ZÁPADOČESKÁ UNIVERZITA V PLZNI

IT bezpečnost

Phishing

Školení pro uživatele sítě WEBnet

Aleš Padrta, Jiří Čepák / 9. 2. 2018

ÚVOD

Teroristický útok vs. Kybernetický útok

- Několik společných rysů
  - **Útočník** (terorista vs. hacker)
  - **Cíl** (osoby na vymezeném prostoru vs. zaměstnanci ZČU)
  - **Zbraň** (bomba vs. email se závadnou přílohou nebo odkazem)

Teroristický útok vs. Kybernetický útok

- Několik společných rysů
  - **Útočník** (terorista vs. hacker)
  - **Cíl** (osoby na vymezeném prostoru vs. zaměstnanci ZČU)
  - **Zbraň** (bomba vs. email se závadnou přílohou nebo odkazem)

- Jeden odlišný rys
  - Lidé se při teroristickém útoku dají na útěk …
  - ALE uživatelé PC při kybernetickém útoku klikají …

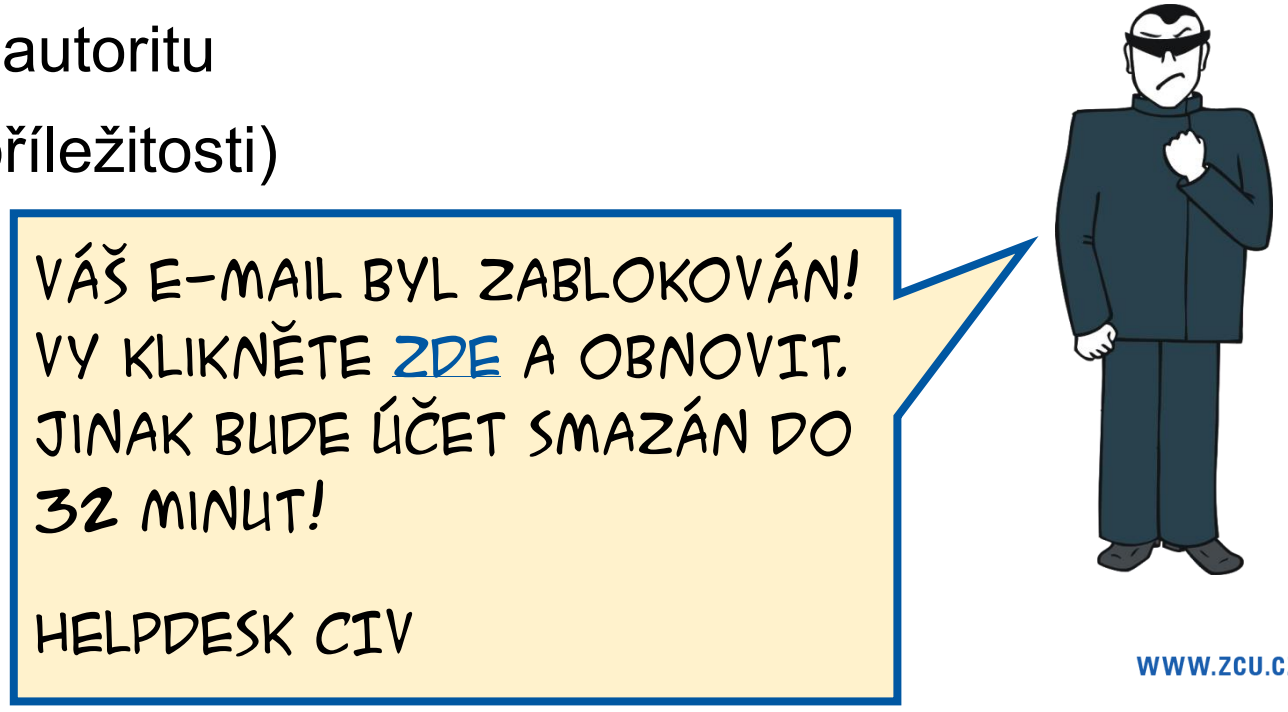
Nepříjemné důsledky

- Ovládnutí počítače útočníkem
  - Využití výkonu počítače
  - Odposlechnutí přihlašovacích údajů
  - Počítač s kamerou ⇨ přenos obrazu a zvuku, pořizování záznamu
  - Zneužívání počítače k dalším (kyber)útokům
  - Zašifrování vašich souborů
- Únik informací
  - Přihlašovací údaje
  - Výsledky výzkumu
  - …

Phishing? Phishing!

Phishing

- „Rhybaření“ = „lákání na udičku“
  - Cíleno na uživatele
  - Donucení ke sdělení informací (jméno a heslo)
  - Využití „sociálního inženýrství“
- Typické triky
  - Vydávání se za autoritu
  - Hrozba ztráty (příležitosti)
  - Časová tíseň



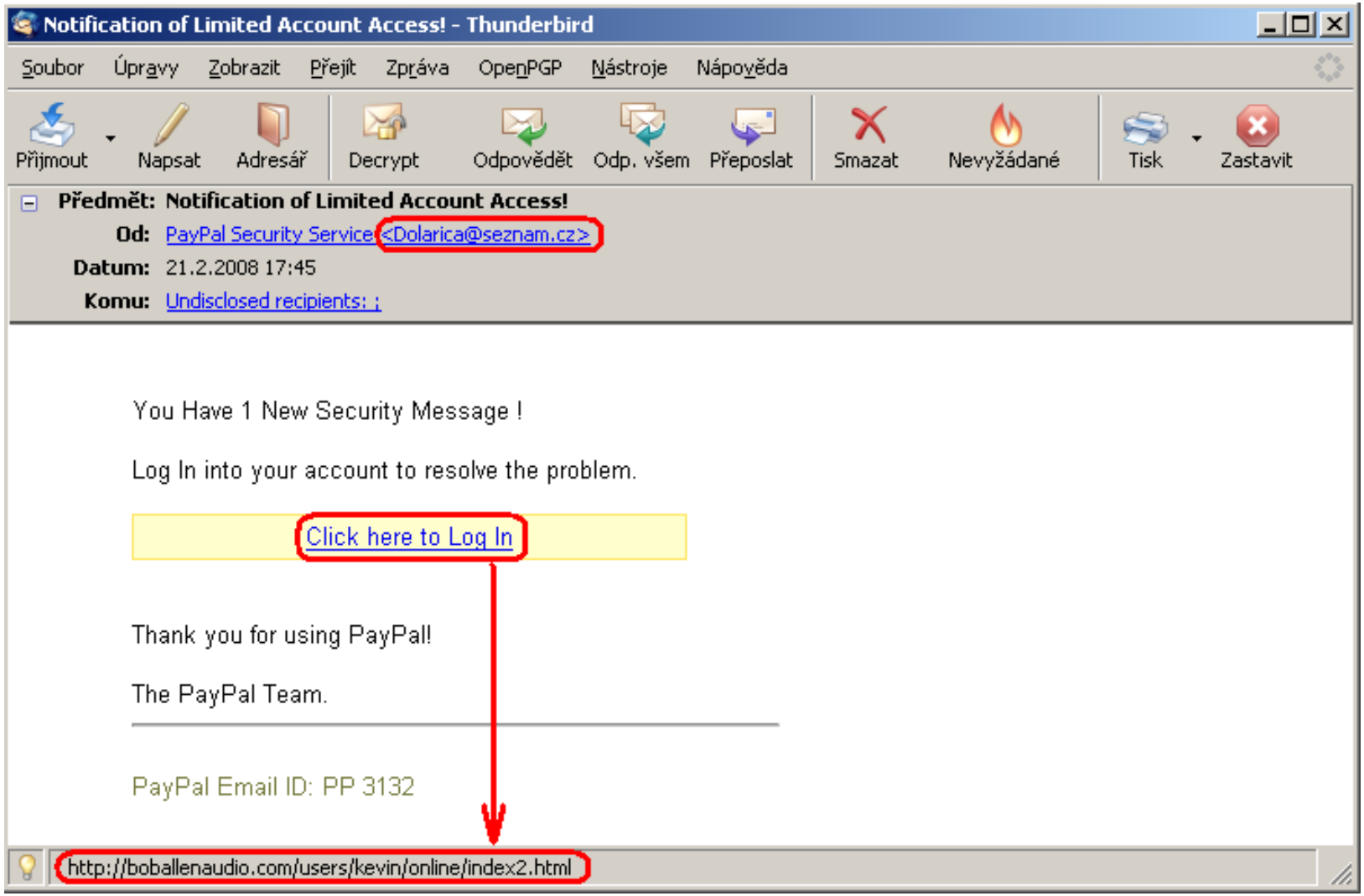
Typy phishingu: Žádost o heslo

- E-mail s požadavkem o **heslo**
  - Hlavní zásada – **nikdy nikomu** jakýmkoli způsobem nesdělujte heslo!

```
Subject: Vážený uživateli
Date:    Mon, 21 Mar 2011 10:00:01 +0100
To:       undisclosed-recipients: ;
From:    "helpdesk@zcu.cz" <helpdesk091@peoplepc.com>
Reply-To:"helpdesk@zcu.cz" <acupgrade@superposta.com>

Vážený uživateli

Naším cílem je poskytovat kvalitní podporu pro naše zákazníky.
Takže můžeme nejlépe pomoci, odpovědět na následující poté, co jste obdrželi.

V současné době provádí údržbu a aktualizaci našich
Služby účtů databáze, a jako výsledek této vaší
Účty musí být modernizovány.

Omlouváme se za způsobené potíže.

Pokud se tak nestane do 72 hodin bude okamžitě
vypnuté svůj účet z naší databáze.

Prosím, vyplňte formulář níže.

Název účtu:.
heslo:.

Přístupové Členové se dohodli, aby nás následovaly přijatelný Use Policy
Podmínky používání
(C) 1995-2011, Všechna práva vyhrazena
Veškerý obsah na tomto je k dispozici.
"Poštovním účtem PODPORA WEBMAIL ©
ABN 31088377860 Všechna práva vyhrazena

_____
PeoplePC Online
A better way to Internet
http://www.peoplepc.com
```

