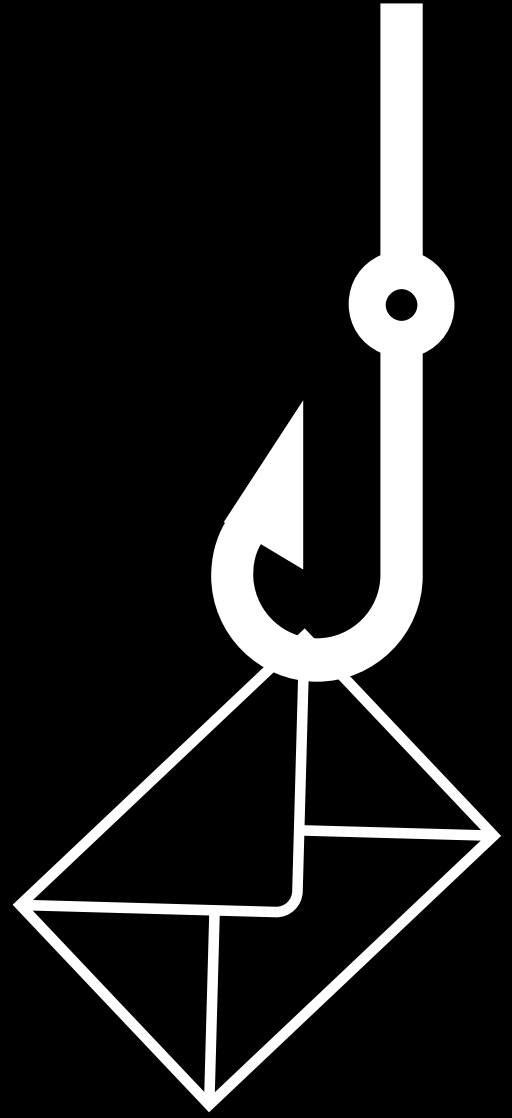
# PHISHING

MARTIN ŠEBELA

SECFEST ZČU

3. 12. 2020



# Phishing

- Phishing = **podvodné e-maily**
- Cílem vylákat **hesla**, údaje k **platební kartě**, zneužít **identitu**, …
- **Podvodné stránky**
- Podvodné zprávy na **sociálních sítích**

- Případ z ČR – přes phishing k pašování drog, až do hongkongského vězení
  - irozhlas.cz/zpravy-svet/smatana-duchodce-hongkong-pasovani-podcast-vinohradska-12_1912040600_cen

ct24.ceskatelevize.cz/ekonomika/3215239-pres-whatsapp-a-messenger-se-siri-podvodna-zprava-o-kuponu-do-albertu-laka-od-lidi

ČT24

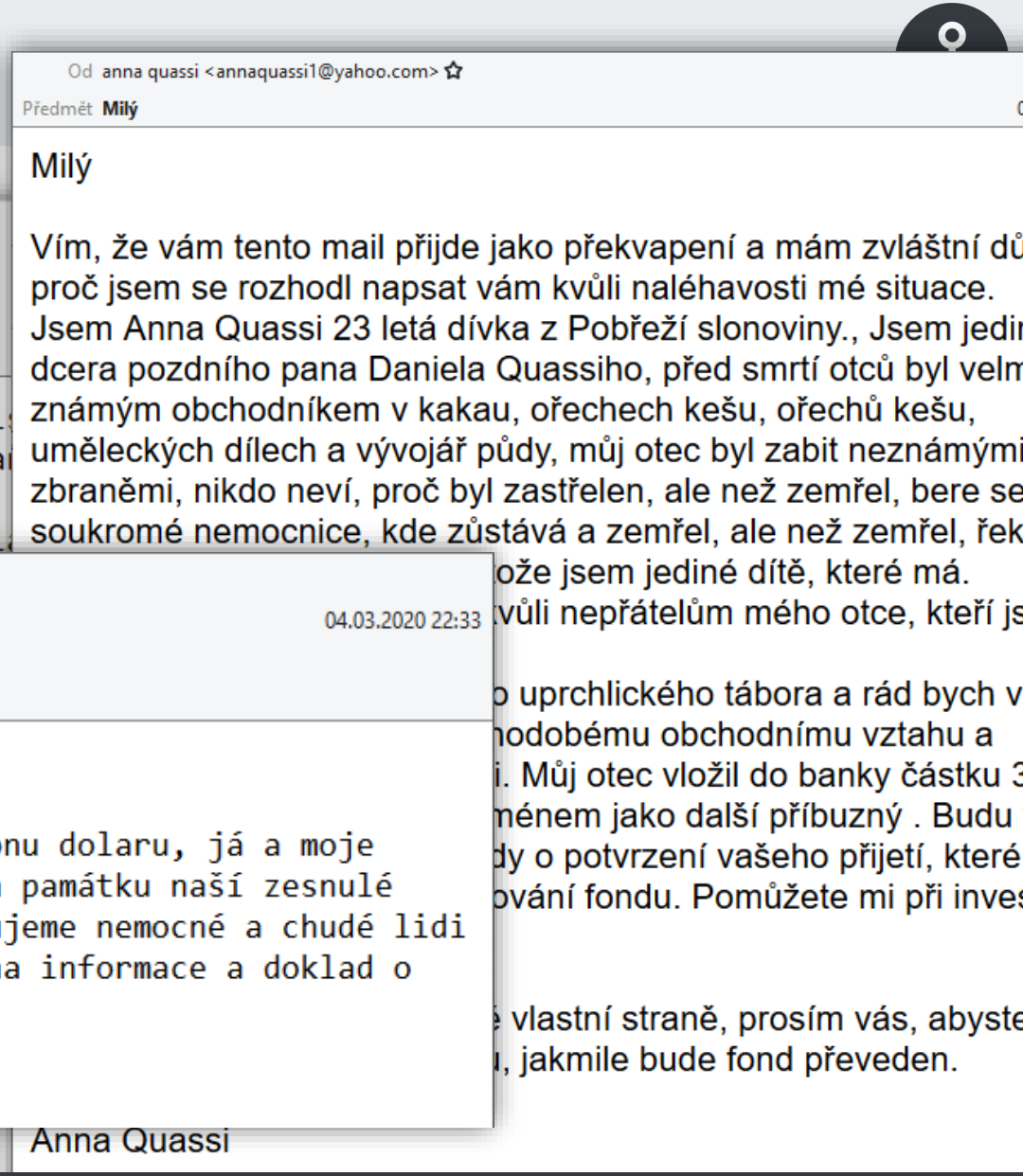
KORONAVIRUS DOMÁCÍ SVĚT REGIONY EKONOMIKA KULTURA MÉDIA VĚDA

Přes WhatsApp a Messenger se šíří podvodná zpráva o kuponu do Albertu. Láká od lidí údaje k platebním kartám

27. 10. 2020

Komunikačními aplikacemi WhatsApp a Messenger se mezi českými uživateli šíří podvodná phishingová zpráva nabízející elektronické kupony v hodnotě tři tisíce korun od supermarketů Albert. Součástí zprávy je odkaz, který uživatele pošle na podvodnou stránku. Ta je následně vybízí k zadání osobních informací včetně údajů platební karty a k dalšímu sdílení zprávy. Podvod je stále aktivní a rychle se šíří. Uvedla to antivirová firma Avast.

