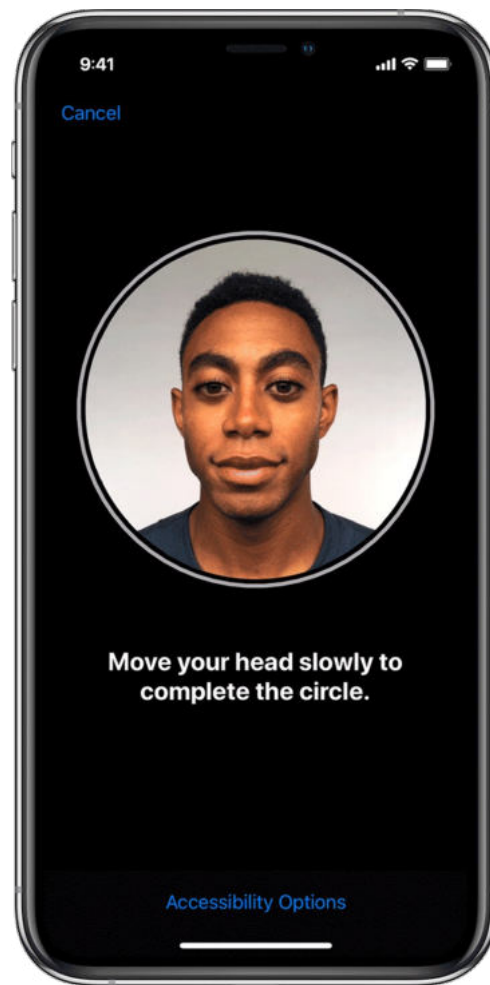
Co znám



Co mám



Co jsem



Kdo všechno zná mé heslo?



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?

Kontrola přihlášení/zabezpečení

- Kdo a odkud je přihlášený
- Notifikace, že se někdo přihlásil



Kontrola zabezpečení

Všechny problémy byly vyřešeny

	Nastavení Gmailu 2 citlivá nastavení	▼
	Vaše zařízení 3 přihlášená zařízení	▼
	Nedávné události zabezpečení Žádné události za 28 d	▼
	Dvoufázové ověření Dvoufázové ověření je zapnuto	▼
	Přístup třetích stran 1 aplikace s přístupem k vašim datům	▼

[Pokračovat do účtu Google](#)

Apple <noreply@email.apple.com>
komu: mně ▾



Dear Ondřej Šrámek,

Your Apple ID [REDACTED] was used to sign in to iCloud via a web browser.

Date and Time: 31 March 2020, 6:41 am PDT

If the information above looks familiar, you can disregard this email.

If you have not signed in to iCloud recently and believe someone may have accessed your account, go to Apple ID (<https://appleid.apple.com>) and change your password as soon as possible.

Sincerely,

Apple Support

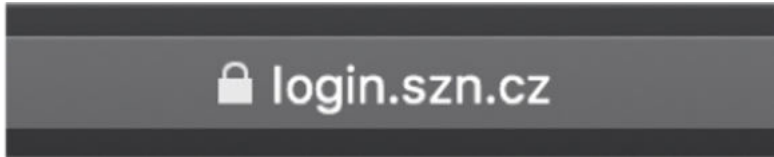
[Apple ID](#) | [Support](#) | [Privacy Policy](#)
Copyright © 2020 Apple Distribution International Ltd. Hollyhill Industrial Estate, Hollyhill, Cork, Ireland. All rights reserved.

Co všechno máte v e-mailu?

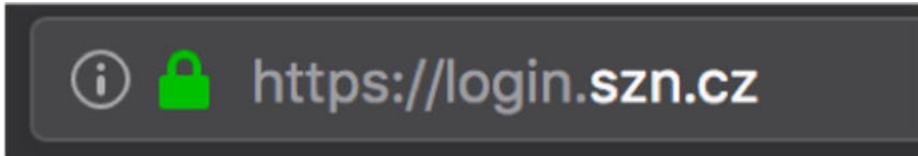
- Zprávu o registraci... (sociální síť, eshop,...)
 - i s heslem!
- Zprávu s magickým odkazem
 - Po kliknutí se přihlásíte, např. Facebook
 - Máte od někoho zprávu
 - Změnili jste si heslo
 - Chcete si restartovat heslo (zapomněli jste ho)
- Je lepší nic z výše uvedeného ve schránce nemít
 - Když se Vám někdo dostane do e-mailu, má všechno...

