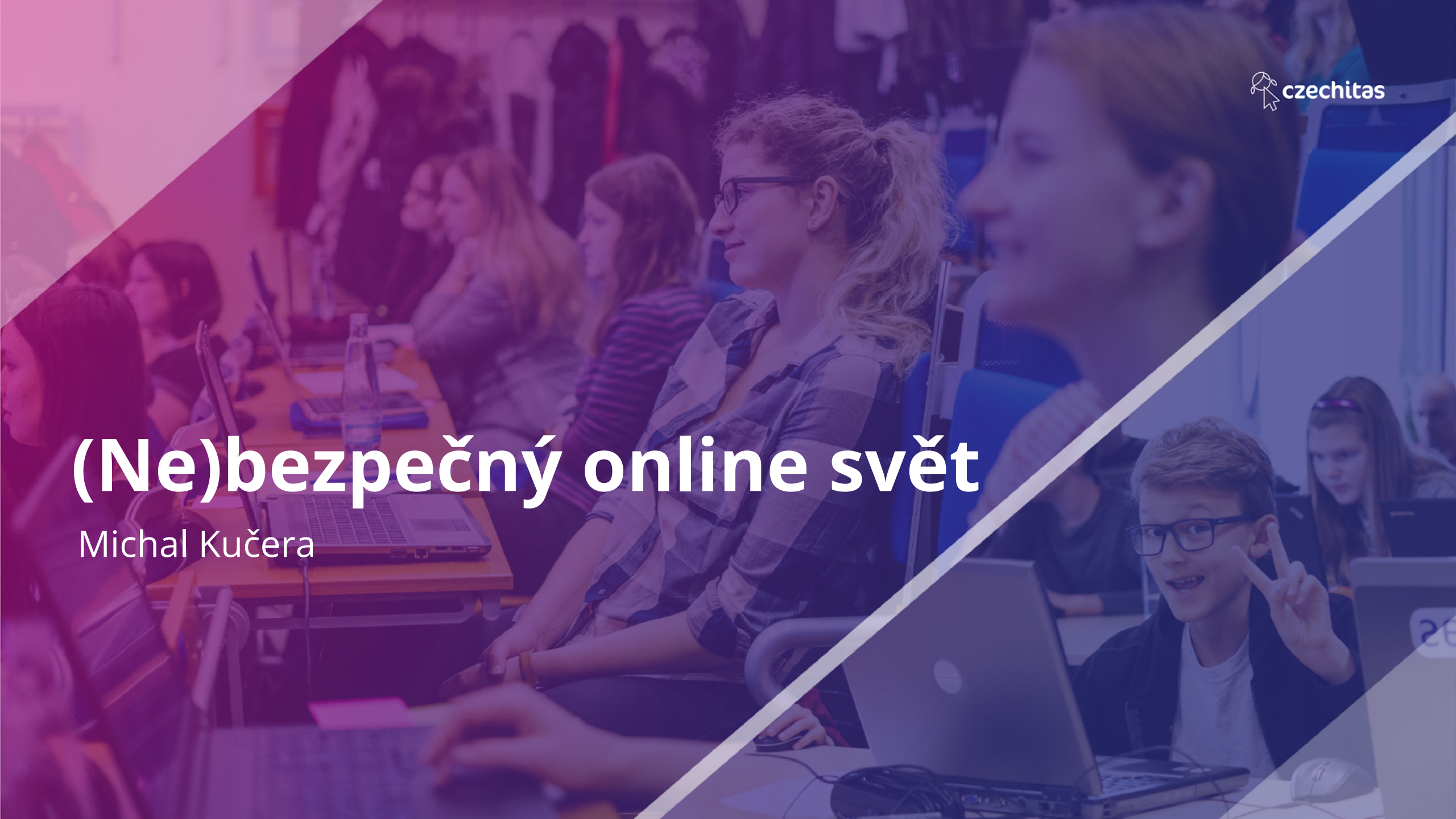


czechitas

(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

czechitas

Social Engineering

Modus Operandi

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

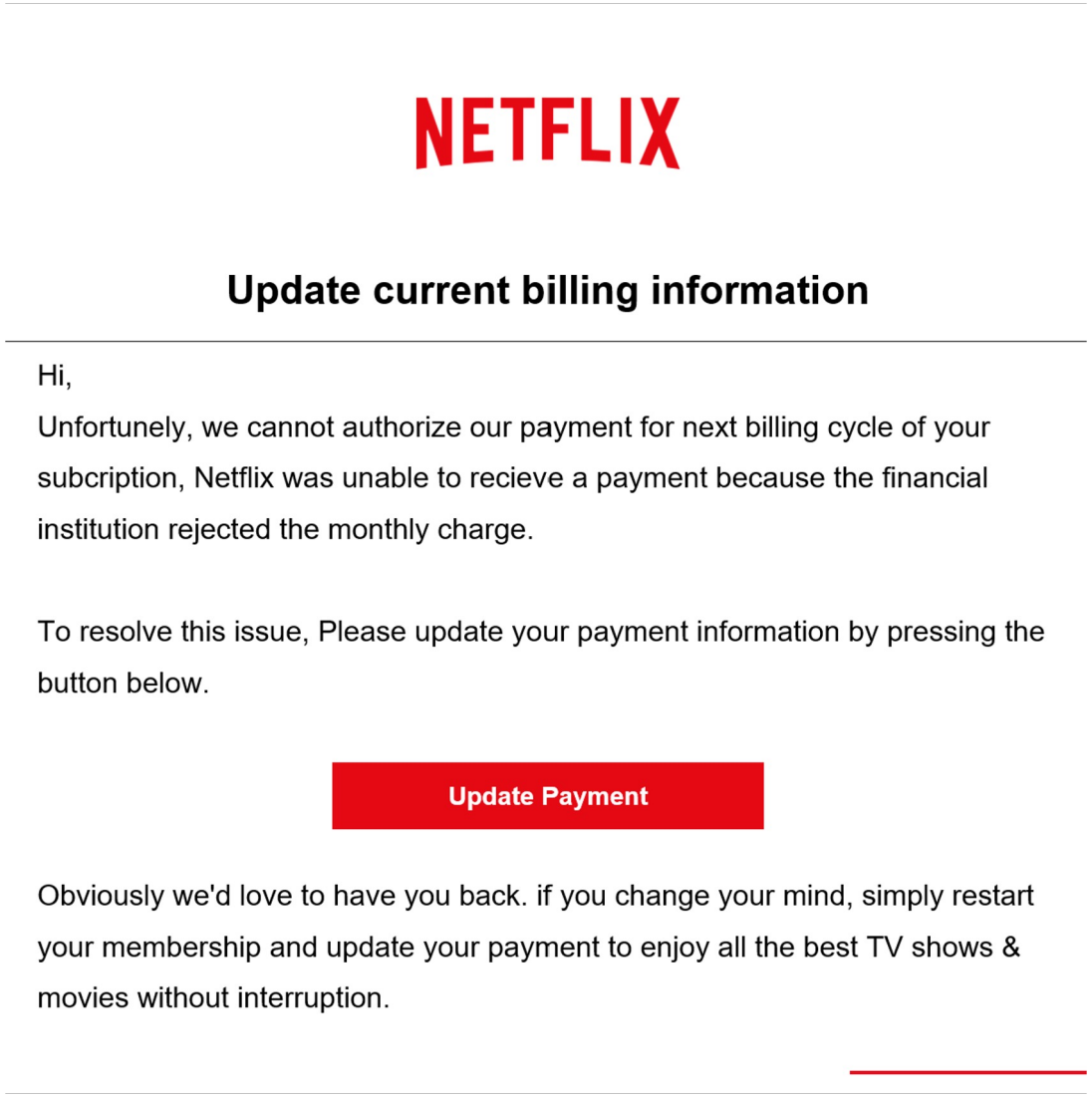
Phishing

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,

Unfortunely, we cannot authorize our payment for next billing cycle of your subcription, Netflix was unable to recieve 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

HM Herman Maier <v-hemaie@support.mlcrosoftonlline.ml>
To Michal Kučera

Reply | Reply All | Forward | ...
Sun 2/9/2020 2:33 PM

Microsoft 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 reconsent permissions to blog app. Then we will finish the task and everyone who did not reconsent will be unable to log in.

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

Thank You

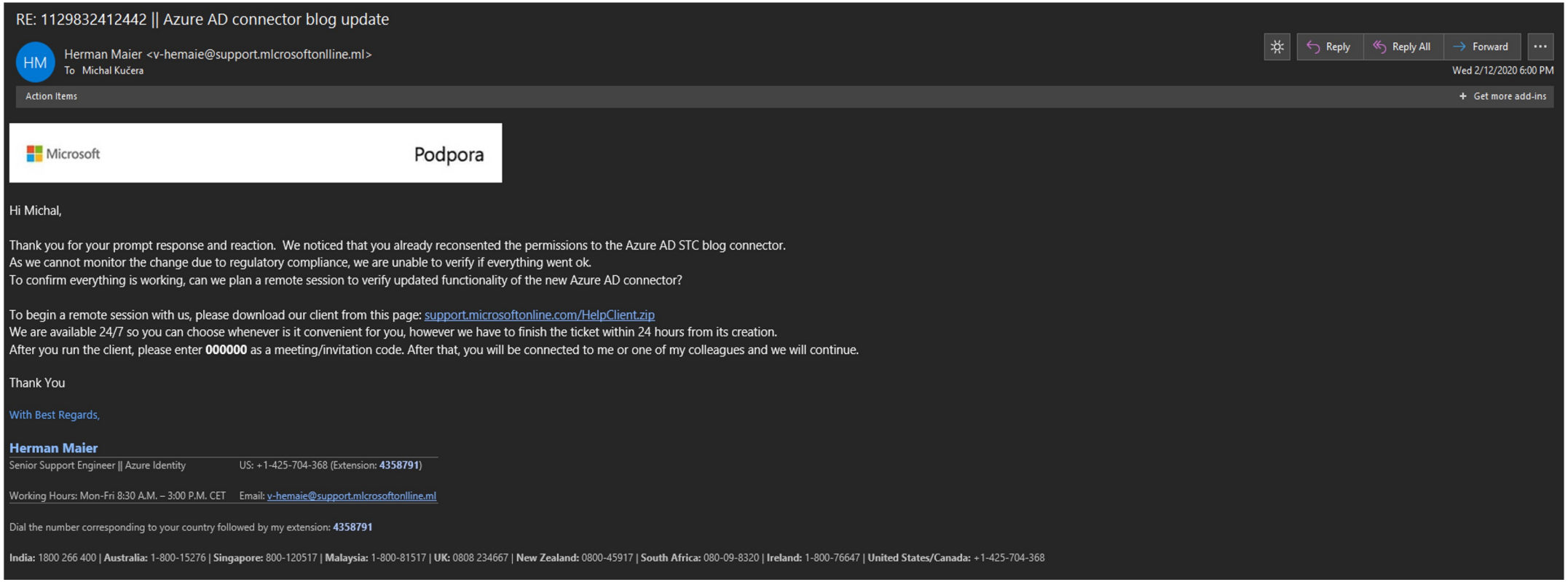
With Best Regards,

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.mlcrosoftonlline.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