Typy phishingu: E-mail s odkazem na stránku

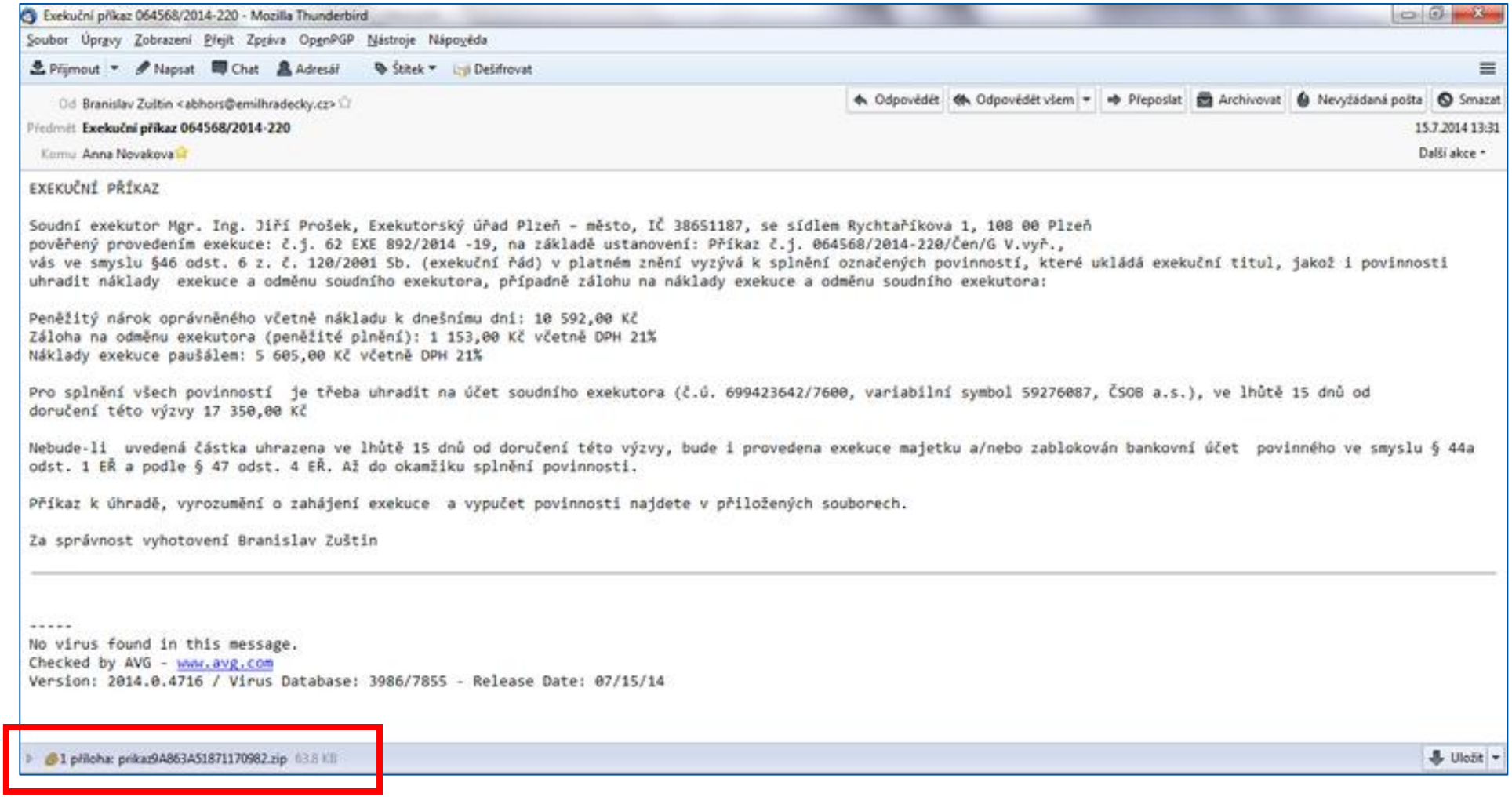
- E-mail s odkazem na (vizuálně podobné) podvodné stránky



Typy phishingu: E-mail s odkazem na stránku

Typy phishingu: Závadná příloha

- E-mail se závadnou přílohou – např. exekuční příkaz, faktura…



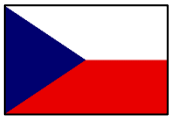
Odkazy (nejen) v e-mailech

Rozbor odkazu (URL – Uniform Resource Locator)

Rozbor odkazu (URL – Uniform Resource Locator)

http://www.gjszlin.cz/gztgm/dispnews.php?idm=1&p=3

protokol | název serveru | cesta | název skriptu | parametry stránky



U tří koťátek

Výčep

Rozbor názvu serveru (doménového jména)

komiks.civ.zcu.cz

U tří koťátek | Pražská | PLZEŇ 

Rozbor názvu serveru (doménového jména)

komiks.civ.zcu.cz

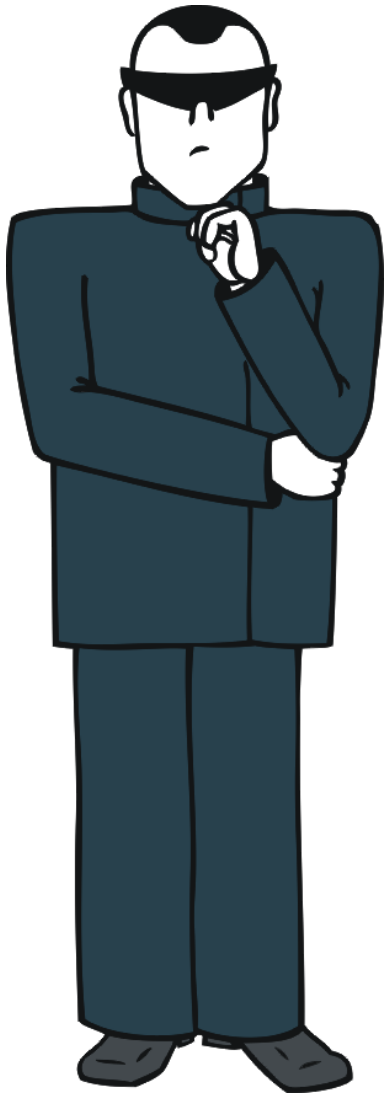
komiks.civ.zdu.cz

Rozbor názvu serveru (doménového jména)

komiks.civ.zcu.cz

komiks.civ.zcu.bz

Malý kvíz

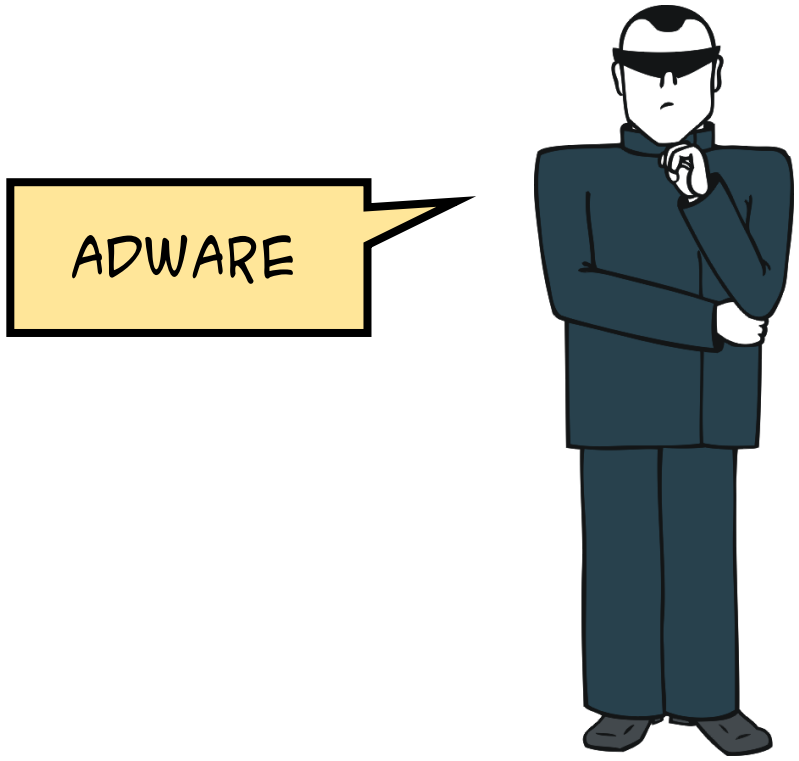


Kvíz – 1

http://xafylopaxwzwhcxwla.com

Kvíz – 1

http://xafylopaxwzwhcxwla.com



Kvíz – 2

https://www.llanfairpwllgwyngyllgogerychwyrndrobwllllantysiliogogogoch.co.uk/

Kvíz – 2

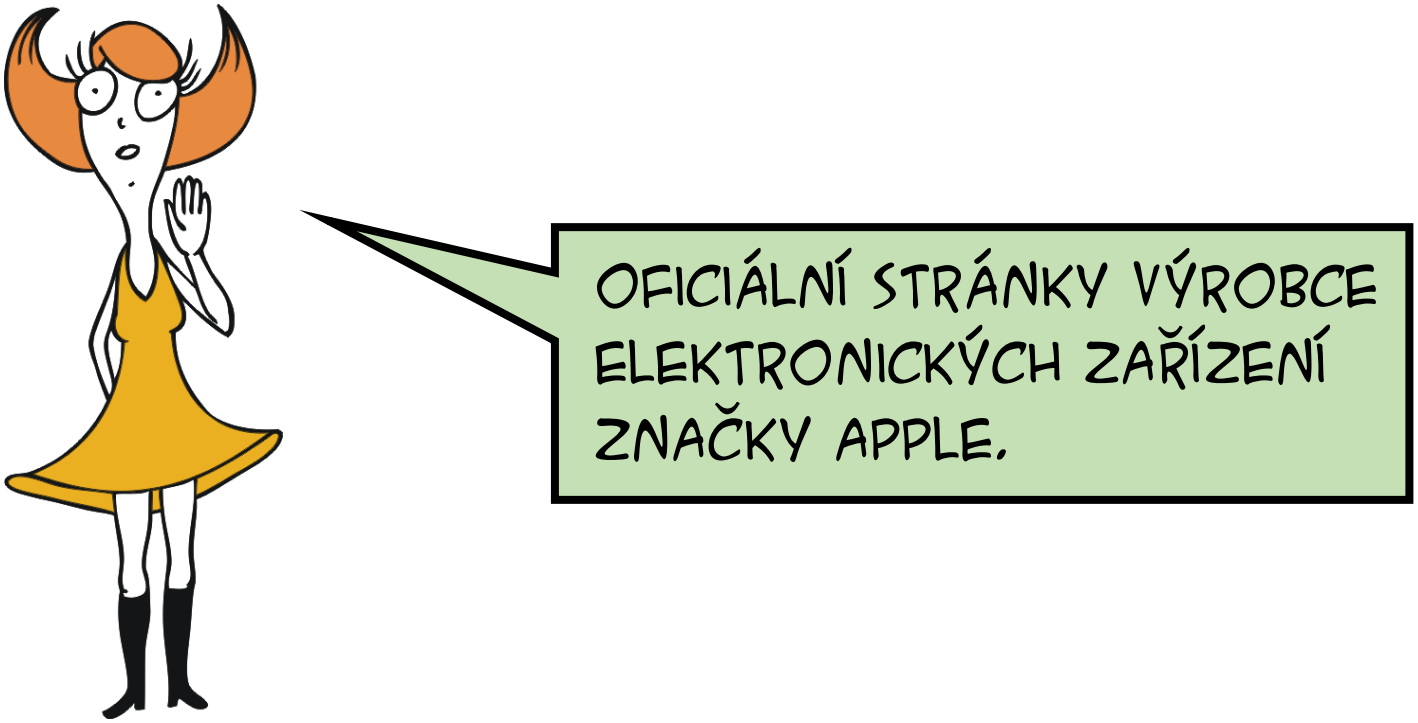
https://www.llanfairpwllgwyngyllgogerychwyrndrobwllllantysiliogogogoch.co.uk/

