

# IT bezpečnost Phishing



Školení pro uživatele sítě WEBnet

# 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
  - ▶ ...

TO JE SMŮLA  
JAKOU BYCH  
TEDA NIKOMU  
NEPŘÁL ...



# 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

VÁŠ E-MAIL BYL ZABLOKOVÁN!  
VY KLIKNĚTE [ZDE](#) A OBNOVIT.  
JINAK BUDE ÚČET SMAZÁN DO  
32 MINUT!

HELPDESK CIV



# 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 vaši
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

From: **PayPal** <[nobody@neoweb-01.neotericuk.co.uk](mailto:nobody@neoweb-01.neotericuk.co.uk)>

Date: 2018-02-19 14:52 GMT+01:00

Subject: Your account will be closed !

To: [REDACTED]@seznam.cz

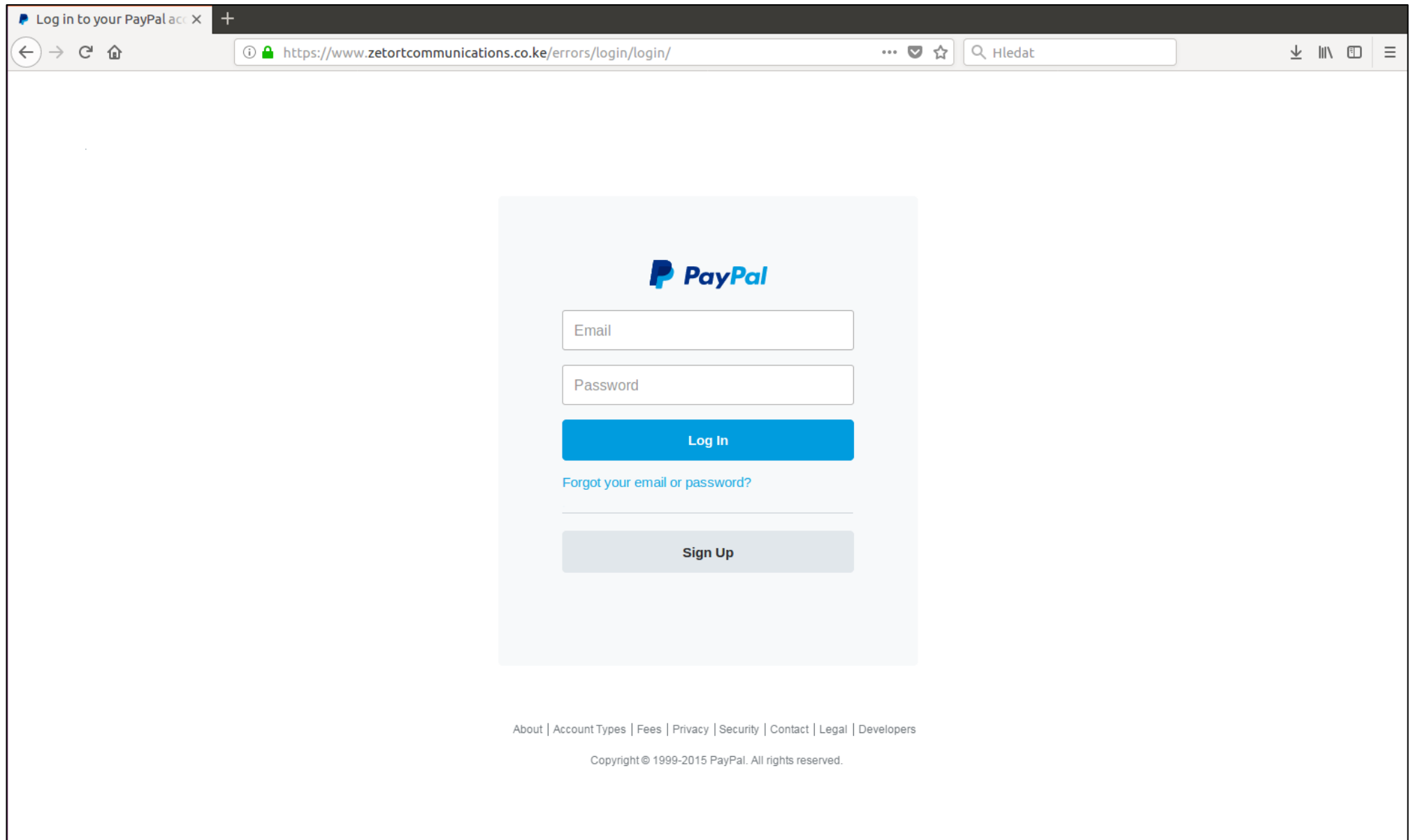
**PayPal**

Dear Customer,

**We are sorry to inform you that you can not access all your account advantages due to account limitation. You must confirm your correct data to activate your account again due to our new security update. Thanks**

[Reslove My Account](#)