RE: 1129832412442 || Azure AD connector blog update

HM Herman Maier <v-hemaie@support.mlcrosoftonlline.ml>
To Michal Kučera

Reply | Reply All | Forward | ...
Wed 2/12/2020 6:00 PM

Action Items | + Get more add-ins

Microsoft Podpora

Hi Michal,

Thank you for your prompt response and reaction. We noticed that you already reconsented the permissions to the Azure AD STC blog connector.
As we cannot monitor the change due to regulatory compliance, we are unable to verify if everything went ok.
To confirm everything is working, can we plan a remote session to verify updated functionality of the new Azure AD connector?

To begin a remote session with us, please download our client from this page: support.microsoftonline.com/HelpClient.zip
We are available 24/7 so you can choose whenever is it convenient for you, however we have to finish the ticket within 24 hours from its creation.
After you run the client, please enter **000000** as a meeting/invitation code. After that, you will be connected to me or one of my colleagues and we will continue.

Thank You

With Best Regards,

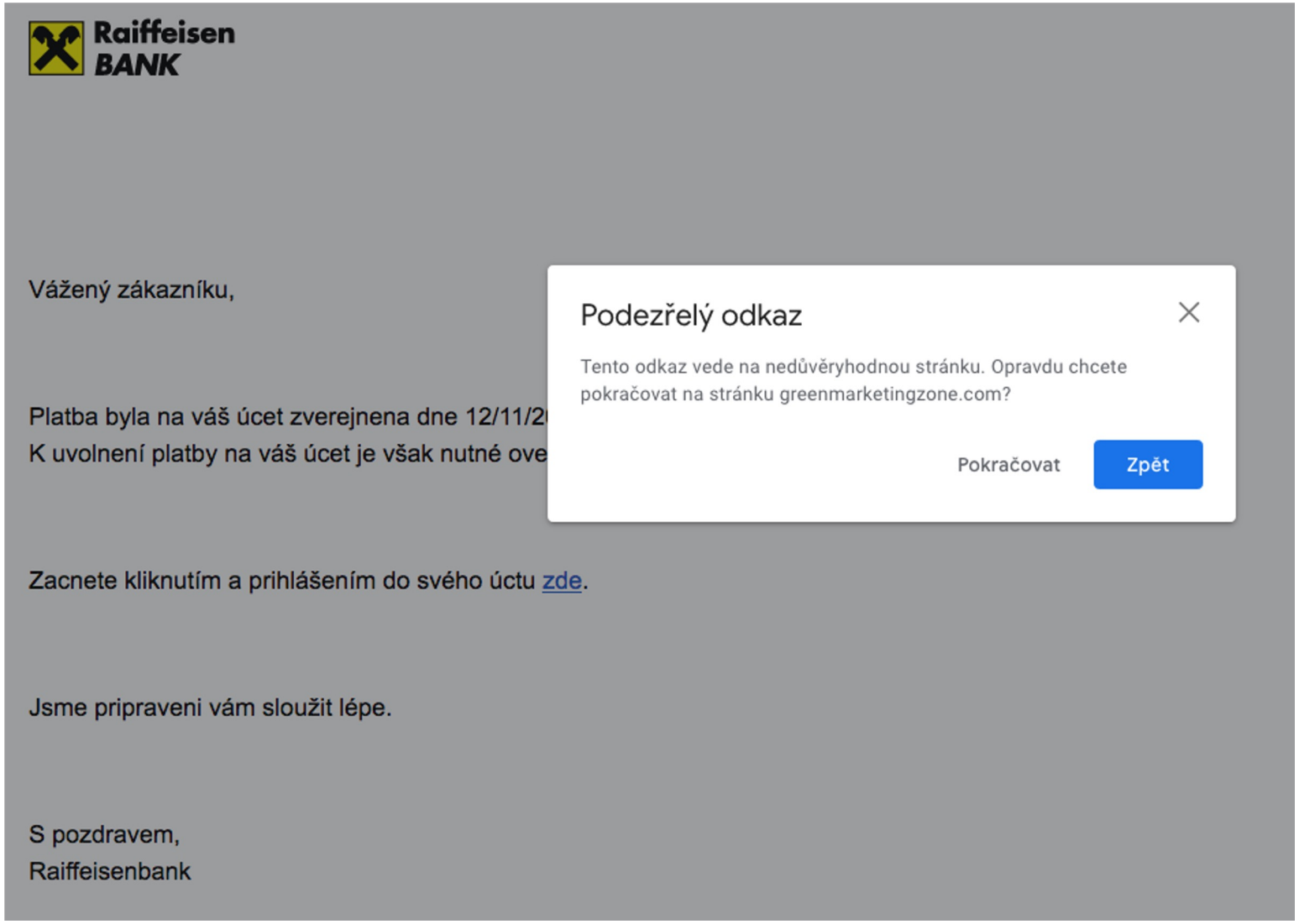
Herman Maier
Senior Support Engineer || Azure Identity US: +1-425-704-368 (Extension: **4358791**)

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

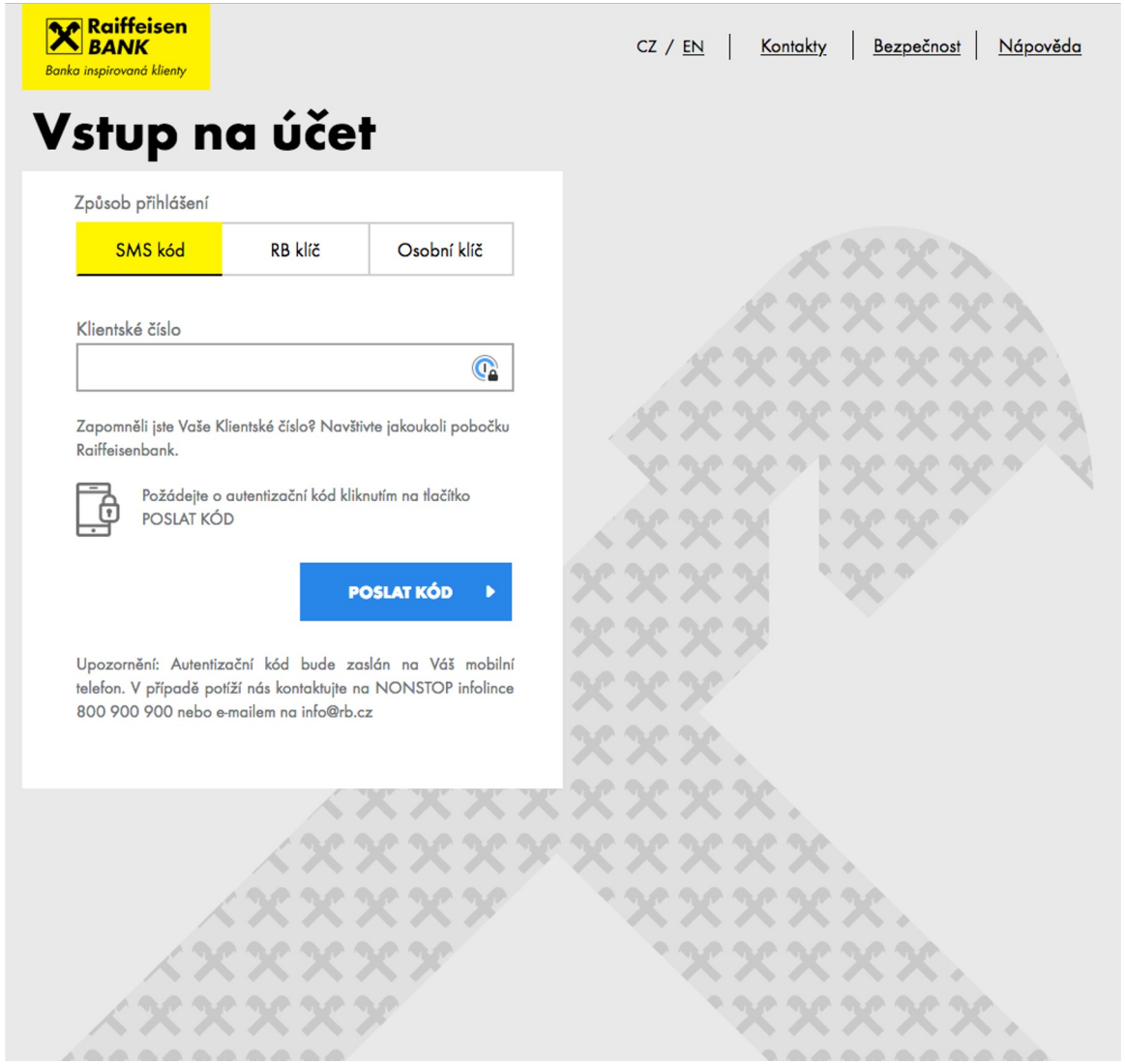
Dial the number corresponding to your country followed by my extension: **4358791**