Kvíz – 3

http://apple.com/iphone7

Kvíz – 3

http://apple.com/iphone7



Kvíz – 4

http://apple.com-iphone7.com

Kvíz – 4

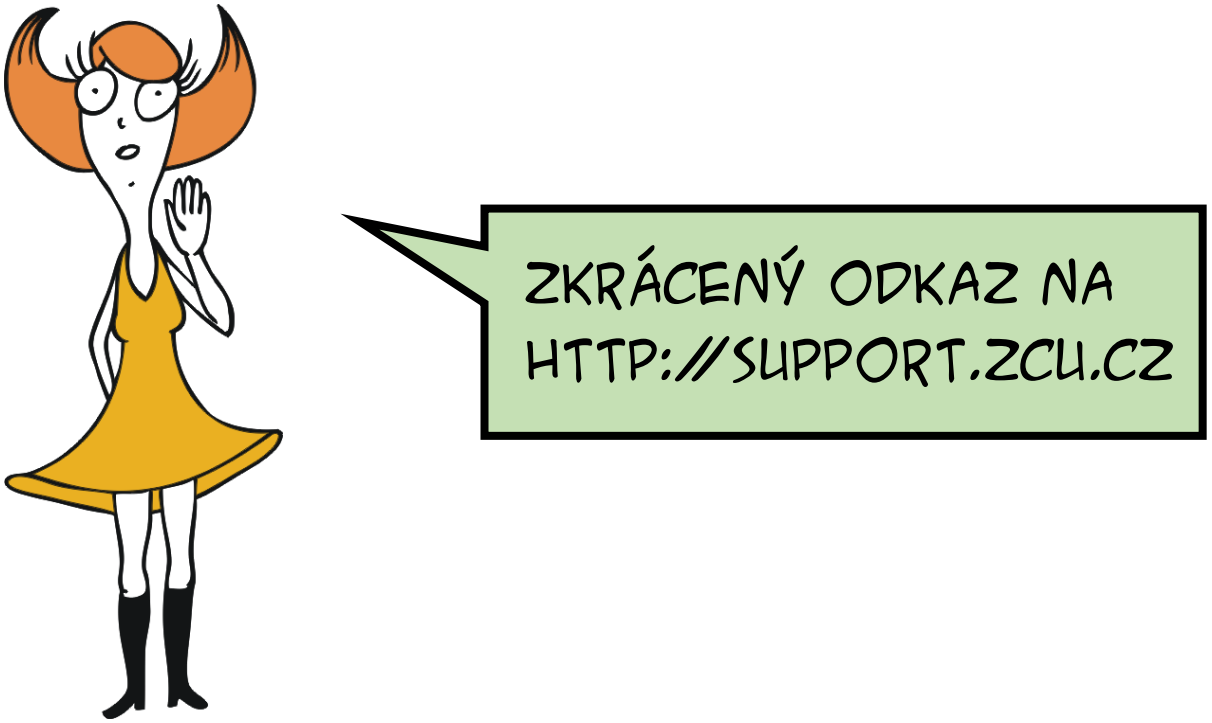
http://apple.com-iphone7.com

Kvíz – 5

http://goo.gl/Qaloqr

Kvíz – 5

http://goo.gl/Qaloqr



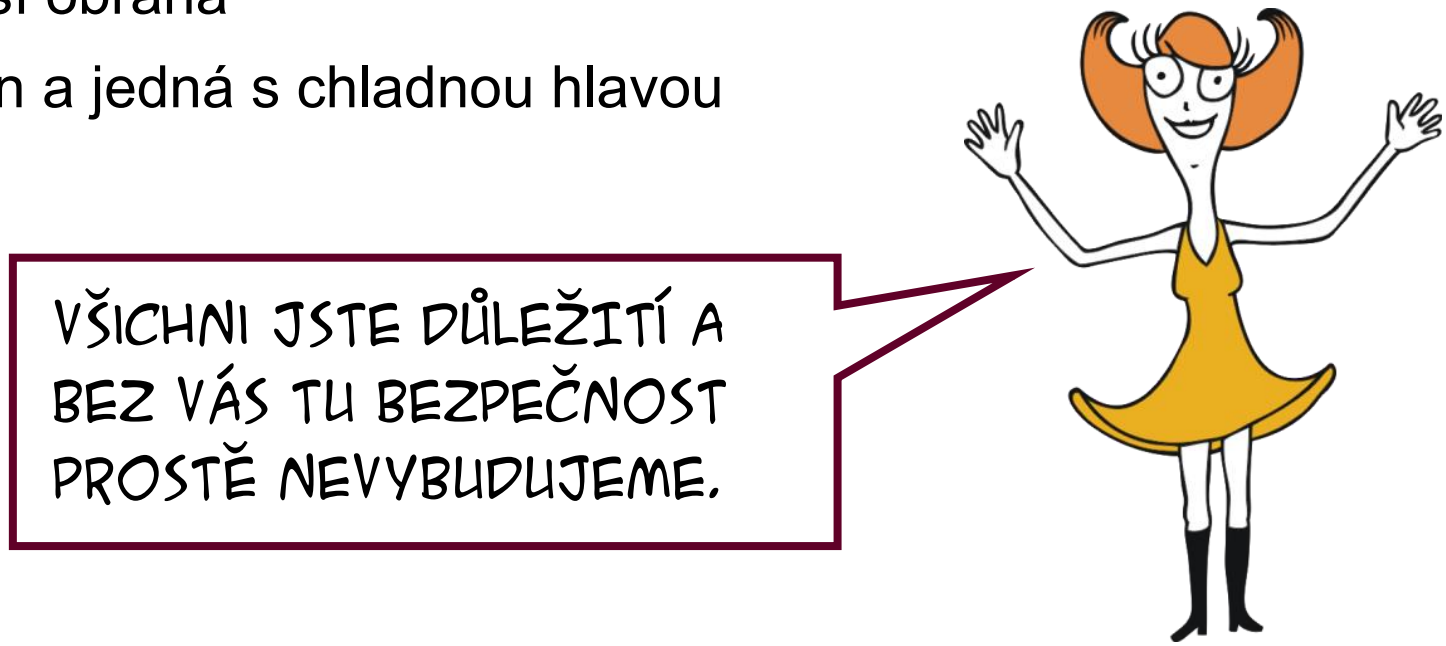
Jak se v tom vyznat?

Není to jednoduché

- Obecné pravidlo neexistuje
  - Víc informací, znalostí = výhoda
- Dobře připravený a cílený podvod
  - Problém pro každého
- Běžné podvody
  - Zvládne poznat každý
  - Drtivá většina

Jste důležití!

- **Technické prostředky**
  - Na ZČU aplikovány
  - Dokáží reagovat na nové hrozby až se zpožděním
- **Uživatel sítě WEBnet**
  - Nejúčinnější obrana
  - Je-li poučen a jedná s chladnou hlavou



Odhalte podvod v pěti krocích

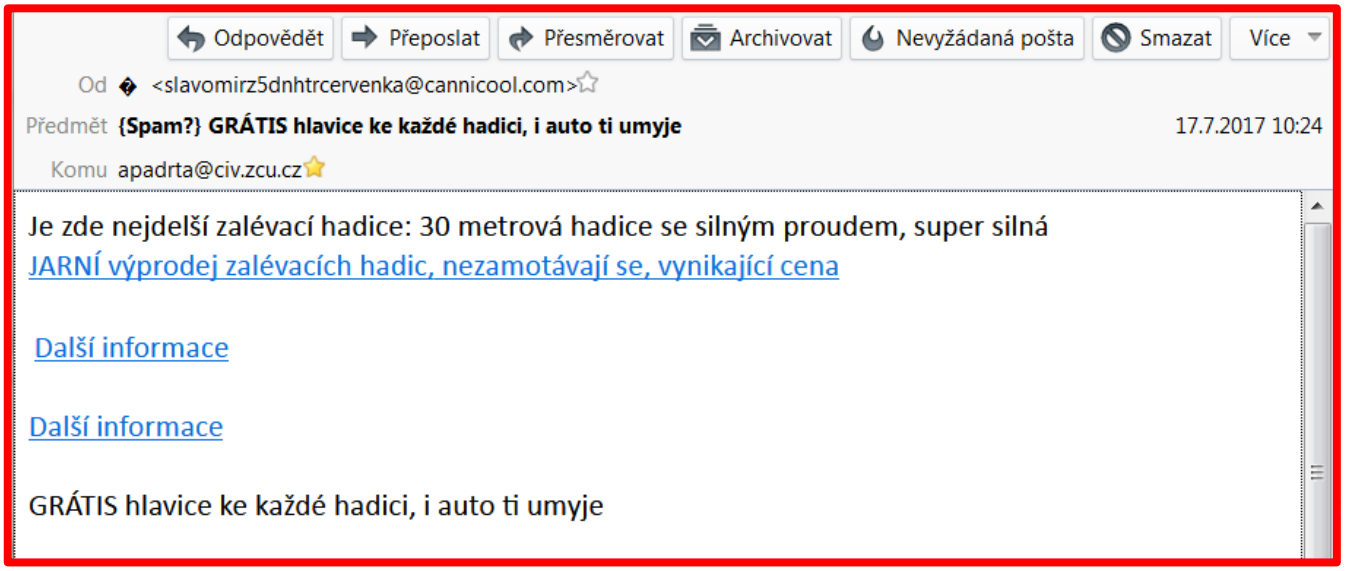
1. krok

- **Očividný spam**
  - Nevyžádané reklamní sdělení
  - např. odpuzovač myší a potkanů 1+1 zdarma, super hadice, …

Předmět: {Spam?} Odpuzovač myší + potkanů v akcii 1 + 1, účinný i proti hmyzu
Od: "Otokar Zapletal" <otokarzg1w5pazapletal@henrygl.com>
Date: Mon, 24 Apr 2017 16:51:04 +0000