Zabezpečená komunikace

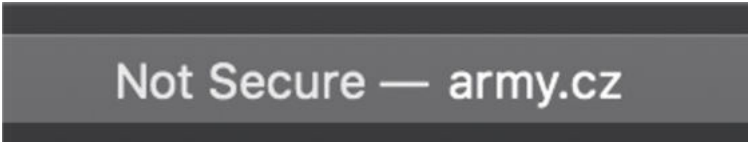
- Vždy, když zadáváte data
 - Osobní údaje
 - Číslo karty
 - Heslo
 - 2FA
- Chcete **věřit** obsahu
 - Úřady
- Konec EV certifikátů
- Bez certifikátu = **nezabezpečeno!**



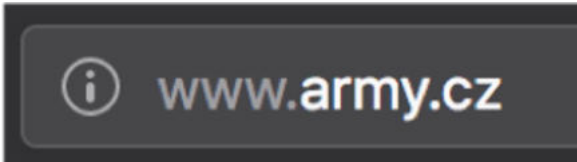
login.szn.cz



https://login.szn.cz



Not Secure — army.cz



www.army.cz

Koupíte si lístek na koncert?



KOUPIT VSTUPENKU

STŘEDA 13. 11.
■ VOXEL + HOSTÉ
19:30, VELKÝ SÁL

KATEGORIE VSTUPENEK A CENA		POČET	
STÁNI: 270 Kč		0	
		CELKEM	
		0 Kč	
JMÉNO		PŘÍJMENÍ	
E-MAIL		TELEFON	
PLATEBNÍ METODA			
PLATBA KARTOU		MŮŽES ZAPLATIT KARTOU VISA NEBO MASTERCARD.	
ČÍSLO KARTY	MĚSÍC	ROK	CVV
☐ SOUHLASÍM SE ZASÍLÁNÍM NOVINEK OD GOOUT A POŘADATELE. CHCEŠ VĚDĚT VÍC?			
☐ NÁKUPEM VSTUPENEK SOUHLASÍM S OBCHODNÍMI PODMÍNKAMI GOOUT A BERU NA VĚDOMÍ ZÁSADY SOUKROMÍ.			

ZAPLATIT KARTOU

Druhý faktor

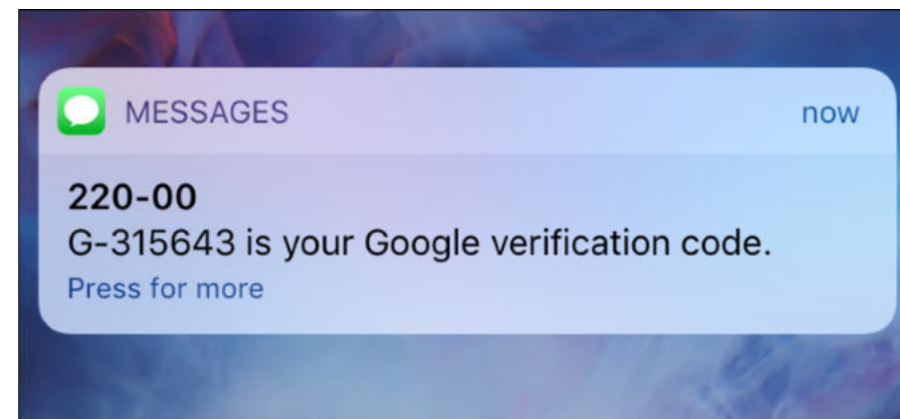
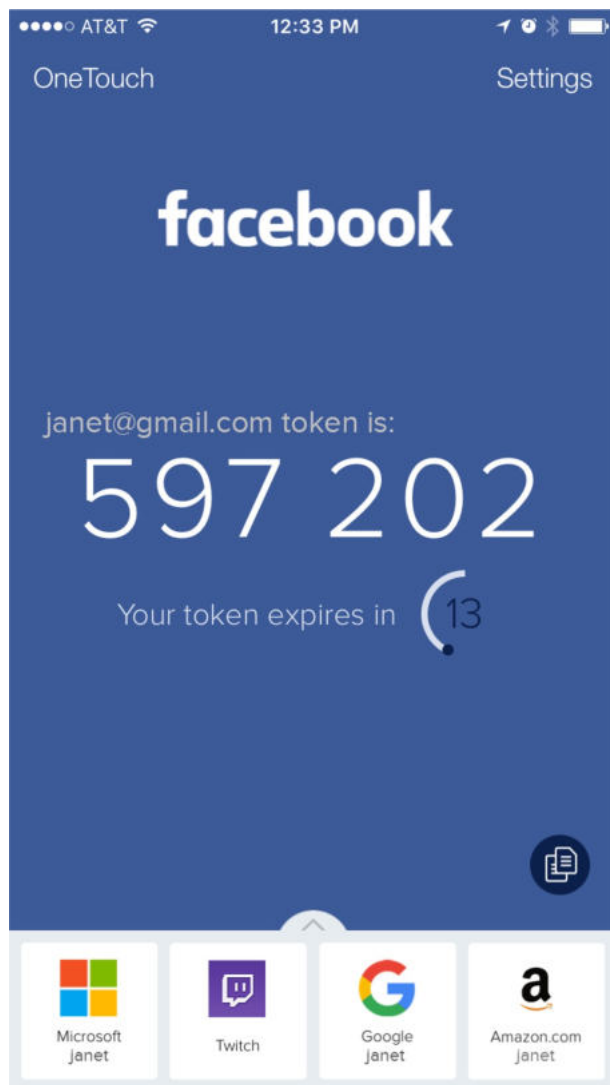
Proč další krok při přihlášení?