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

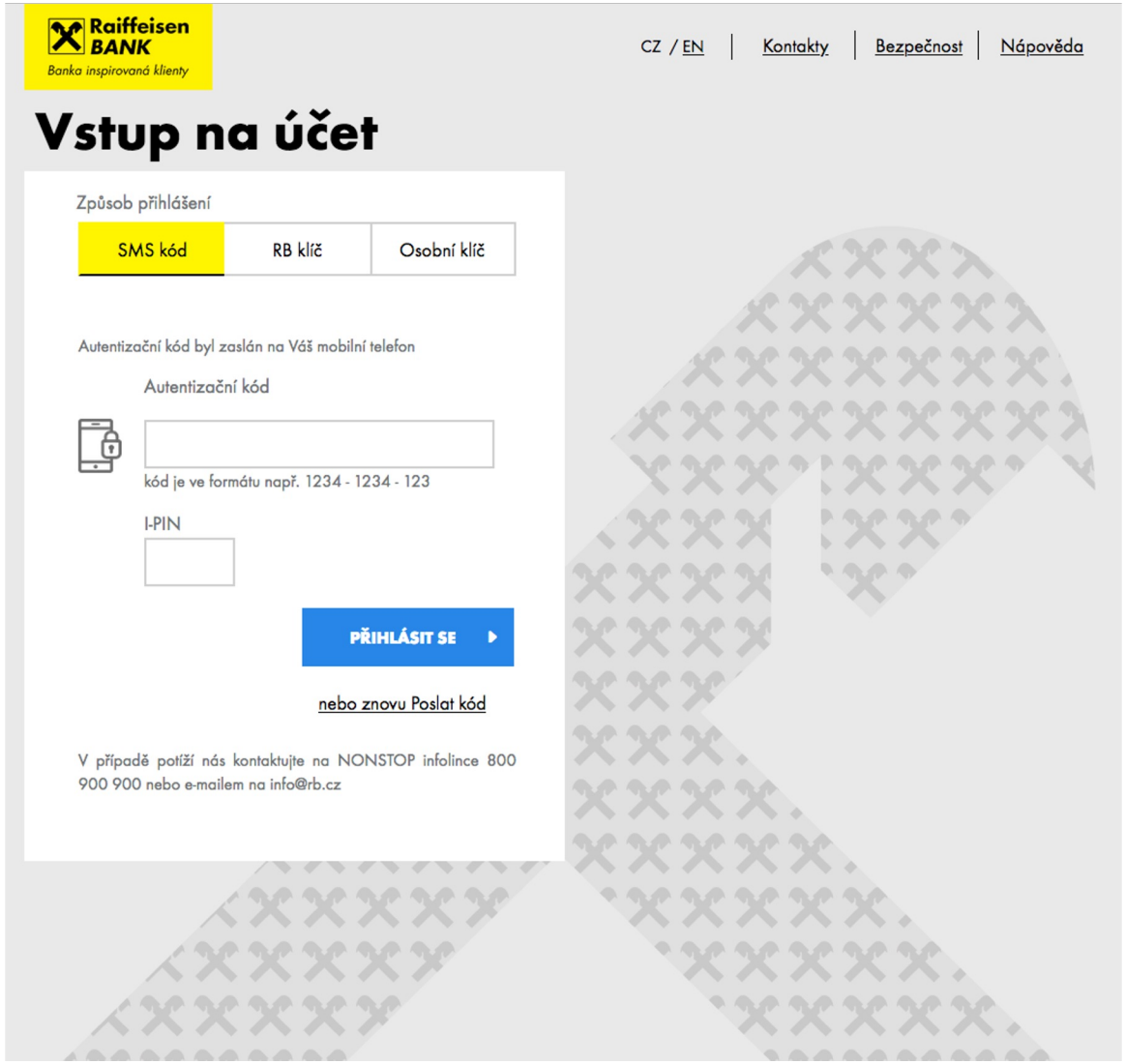
Phishing: bankovnictví 1/5



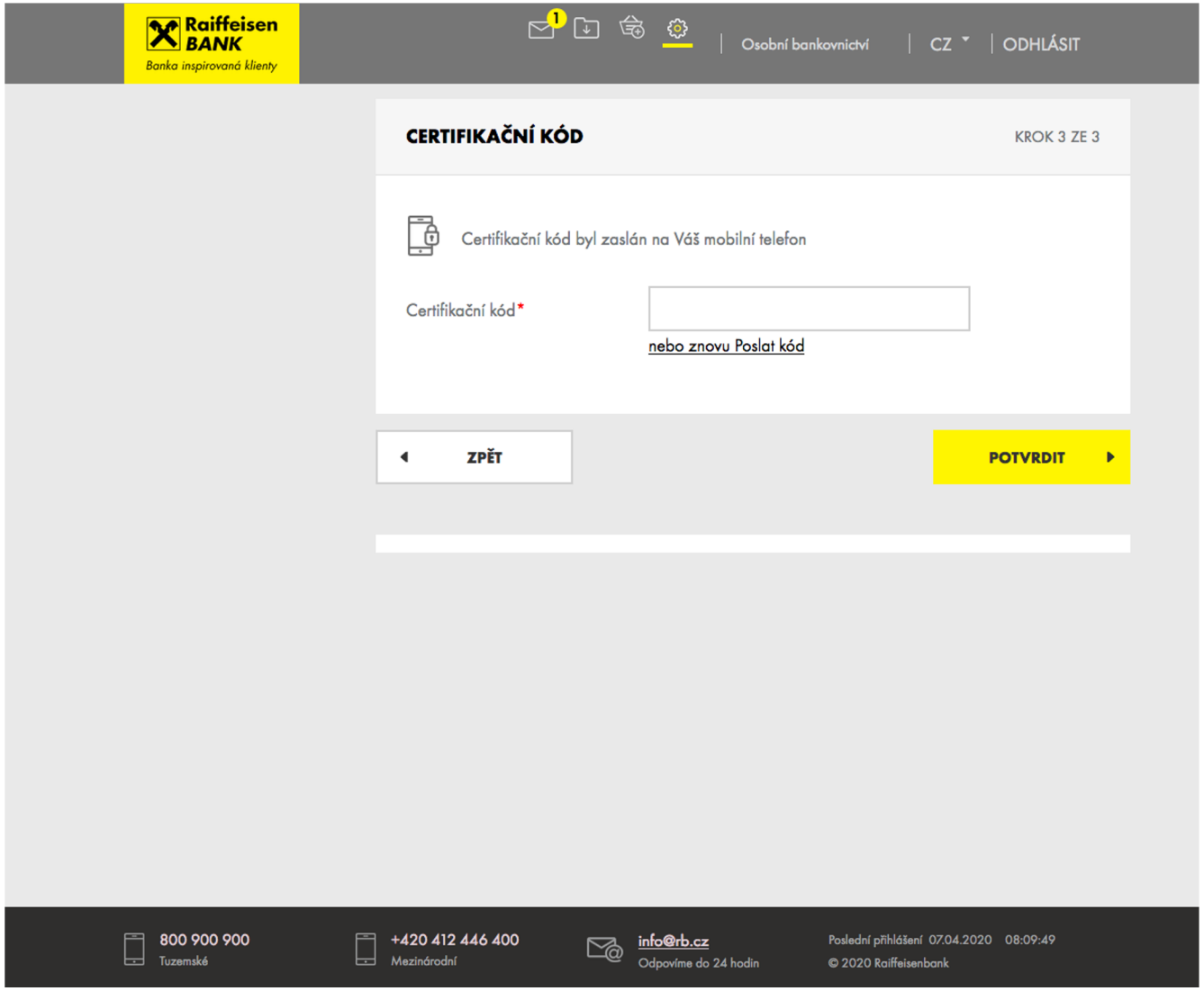
Phishing: bankovnictví 2/5



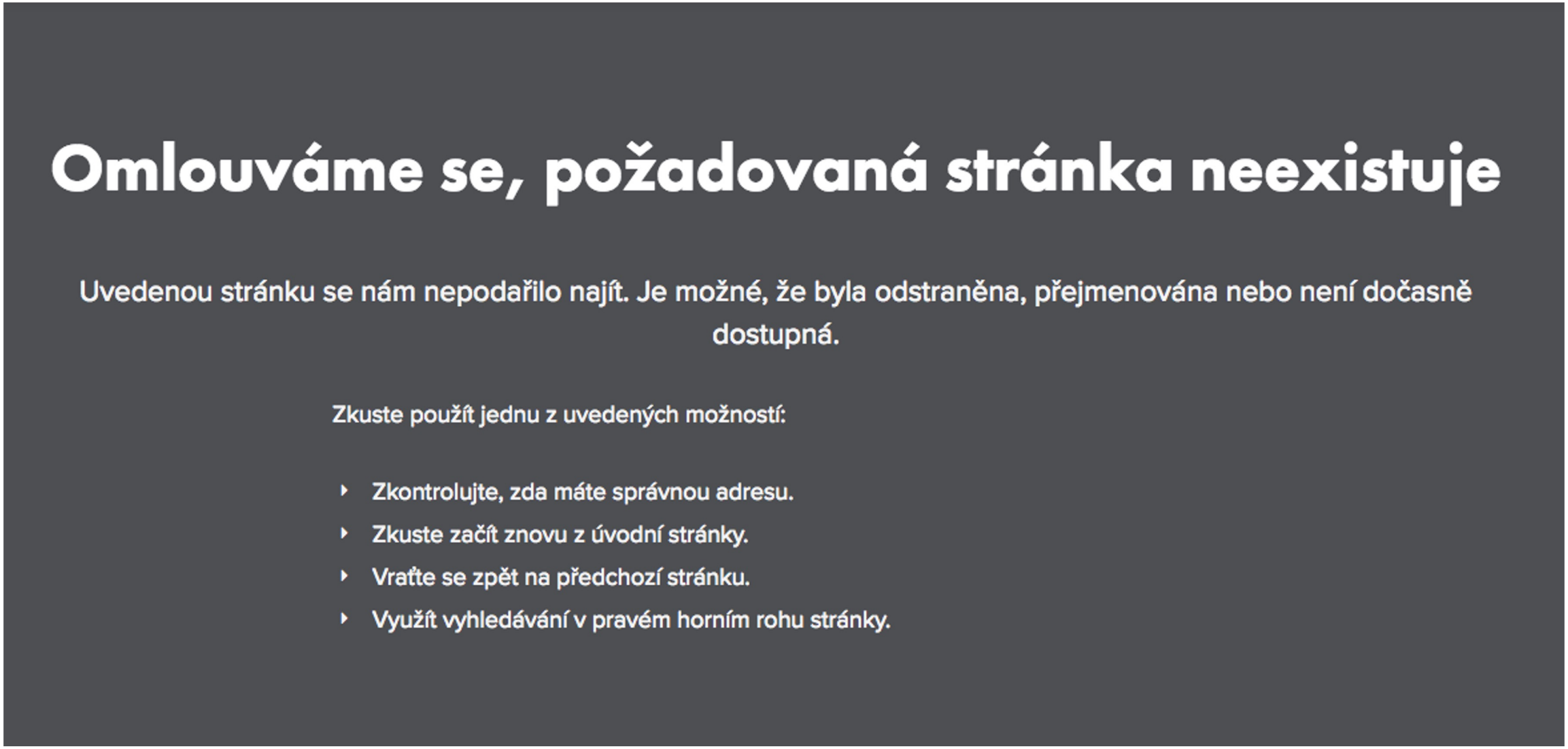
Phishing: bankovnictví 3/5



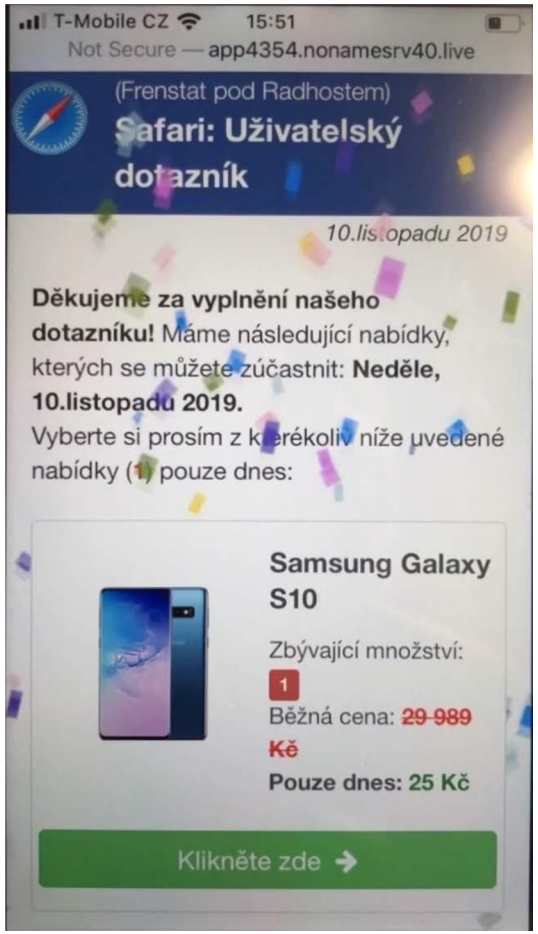
Phishing: bankovnictví 4/5



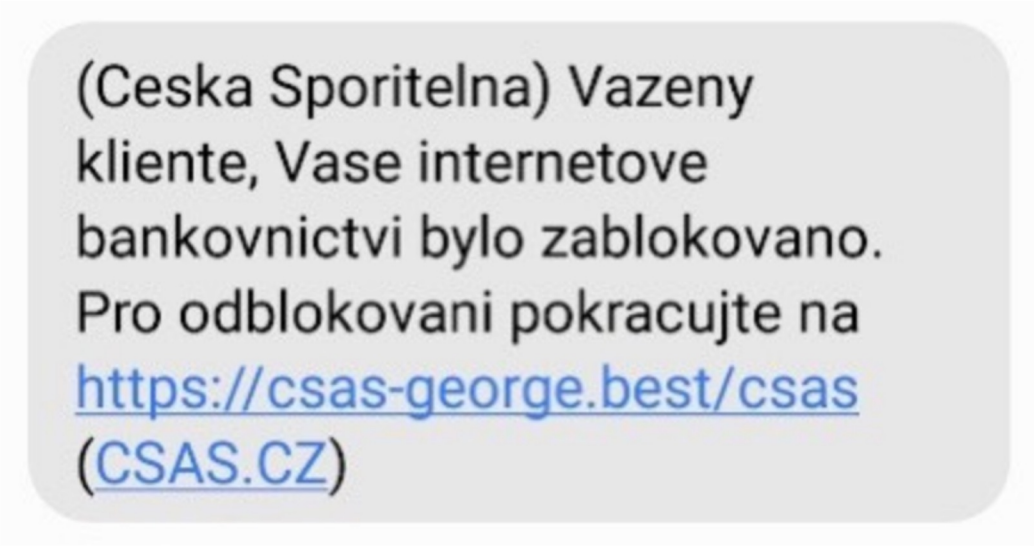
Phishing: bankovnictví 5/5