# Typy phishingu: E-mail s odkazem na stránku

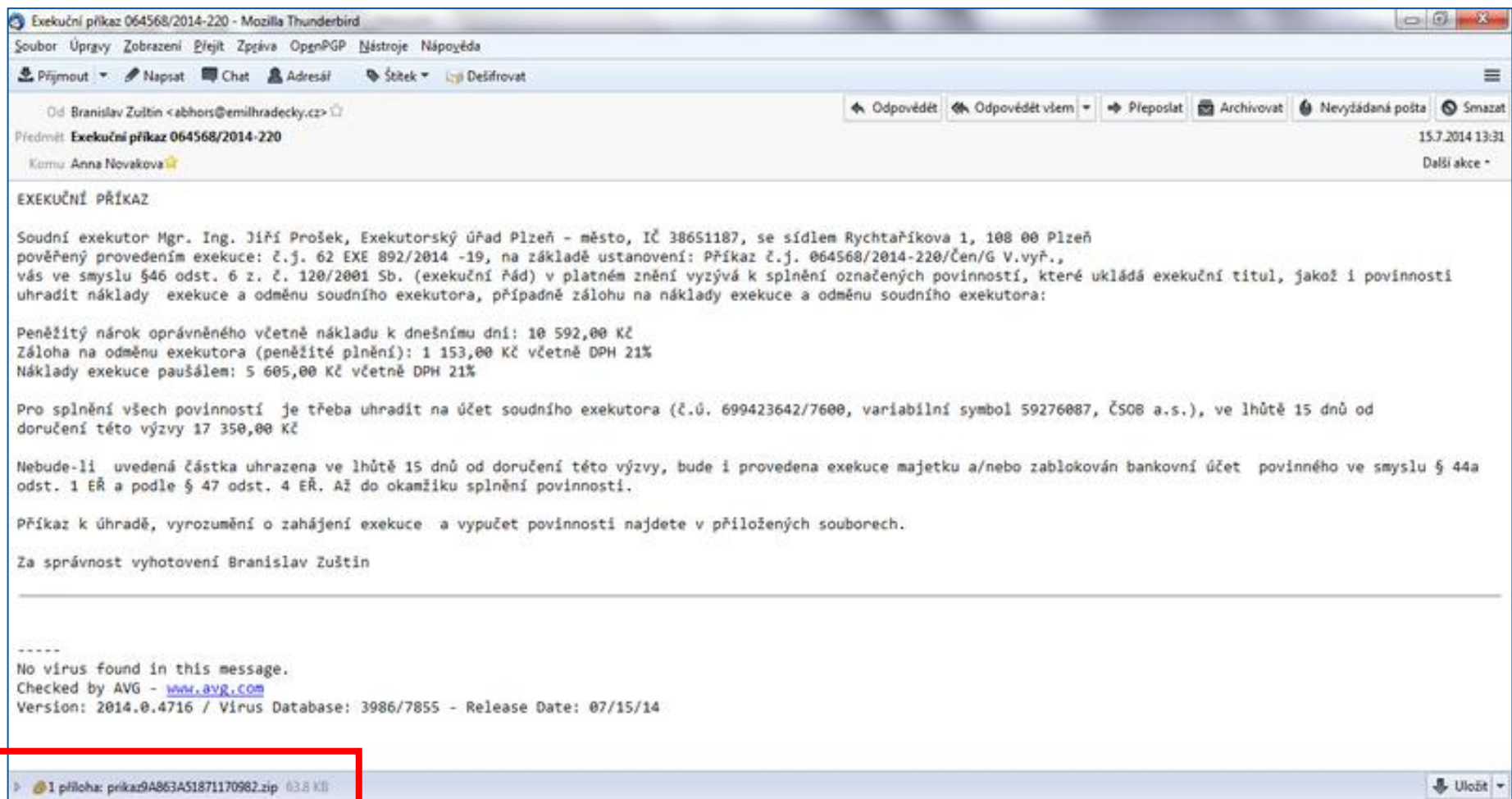


# Typy phishingu: E-mail s odkazem na stránku

The screenshot shows a web browser window with a single tab titled "Log in to your PayPal acc X". The address bar contains the URL <https://www.zetortcommunications.co.ke/errors/login/login/>. A black box highlights this URL, and a black arrow points upwards from the box towards the browser's navigation buttons. The page content features the PayPal logo at the top, followed by input fields for "Email" and "Password", a blue "Log In" button, a link for "Forgot your email or password?", and a grey "Sign Up" button. At the bottom of the page, there is a footer with links for "About", "Account Types", "Fees", "Privacy", "Security", "Contact", "Legal", and "Developers", along with a copyright notice: "Copyright © 1999-2015 PayPal. All rights reserved."

# Typy phishingu: Závadná příloha

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



# Odkazy (nejen) v e-mailech

# 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

# 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

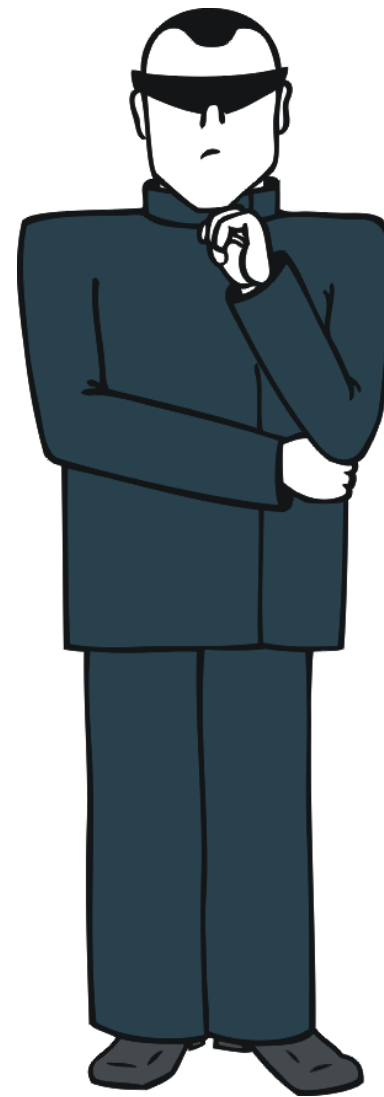


komiks.civ.zcu.bz





# Malý kvíz



<http://xafylopaxwzwhcxwla.com>

<http://xafylopaxwzwhcxwla.com>

ADWARE



<https://www.lanfairpwllgwyngyllgogerychwyrndrobwlllantysiliogogoch.co.uk/>

<https://www.llanfairpwllgwyngyllgogerychwyrndrobwlllantysiliogogogoch.co.uk/>



WEBOVÉ STRÁNKY OBCE VE  
WALESU, KTERÁ DRŽÍ SVĚTOVÝ  
REKORD V DÉLCE NÁZVU.

<http://apple.com/iphone7>



<http://apple.com/iphone7>



OFICIÁLNÍ STRÁNKY VÝROBCE  
ELEKTRONICKÝCH ZAŘÍZENÍ  
ZNAČKY APPLE.

<http://apple.com-iphone7.com>

<http://apple.com-iphone7.com>

MALWARE



<http://goo.gl/Qaloqr>

<http://goo.gl/Qaloqr>



ZKRÁCENÝ ODKAZ NA  
[HTTP://SUPPORT.ZCU.CZ](http://support.zcu.cz)

# Jak se v tom vyznat?

# Není to jednoduché

TO MI, TEDY ŘEKNĚTE,  
CO MÁM DĚLAT ...

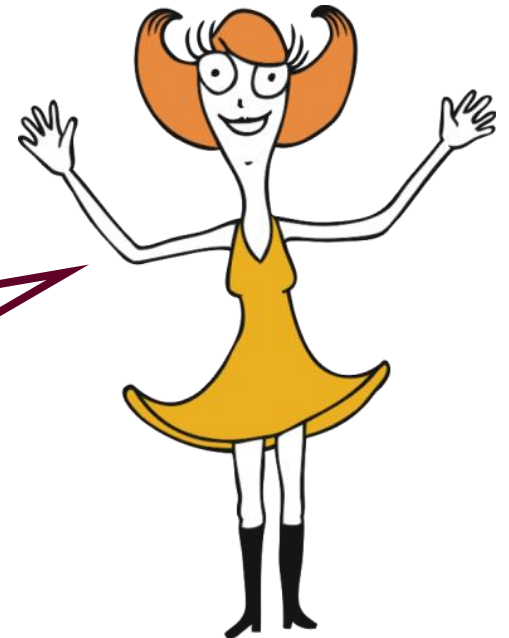


- ▶ Obecné pravidlo neexistuje
  - ▶ Víc informací, znalostí = výhoda
- ▶ Dobře připravený a cílený podvod
  - ▶ Problém pro každého
- ▶ Běžné podvody
  - ▶ Zvládne poznat každý
  - ▶ Drtivá většina

# 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

VŠICHNI JSTE DŮLEŽITÍ A  
BEZ VÁS TU BEZPEČNOST  
PROSTĚ NEVYBUDUJEME.





# 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 akci 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 akci 1 + 1, účinný i proti hmyzu

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

Odpovědět Přeposlat Přesměrovat Archivovat Nevyžádaná pošta Smazat Více

Od <slavomirz5dnhtrcervenka@cannicool.com>☆

Předmět (Spam?) GRÁTIS hlavice ke každé hadici, i auto ti umyje

17.7.2017 10:24

Komu apadrta@civ.zcu.cz★

Je zde nejdelší zalévací hadice: 30 metrová hadice se silným proudem, super silná  
[JARNÍ výprodej zalévacích hadic, nezamotávají se, vynikající cena](#)

[Další informace](#)

