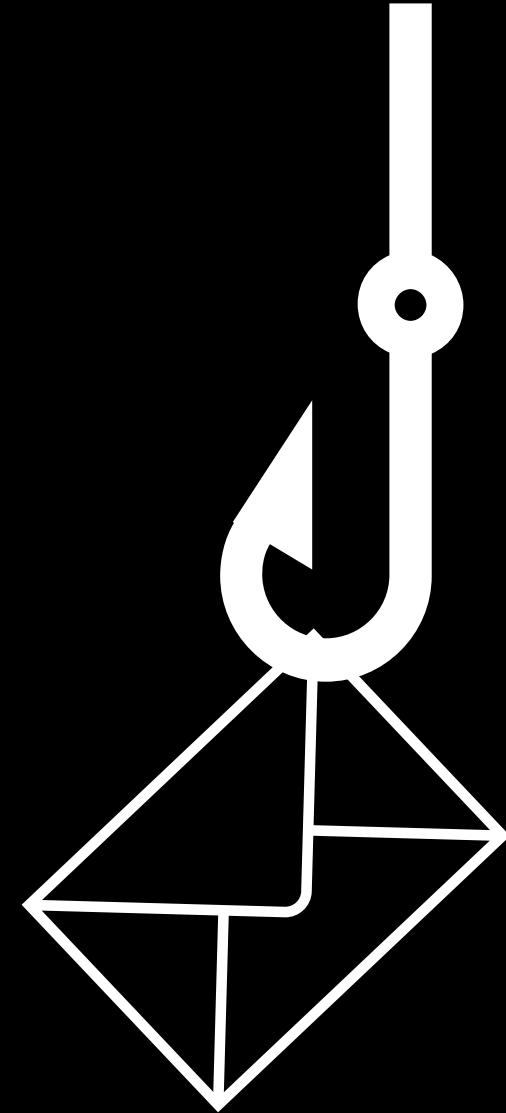


PHISHING

MARTIN ŠEBELA

SECFEST ZČU

3. 12. 2020





- Phishing = **podvodné e-mail**
- 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
 - irozhlaz.cz/zpravy-svet/smatana-duxodce-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

24

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 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. listopadu 2018 jsem vyhrál loterii 343,9 milionu Powerball, část z ní daruji deseti šťastlivcům a organizaci Ten Charity. Váš e-mail vyšel jako vítěz. Okamžitě kontaktujte reklamní oddělení ohledně reklamní kampaně.
Kontakt: [lerynnewestcallumfoundation2020@outlook.com](#)

Hello, I am Lerynne West, you have a donation of 1,930,000.00 EUR. On 5th Nov 2018 I won the 343.9 million Powerball lottery, part of which I am donating to 10 lucky people and the organization Ten Charity. Your email came up as the winner. Please contact the advertising department immediately regarding the advertising campaign.
Contact: [lerynnewestcallumfoundation2020@outlook.com](#)

This Communication is Confidential

Hotovo

Od lakshay.agarwal@skpatodia.in ☆
Předmět **1,5 milionu dolaru darováno**
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 zemřela na rakovinu, rádi oslovujeme nemocné a chudé lidi ve vaší komunitě a na celém světě. Odpovezte na informace a doklad o vašem vyhraném lotto fondu.