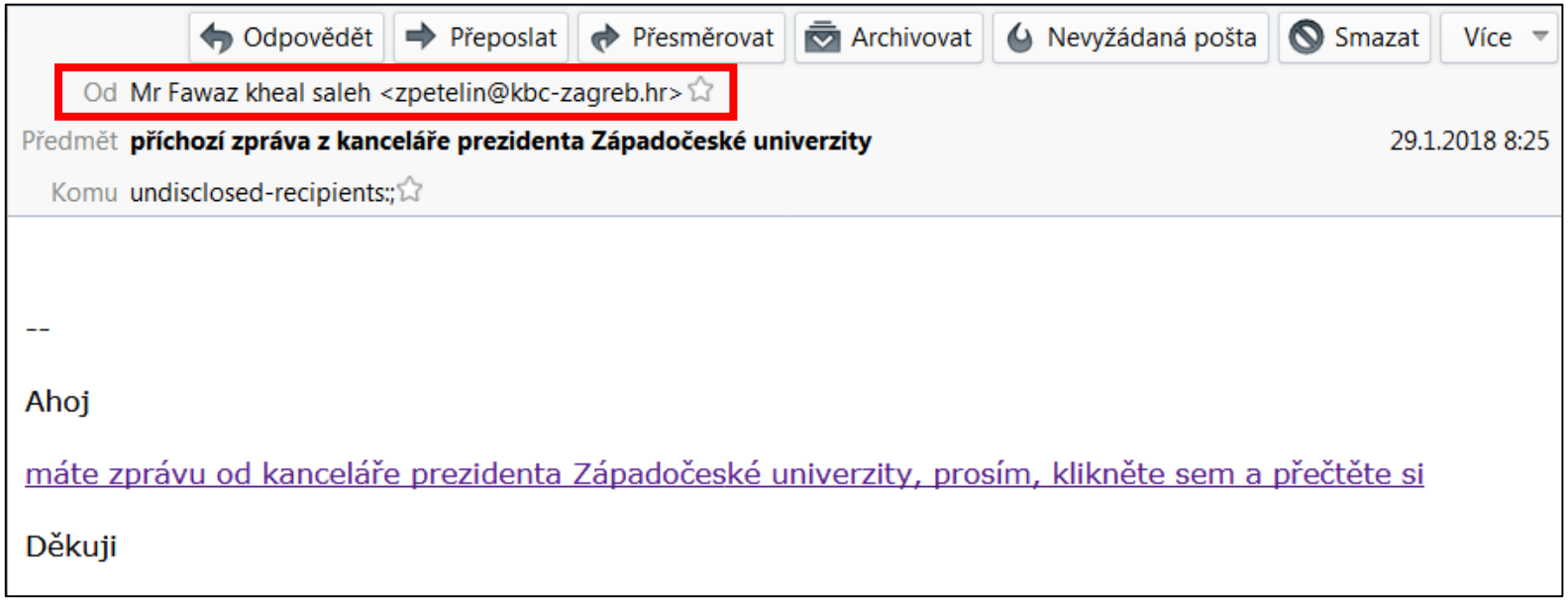
Odpuzovač myší + potkanů v akcii 1 + 1, účinný i proti hmyzu

Odpuzovač myší v senzační nabídce: jako bonus dostaneš ještě jeden »



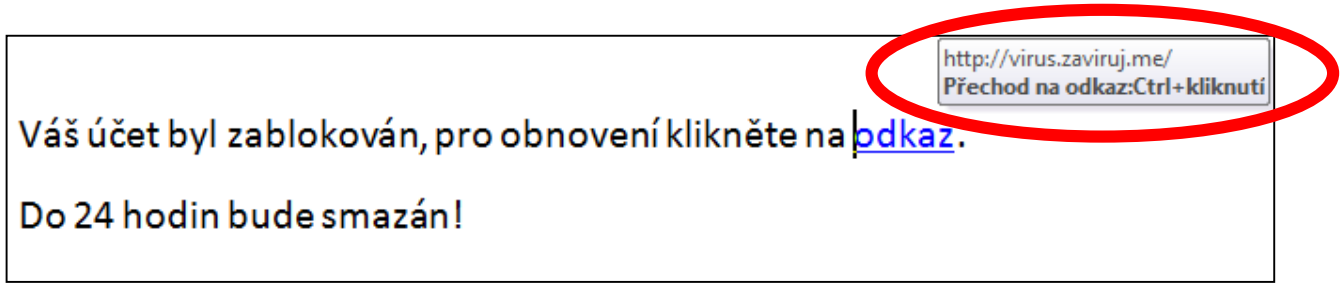
2. krok

- **Podezřelého odesílatele**
  - Znám odesílatele? Nebo aspoň doménu?
  - Jméno (popisek) před adresou vs. e-mailová adresa
  - Odesílatele lze podvrhnout – jistotou je elektronický podpis
  - Odlišnost může být i pouze v jednom písmenu!
  - Při podezření podvrhu ověřit jiným kanálem (např. telefonicky)



3. krok

- **Podezřelý obsah**
  - Neočekávaný druh zprávy
    - Nabídky na seznámení, životopis, fakturu, …
  - Obsah není charakteristický pro odesílatele
    - Uklízečka upozorňuje na novou směrnici o publikacích do RIV
  - Neodpovídající jazyk
    - Česká banka píše anglicky
    - Pan herrmann.muller@web.de píše česky
  - Neodpovídající úroveň jazyka
    - Hovorový jazyk v „oficiální zprávě“ apod.
  - Obsahuje odkazy na pochybné stránky



4. krok

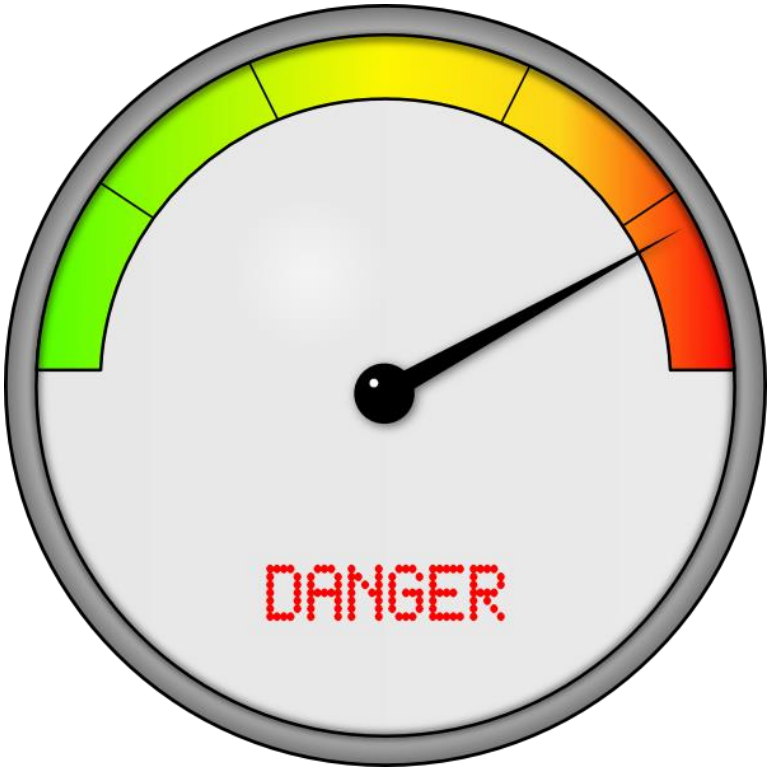
- **Přítomnost psychologického nátlaku**
  - Zaklínání se autoritou
    - My můžeme (odebrat, zablokovat, pokutovat, …)
  - Hrozba ztráty (příležitosti)
    - Přijdete o …
    - Nedostanete …
  - Časová tíseň
    - Teď, hned, spěchejte
    - Kupujte, nebudou!

5. krok

- **Podezřelé přílohy**
  - Proč zrovna příloha?
    - Cíl útočníka: spustit kód (aplikaci)
    - Způsob spuštění: uživatel
  - Sociální inženýrství
    - Pretexting (v textu se píše o faktuře ⇨ musí to být faktura)
  - Výzva k povolení „spuštění“
    - Makra v kancelářských aplikacích (MS Office, Libre Office)
    - Javascript / přístup na web v PDF souborech
  - Přípona souboru = dobré vodítko
    - Ve výchozím stavu … skryty ☹
    - Podezřelé: .zip, .rar, .exe, .js, .bat, .wsf atd.

Vyhodnocení doručené zprávy

Určitě je v pořádku

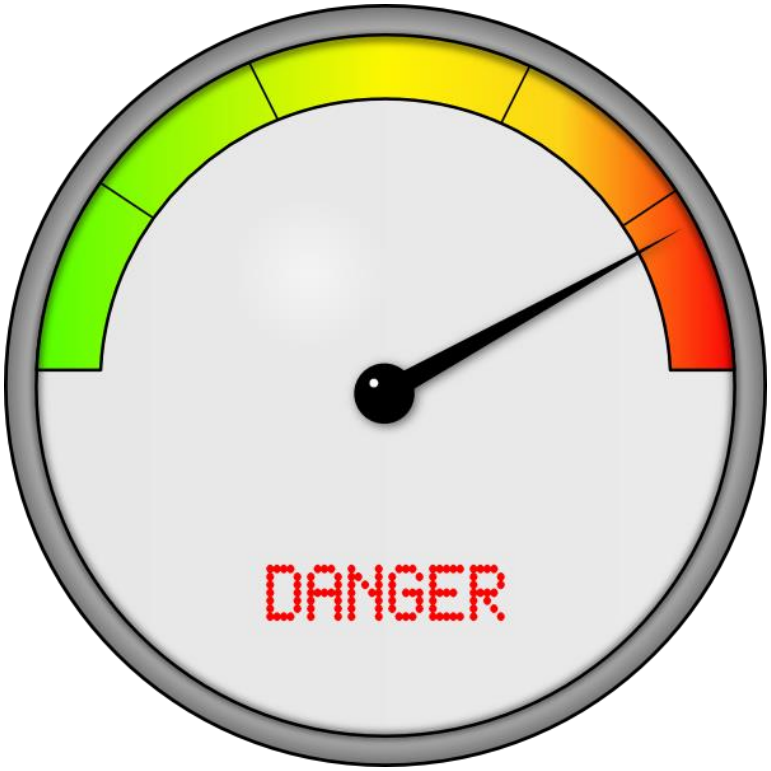


Určitě je to podvod

Vyhodnocení doručené zprávy

Určitě … NEVÍM

Určitě je v pořádku



Určitě je to podvod

Kdo mi pomůže rozhodnout?

- Dilema
  - Možná jde podvod ⇨ chci ignorovat
  - Možná je to pracovní povinnost ⇨ chci otevřít
- Možné řešení
  - Poraďte se s pracovníky CIV
  - Přepošlete operator@service.zcu.cz
  - Zjistíte, co si myslíme my

Mám jistotu, že to je podvodný e-mail, co dál?