# Phishing dříve



Od anna quassi <annaquassi1@yahoo.com>
Předmět **Milý** 04.04.2020 12:56

Milý

Vím, že vám tento mail přijde jako překvapení a mám zvláštní důvod, proč jsem se rozhodl napsat vám kvůli naléhavosti mé situace. Jsem Anna Quassi 23 letá dívka z Pobřeží slonoviny., Jsem jediná dcera pozdního pana Daniela Quassiho, před smrtí otců byl velmi dobře známým obchodníkem v kakau, ořechech kešu, ořechů kešu, uměleckých dílech a vývojář půdy, můj otec byl zabit neznámými zbraněmi, nikdo neví, proč byl zastřelen, ale než zemřel, bere se do soukromé nemocnice, kde zůstává a zemřel, ale než zemřel, řekl mi o
ože jsem jediné dítě, které má.
vůli nepřátelům mého otce, kteří jsou

o uprchlického tábora a rád bych vás
nodobému obchodnímu vztahu a
i. Můj otec vložil do banky částku 3,5
ménem jako další příbuzný . Budu vám
dy o potvrzení vašeho přijetí, které mi
ování fondu. Pomůžete mi při investici a

vlastní straně, prosím vás, abyste je
, jakmile bude fond převeden.

Anna Quassi

Od WordPress@sastipen.ro
Předmět **vyhrál jsi!!!you won!!!**
Odpověď lerynnewestcallumfoundation2020@outlook.com
Komu Recipients <WordPress@sastipen.ro>

Dobrý den, jsem Lerynne West, máte dar 1 930 000,00 EUR. 5. li
2018 jsem vyhrál loterii 343,9 milionu Powerball, část z ní da
deseti štastlivcum a organizaci Ten Charity. Váš e-mail vyšel
vítezne. Okamžite kontaktujte reklamacní oddelení ohledne rekl
Kontakt: leryn

Hello, I am Le
the 343.9 mill
donating part
Your email cam
urgently for c
lerynnewestcal
This Communica

Hotovo

Od lakshay.agarwal@skpatodia.in
Předmět **1,5 milionu dolaru darováno** 04.03.2020 22:33
Odpověď mmnuelfan@gmail.com
Komu Recipients <lakshay.agarwal@skpatodia.in>

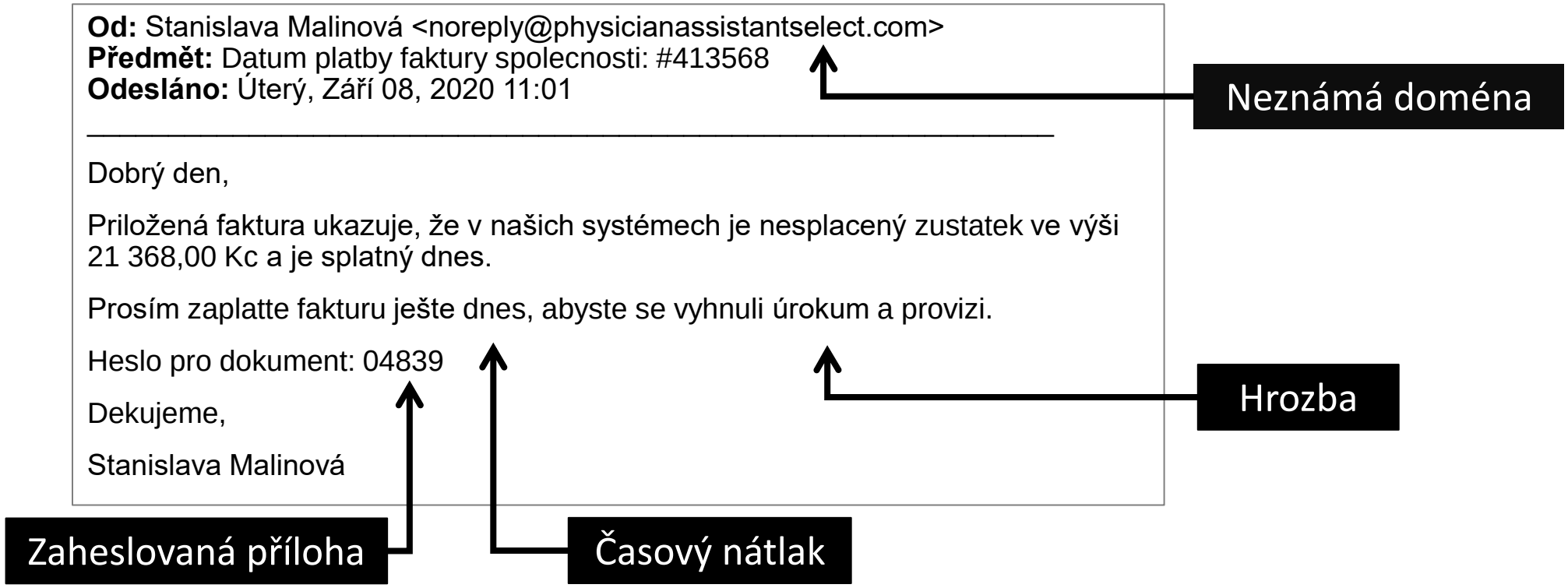
Milý

Vyhrál jsem jackpot lotto ve výši 768,41 milionu dolaru, já a moje rodina jsme darovali 1,5 milionu dolaru vám na památku naší zesnulé sestry, která zemrela na rakovinu, rádi oslovujeme nemocné a chudé lidi ve vaší komunite a na celém svete. Odpovezte na informace a doklad o mých vyhraných lotto fondech.