Manuel Franco

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

Milý

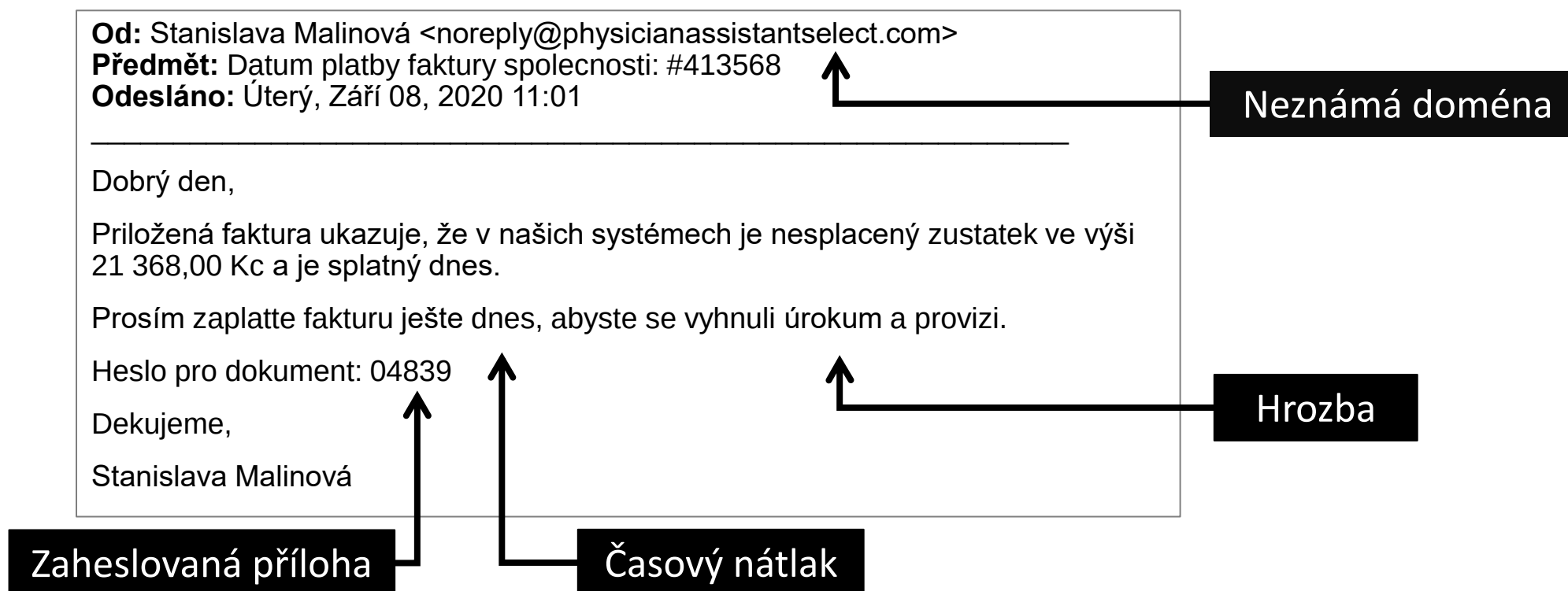
Vím, že vám tento mail přijde jako překvapení a mám zvláštní důvod, proč jsem se rozhodl napsat vám kvůli naléhavosti mé situace. Jsem Anna Quassi 23 letá dívka z Pobřeží slonoviny., Jsem jediná dcera pozdního pana Daniela Quassiho, před smrtí otce byl velmi dobře známým obchodníkem v kakau, ořechech 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 své dceři, že jsem jediné dítě, které má. Prosím vás, pomozte mi kvůli nepřátelům mého otce, kteří jsou v úkrytu v uprchlickém táboře a rád bych vás navštívil v podobném obchodnímu vztahu a pomohl vám. Můj otec vložil do banky částku 3,5 milionu dolarů, budu vám děkovat jako další příbuzný. Budu vám děkovat za potvrzení vašeho přijetí, které mi pomůže v investování fondu. Pomůžete mi při investici a pomůžete mi v mém vlastním táboře, prosím vás, abyste je navštívili, jakmile bude fond převeden.

Anna Quassi

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

Od: <soukromý e-mail studenta>

Předmět: Re: Studium - Oznámení o ubytovacím stipendiu

Odesláno: Středa, Listopad 18 2020 22:16:51

I have made some edits. Please check.

Reakce „studenta“ na ubytovací stipendium

[https://drive.google.com/uc?id=118oBvJqKx8\(...\) &export=download](https://drive.google.com/uc?id=118oBvJqKx8(...) &export=download)

Archive password: 1340

Zaheslovaná příloha na Google Drive

Dne 14.10.2020 jste požádal(a) o přiznání ubytovacího stipendia s prohlášením
"Prohlašuji, že splňuji podmínky pro přiznání ubytovacího stipendia stanovené v článku 6 Stipendijního řádu Západočeské univerzity v Plzni". (...)

Automatický e-mail z univerzitního systému

Phishing: podvodná stránka



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

Odesílatel vypadá důvěryhodně

Vážený zákazníku,

Platba byla na váš účet zveřejněna dne 10/11/2020. K uvolnění platby na váš účet je však nutné overení.

Zacnete kliknutím a přihlášením do svého účtu zde.

Jsme připraveni vám sloužit lépe.