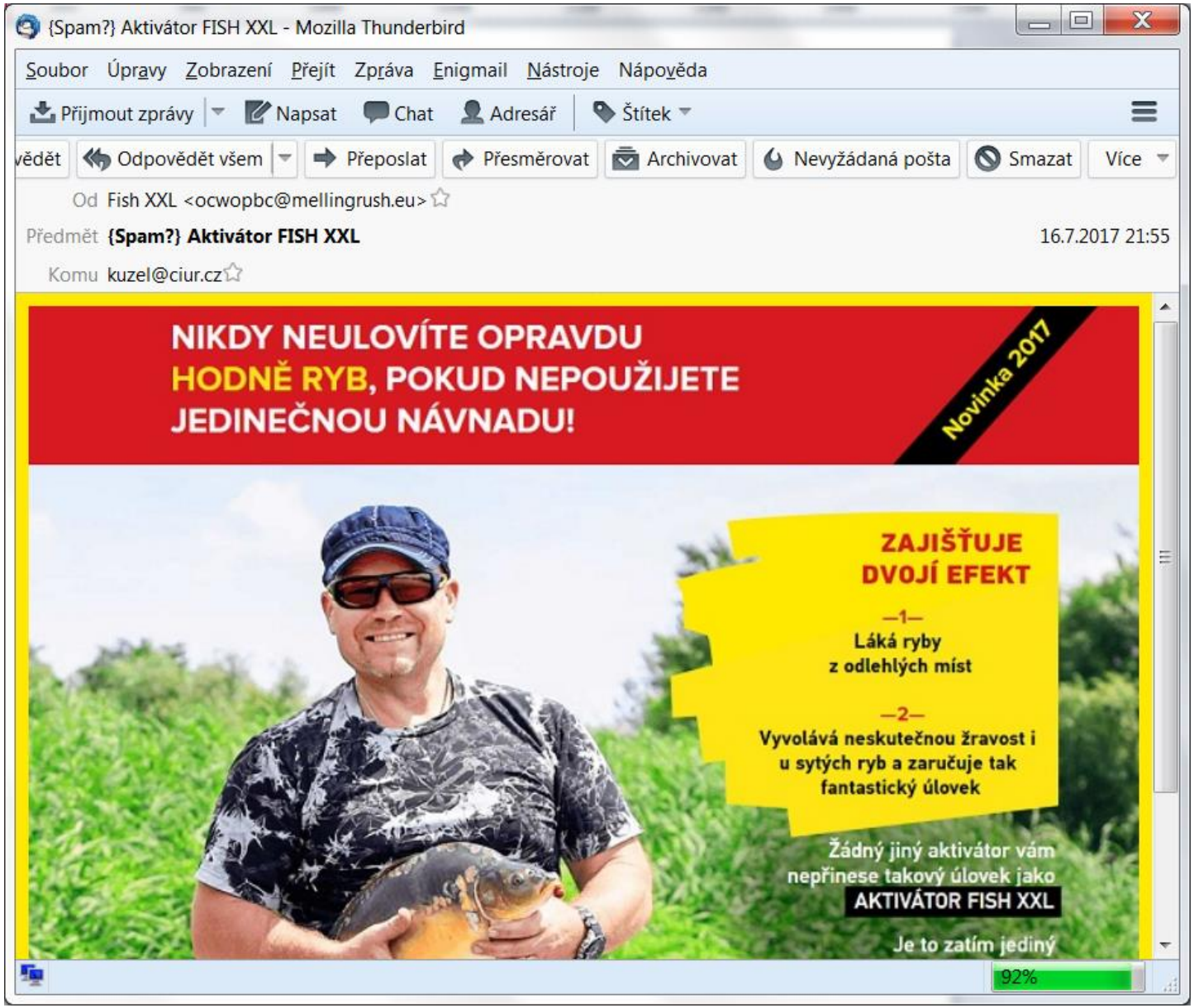
- „Novinky“ na stránce uživatelské podpory
  - http://support.zcu.cz/
- Je tam popsán „můj podvodný e-mail“?
  - Není ⇨ nahlásím (přepošlu) zprávu na operator@service.zcu.cz
  - Je ⇨ můžu také poslat (statistika – vyhodnocení počtu)
- Rozhodně se neřídím instrukcemi v e-mailu
  - Neklikám na odkazy
  - Neotvírám přílohy
  - Neodpovídám
  - Neposílám údaje

Co už víte?

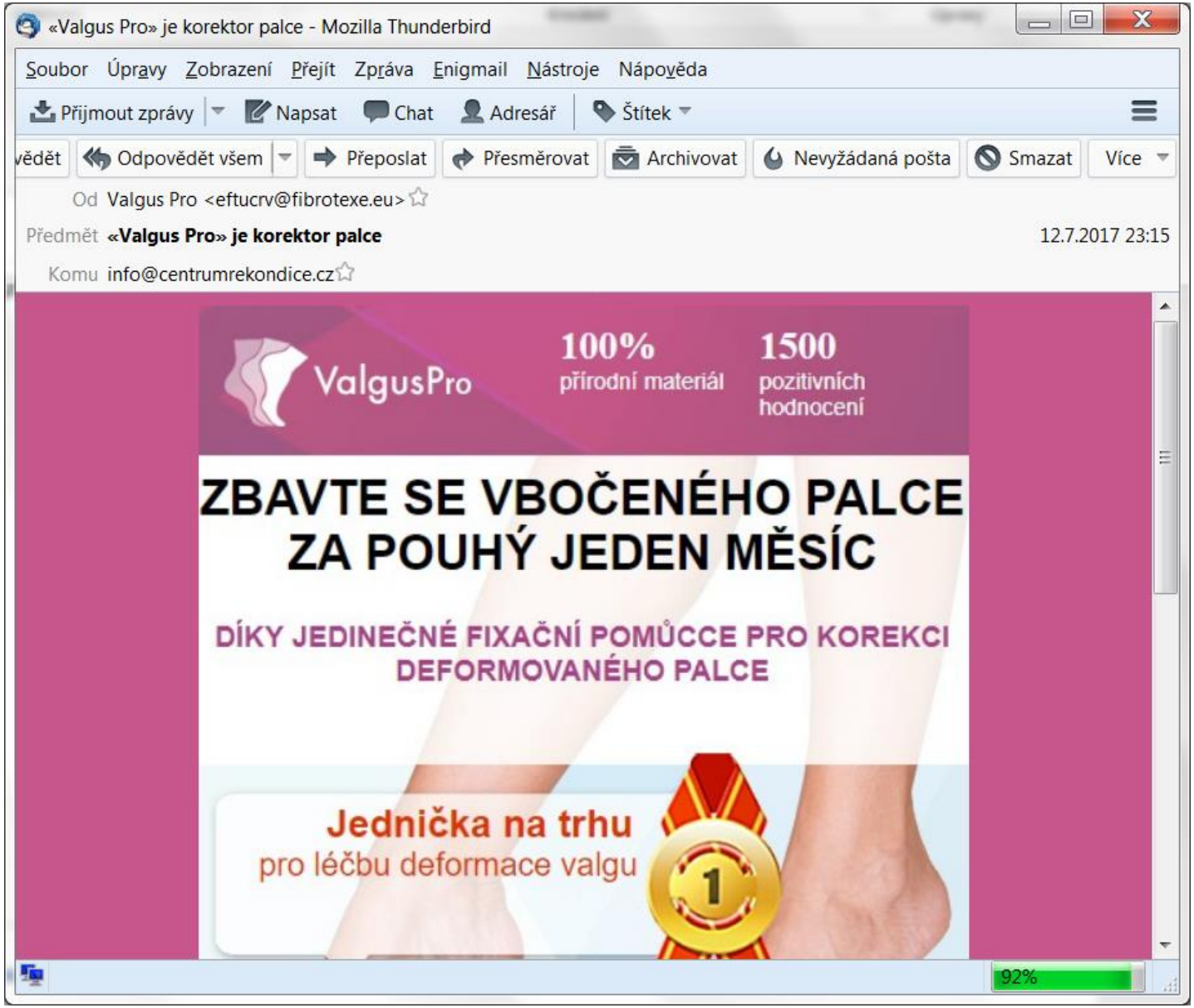
- Co hrozí po úspěšném útoku
- Co je phishing, jeho typy a znaky
- Co byste měli poznat sami
- Jak se správně zachovat
- Kdo vám pomůže, když si nevíte rady

Ukázky z praxe

E-mail č. 1 – Očividný spam



E-mail č. 2 – Očividný spam



E-mail č. 3 – Podezřelý odesilatel

Od Jessica Jones <ucqidty@svensinc.biz.ua>

Přijmout zprávy | Napsat | Chat | Adresář | Štítek

vědět | Odpovědět všem | Přeposlat | Přesměrovat | Archivovat | Nevyžádaná pošta | Smazat | Více

Od Jessica Jones <ucqidty@svensinc.biz.ua>

Předmět **{Spam?} Hi, this is Jessica Jones** 22.11.2017 2:38

Komu ales.horky@century21.cz

Hi, this is Jessica!

Katy sent me your contacts, as I really liked during our meeting 2 months ago. I can't forget our meeting with you, and I want to be friends with you.
To make it easier for me to remember - here are my photos.

My profile in Facebook >>>

Best regards,
Jessica Jones

92%

E-mail č. 4 – Podezřelý odesilatel

Od Lonely Danulenka <bluster150@zeus.eonet.ne.jp>

Přijmout zprávy | Napsat | Chat | Adresář | Štítek

Odpovědět | Odpovědět všem | Přeposlat | Přesměrovat | Archivovat | Nevyžádaná pošta | Smazat | Více

Od Lonely Danulenka <bluster150@zeus.eonet.ne.jp>

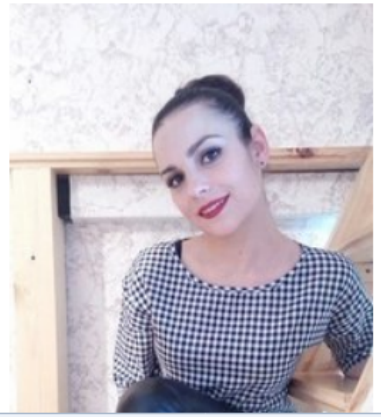
Předmět **Dobry den! Jak je vas den? Jmenuji se Dana.** 2.1.2018 10:06

Odpověď Lonely Danulenka <dan.paradies964@gmail.com>

Komu krakonos@nomi.cz

Dobre odpoledne! Jak se citite? Me jmeno je velmi krasna - Dana, ze jsem v krasnem veku - Mam 30 let. Nejsem vdana, nemam deti. Mym snem je najit osobu, se kterymi se budeme navzajem rozumime a vymenovat si nazory. Chci najit silny, odvazny, zodpovedny clovek, se kterym by to byt bezpecne.. Nechci hrat zadne hry, jsem hledal nekoho, kdo me bude milovat a nikdy nebude podvadet. Budu cekat na vasi odpoveď prostrednictvim e-mailu. To nejlepsi nas teprve ceka. S pranim vseho nejlepsiho, Danuska,