Phishing: reklama

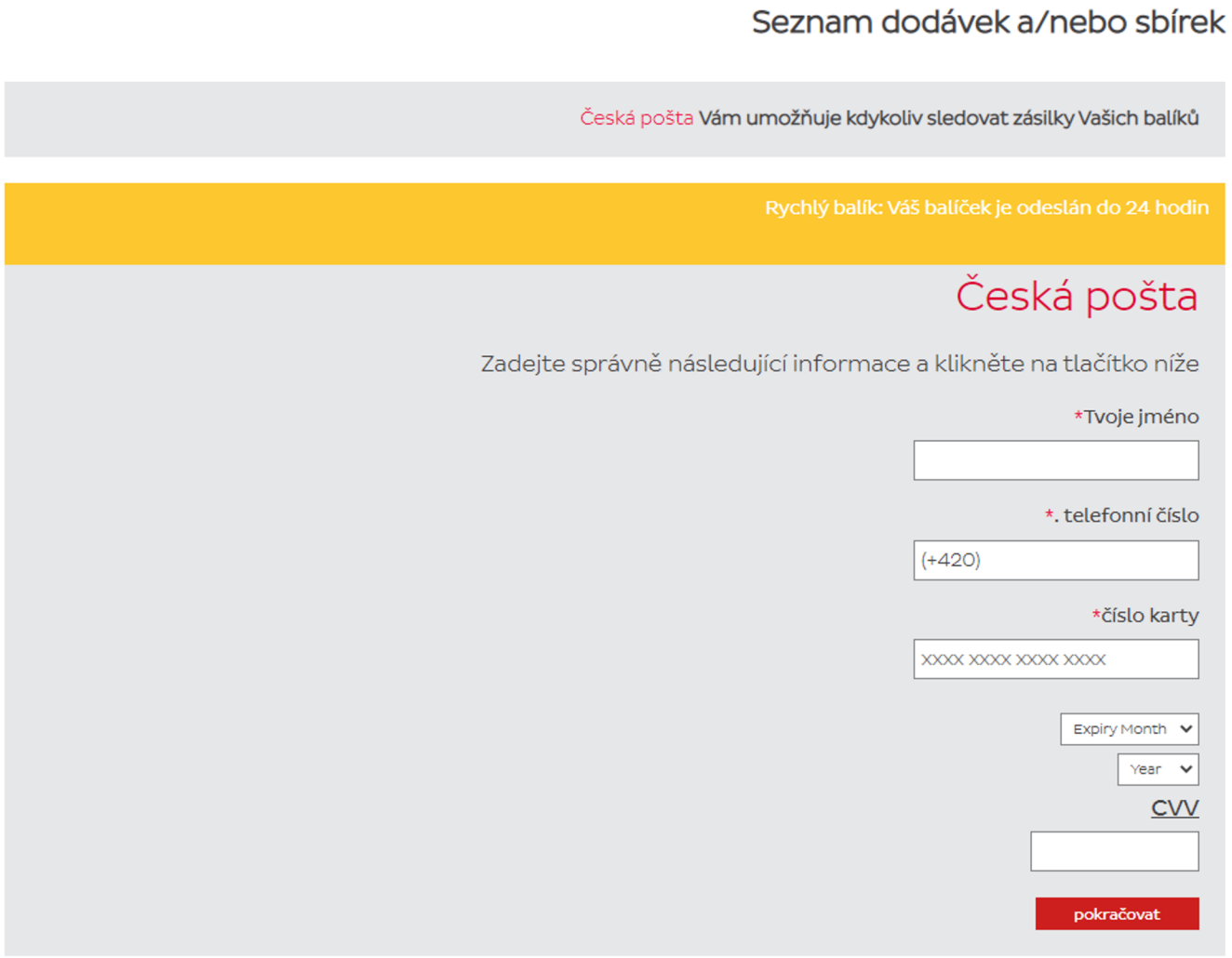


Phishing: obchod, banka

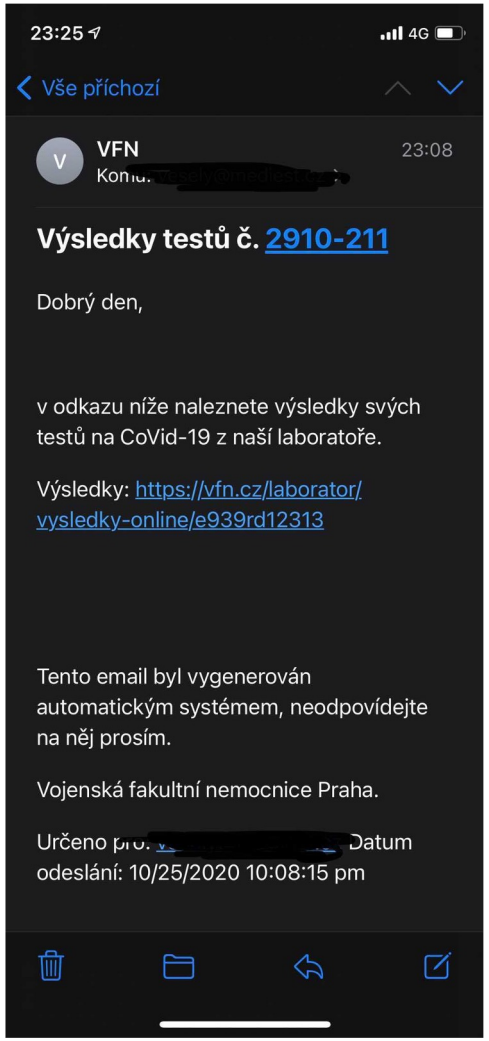


Phishing: česká pošta

Phishing: česká pošta



Phishing: test na COVID



Informace o produktu

Stav: Nové / Málo používané

Množství: 1

Cena: **1000 Kč**

Informace o doručení

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 Denik maleho poseroutky - 1. az 7. dil
1000 Kč