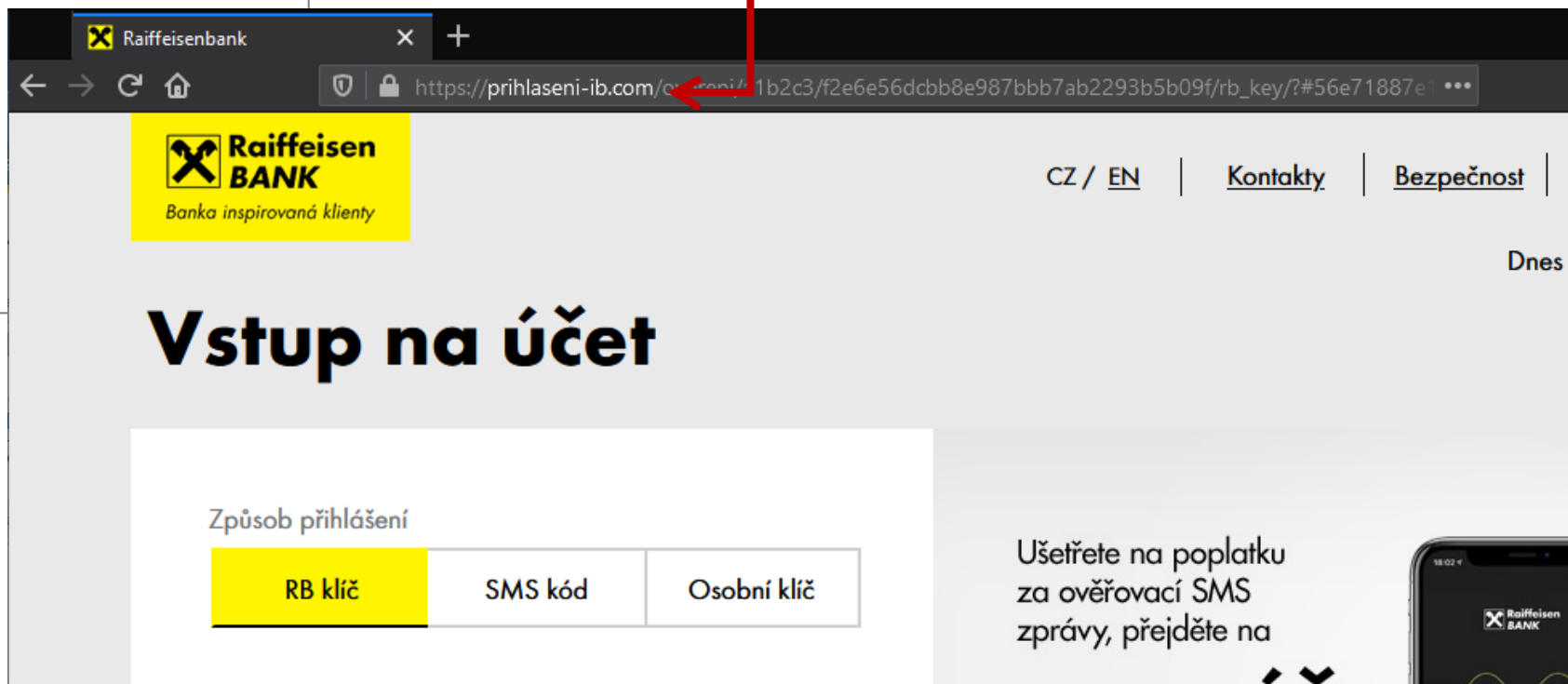
S pozdravem,

Raiffeisenbank

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

Odkaz po najetí kurzorem na „zde“.