CAM-778.jpg



1 příloha: CAM-778.jpg 19,8 KB Uložit

Hotovo 92%

E-mail č. 4 – Podezřelý obsah

Dobry den! Jak je vas den? Jmenuji se Dana. - Mozilla Thunderbird

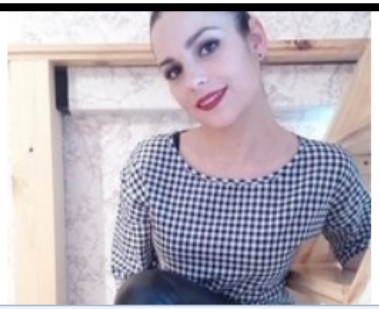
Soubor Úpravy Zobrazení Přejít Zpráva Enigmail Nástroje Nápověda

Přijmout zprávy | Napsat | Chat | Adresář | Štítek

Odpovědět | Odpovědět všem | Přeposlat | Přesměrovat | Archivovat | Nevyžádaná pošta | Smazat | Více

Od Lonely Danulenka <bluster150@zeus.eonet.ne.jp>

Dobre odpoledne! Jak se citite? Me jmeno je velmi krasna - Dana, ze jsem v krasnem veku - Mam 30 let. Nejsem vdana, nemam deti. Mym snem je najit osobu, se kterymi se budeme navzajem rozumime a vymenovat si nazory. Chci najit silny, odvazny, zodpovedny clovek, se kterym by to byt bezpecne.. Nechci hrat zadne hry, jsem hledal nekoho, kdo me bude milovat a nikdy nebude podvadet. Budu cekat na vasi odpoveď prostrednictvim e-mailu. To nejlepsi nas teprve ceka. S pranim vseho nejlepsiho, Danuska,