Manuel Franco

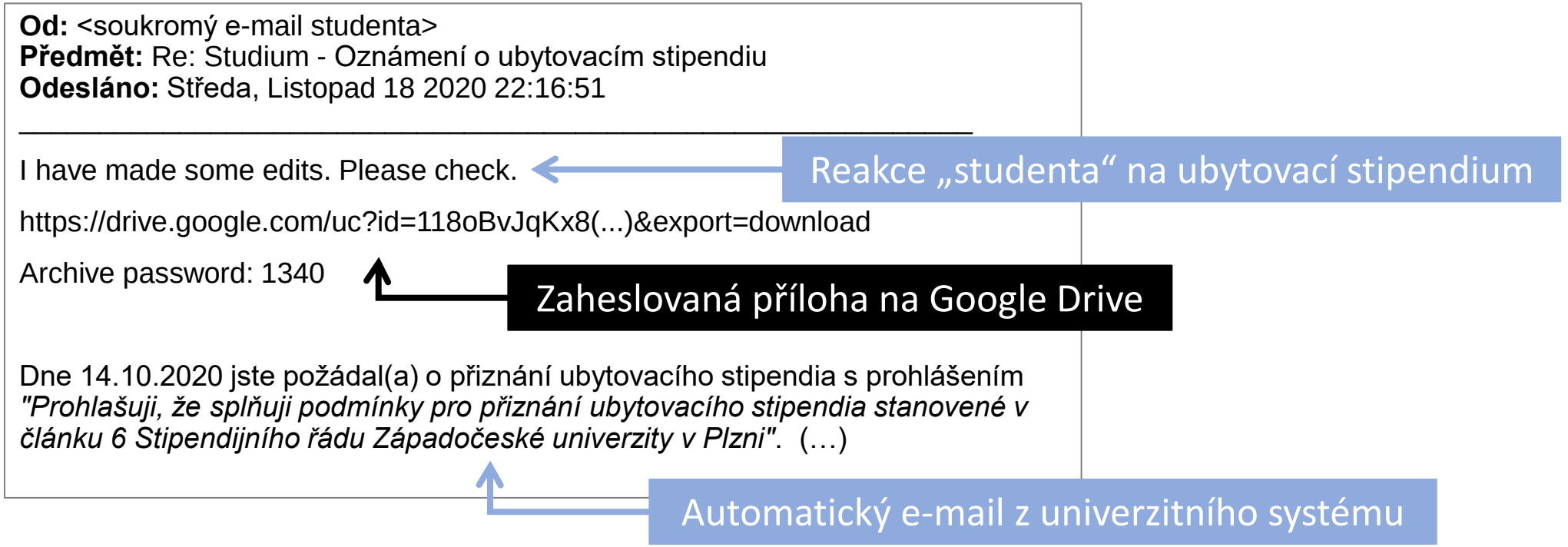
# Phishing: nezaplacená faktura

- Příklad: **nezaplacená faktura**
- Součástí je zaheslovaná příloha, která obsahuje malware místo faktury



# Phishing: zneužití identity

- Příklad: **zneužitý soukromý e-mail** studenta
- Automatické odpovědi na e-maily z historie
- E-maily s odkazy na malware přišly na helpdesk a vyučujícím studenta



# Phishing: podvodná stránka

**Od:** "Raiffeisenbank" <Platba@rb.cz>
**Předmět:** Platba pozdržena / Payment on hold.
**Odesláno:** Tue, 10 Nov 2020 15:47:22

---

Vážený zákazníku,

Platba byla na váš úcet zverejnena dne 10/11/2020. K uvolnení platby na váš úcet je však nutné overení.

Zacnete kliknutím a prihlášením do svého úctu zde.

Jsme pripraveni vám sloužit lépe.

S pozdravem,

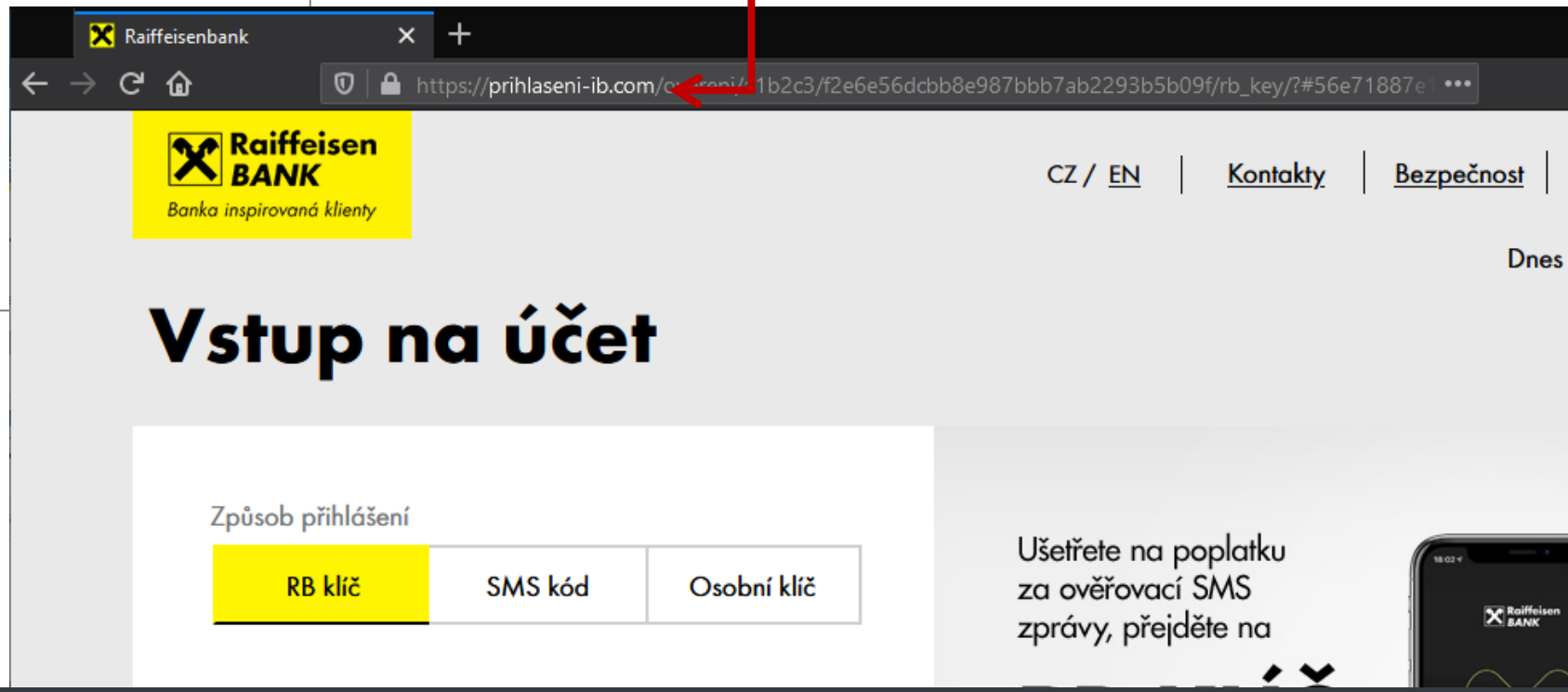
Raiffeisenbank

https://www.hashtagtrends.us/wp-admin/aspx.php

Odesílatel vypadá důvěryhodně

Odkaz po najetí kurzorem na „zde“.

Podvodná stránka, která se snaží napodobit přihlášení do elektronického bankovnictví.



# Phishing: podvodná stránka

**Od:** "DPD" <admin@frasindo.cz>
**Předmět:** Vaše zásilka je aktuálně uložena v našem místním skladu
**Odesláno:** Sat, 28 Nov 2020 22:09:20

---

Vaše zásilka je aktuálně uložena v našem místním skladu. Pokud však akce nebude provedena do 48 hodin, bude vrácena odesílateli.