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



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 -

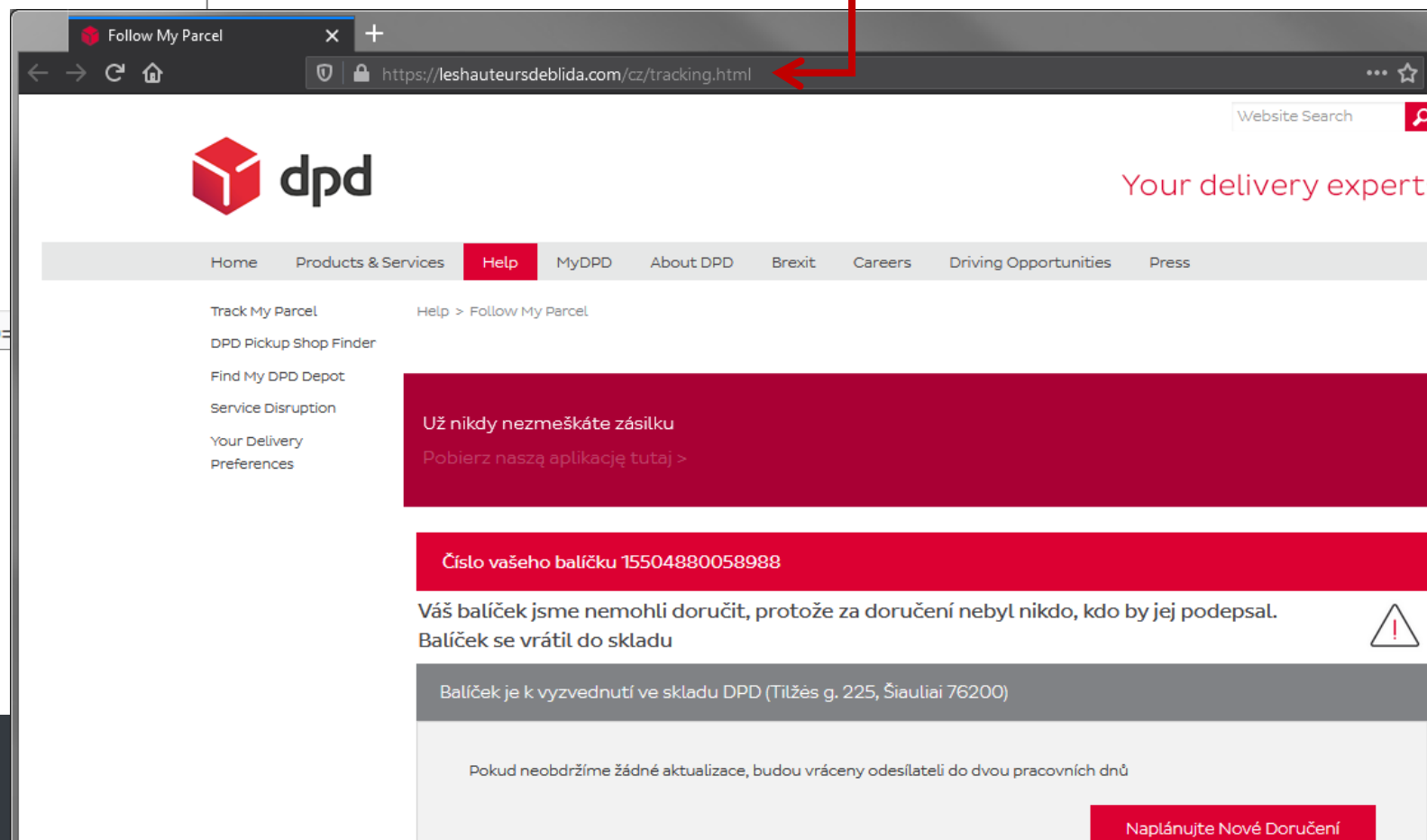
Za jakýkoliv pokud o opětovné doručení bude účtován poplatek 19,00 Kč protože již byly provedeny dva pokusy o doručení.

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

Od: "Dr. Marek Chudoba" <yvanrouiller@bluewin.ch>
Předmět: Koronavirus: Důležité bezpečnostní informace
Odesláno: Mon, 16 Mar 2020 1:41:52

Doména, která
nevypadá na *WHO*

Koronavirus: Důležité bezpečnostní informace

Vážený pane / paní,

V souvislosti s tím, že ve vašem regionu byly zaznamenány případy nákazy koronavirem, připravila Světová zdravotnická organizace dokument, který obsahuje všechna nezbytná opatření proti nákazy koronavirem, jakož i mapu, na níž jsou vyznačena místa infekce. Důrazně doporučujeme, abyste se co nejdříve seznámili s dokumentem připojeným k této zprávě!