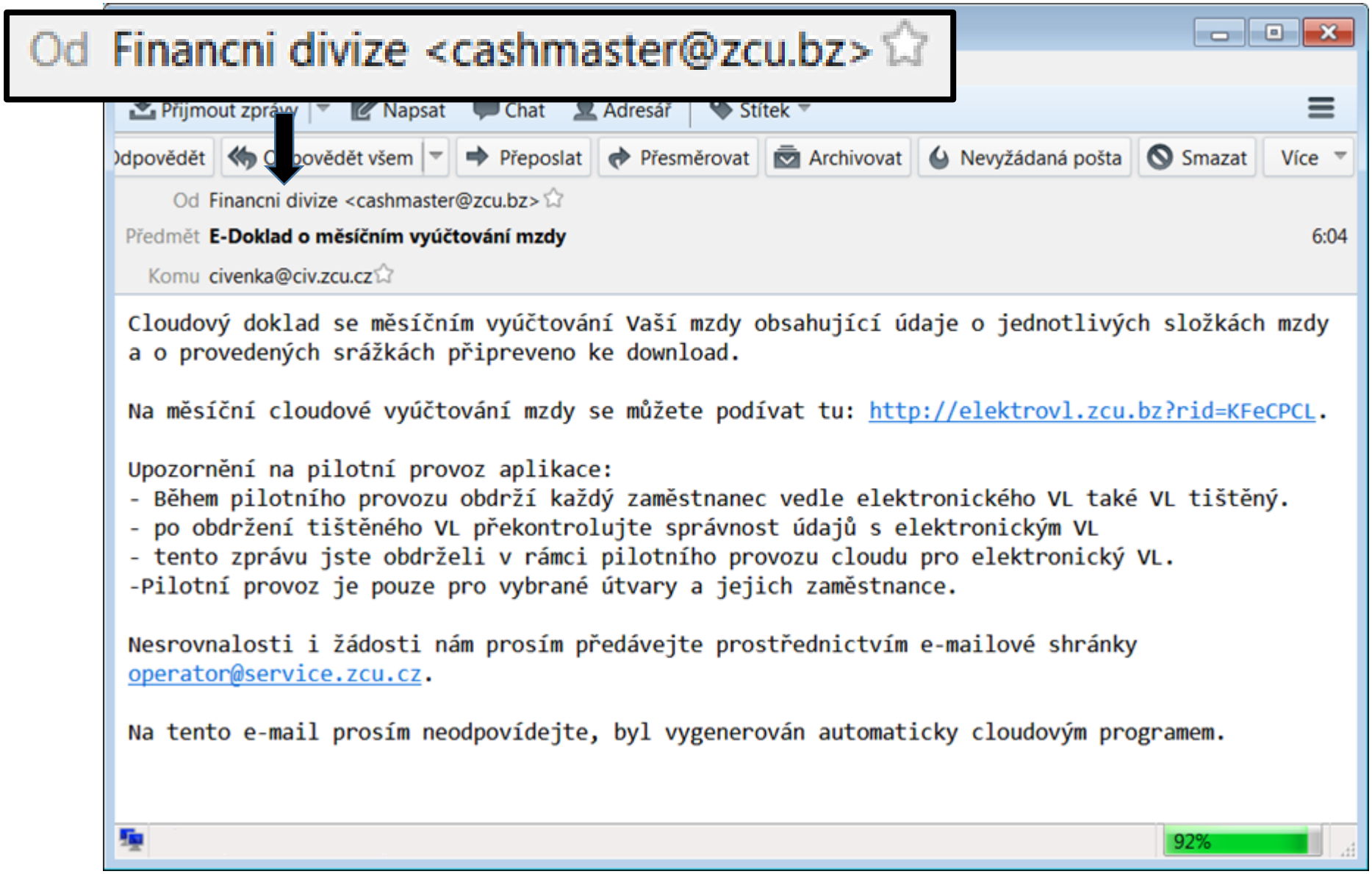
1 příloha: CAM-778.jpg 19,8 KB

Uložit

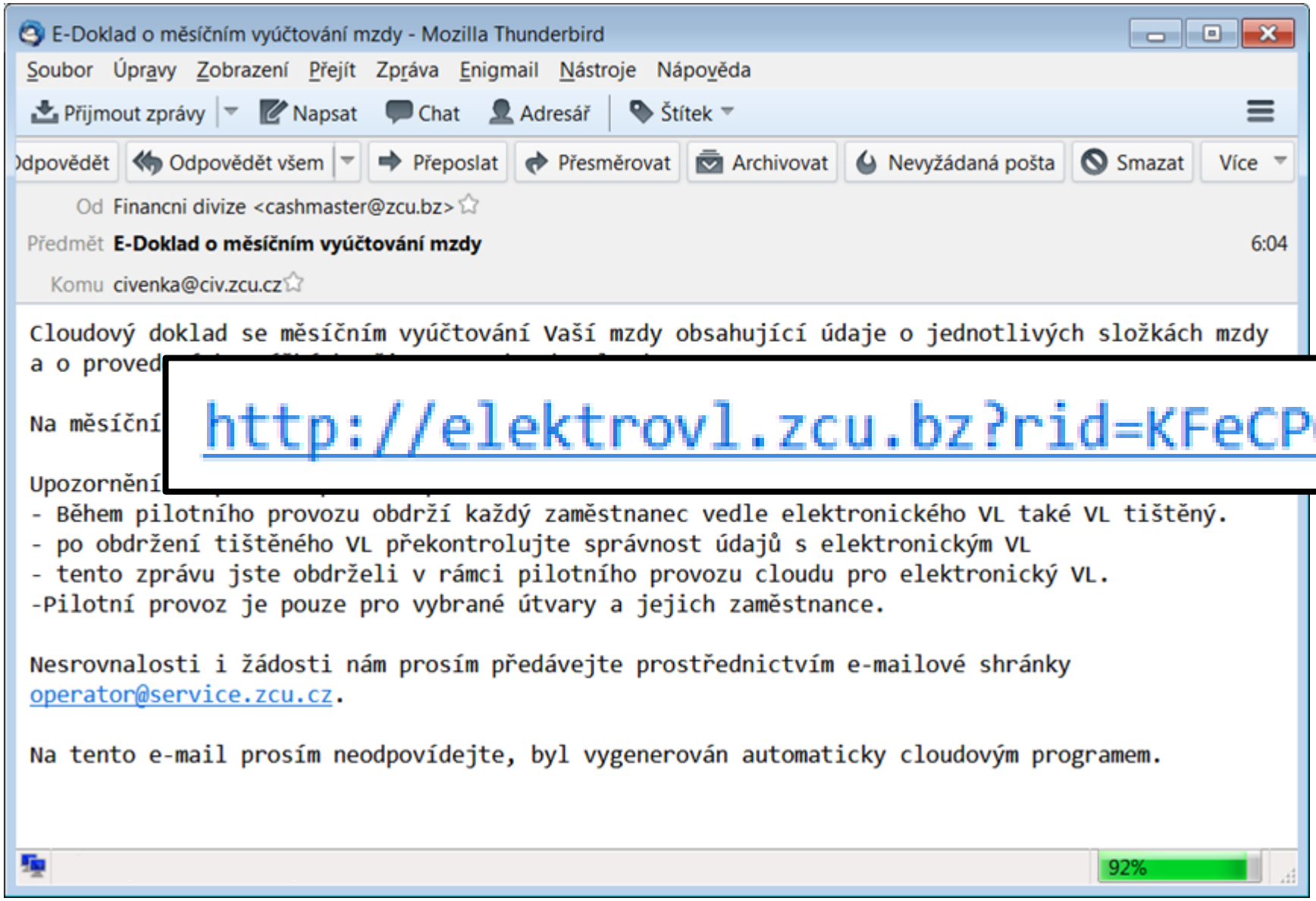
Hotovo

92%

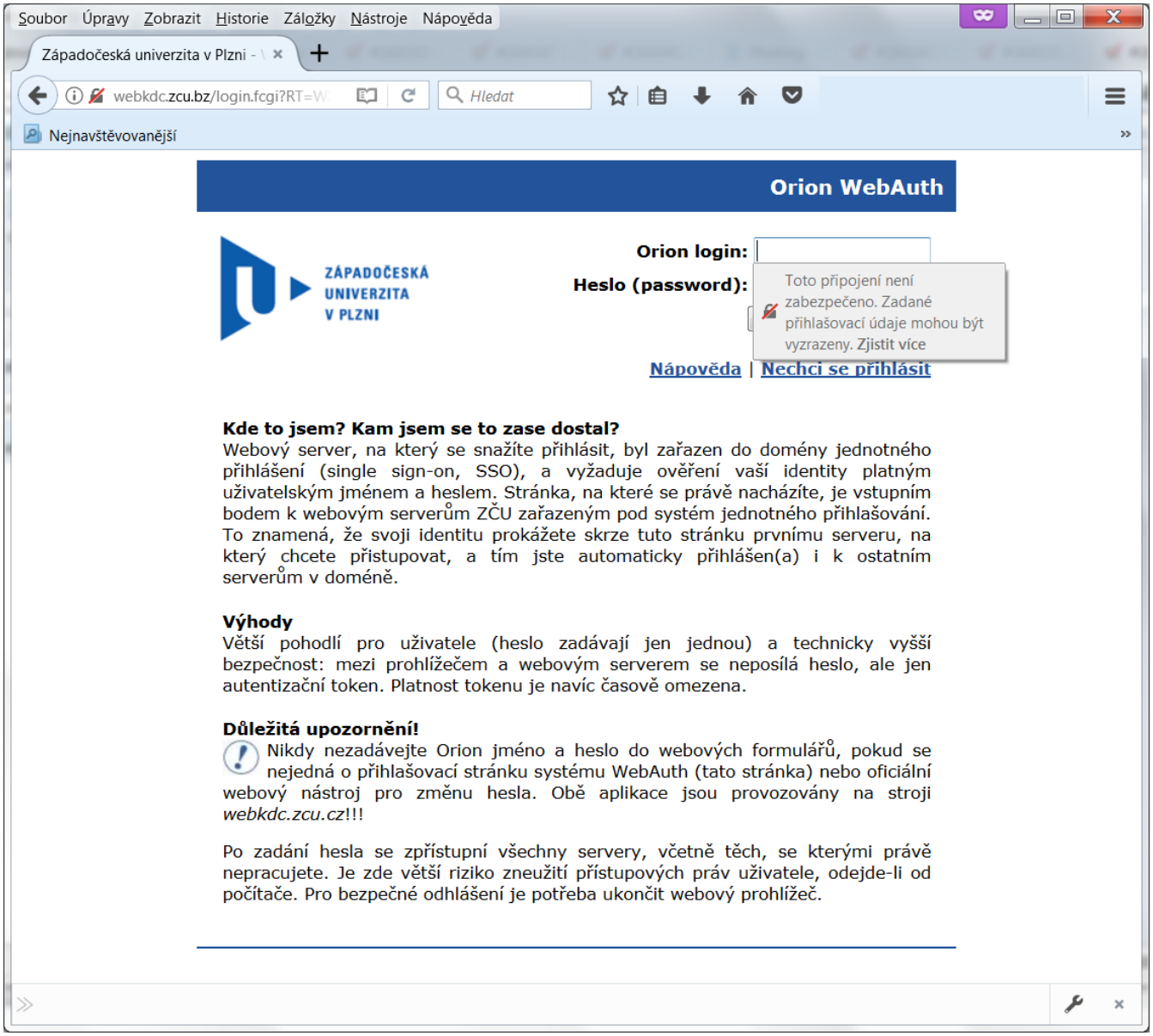
E-mail č. 5 – Podezřelý odesilatel



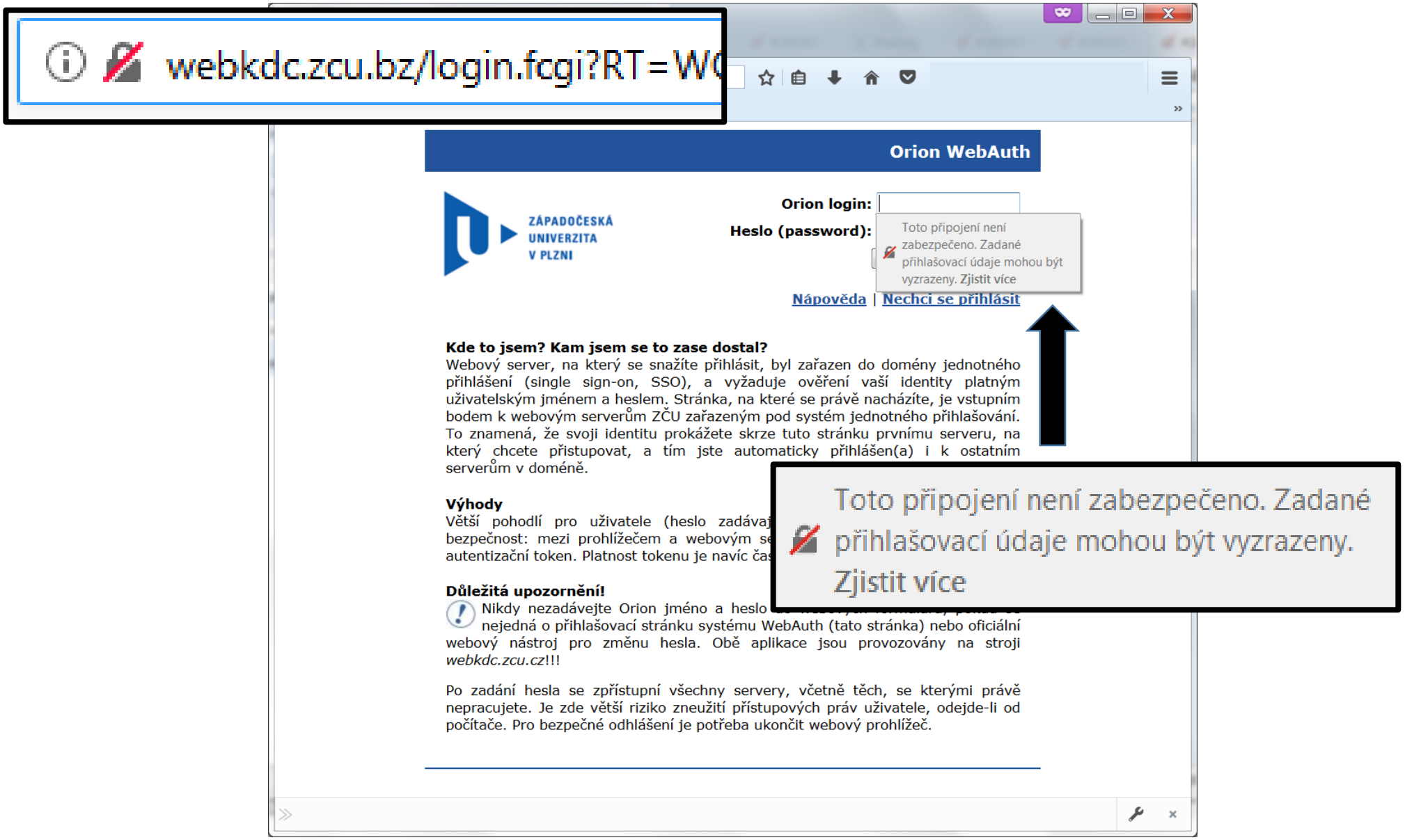
E-mail č. 5 – Podezřelý obsah (odkaz)