Získat prostředky

Provádějte platby bezpečně
Kliknutím na tlačítko „Získat prostředky" souhlasíte s podmínkami používání online služby „Bezpečná nabídka".

https://bazoscz.ordrs4348.biz/?pay

@(Bazoš.sk

Zadání bankovní karty

Jméno a příjmení držitele karty

Číslo karty

Datum ukončení platnosti (mm/yy)

CVC/CVV

Další

https://bazoscz.ordrs4348.biz/?lk

mBank 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

https://bazoscz.ordrs4348.biz/?load

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

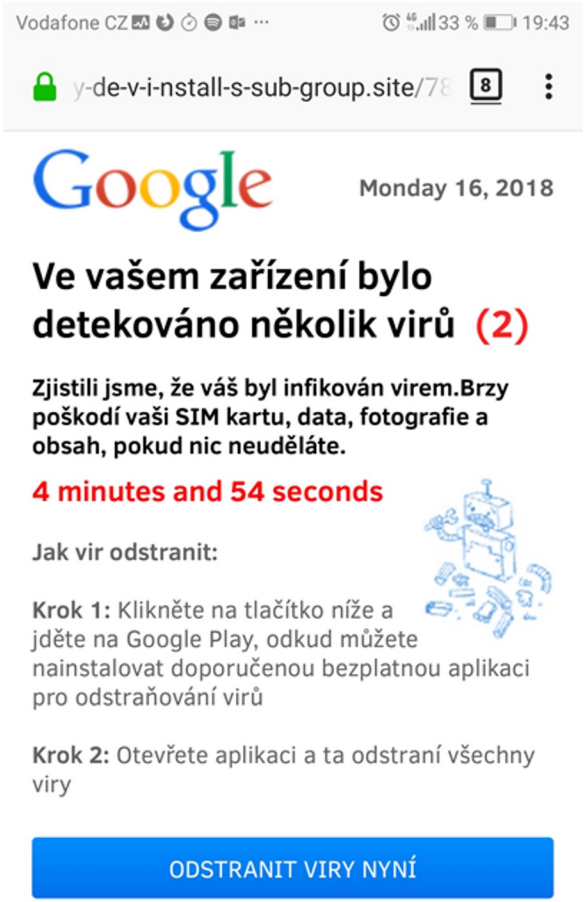
- Otevřete si Phishing Quiz

- Zadejte požadované údaje a odhalte phishing

Malware

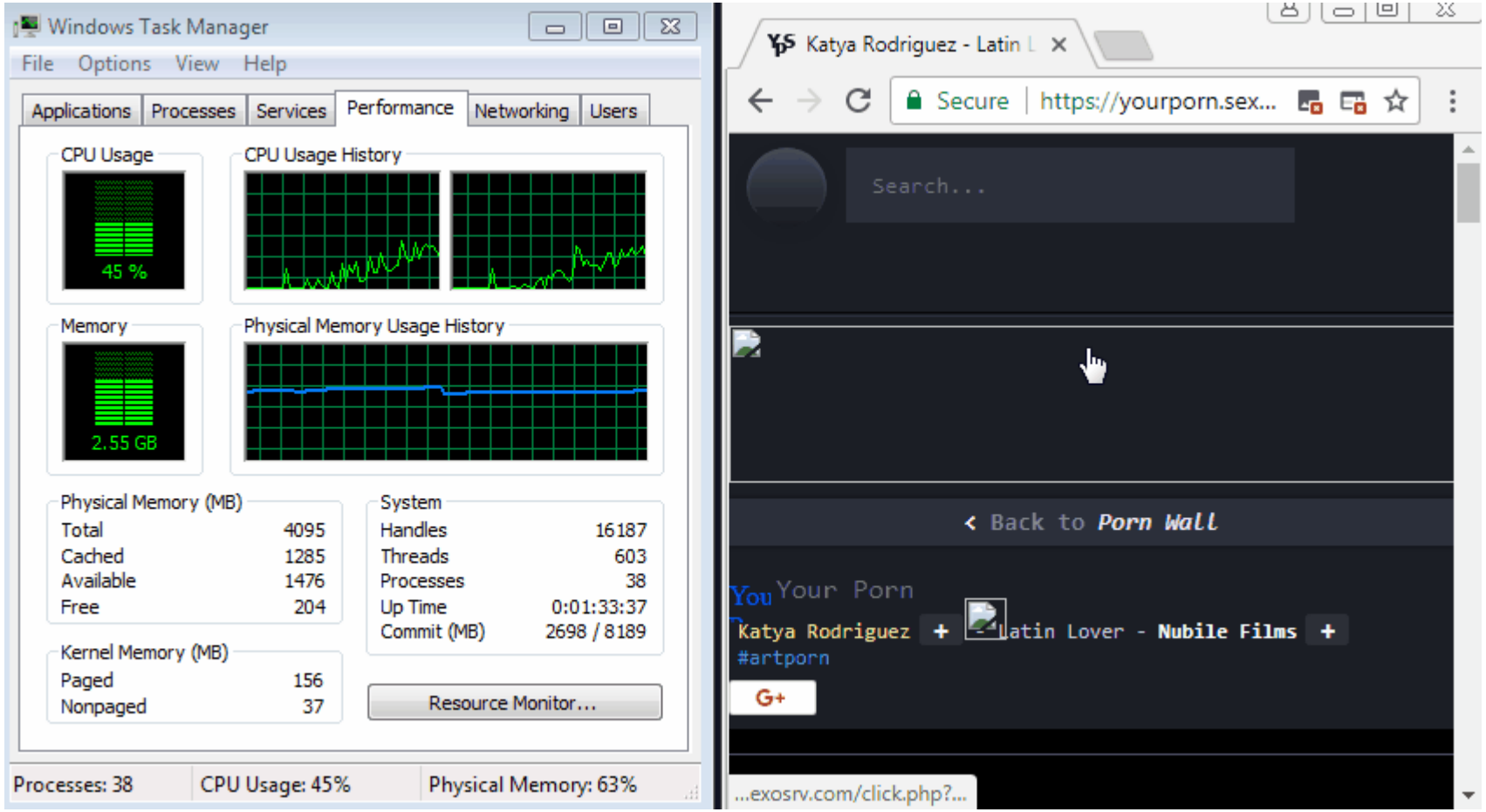
Malware


Vodafone CZ
05:44
70 %
AA
support.appie.com.systemnotific
Apple Security
Thursday
24 October 2019
(3) Viruses has been detected on your iPhone and battery has been infected and damaged.
If you do not remove this malware now, it may cause more damage to your device. How to fix this:
Step 1: Tap the button below & install the recommended virus protection tool for free from the AppStore.
Step 2: Run the app to remove all malware to repair
(1) SYSTEM NOTIFICATION
Please Read Important Notification Regarding Your iOS Device.
OK


Vodafone CZ
33 %
19:43
y-de-v-i-nstall-s-sub-group.site/7
8
Google
Monday 16, 2018
Ve vašem zařízení bylo detekováno několik virů (2)
Zjistili jsme, že váš byl infikován virem.Brzy poškodí vaši SIM kartu, data, fotografie a obsah, pokud nic neuděláte.
4 minutes and 54 seconds
Jak vir odstranit:
Krok 1: Klikněte na tlačítko níže a jděte na Google Play, odkud můžete nainstalovat doporučenou bezplatnou aplikaci pro odstraňování virů
Krok 2: Otevřete aplikaci a ta odstraní všechny viry
ODSTRANIT VIRY NYNÍ