Vyberte prosím jednu z následujících možností:

- Zkuste doručit znovu -

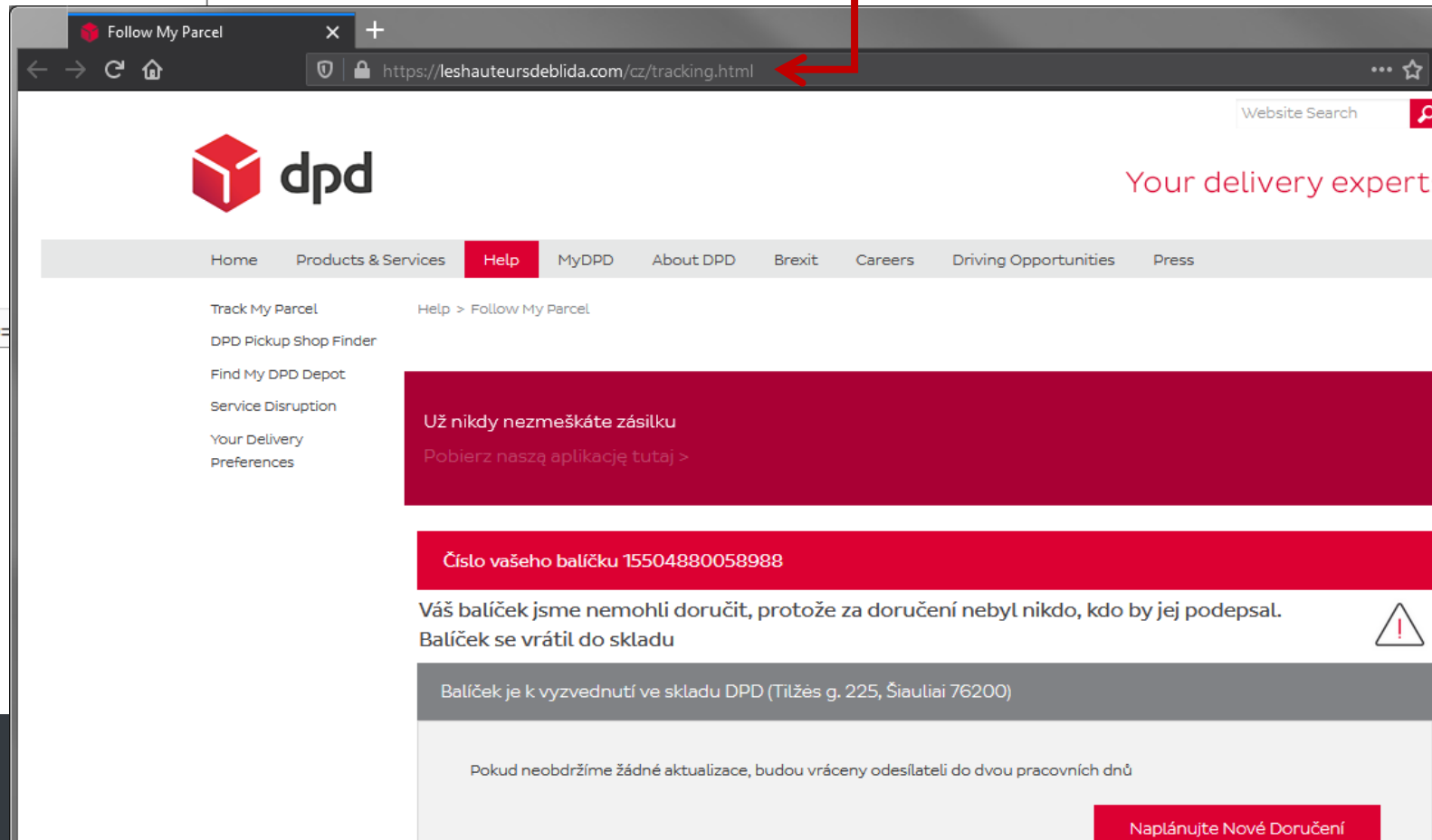
Za jakýkoliv pokud o opětovné doručení bude účtován poplatek 19,00 Kč protože již byly provedeny dva pokusy o doručení.

DPD Group @ 2020

newdw1.3o74yx9mm7tfd86.pakhoster.pk/?rarara=b3BlcmF0b3JAc2VydmljZS56Y3UuY3o=

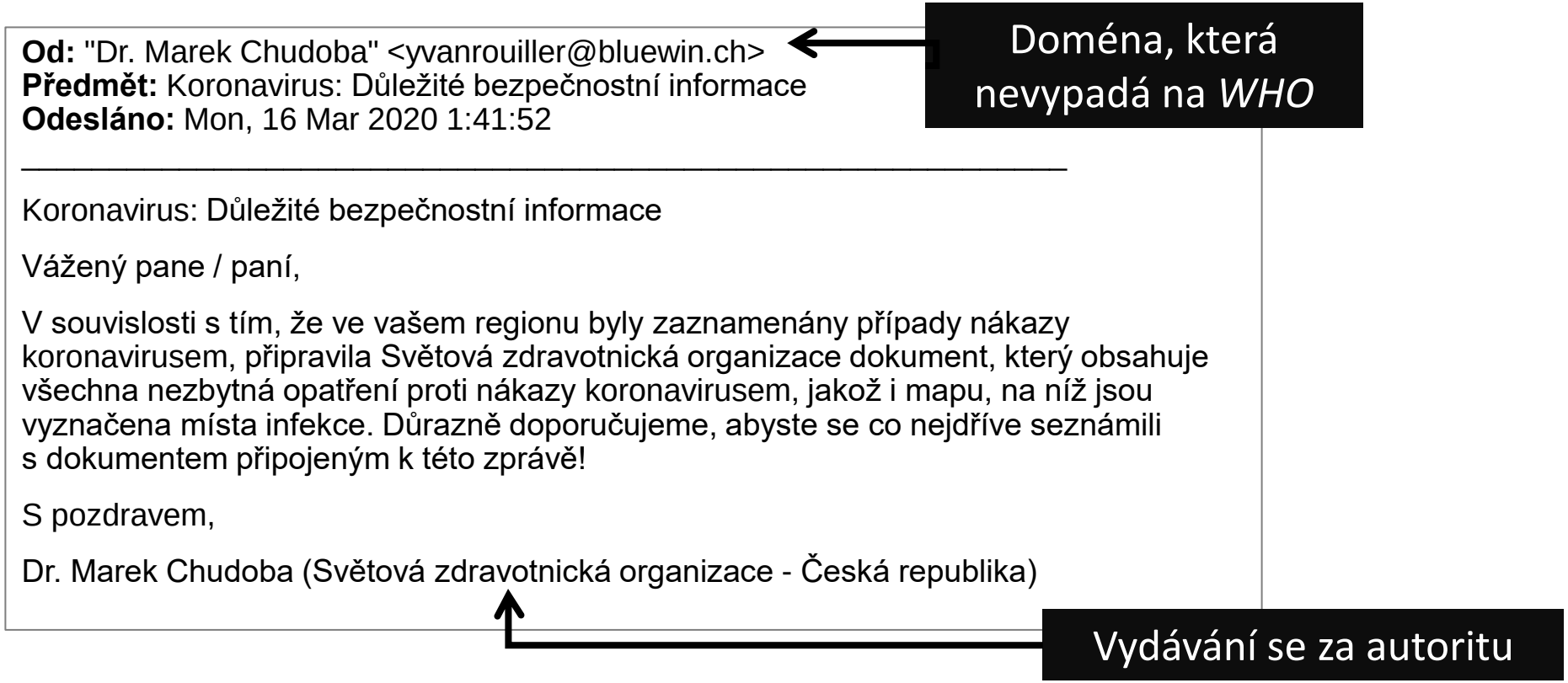
Odkaz po najetí kurzorem na „zde“.

Podvodná stránka, která se snaží napodobit stránky dopravce.



# Phishing a COVID-19

- Dokument „s opatřeními“ proti *COVID-19* od *WHO*
- V příloze dokument (`.doc`) obsahující malware



# Phishing a COVID-19

- *Martketka:* „Seznamování“ během karantény?