S pozdravem,

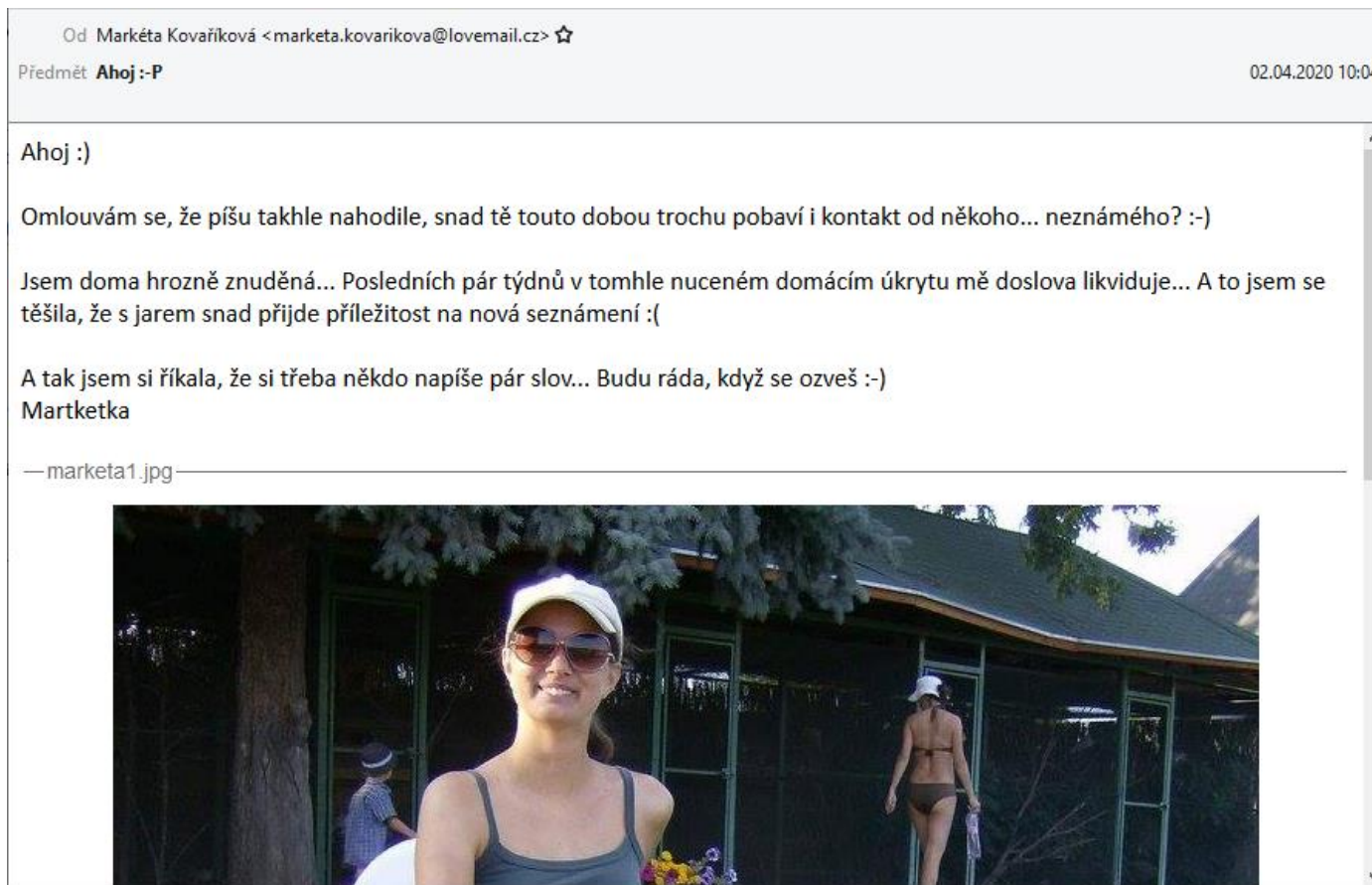
Dr. Marek Chudoba (Světová zdravotnická organizace - Česká republika)