Malware - ransomware

Malware – cryptojacking



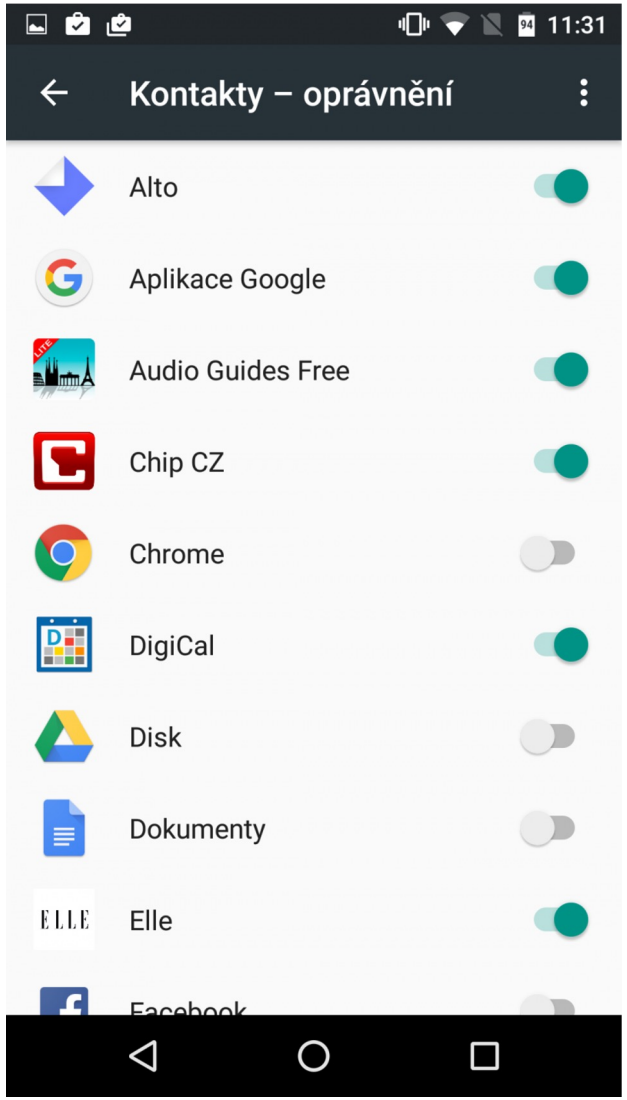
Antivirus

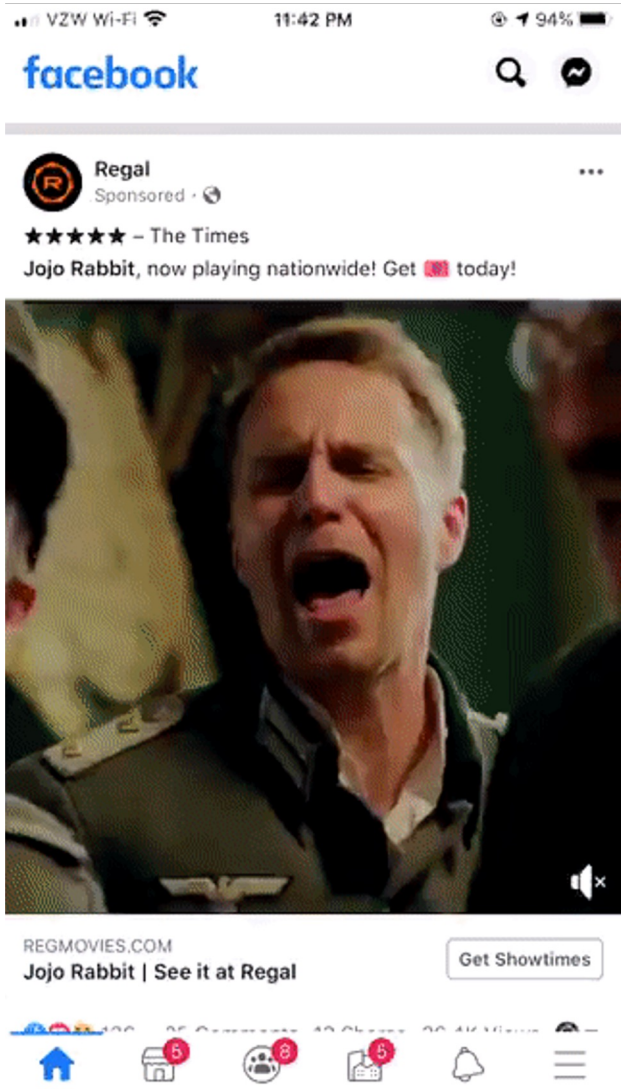
- Pravidlo č. 1 – aktualizujte
- **Základní funkcionality:** ochrana v reálném čase, pravidelná aktualizace virové databáze
- **Prémiové funkce:** Pokročilé webové štíty, správce hesel, rodičovská ochrana, šifrování apod.

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





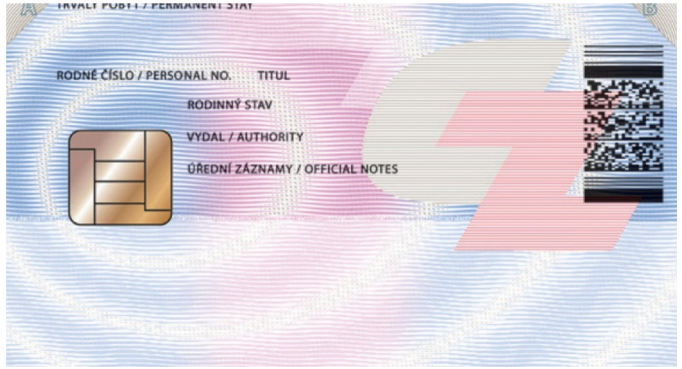
Přihlašování

Co znám


123456
password
12345678
123456789
qwerty
12345
1234
1234567
1234567890
superman
monkey
letmein
fuckyou
dragon
football
baseball
shadow
mustang
master
michael
abc123
111111
696969
666666
123123
7777777
trustno1
jennifer
jordan
qwertyuiop
654321
asshole
harley
hunter
1qaz2wsx
andrew
buster
hockey
pussy
jessica
sunshine
cheese
zxcvbn
112233
fuckme
killer
qazwsx
123qwe
tigger
batman
000000
asdfgh
starwars
zxcvbnm
123321
iloveyou
computer
robert
charlie
klaster
soccer
amanda
pepper
george
555555
2000
121212
ranger
michelle
princess
chelsea
joshua
159753
taylor
987654321
gfhjkm
dallas
austin
thunder
diamond
ashley
cookie
chicken
love
6969
1111
11111111
samantha
matrix
yankees
access
ginger
falcon
internet
cowboy
morgan
william
phoenix
patrick
anthony
jackson
heather
aaaaaa
maggie
hammer
thomas
richard
777777
fuck
freedom
hello
1234qwer
test
maverick
corvette
merlin
orange
silver
pass
summer
sexy
whatever
bailey
scooter
mickey
justin
daniel
secret
matthew
bigdog
welcome
guitar
222222
nicole
88888888
131313
golfer
peanut
biteme
ferrari
martin
andrea
fucker
smokey
snoopy
camaro
sparky

Co mám


AT&T
12:33 PM
OneTouch
Settings
facebook
janet@gmail.com token is:
597 202
Your token expires in
13
Microsoft
janet
Twitch
Google
janet
Amazon.com
janet


RODNÉ ČÍSLO / PERSONAL NO.
TITUL
RODINNÝ STAV
VYDAL / AUTHORITY
ÚŘEDNÍ ZÁZNAMY / OFFICIAL NOTES


something you
KNOW
something you
HAVE
secure
ACCESS
internet id
password
Sign In
prove
it's you

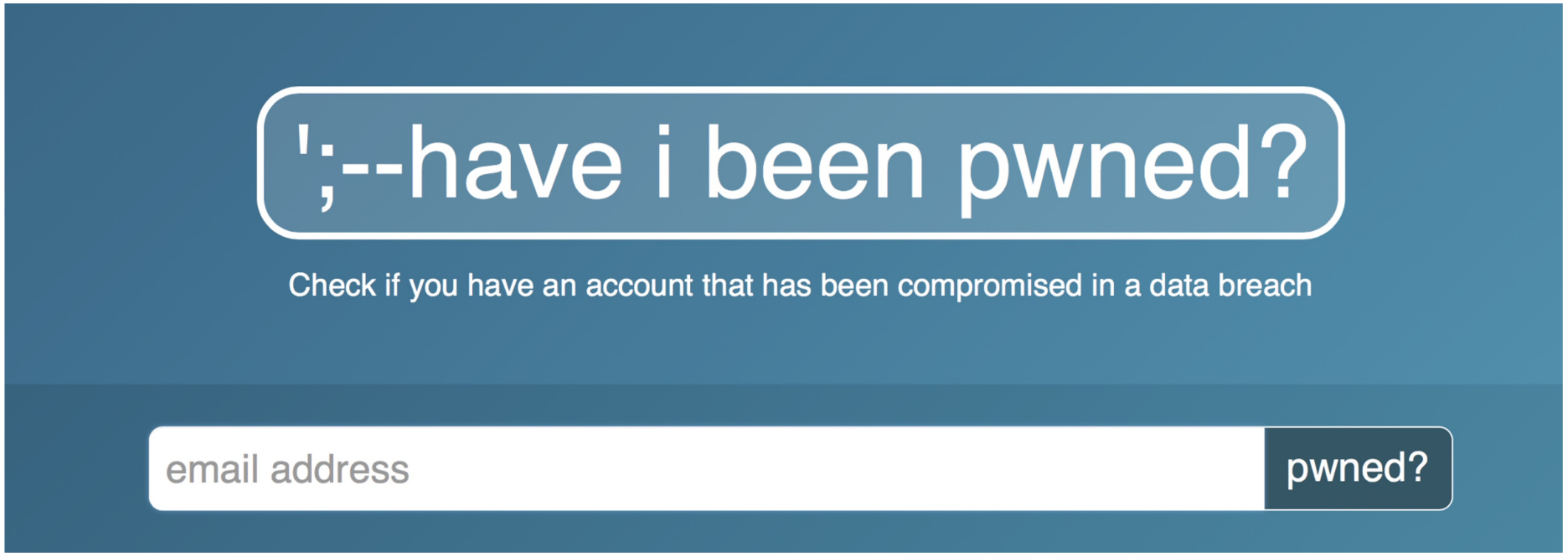
Co jsem


9:41
100 %
Zrušit
Položte prst
Opakovaně pokládejte prst na tlačítko plochy.


9:41
Cancel
Move your head slowly to complete the circle.
Accessibility Options

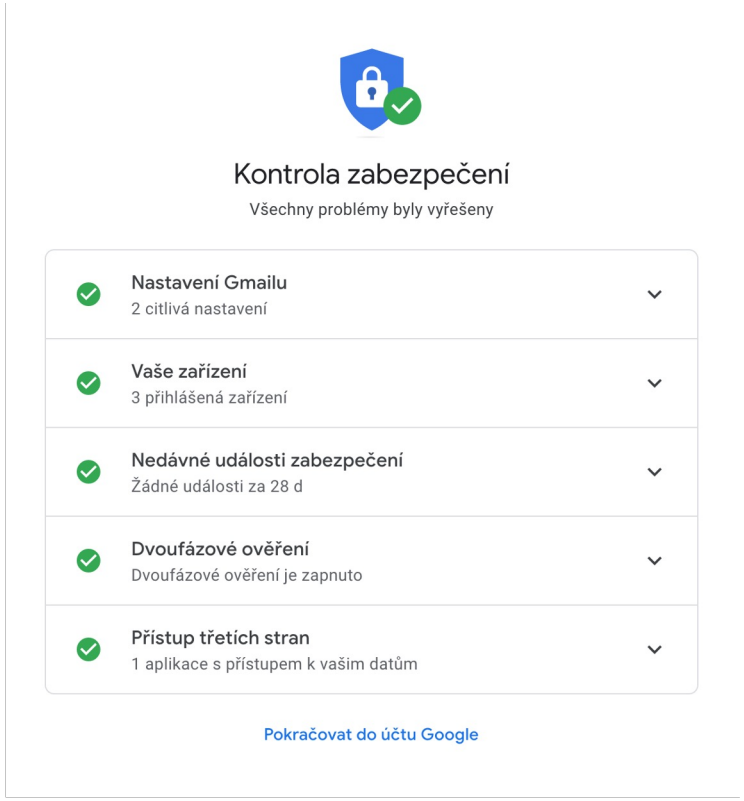
Kdo všechno zná mé heslo?