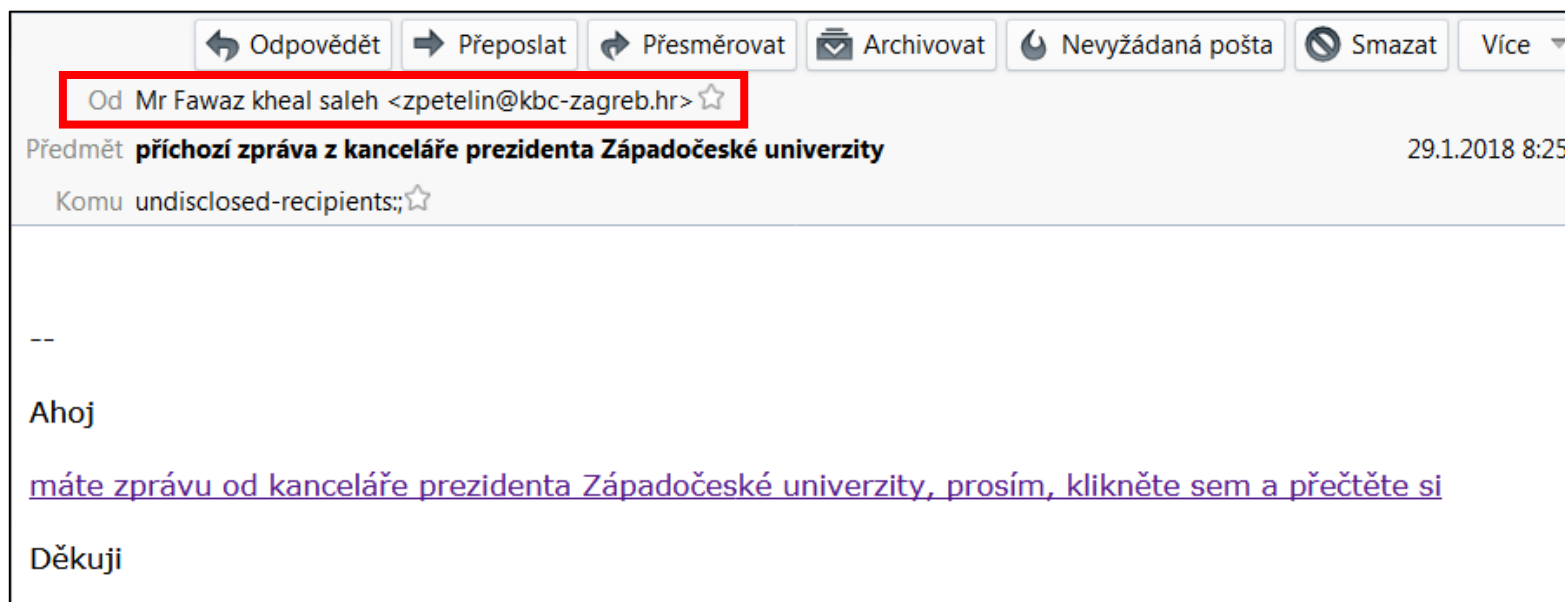
[Další informace](#)

GRÁTIS hlavice ke každé hadici, i auto ti umyje

## 2. krok

### ▶ Podezřelého odesílatele

- ▶ Znáám 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 čerpání dovolené
- ▶ Neodpovídající jazyk
  - ▶ Česká banka píše anglicky
  - ▶ Pán s emailovou adresou [herrmann.muller@web.de](mailto:herrmann.muller@web.de) píše česky
- ▶ Neodpovídající úroveň jazyka
  - ▶ Hovorový jazyk v „oficiální zprávě“ apod.
- ▶ Obsahuje odkazy na pochybné stránky

Váš účet byl zablokován, pro obnovení klikněte na [odkaz](#).

Do 24 hodin bude smazán!

<http://virus.zaviruj.me/>  
Přechod na odkaz:Ctrl+kliknutí

## 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

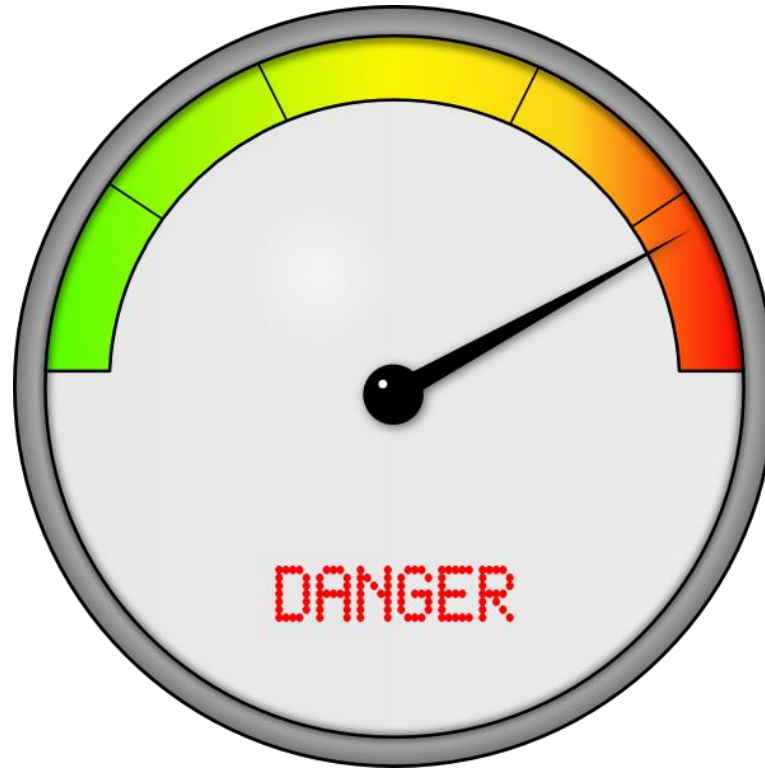
### ▶ Přípona souboru = dobré vodítko

▶ Ve výchozím stavu ... skryty ☹

▶ Podezřelé: .zip, .rar, .exe, .js, .bat, .wsf atd.

# Vyhodnocení doručené zprávy

Určitě je v pořádku

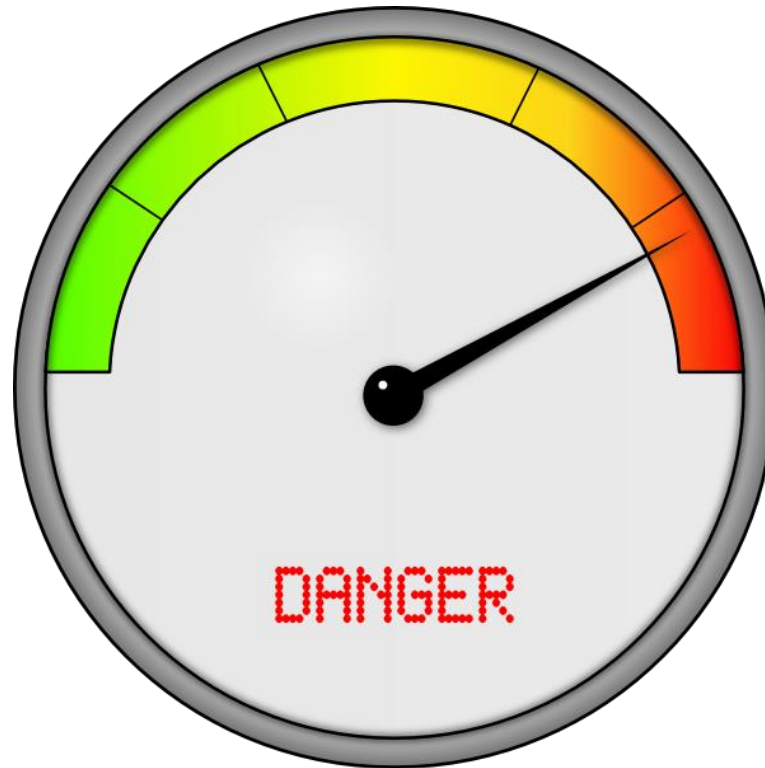


Určitě je to podvod

# 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

- ▶ Poradte se s pracovníky CIV
- ▶ Přepošlete [operator@service.zcu.cz](mailto:operator@service.zcu.cz)
- ▶ Zjistíte, co si myslíme my

A JÁ SE NA TO  
MRKNU OSOBNĚ



# 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 (pře pošlu) zprávu na [operator@service.zcu.cz](mailto: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

PARÁDA, POZNALA JSEM  
PODVOD ... ALE CO TEĎ?