Od Markéta Kovaříková <marketa.kovarikova@lovemail.cz>

Předmět **Ahoj :-P** 02.04.2020 10:04

Ahoj :)

Omlouvám se, že píšu takhle nahodile, snad tě touto dobou trochu pobaví i kontakt od někoho... neznámého? :-)

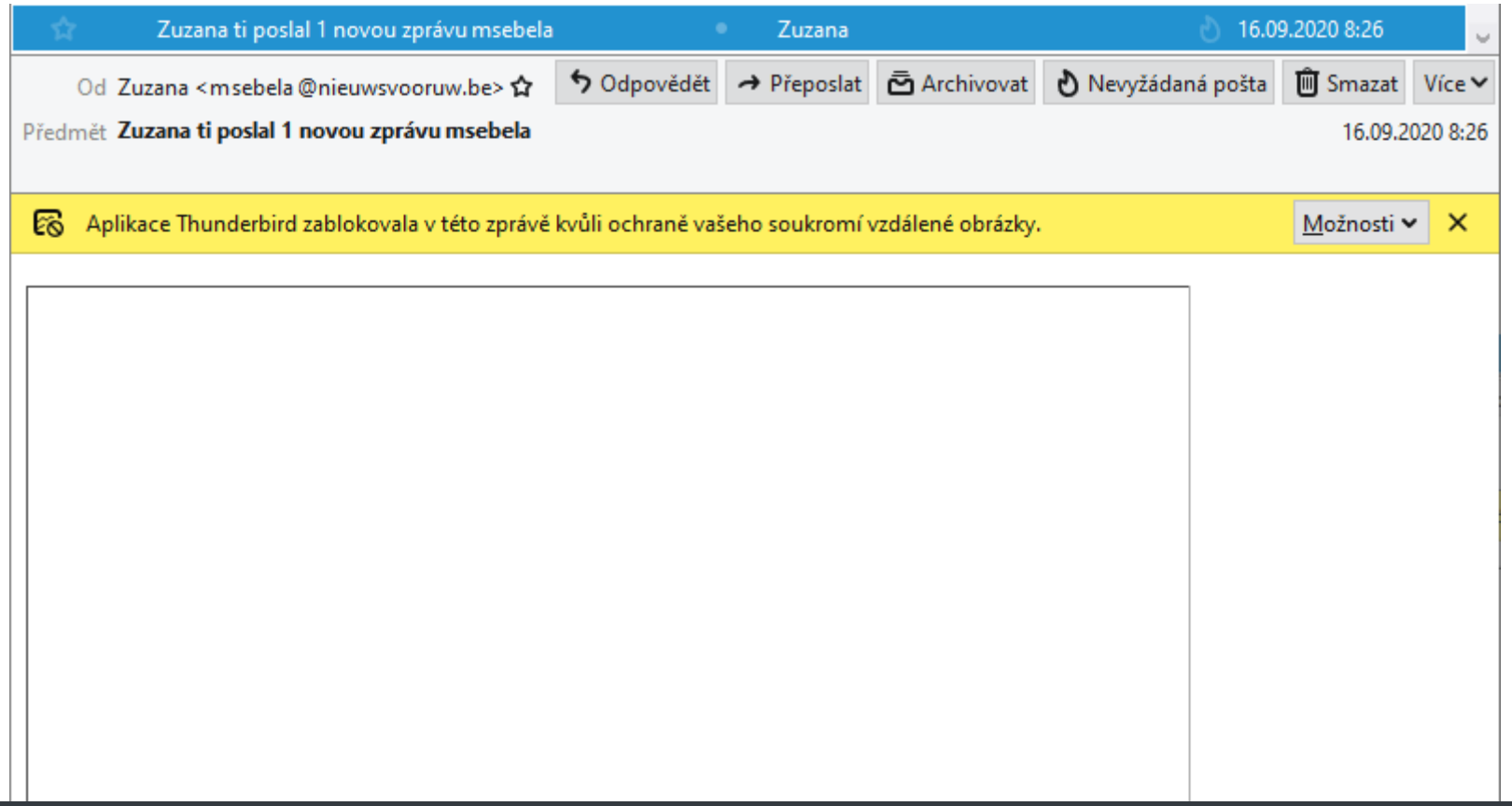
Jsem doma hrozně znuděná... Posledních pár týdnů v tomhle nuceném domácím úkrytu mě doslova likviduje... A to jsem se těšila, že s jarem snad přijde příležitost na nová seznámení :(

A tak jsem si říkala, že si třeba někdo napíše pár slov... Budu ráda, když se ozveš :-)
Martketka