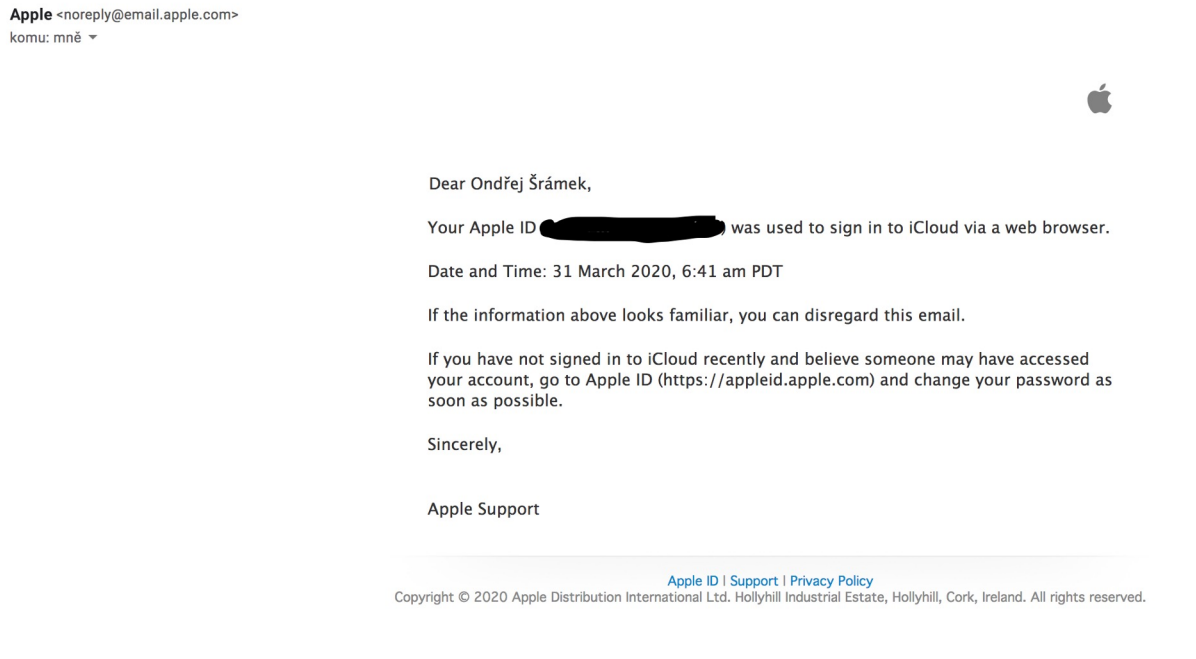
czechitas



Kontrola přihlášení/zabezpečení

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





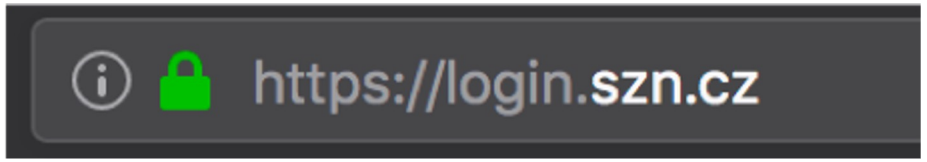
Co všechno máte v e-mailu?

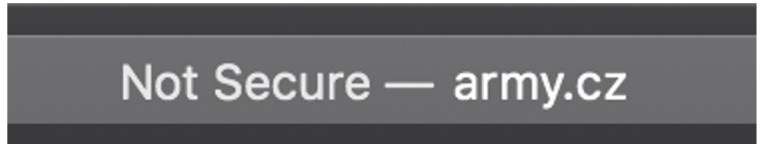
- Zprávu o registraci… (sociální síť, eshop,…)
  - i s heslem!
- Zprávu s magickým odkazem
  - Po kliknutí se přihlásíte, např. Facebook
    - Máte od někoho zprávu
    - Změnili jste si heslo
    - Chcete si restartovat heslo (zapomněli jste ho)

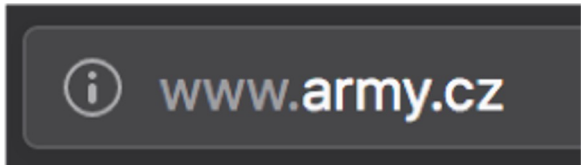
- Je lepší nic z výše uvedeného ve schránce nemít
  - Když se Vám někdo dostane do e-mailu, má všechno…

Zabezpečená komunikace

- Vždy, když zadáváte data
  - Osobní údaje
  - Číslo karty
  - Heslo
  - 2FA
- Chcete **věřit** obsahu
  - Úřady

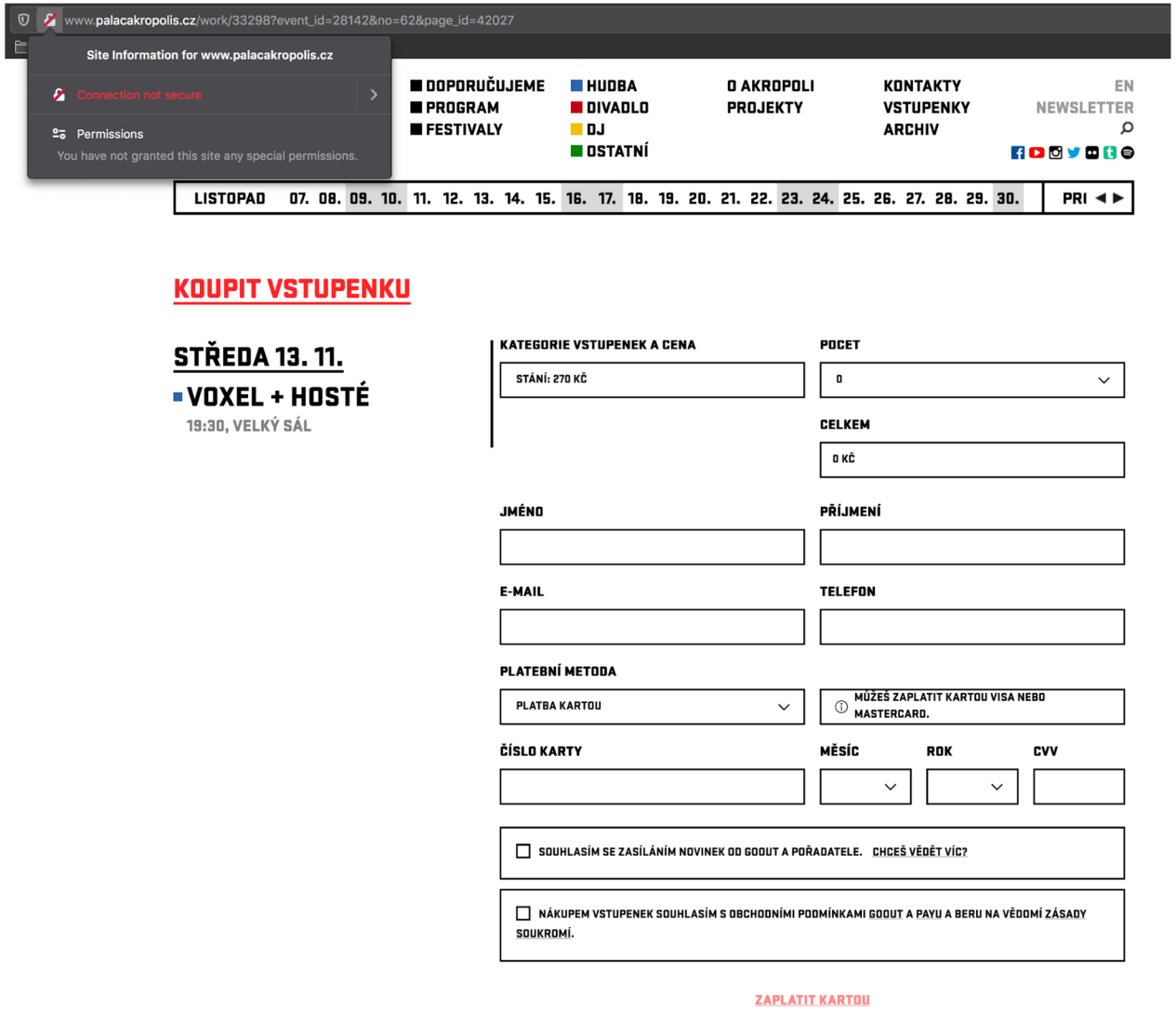






- Konec EV certifikátů
- Bez certifikátu = **nezabezpečeno**!

Koupíte si lístek na koncert?



Druhý faktor

Proč další krok při přihlášení?

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

Jak?

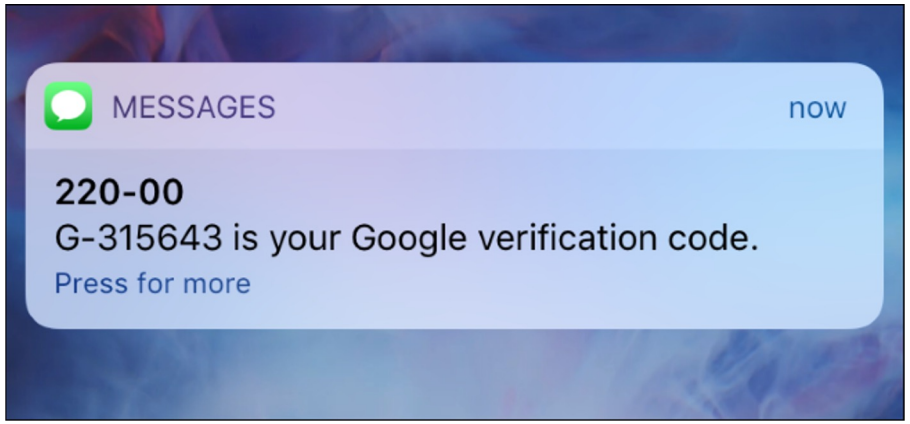
- Speciální aplikace (Authy, Duo, Google Authenticator,...)
- Speciální zařízení (RSA Authenticator, YubiKey,...)
- Nativní součást systému
  - Android: Push notifikace (přístup ke Google službám)
  - iOS: Touch ID/Face ID

- Zaslání kódu e-mailem
- SMS

Příklady


AT&T
12:33 PM
OneTouch
Settings
facebook
janet@gmail.com token is:
597 202
Your token expires in
13
Microsoft
janet
Twitch
Google
janet
Amazon.com
janet


9:41
100 %
Zrušit
Položte prst
Opakovaně pokládejte prst na tlačítko plochy.