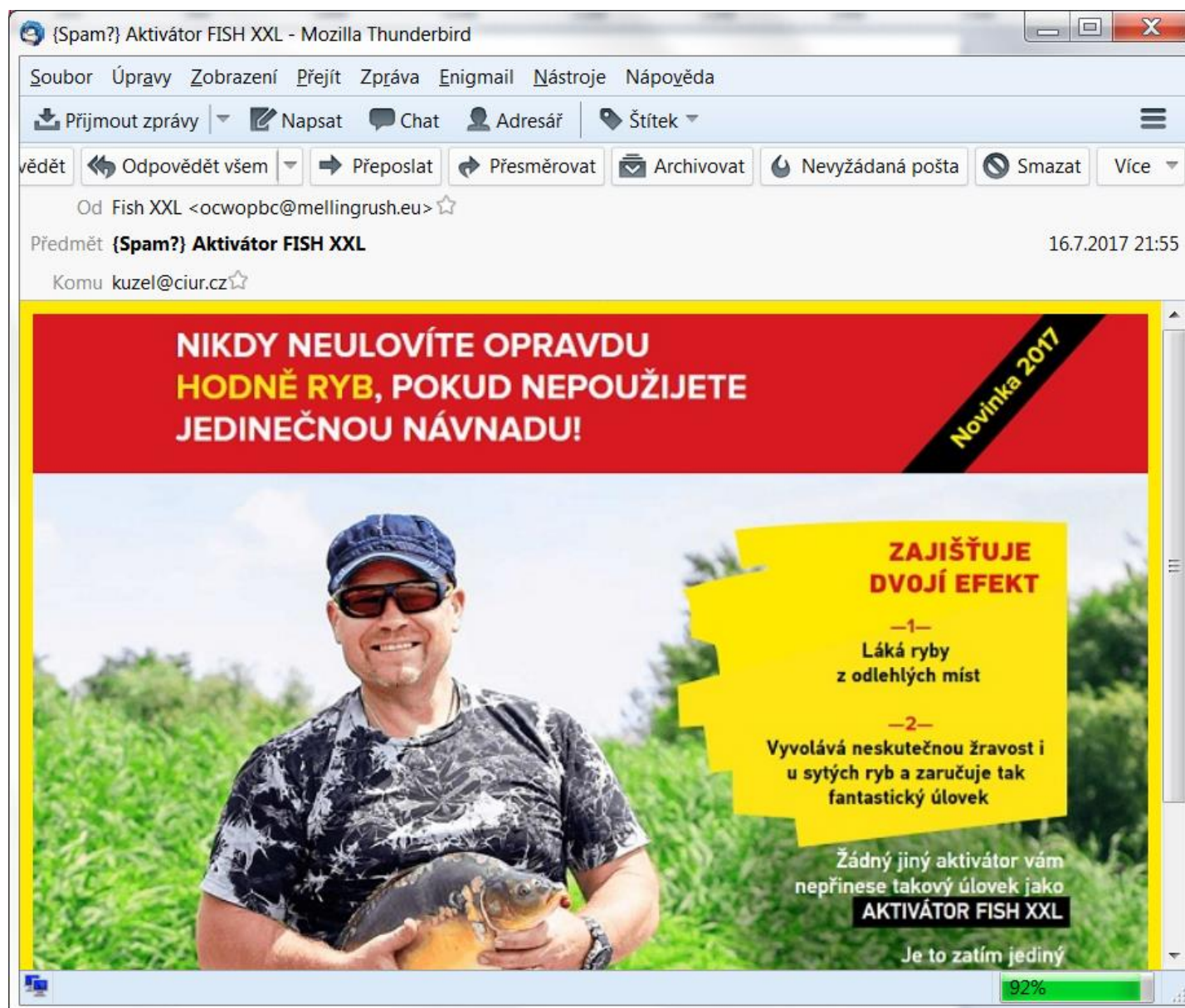


# Co už víte?

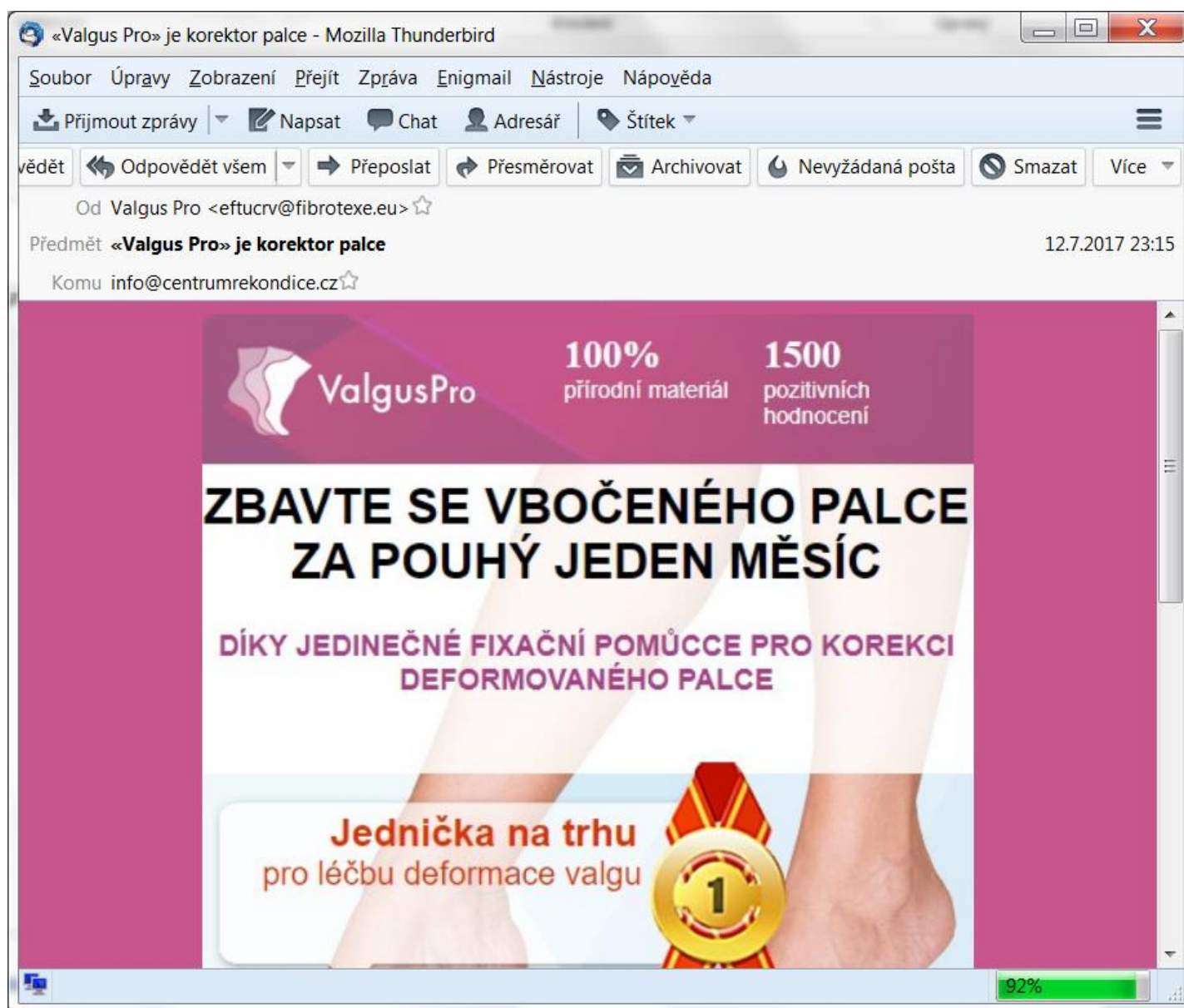
- ▶ Co hrozí po úspěšném útoku
- ▶ Co je phishing, jeho typy a znaky
- ▶ Co byste měli poznat sami
- ▶ Jak se správně zachovat
- ▶ Kdo vám pomůže, když si nevíte rady