- Nařízení (směrnice PSD2)
 - Internetové bankovníctví, potvrzení platby kartou on-line,...
- Ztížení prolomení účtu
 - Heslo může znát kde kdo...
 - Ale kód/zařízení (zpravidla) má jen ten správný člověk

Jak?

- Speciální aplikace (Authy, Duo, Google Authenticator,...)
- Speciální zařízení (RSA Authenticator, YubiKey,...)
- Nativní součást systému
 - Android: Push notifikace (přístup ke Google službám)
 - iOS: Touch ID/Face ID
- Zaslání kódu e-mailem
- SMS

Příklady



Co dělat se záložními kódy

- Záložní přístup do účtu
 - Když všechno selže (ztratíte telefon, ukradnou Vám ho,...)
- Ideálně vytisknout a vložit do obálky, zalepit
 - Trezor
 - Zamčený šuplík

Co když moje oblíbená služba neumí...

- Kontaktujte provozovatele
- email.cz
 - E-Mail řešení od Seznam.cz podporuje pouze proprietární apku

SMS 2FA

- Stále používaná metoda
 - Nedoporučovaná (NIST 800-63B) od poloviny roku 2017
- Pokud není jiná alternativa je to lepší než nic
 - Existuje-li lepší, použijte ji!

Heslo

Lepítko s heslem



Uhodnout heslo není těžké

- Nejčastější heslo je 123456
- Jméno přítele/přítelkyně + nějaké číslo
- Jméno syna/dcery + rok narození
- Telefon
- Rodné číslo
- Oblíbená kapela, fotbalový klub
- Oblíbený herec/herečka
- Domácí mazlíček
- Password Reuse



Kdo všechno zná mé heslo?

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address

pwned?

[Aktivita] Zná někdo mé heslo?

- Otevřete si [Have I Been Pwned](#)
- Zadejte Váš e-mail
- Notifikoval Váš provozovatel o úniku?
- Co jste udělali?
- Pamatujete si to heslo?
- Kde všude jste takové heslo měli?
 - Změnili jste to heslo i jinde?

Jaké by mělo být moje heslo?

- Dlouhé (ideálně 13 a více znaků)
- Komplexní (malé, velké, speciální a numerické znaky)
- Nenajdete ho ve slovníku (ani když více slov zřetězíte)
- O generování a uložení se postará správce hesel
 - Vyjma jednoho...

A co kontrolní otázka?

- Záložní přístup k účtu (e-mail,...)
- Jméno matky za svobodna není ideální
 - Stejně jako oblíbený herec, film, jídlo,...
 - Obecně, pokud je odpověď uhádnutelná není to dobře
- Ideálně
 - Druhý e-mail
 - Push notifikace
 - Telefon (přijde Vám SMS)