—marketa1.jpg—

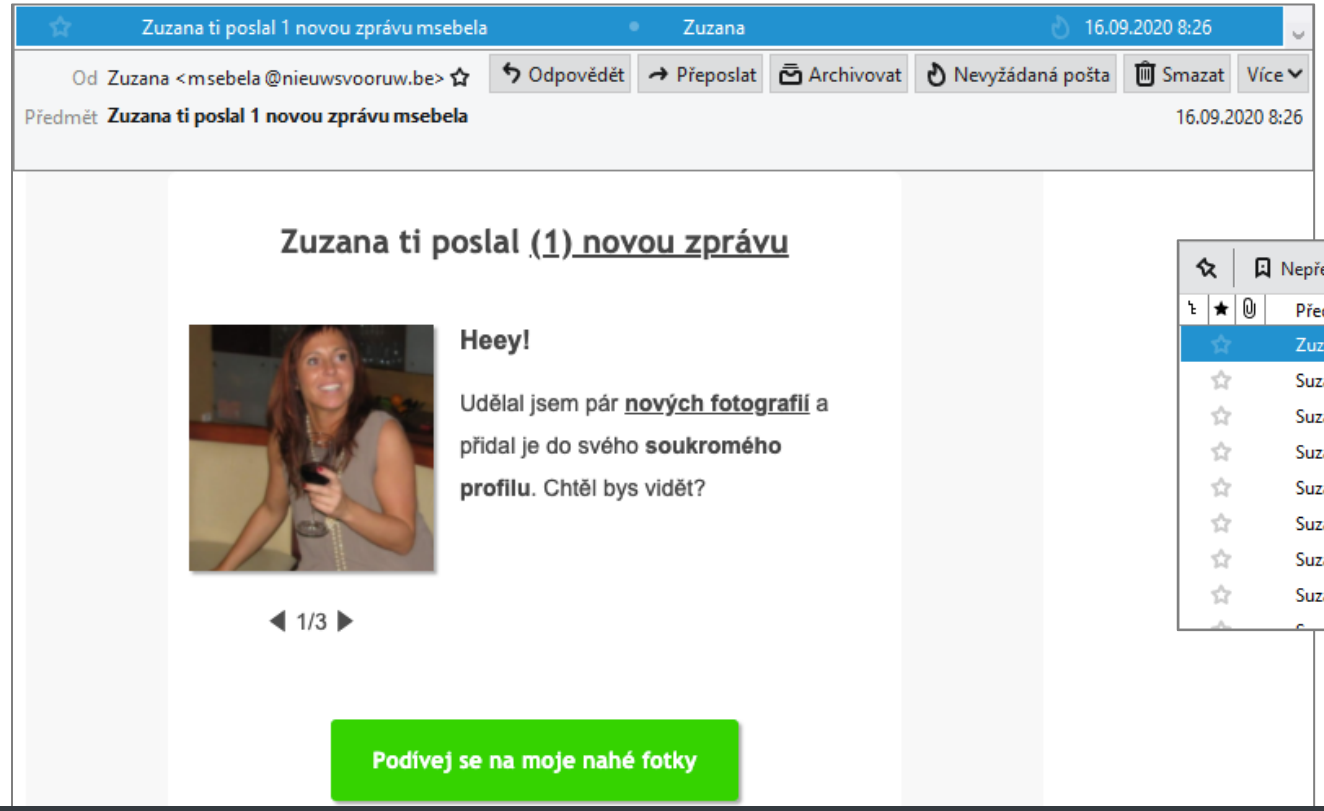
# Sledovací obrázky v e-mailech

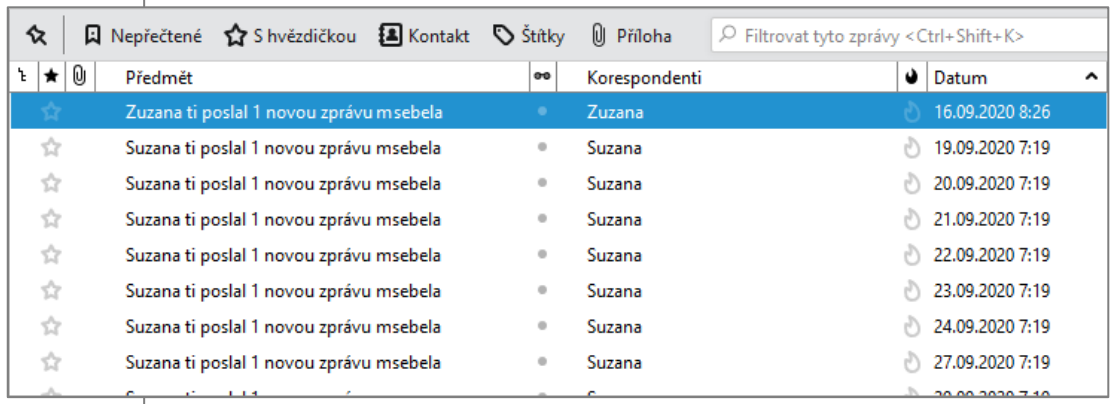
- Lišta s upozorněním na zobrazení obrázků v e-mailu



# Sledovací obrázky v e-mailech

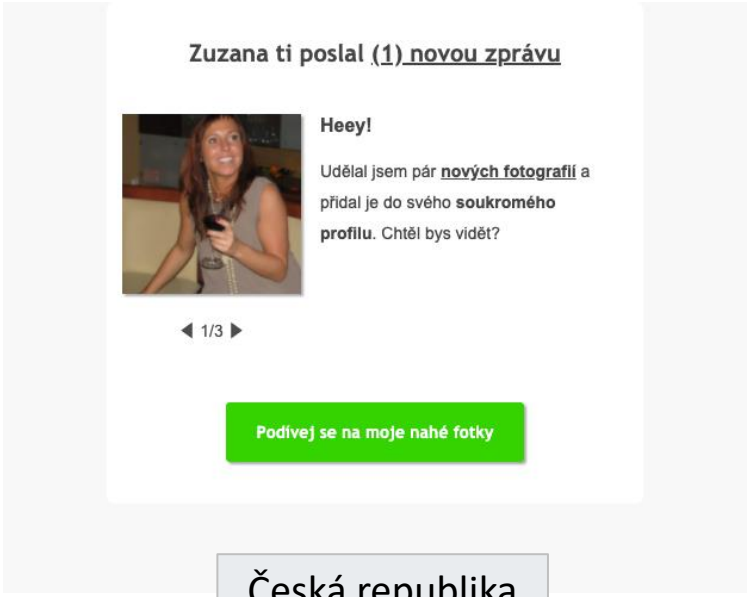
- Zobrazením obrázku došlo k potvrzení, že e-mail uživatel přečetl
- Typicky se jedná o průhledné 1×1 pixel velké obrázky



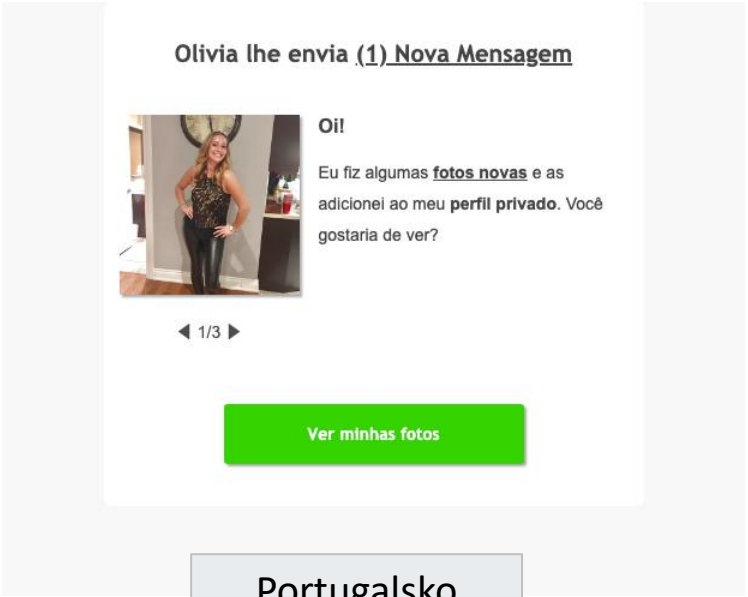



# Sledovací obrázky v e-mailech

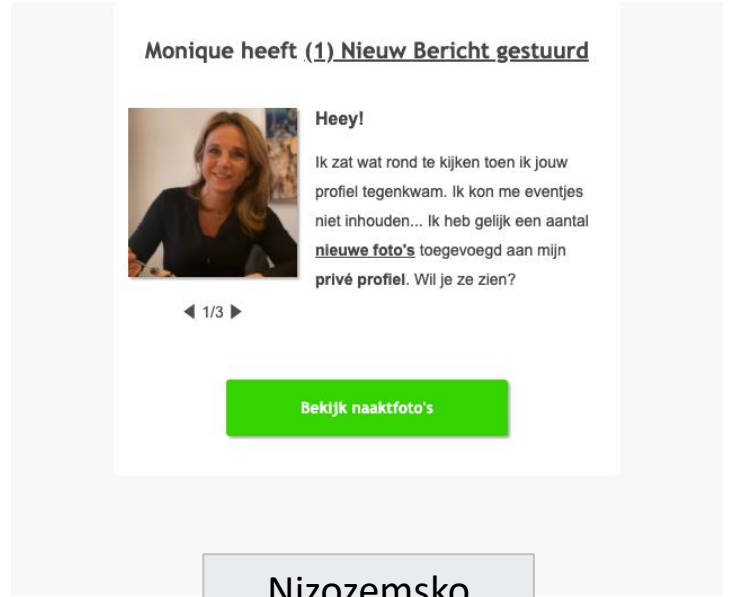
- Zjištěna mutace stejného e-mailu pro několik států:
  - CZ, AT, DE, PL, BE, CH, NL, PT, IE, UK