# Ukázky z praxe

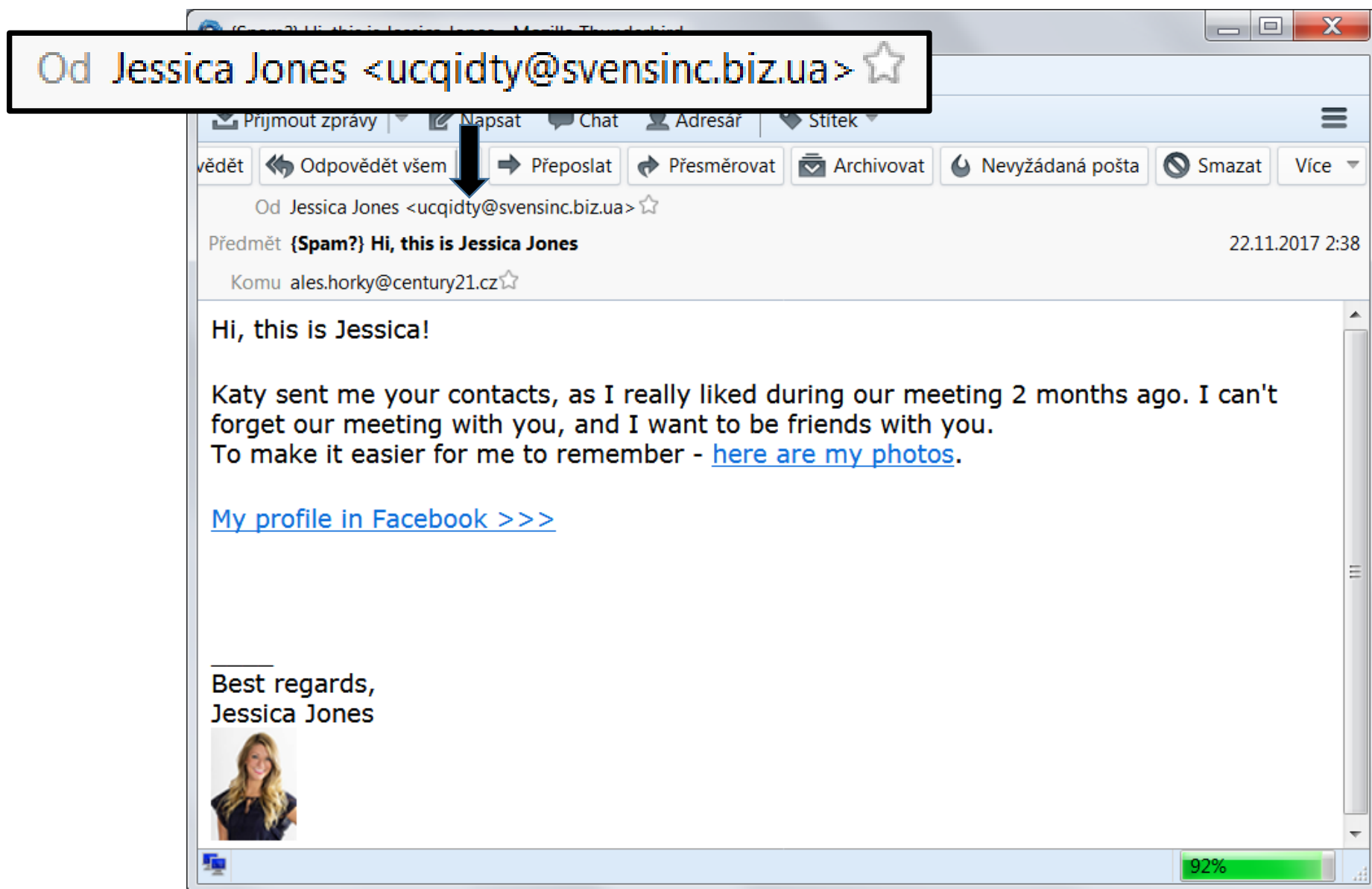
# E-mail č. 1 – Očividný spam



# E-mail č. 2 – Očividný spam



# E-mail č. 3 – Podezřelý odesílatel



# E-mail č. 4 – Podezřelý odesílatel

Od Lonely Danulenska <bluster150@zeus.eonet.ne.jp> ☆

☑ Přijmout zprávy | ✎ Napsat | Chat | 👤 Adresář | 🏷 Štítek ▾

↩ Odpovědět | ↩ Odpovědět všem ▾ | ➡ Přeposlat | ↶ Přesměrovat | 📁 Archivovat | 🔄 Nevyžádaná pošta | 🗑 Smazat | ☰ Více ▾

Od Lonely Danulenska <bluster150@zeus.eonet.ne.jp> ☆

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

Odpověď Lonely Danulenska <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 odpoved' prostrednictvim e-mailu. To nejlepsi nas teprve ceká. S pranim vseho nejlepsiho, Danuska,