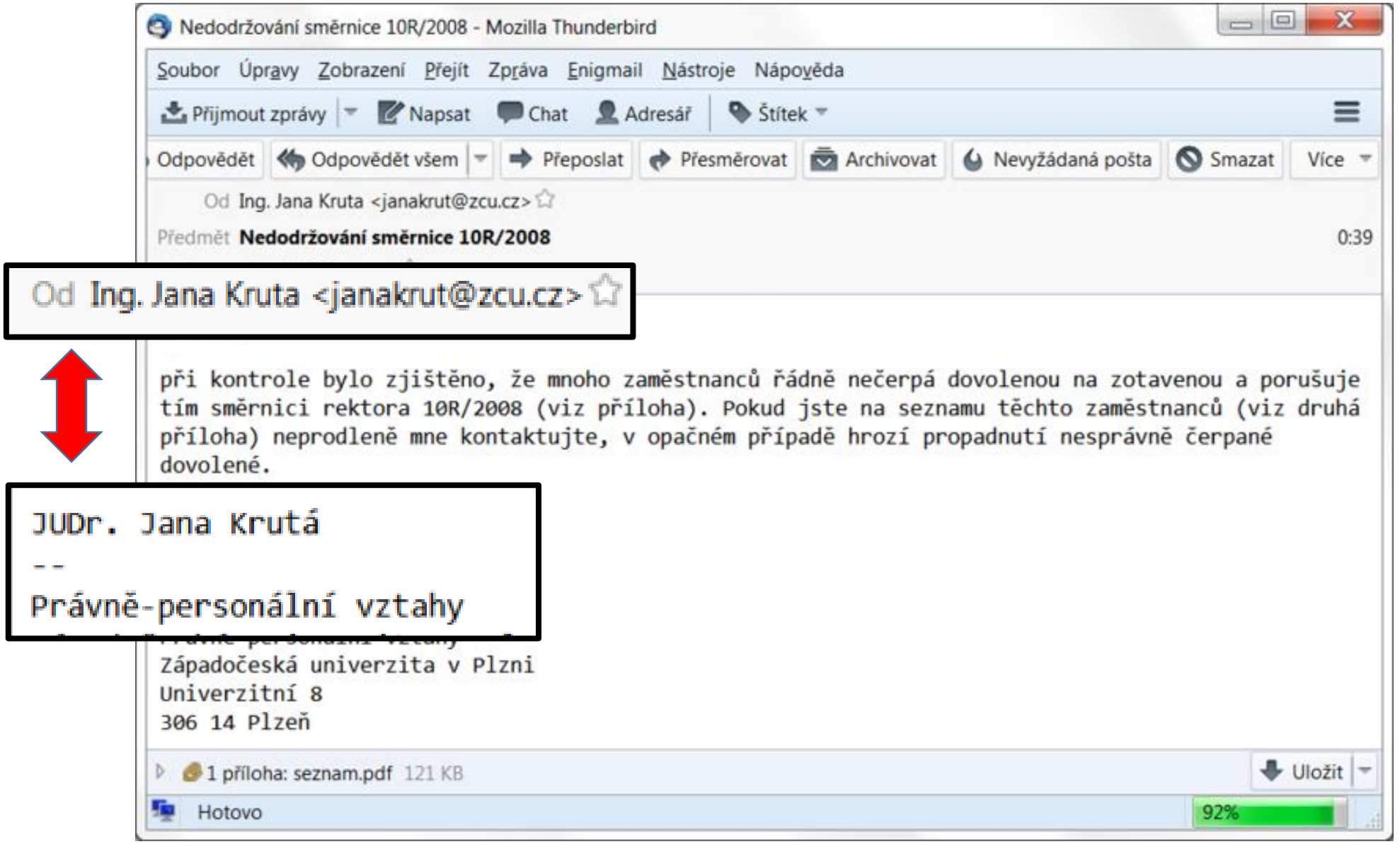
E-mail č. 5 – Odkazovaná stránka



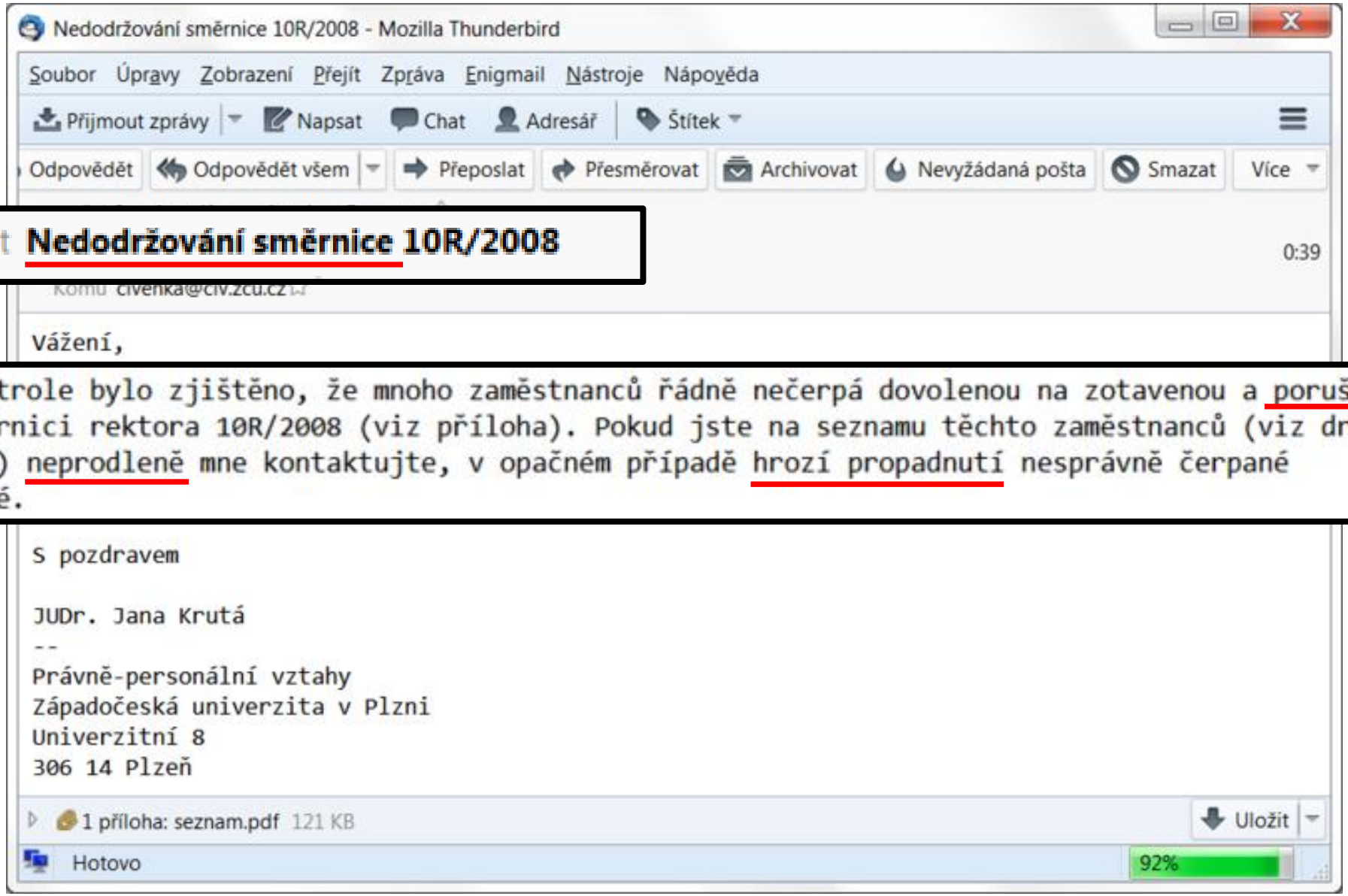
E-mail č. 5 – Odkazovaná stránka



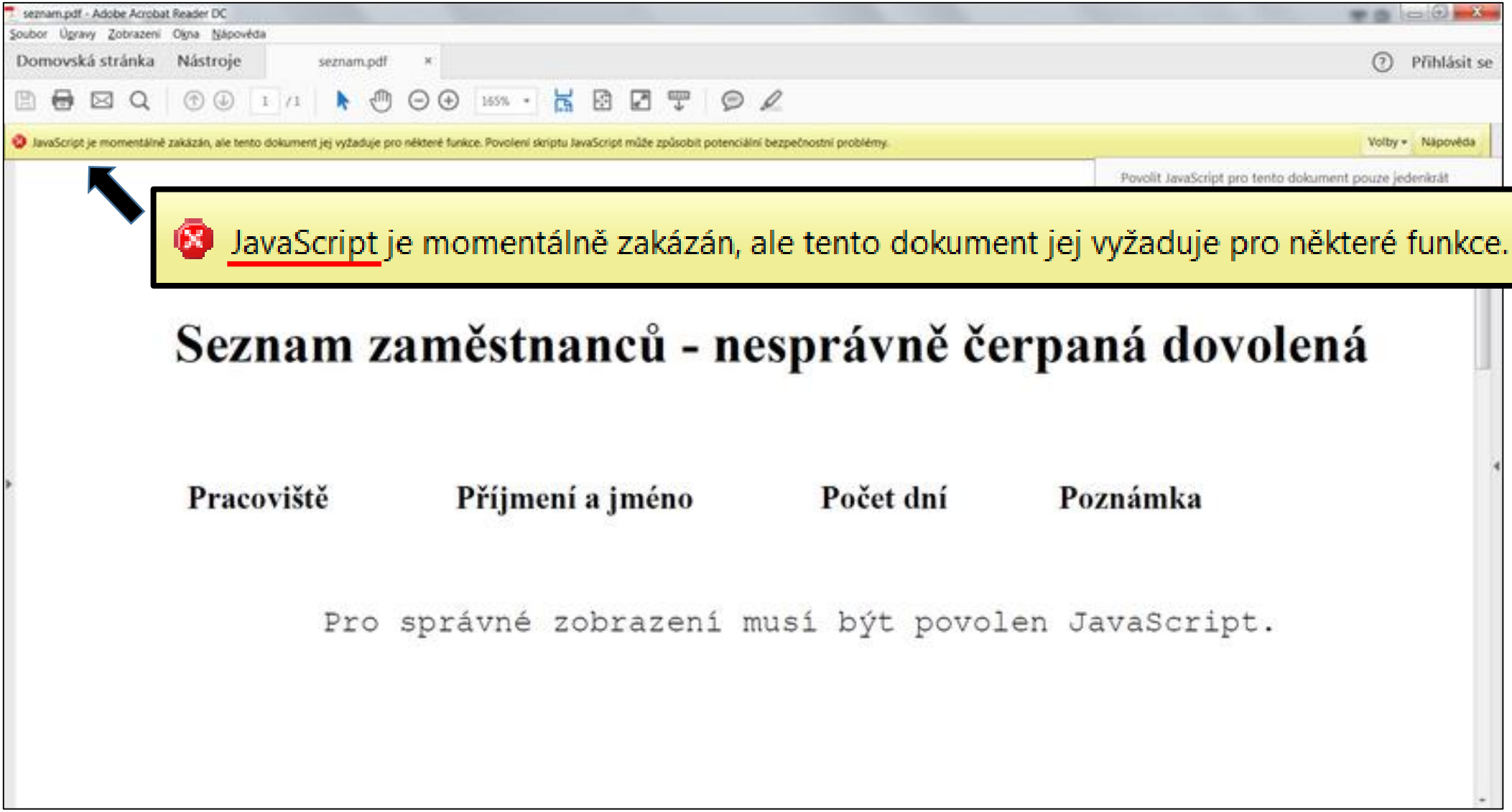
E-mail č. 6 – Podezřelý obsah (trochu)



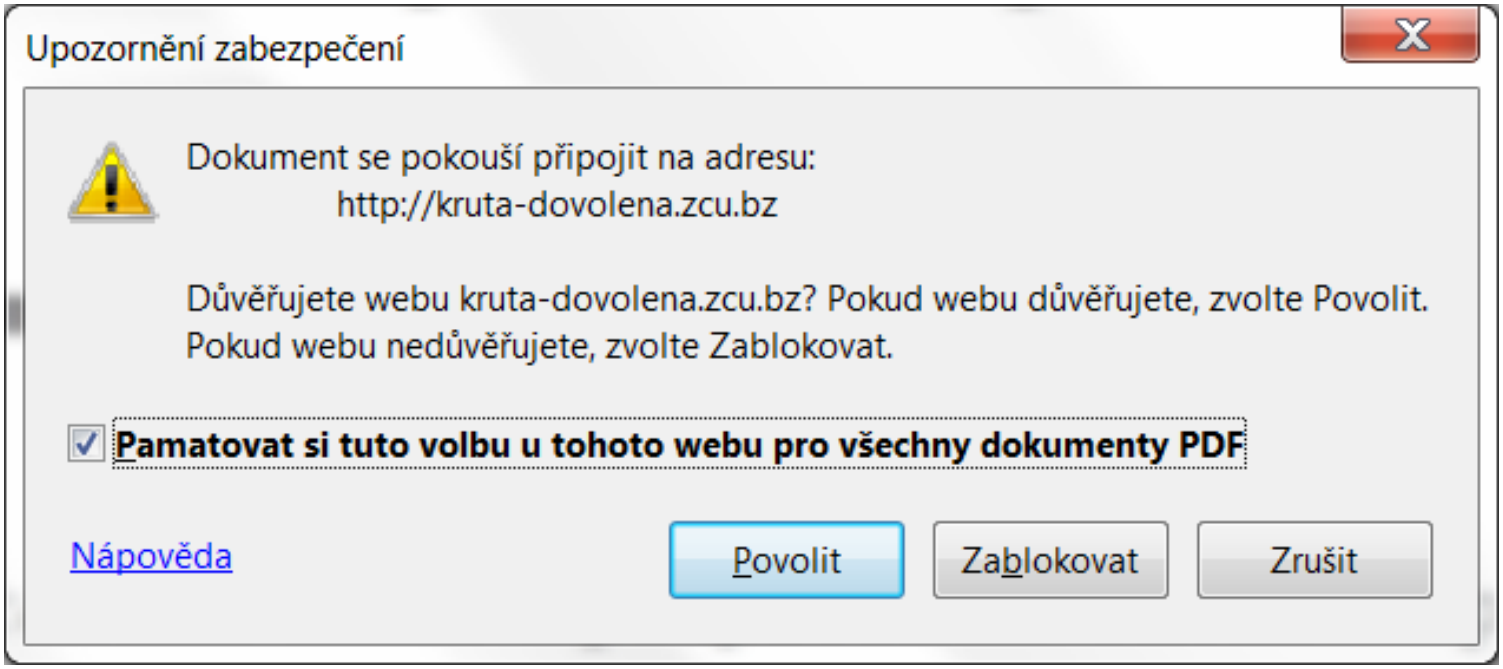
E-mail č. 6 – Psychologický nátlak



E-mail č. 6 – Podezřelá příloha



E-mail č. 6 – Podezřelá příloha



Dokument se pokouší připojit na adresu:
http://kruta-dovolena.zcu.bz

ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

Děkuji za pozornost

Prostor pro diskusi

Aleš Padrta, Jiří Čepák

apadrta@civ.zcu.cz, cepakj@civ.zcu.cz