Vydávání se za autoritu

Phishing a COVID-19



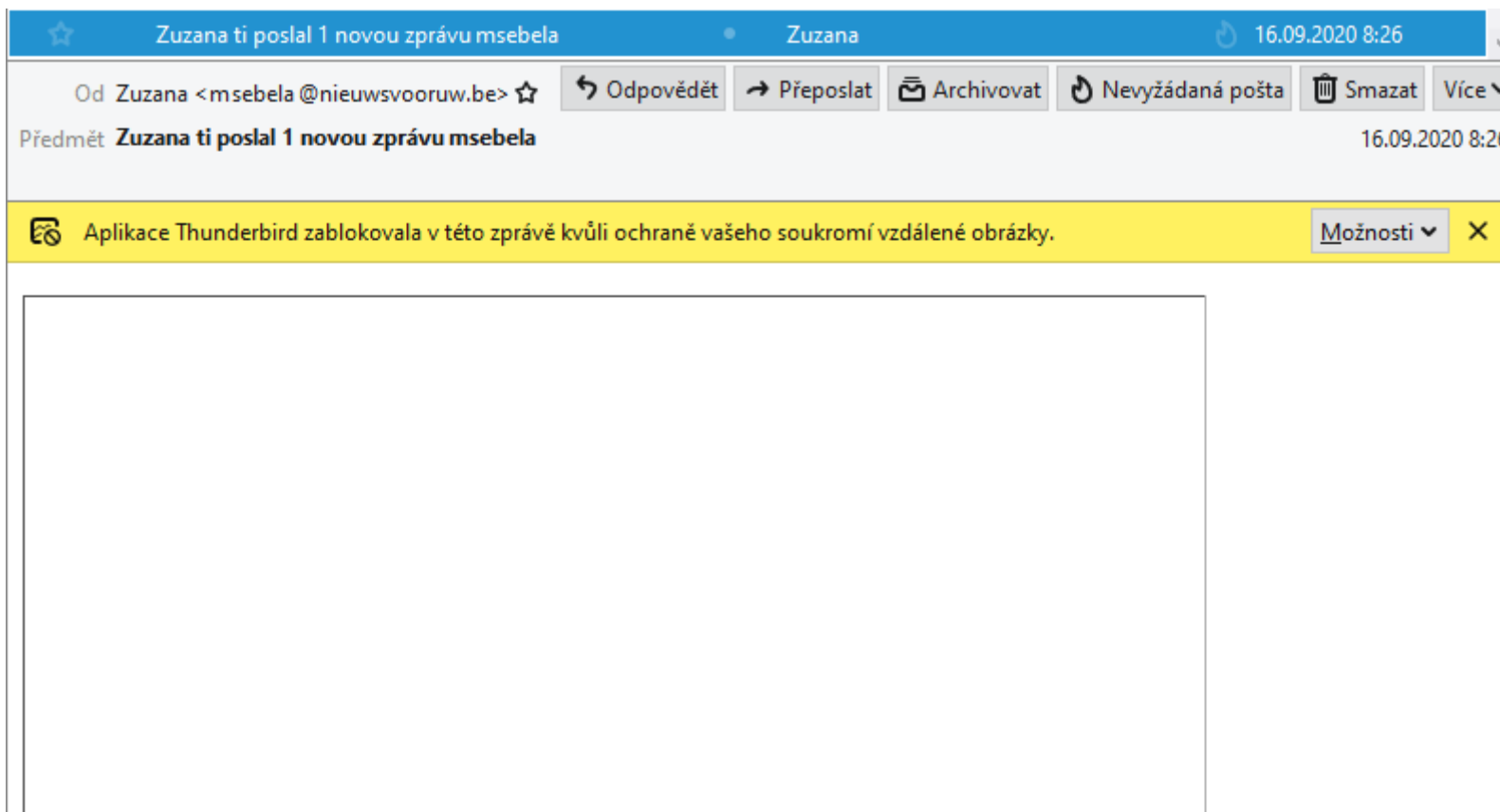
- *Martketka*: „Seznamování“ během karantény?