—CAM-778.jpg—

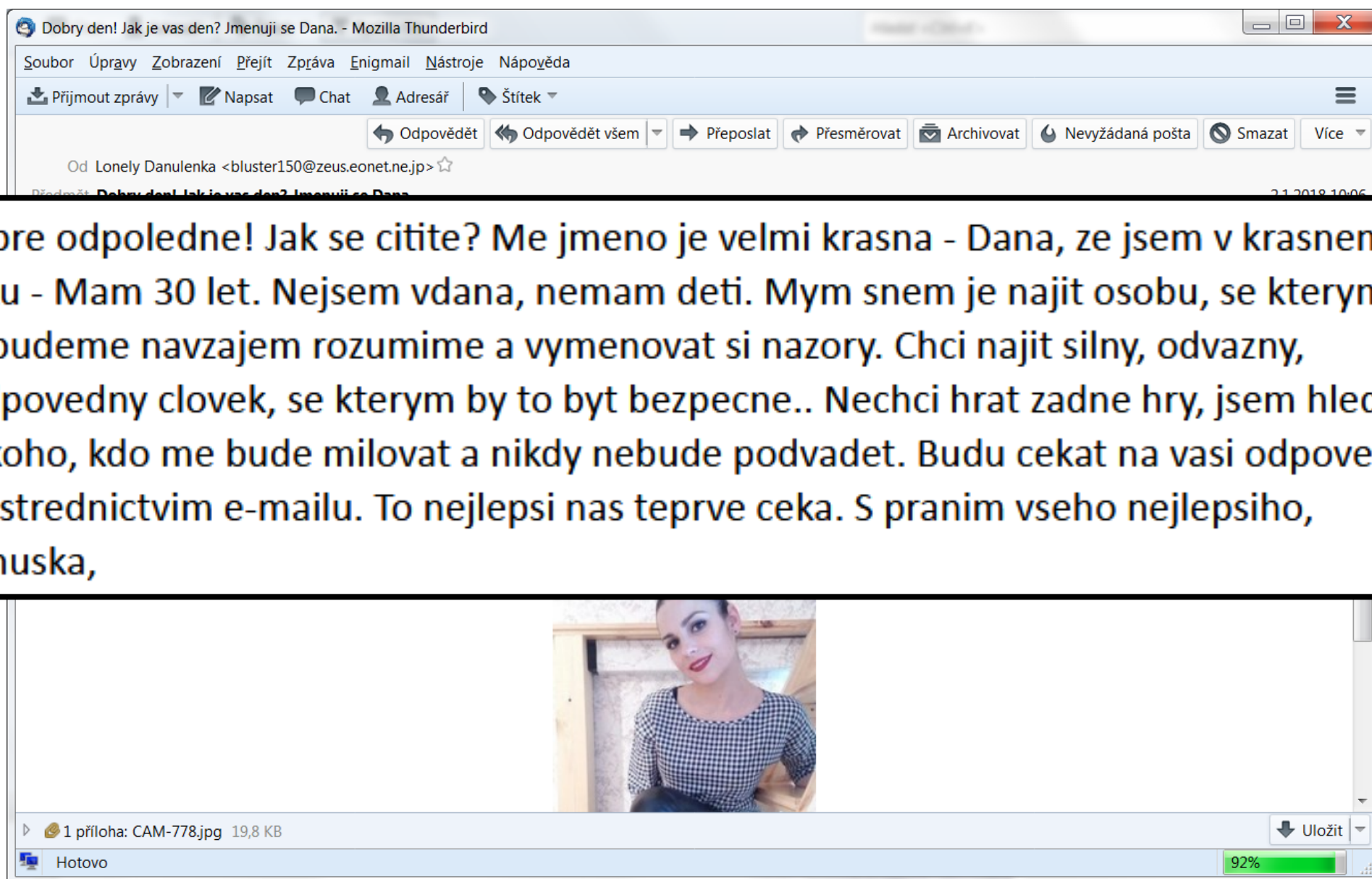


1 příloha: CAM-778.jpg 19,8 KB

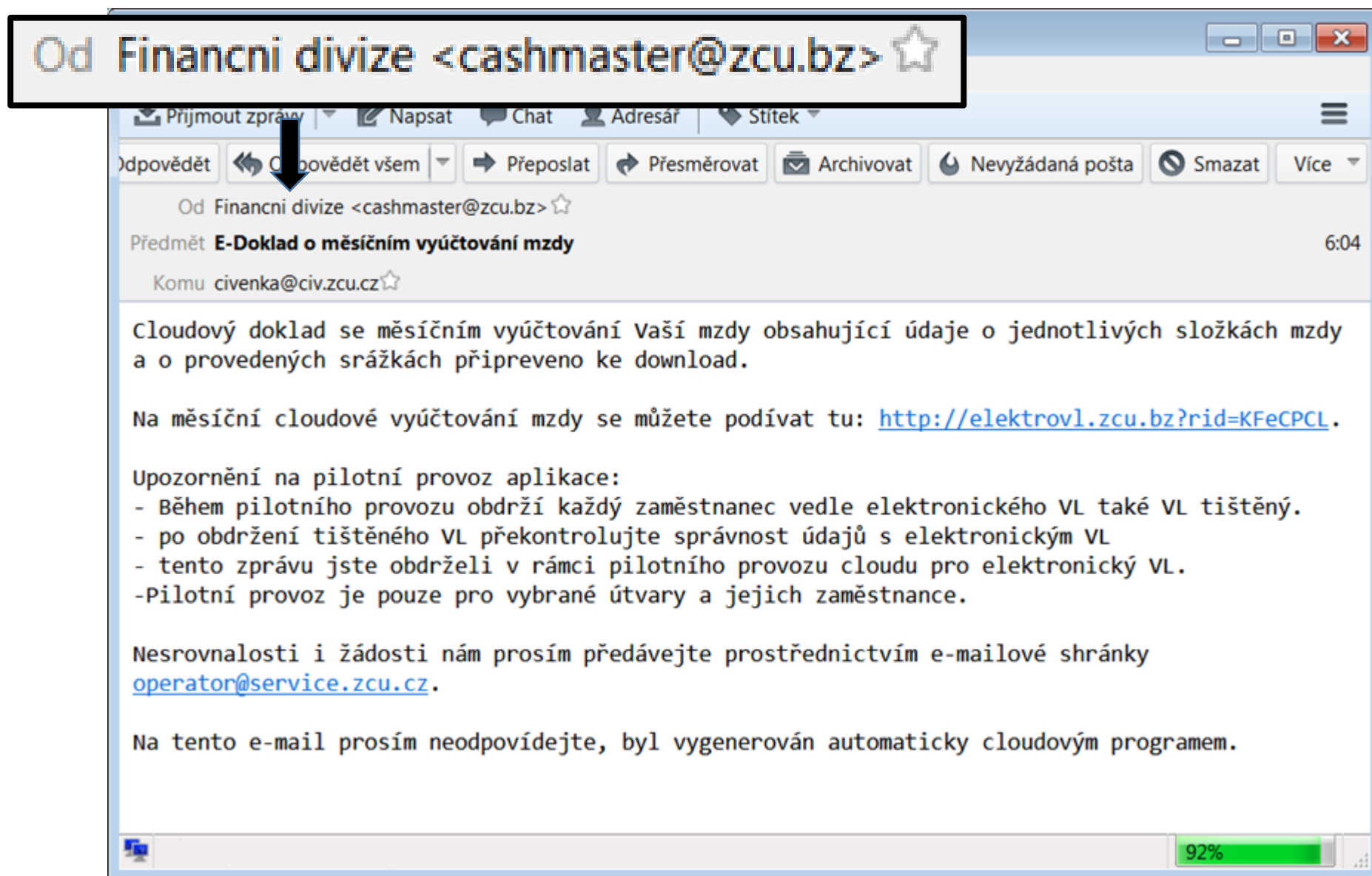
Hotovo 92%



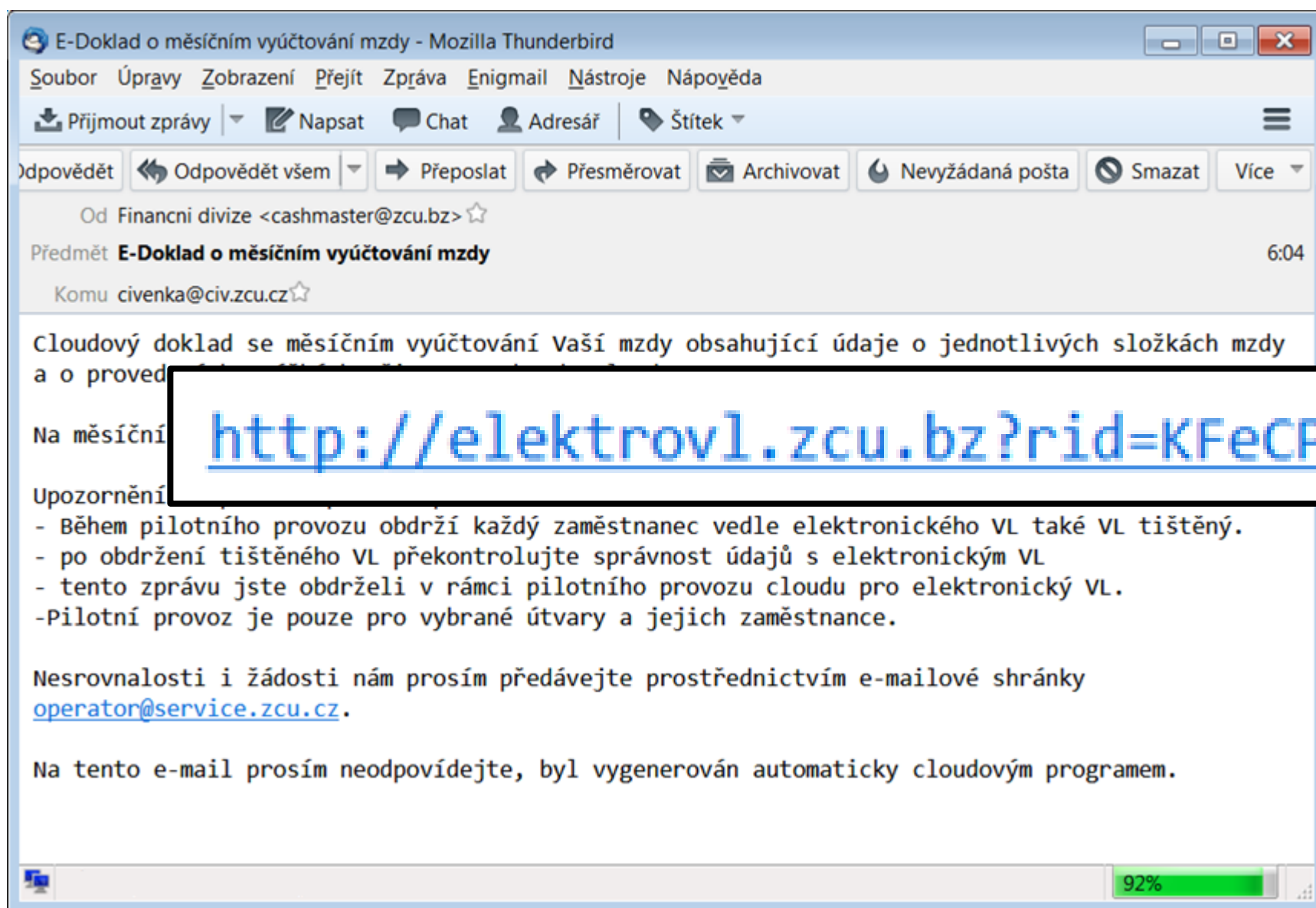
# E-mail č. 4 – Podezřelý obsah



# E-mail č. 5 – Podezřelý odesílatel



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



# E-mail č. 5 – Odkazovaná stránka


Soubor Úpravy Zobrazit Historie Záložky Nástroje Nápověda

Západočeská univerzita v Plzni - 1 x +

webkdc.zcu.cz/login.fcgi?RT=W Hledat

Nejnavštěvovanější

## Orion WebAuth

 ZÁPADOČESKÁ  
UNIVERZITA  
V PLZNI

Orion login:


Heslo (password):

Toto připojení není zabezpečeno. Zadané přihlašovací údaje mohou být vyzrazeny. Zjistit více

[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 prvnímu 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!**  
 Nikdy nezasílejte Orion jméno a heslo do webových formulářů, pokud se nejedná o přihlašovací stránku systému WebAuth (tato stránka) nebo oficiální webový nástroj pro změnu hesla. Obě aplikace jsou provozovány na stroji *webkdc.zcu.cz!!!*

Po zadání hesla se zpřístupní všechny servery, včetně těch, se kterými právě nepracujete. Je zde větší riziko zneužití přístupových práv uživatele, odejde-li od počítače. Pro bezpečné odhlášení je potřeba ukončit webový prohlížeč.

# E-mail č. 5 – Odkazovaná stránka

The screenshot shows a web browser window with the address bar containing the URL `webkdc.zcu.bz/login.fcgi?RT=WC`. The page title is "Orion WebAuth". The page content includes the logo of Západočeská univerzita v Plzni and a login form with fields for "Orion login:" and "Heslo (password):". A security warning box is overlaid on the password field, stating: "Toto připojení není zabezpečeno. Zadané přihlašovací údaje mohou být vyzrazeny. Zjistit více". A black arrow points from this box to a larger warning box in the bottom right corner of the page, which contains the text: "Toto připojení není zabezpečeno. Zadané přihlašovací údaje mohou být vyzrazeny. Zjistit více".