Česká republika




Portugalsko




Nizozemsko

# Phishingator

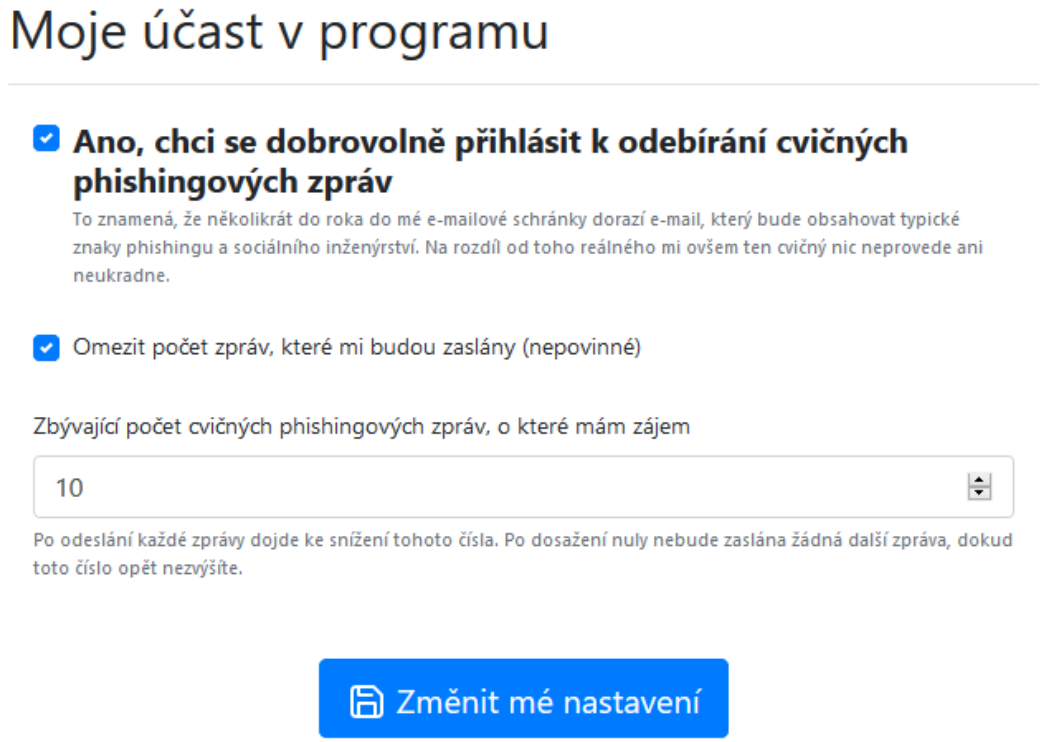
- Systém pro rozesílání cvičných phishingových zpráv

A nechtěl bys jednou za čas poslat cvičný phishing? Abys nezapomněl…

Radši ten cvičný než ten skutečný!

# Přihlášení do Phishingatoru

- **Dobrovolné** odebírání phishingu
  - https://phishingator.zcu.cz
- Přihlášení **univerzitním** kontem
  - Studenti i zaměstnanci ZČU
- Možnost kdykoliv pozastavit účast
- Nastavení **limitu zpráv**



# Cvičný phishing: expirace hesla

- Příklad cvičného phishingu z *Phishingatoru*

**Od:** zcu.cz <pass.hunter@gmail.com>
**Předmět:** Warning: Email Password Will Be Expire Soon
**Odesláno:** Pátek, Září 11, 2020 11:40

Email Password Message

*The password to your email msebela@civ.zcu.cz is expiring on 15/09/2020.*

To continue using this email and retain password kindly use the keep

same passwo button below

Keep Same Password Here

http://mail.webzcu.eu/?ha0_91dl

Please note that you can only download or read the message with the

email msebela@civ.zcu.cz this message was sent to

No third-party access

© ZCU

Neznámý odesílatel

Časový nátlak

Odkaz na podvodnou stránku, která se snaží napodobit zcu.cz

Copyright si tam může napsat kdokoliv

# Cvičný phishing: expirace hesla

(…)

To continue using this email and retain password kindly use the keep

same passwo button below

Keep Same Password Here

http://mail.webzcu.eu/?ha0_91dl

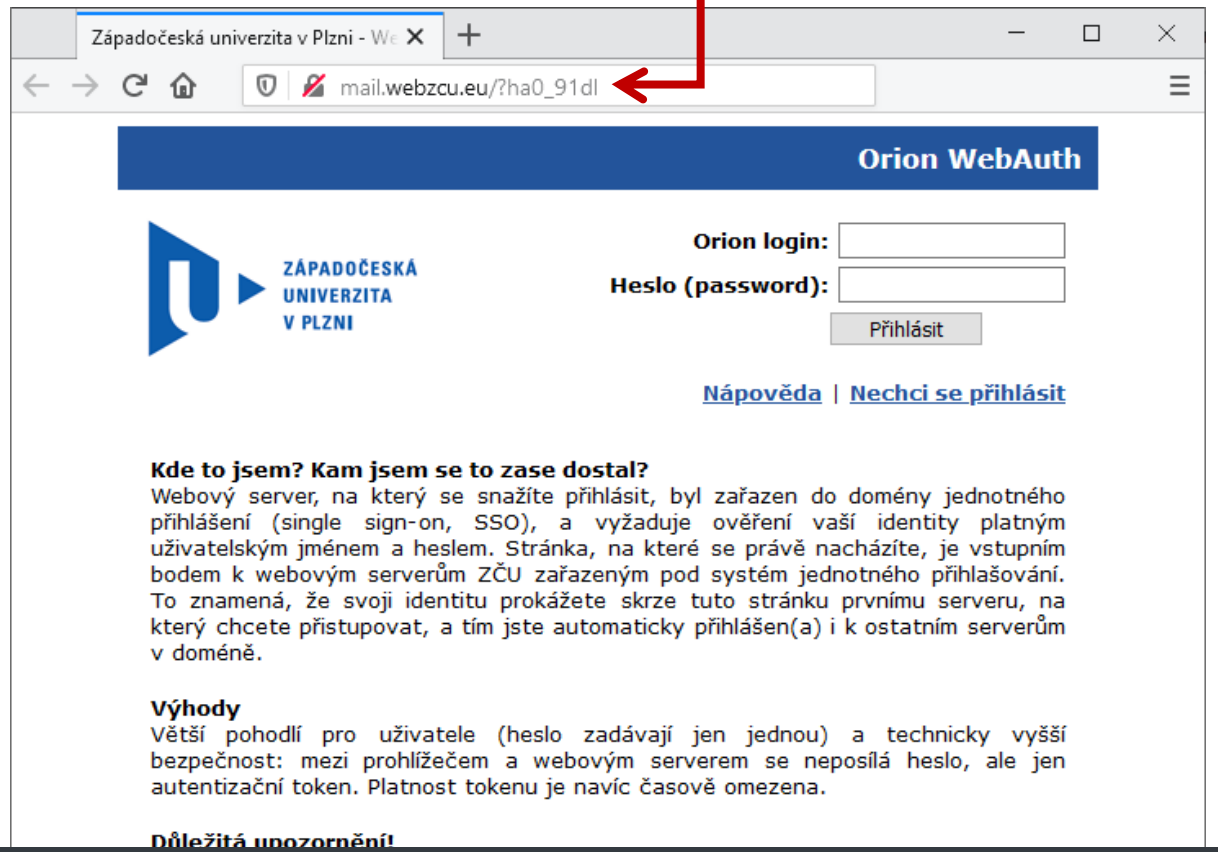
Please note that you can only download or read the message with the