Správce hesel

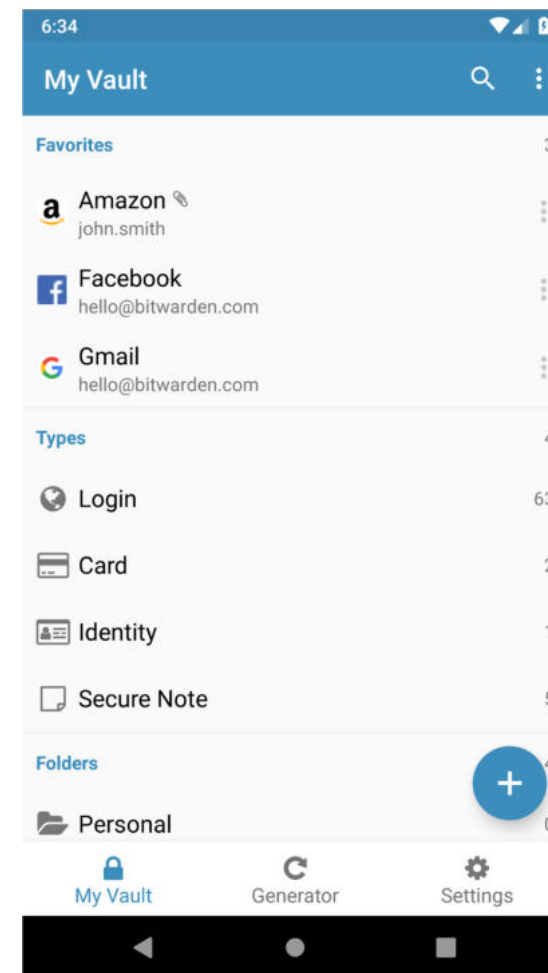
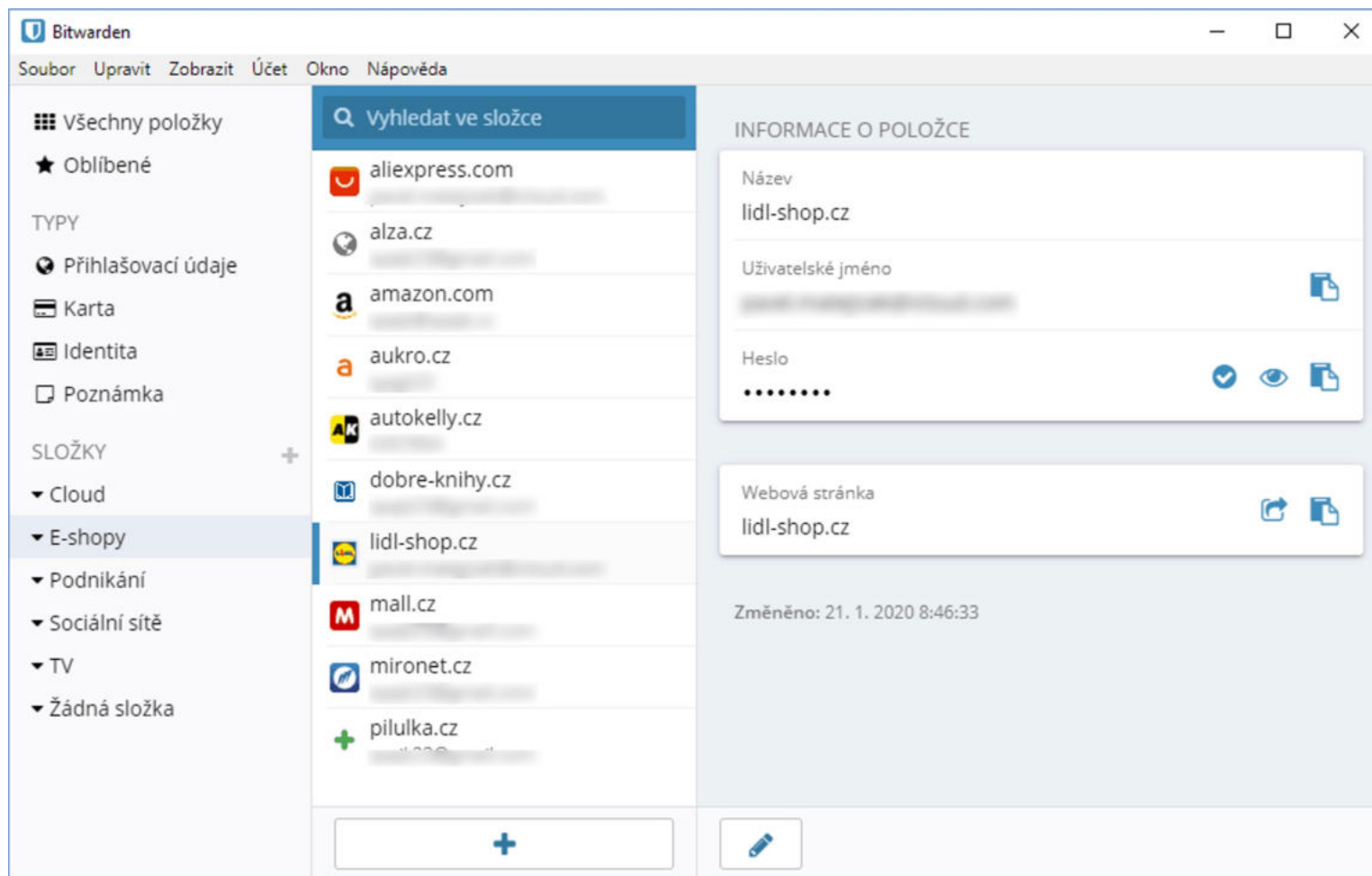
Lístčky nestačí...