**Orion WebAuth**

**Orion login:**

**Heslo (password):**

Toto připojení není zabezpečeno. Zadané přihlašovací údaje mohou být vyzrazeny. Zjistit více

[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 prvnímu serveru, na který chcete přistupovat, a tím jste automaticky přihlášen(a) i k ostatním serverům v doméně.

**Výhody**  
Větší pohodlí pro uživatele (heslo zadáváte jen jednou) a vyšší bezpečnost: mezi prohlížečem a webovým serverem se předává bezpečnostní autentičací token. Platnost tokenu je navíc časově omezená.

**Důležitá upozornění!**  
Nikdy nezasílejte Orion jméno a heslo do e-mailů, ani je nezasílejte nikomu. Pokud se nejedná o přihlašovací stránku systému WebAuth (tato stránka) nebo oficiální webový nástroj pro změnu hesla. Obě aplikace jsou provozovány na stroji `webkdc.zcu.cz!!!`

Po zadání hesla se zpřístupní všechny servery, včetně těch, se kterými právě nepracujete. Je zde větší riziko zneužití přístupových práv uživatele, odejde-li od počítače. Pro bezpečné odhlášení je potřeba ukončit webový prohlížeč.

Toto připojení není zabezpečeno. Zadané přihlašovací údaje mohou být vyzrazeny. Zjistit více

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

Nedodržování směrnice 10R/2008 - 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 Ing. Jana Kruta <janakrut@zcu.cz> ☆

Předmět **Nedodržování směrnice 10R/2008** 0:39

Od Ing. Jana Kruta <janakrut@zcu.cz> ☆

při kontrole bylo zjištěno, že mnoho zaměstnanců řádně nečerpá dovolenou na zotavenou a porušuje tím směrnici rektora 10R/2008 (viz příloha). Pokud jste na seznamu těchto zaměstnanců (viz druhá příloha) neprodleně mne kontaktujte, v opačném případě hrozí propadnutí nesprávně čerpané dovolené.