email msebela@civ.zcu.cz this message was sent to

No third-party access

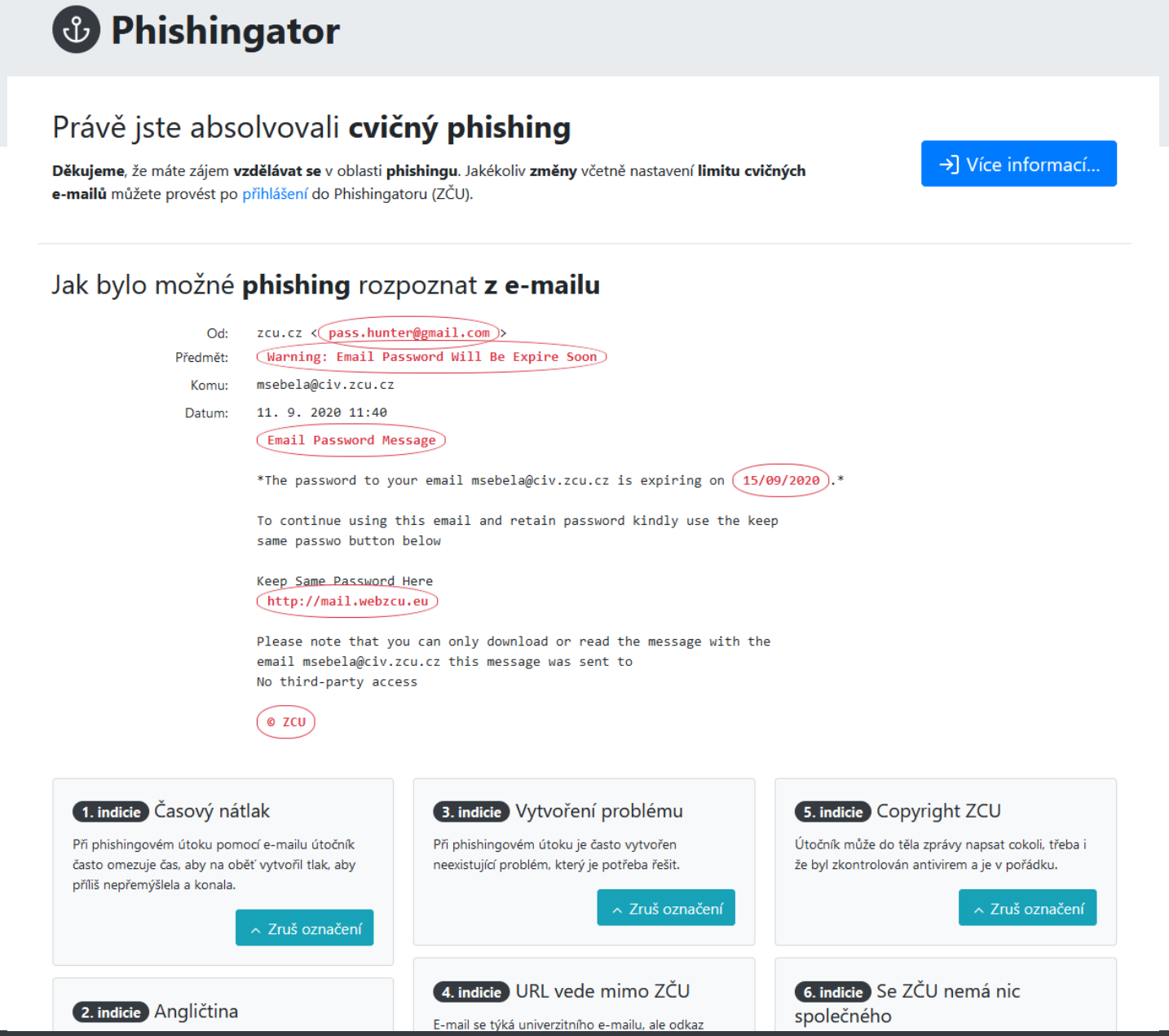
© ZCU

Cvičná podvodná stránka, která se snaží napodobit přihlášení na ZČU, ale adresa je mail.webzcu.eu (jediná správná je zcu.cz).



# Phishingator

- Cílem **vzdělávat uživatele**
- Upozornění na **indicie**
  - V podvodném **e-mailu**
  - Na podvodné **stránce**
- Zpětná vazba od uživatelů

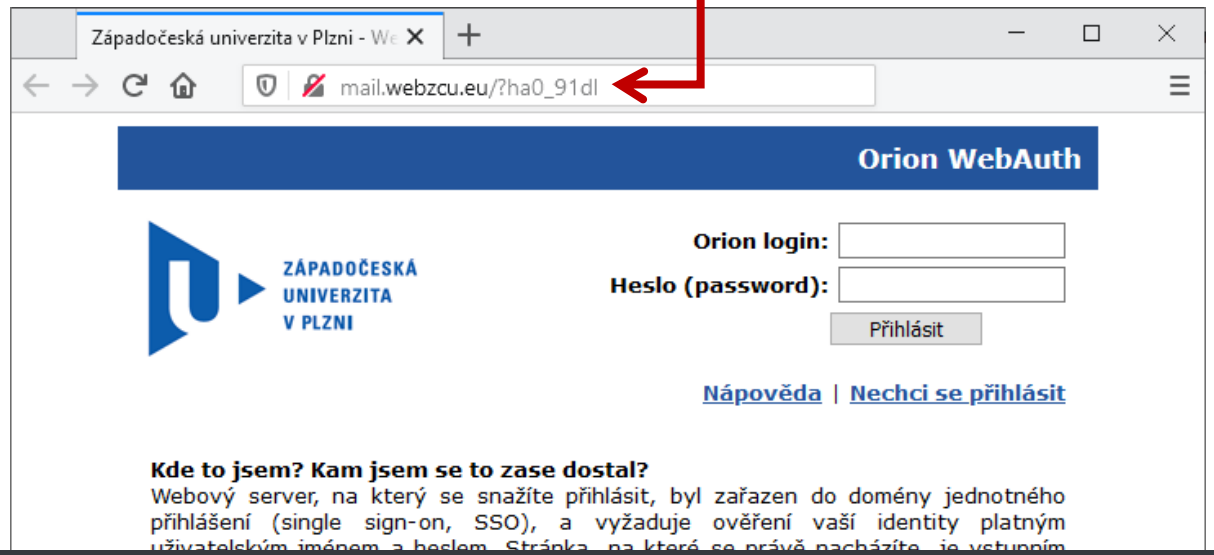


# Závěr

## Phishing tu byl, je a bude.

- Pozor, kam vedou **odkazy**
- **Phishingator**
  - phishing nanečisto
  - https://phishingator.zcu.cz

Podvodná stránka, která se snaží napodobit přihlášení na ZČU, ale adresa je mail.webzcu.eu (jediná správná je zcu.cz).



# Dotazy

?

**Martin Šebela**
msebela@civ.zcu.cz