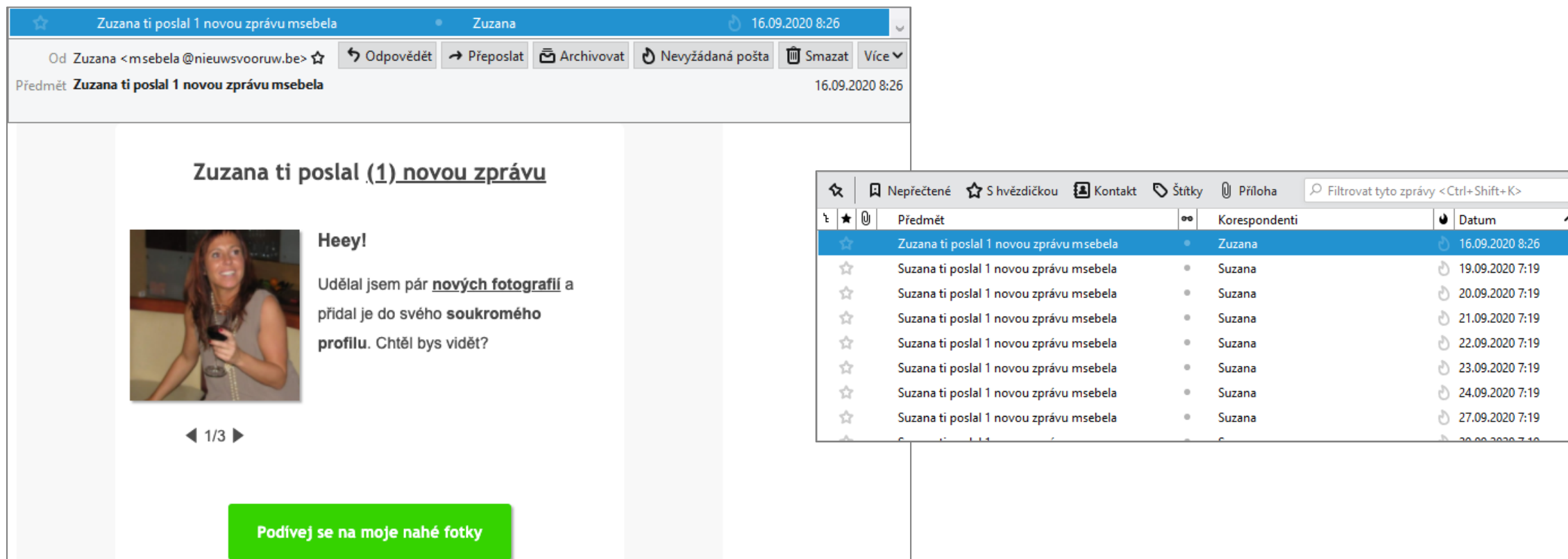
Sledovací obrázky v e-mailech



- Lišta s upozorněním na zobrazení obrázků v e-mailu



- 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

Zuzana ti poslal (1) <u>novou zprávu</u>  Česká republika	Olivia lhe envia (1) <u>Nova Mensagem</u>  Portugalsko	Monique heeft (1) <u>Nieuw Bericht gestuurd</u>  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!



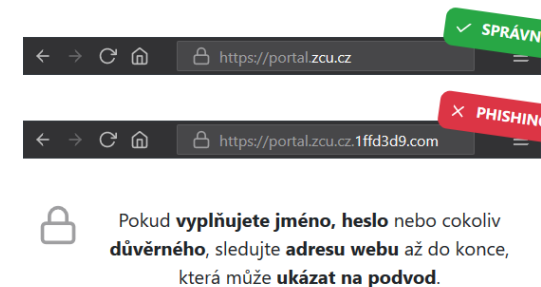
Co je to ten phishing?

Phishing [fíʃɪŋ] je **podvodná zpráva**, která uživatele láká na **něco neuvěřitelného**, nebo se mu snaží nějakým způsobem **vyhrožovat** či **napodobovat** jinou známou **instituci/osobu** a jejím jménem uživatele **o něco žádat**.

Útočníci tyto zprávy rozesílají v **obrovském množství**, přičemž jejich **cílem je poškodit uživatele** (a často i instituci, se kterou je e-mail spojen). Z uživatelů se snaží typicky **získat přihlašovací** či jiné **důvěrné údaje** (například **číslo platební karty**).

Uživatelé si často bohužel tuto **hrozbu nepřipouští** nebo dokonce o ní **vůbec neví** a **nahrávají** tak **útočníkům**.

[Více o phishingu »](#)



Pokud **vyplňujete jméno, heslo** nebo cokoliv **důvěrného**, sledujte **adresu webu** až do konce, která může **ukázat na podvod**.

Přihlášení do Phishingatoru



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

Moje účast v programu

☒ **Ano, chci se dobrovolně přihlásit k odebírání cvičných phishingových zpráv**

To znamená, že několikrát do roka do mé e-mailové schránky dorazí e-mail, který bude obsahovat typické znaky phishingu a sociálního inženýrství. Na rozdíl od toho reálného mi ovšem ten cvičný nic neprovede ani neukradne.

☒ Omezit počet zpráv, které mi budou zaslány (nepovinné)

Zbývající počet cvičných phishingových zpráv, o které mám zájem

10



Po odeslání každé zprávy dojde ke snížení tohoto čísla. Po dosažení nuly nebude zaslána žádná další zpráva, dokud toto číslo opět nezvýšíte.

 Změnit mé nastavení

Cvičný phishing: expirace hesla



- Příklad cvičného phishingu z *Phishingatoru*

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

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

Neznámý odesílatel

Email Password Message

Časový nátlak

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

Copyright si tam může napsat kdokoliv

Cvičný phishing: expirace hesla



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

(...)