JUDr. Jana Krutá  
--  
Právně-personální vztahy

Západočeská univerzita v Plzni  
Univerzitní 8  
306 14 Plzeň

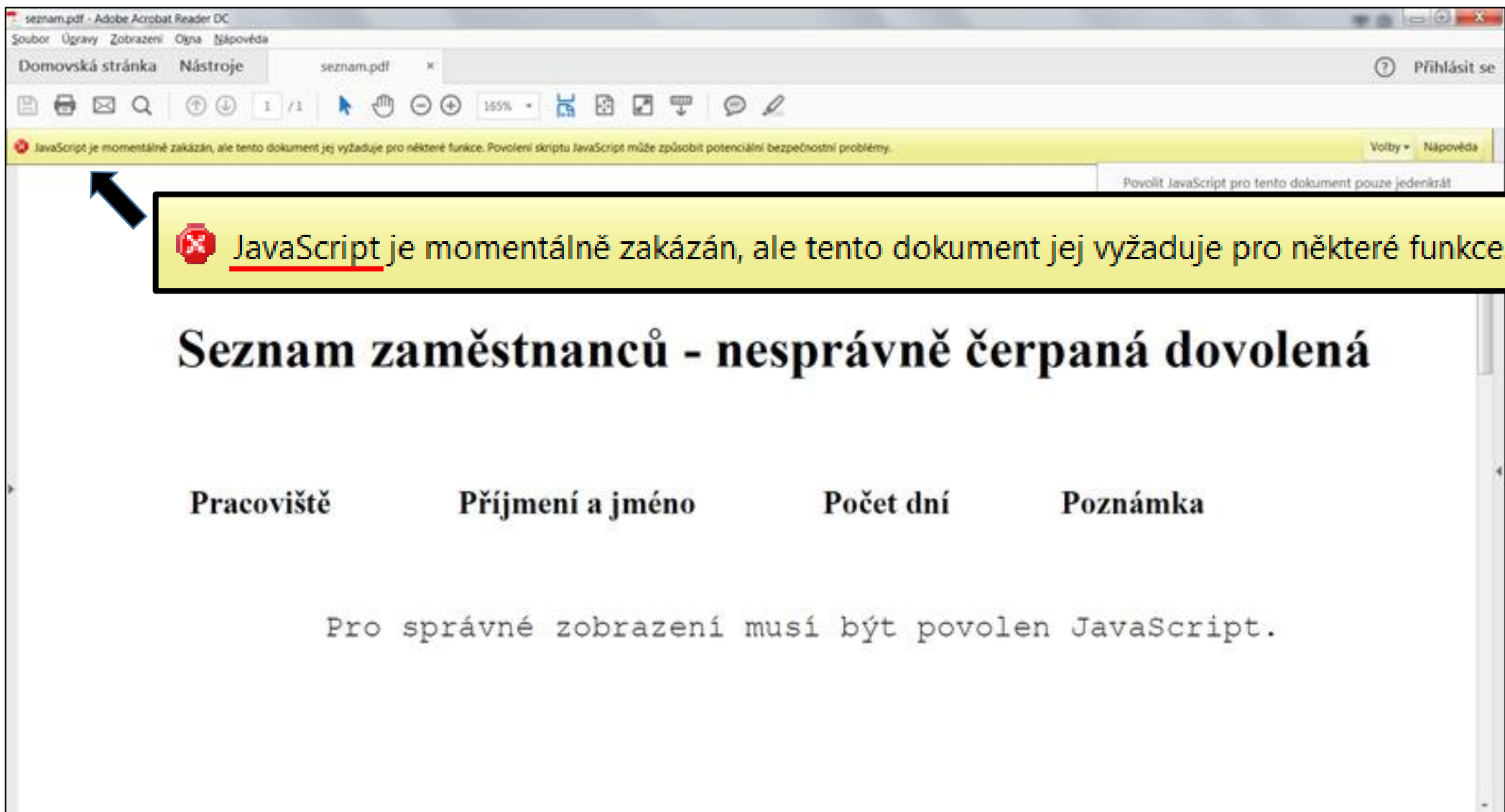
1 příloha: seznam.pdf 121 KB Uložit

Hotovo 92%

# E-mail č. 6 – Psychologický nátlak



# E-mail č. 6 – Podezřelá příloha



The screenshot shows the Adobe Acrobat Reader DC interface. A yellow warning bar at the top states: "JavaScript je momentálně zakázán, ale tento dokument jej vyžaduje pro některé funkce. Povolení skriptu JavaScript může způsobit potenciální bezpečnostní problémy." Below this, a larger yellow box contains the same message with a red 'X' icon and the text: "JavaScript je momentálně zakázán, ale tento dokument jej vyžaduje pro některé funkce." A black arrow points from this box to the warning bar. The main content of the PDF is a table with the title "Seznam zaměstnanců - nesprávně čerpaná dovolená". The table has four columns: "Pracoviště", "Příjmení a jméno", "Počet dní", and "Poznámka". Below the table, the text "Pro správné zobrazení musí být povolen JavaScript." is displayed.

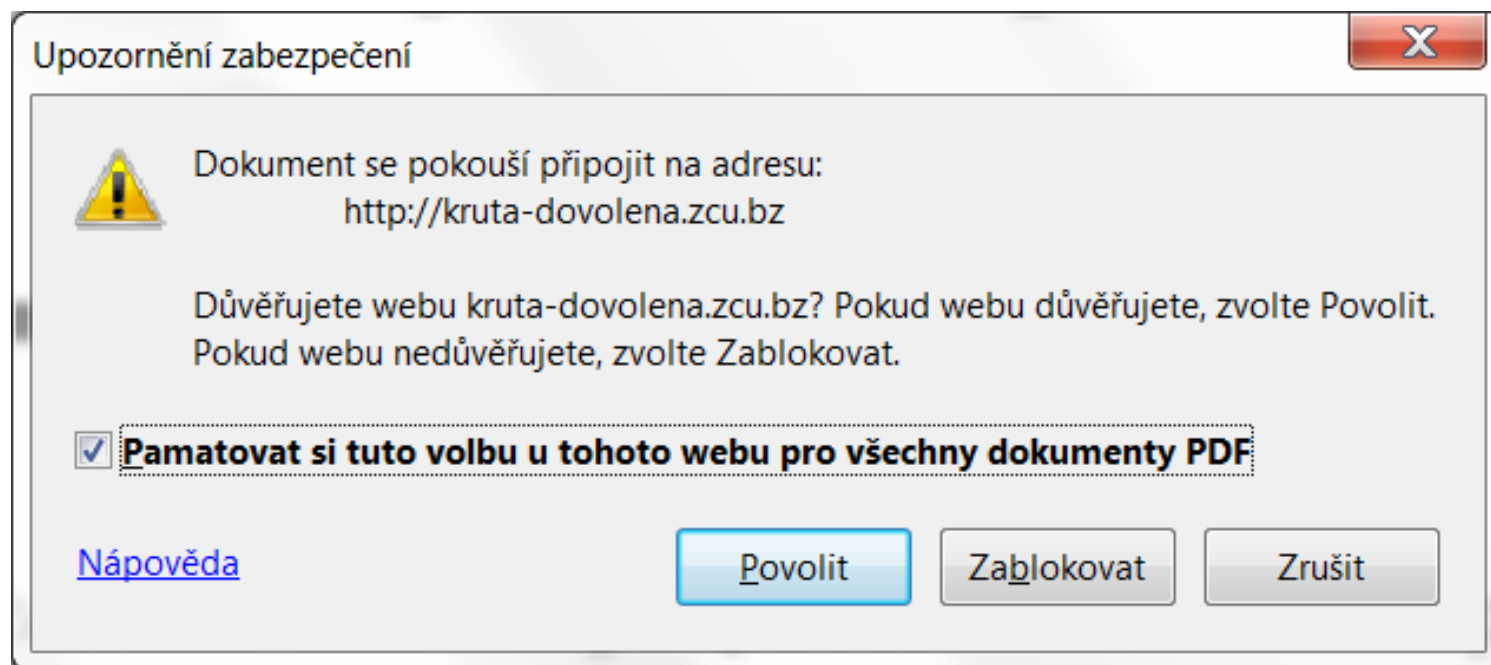
JavaScript je momentálně zakázán, ale tento dokument jej vyžaduje pro některé funkce.

## Seznam zaměstnanců - nesprávně čerpaná dovolená

Pracoviště	Příjmení a jméno	Počet dní	Poznámka
Pro správné zobrazení musí být povolen JavaScript.			



# E-mail č. 6 – Podezřelá příloha



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

# Děkuji za pozornost

# Prostor pro diskusi

---

**Aleš Padrta, Jiří Čepák**

[apadrta@civ.zcu.cz](mailto:apadrta@civ.zcu.cz), [cepakj@civ.zcu.cz](mailto:cepakj@civ.zcu.cz)