- Kolik služeb používáte, stovky?
- Každá služba by měla mít své unikátní heslo.
- Správce hesel
 - Nemusí to být jen aplikace (speciální notýsek jen na hesla)
 - Není vhodné pro každého
 - Aplikace
 - Lokální (jen na jednom zařízení), odjinud se nepřihlásíte
 - Vzdálená (synchronizace napříč zařízeními)

Co by správce hesel měl umět?

- Pamatuje si vaše hesla
 - Včetně historie
- Vygeneruje vám nové (podle zadaných parametrů)
- Kontroluje jestli vaše heslo není kompromitované
- Upozorní vás na vícenásobné použití jednoho hesla
- Pomůže vám s přihlášením (vyplněním údajů)

Správce hesel



Jedno přihlášení pro všechno

Single Sign On (SSO)

Jedno přihlášení (SSO)

- Jedno jméno a heslo pro více služeb
- Přihlašte se pomocí
 - Google
 - Facebook
 - [MojeID](#)
 - Poměrně rozšířené na českém Internetu
 - [BankID](#)
 - Vaše banka váš ověří v přístupu k dalším službám
 - [elidentita](#)
 - V rámci služeb státní správy: Datová schránka, Moje daně,...

mojeiD

- Katalog služeb
 - e-maily, instituce, města, e-shopy, hostingsy a domény
 - <https://www.mojeid.cz/cs/kde-pouzit/kde-pouzit-katalog/>
- Validovaný účet
 - Jednoznačná identifikace uživatele
 - Validace je možná v knihovně a dalších místech
 - <https://www.mojeid.cz/cs/jak-na-to/identifikace-aneb-piny-validace/#map>
- Ověřeno MojeiD
 - Bezplatné získání HW klíčenky
 - <https://overeno.mojeid.cz>
 - Přístup do portálů státní správy

Pojďme zůstat v kontaktu 😊



@mi_kucera



@mi_kucera



/mikucera

michalkucera.com

Zdroje

Souhrn informací z prezentace

- [Rozcestník informací z kurzu](#)
- Včetně zdrojů, častých chyb a toho nejdůležitějšího
- Něco je špatně? Dejte nám, prosím, vědět.

Použité nástroje/aplikace

- uBlock Origin
 - Blokuje reklamy a nevyžádaný obsah
 - Hledejte mezi doplňky Vašeho webového prohlížeče
- Správce hesel
 - Bitwarden, <https://bitwarden.com> ; zdarma
 - Dashlane, <https://www.dashlane.com> ; zdarma *
 - EnPass, <https://www.enpass.io/> ; zdarma *
- 2FA
 - Authy, <https://authy.com>
 - YubiKey, <https://yubikey.cz>

Odkazy na další zdroje I.

- Have I Been Pwned
 - <https://haveibeenpwned.com>
- Should I Click?
 - <https://www.shouldiclick.org/>
- Přehled služeb s podporou 2FA
 - <https://twofactorauth.org/>
- MojeID
 - <https://www.mojeid.cz/>
- Reverse Image Search
 - <https://www.tineye.com/>
- RFC 1855
 - <https://www.hoax.cz/hoax/netiketa>
- The Great Hack (Cambridge Analytica)
 - <https://www.csfd.cz/film/688510-velky-hack/komentare/>
- Social Dilemma
 - <https://www.csfd.cz/film/812238-socialni-dilema/prehled/>

Odkazy na další zdroje II.

- Michal Špaček: Nepoužívám žádnou VPN pro bezpečnost nebo anonymitu
 - <https://www.michalspacek.cz/nepouzivam-zadnou-vpn-pro-bezpecnost-nebo-anonymitu>
- Dezinformační Imunologie Transparency International
 - https://www.youtube.com/playlist?list=PLVflkbZEOn9l5_VcUlwoKXclf7znrMJ5D
- Bezpečnost na Internetu (Televize Seznam)
 - <https://www.televizeznam.cz/video/jak-na-penize/bezpecnost-na-internetu-63977081>
- #martyisdead (mall.tv)
 - <https://www.mall.tv/martyisdead>
 - <https://www.martyisdead.cz>
- Projekt E-Bezpečí
 - <http://www.e-bezpeci.cz>
- Bud' Safe Online (Avast)
 - <https://www.budsafeonline.cz/blog/kyberbezpecnost>
- To se ví
 - <https://www.ceskatelevize.cz/porady/12884096665-to-se-vi/>
- Hoax, SPAM,...
 - <https://manipulatori.cz>
 - <https://www.hoax.cz>