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

Orion WebAuth

**ZÁPADOČESKÁ
UNIVERZITA
V PLZNI**

Orion login:

Heslo (password):

[Nápověda](#) | [Nechci se přihlásit](#)

Kde to jsem? Kam jsem se to zase dostal?
Webový server, na který se snažíte přihlásit, byl zařazen do domény jednotného přihlášení (single sign-on, SSO), a vyžaduje ověření vaší identity platným uživatelským jménem a heslem. Stránka, na které se právě nacházíte, je vstupním bodem k webovým serverům ZČU zařazeným pod systém jednotného přihlašování. To znamená, že svoji identitu prokážete skrze tuto stránku prvním serveru, na který chcete přistupovat, a tím jste automaticky přihlášen(a) i k ostatním serverům v doméně.

Výhody
Větší pohodlí pro uživatele (heslo zadávají jen jednou) a technicky vyšší bezpečnost: mezi prohlížečem a webovým serverem se neposílá heslo, ale jen autentizační token. Platnost tokenu je navíc časově omezena.

Důležitá upozornění!

Phishingator

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



Právě jste absolvovali **cvičný phishing**

Děkujeme, že máte zájem **vzdělávat se** v oblasti **phishingu**. Jakékoliv **změny** včetně nastavení **limitu cvičných e-mailů** můžete provést po **přihlášení** do Phishingatoru (ZČU).

[→ Více informací...](#)

Jak bylo možné **phishing** rozpoznat z **e-mailu**

Od: zcu.cz <pass.hunter@gmail.com>
Předmět: **Warning: Email Password Will Be Expire Soon**
Komu: msebela@civ.zcu.cz
Datum: 11. 9. 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>

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

1. indicie Časový nátlak

Při phishingovém útoku pomocí e-mailu útočník často omezuje čas, aby na oběť vytvořil tlak, aby příliš nepřemýšlela a konala.

[^ Zruš označení](#)

3. indicie Vytvoření problému

Při phishingovém útoku je často vytvořen neexistující problém, který je potřeba řešit.

[^ Zruš označení](#)

5. indicie Copyright ZČU

Útočník může do těla zprávy napsat cokoli, třeba i že byl zkontrolován antivirem a je v pořádku.

[^ Zruš označení](#)

2. indicie Angličtina

4. indicie URL vede mimo ZČU

E-mail se týká univerzitního e-mailu, ale odkaz

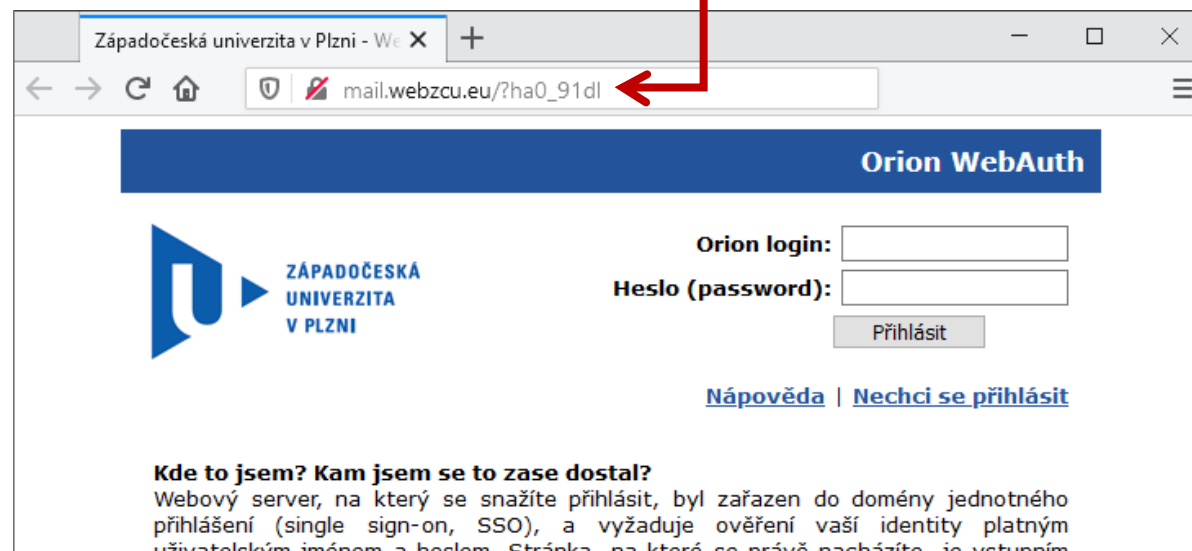
6. indicie Se ZČU nemá nic společného



Phishing tu byl, je a bude.

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

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





Martin Šebela
msebela@civ.zcu.cz