MESSAGES
now
220-00
G-315643 is your Google verification code.
Press for more

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

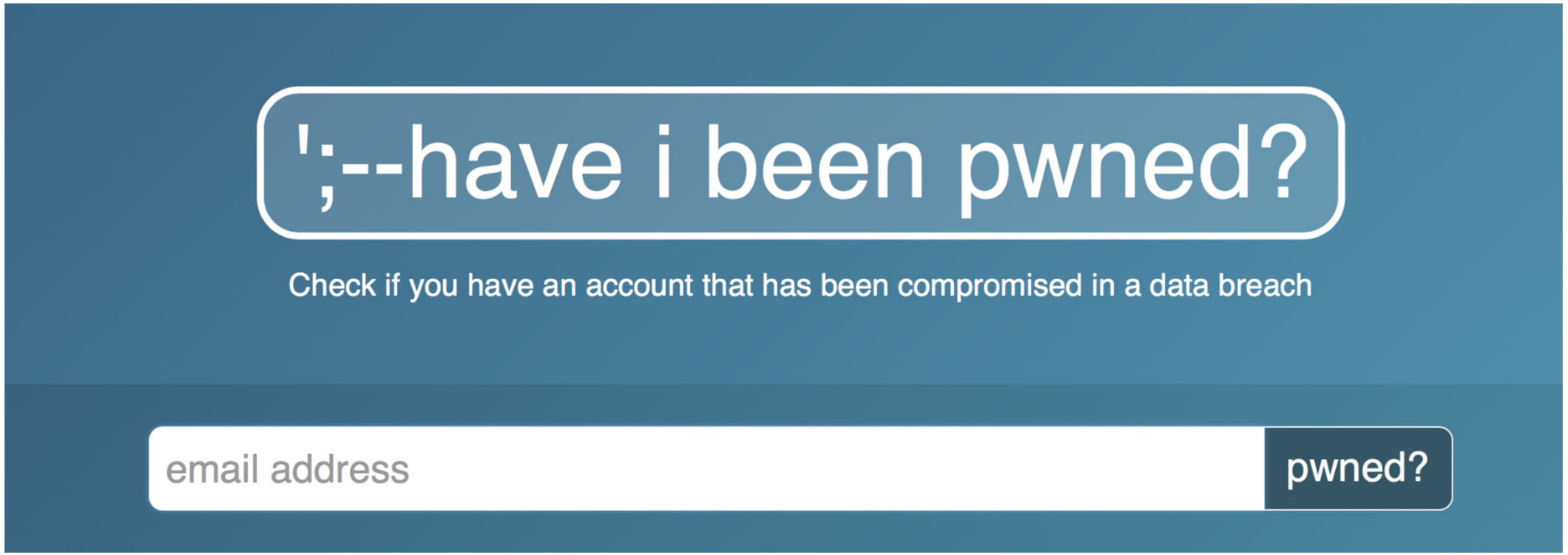
Uhodnout heslo není těžké

- 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?



[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

Lístečky nestačí...

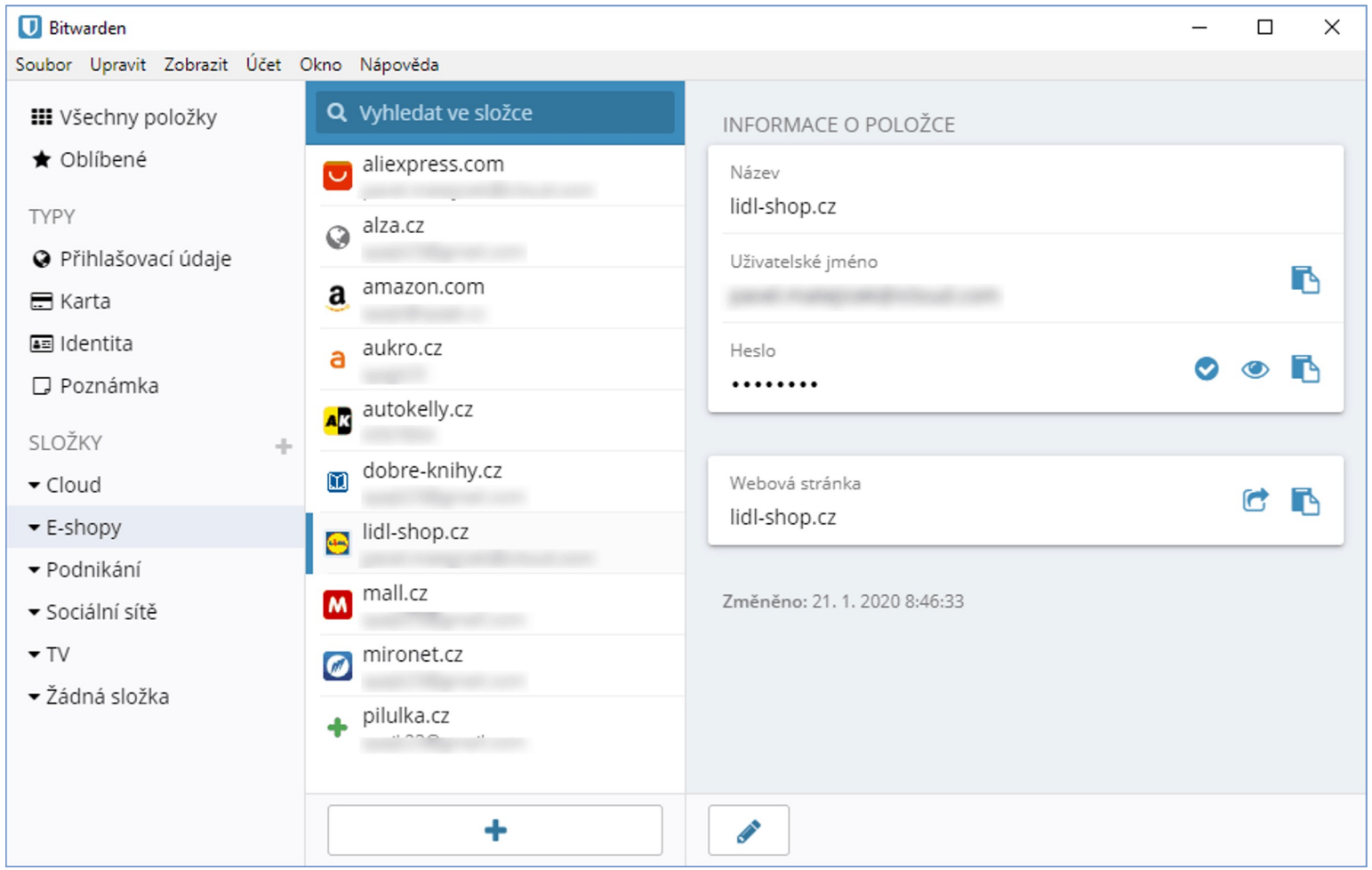
- Kolik služeb používáte, stovky?
- Každá služba by měla mít své unikátní heslo.

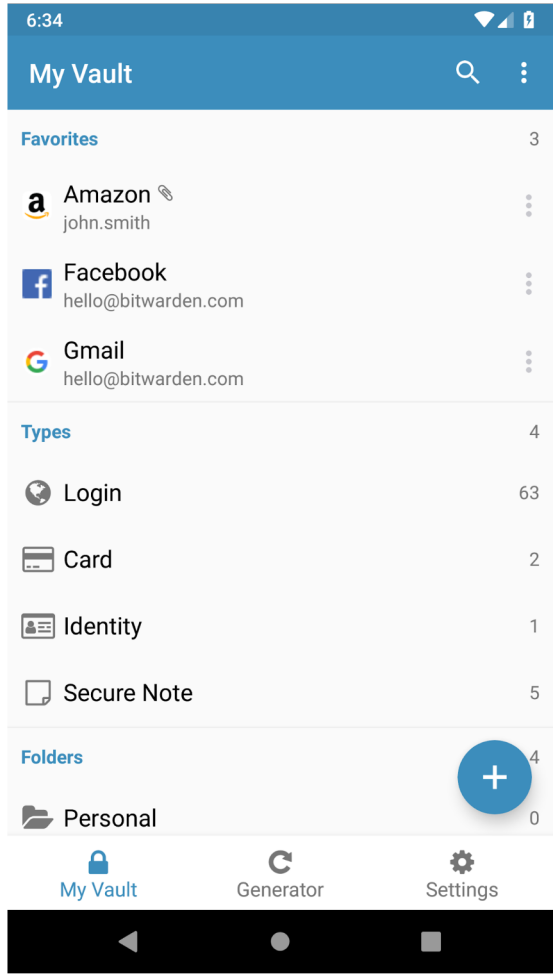
- Správce hesel
  - Nemusí to být jen aplikace (speciální notýsek jen na hesla)
    - Není vhodné pro každého
  - Aplikace
    - Lokální (jen na jednom zařízení), odjinud se nepřihlásíte
    - Vzdálená (synchronizace napříč zařízeními)

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
  - eIdentita
    - V rámci služeb státní správy: Datová schránka, Moje daně,…

mojeiD

- Katalog služeb
  - e-maily, instituce, města, e-shopy, hostingy 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=PLVfIkbZEOn9l5_VcUlwoKXclf7znrMJ5D
- Bezpečnost na Internetu (Televize Seznam)
  - https://www.televizeseznam.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
- Buď 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