ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

IT bezpečnost
Phishing

Školení pro uživatele sítě WEBnet

Jiří Čepák / středa 14. 6. 2017

Teroristický útok vs. Kybernetický útok

- Několik společných rysů
  - Útočník (radikální islamista vs. hacker)
  - Cíl (skupina osob (tzv. měkkých cílů) vs. zaměstnanci ZČU)
  - Čas (vánoční čas (trhy), konec roku vs. zavirovaná PF)
  - Zbraň (po domácku vyrobená bomba vs. spam se závadnou přílohou nebo odkazem)

Teroristický útok vs. Kybernetický útok

- Několik společných rysů
  - Útočník (radikální islamista vs. hacker)
  - Cíl (skupina osob (tzv. měkkých cílů) vs. zaměstnanci ZČU)
  - Čas (vánoční čas (trhy), konec roku vs. zavirovaná PF)
  - Zbraň (po domácku vyrobená bomba vs. spam se závadnou přílohou nebo odkazem)

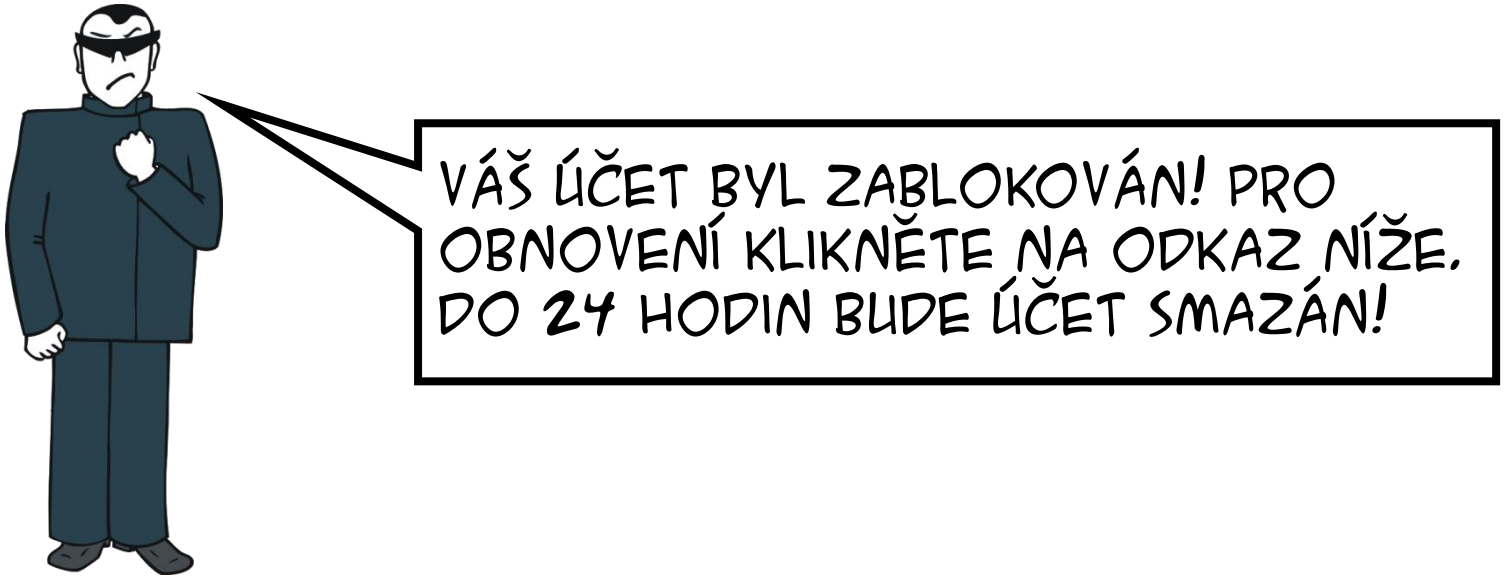
- Jeden odlišný rys
  - Lidé se při teroristickém útoku dají na útěk, ALE uživatelé PC při kybernetickém útoku klikají a zkouší, a pak se nestačí divit

Co hrozí

- Ovládnutí počítače útočníkem (dokáže např. odposlechnout přihlašovací údaje a ty dále zneužívat)
- V případě notebooku s integrovanou kamerou může přenášet obraz a zvuk
- Zašifrování souborů uložených na pevných i síťových discích

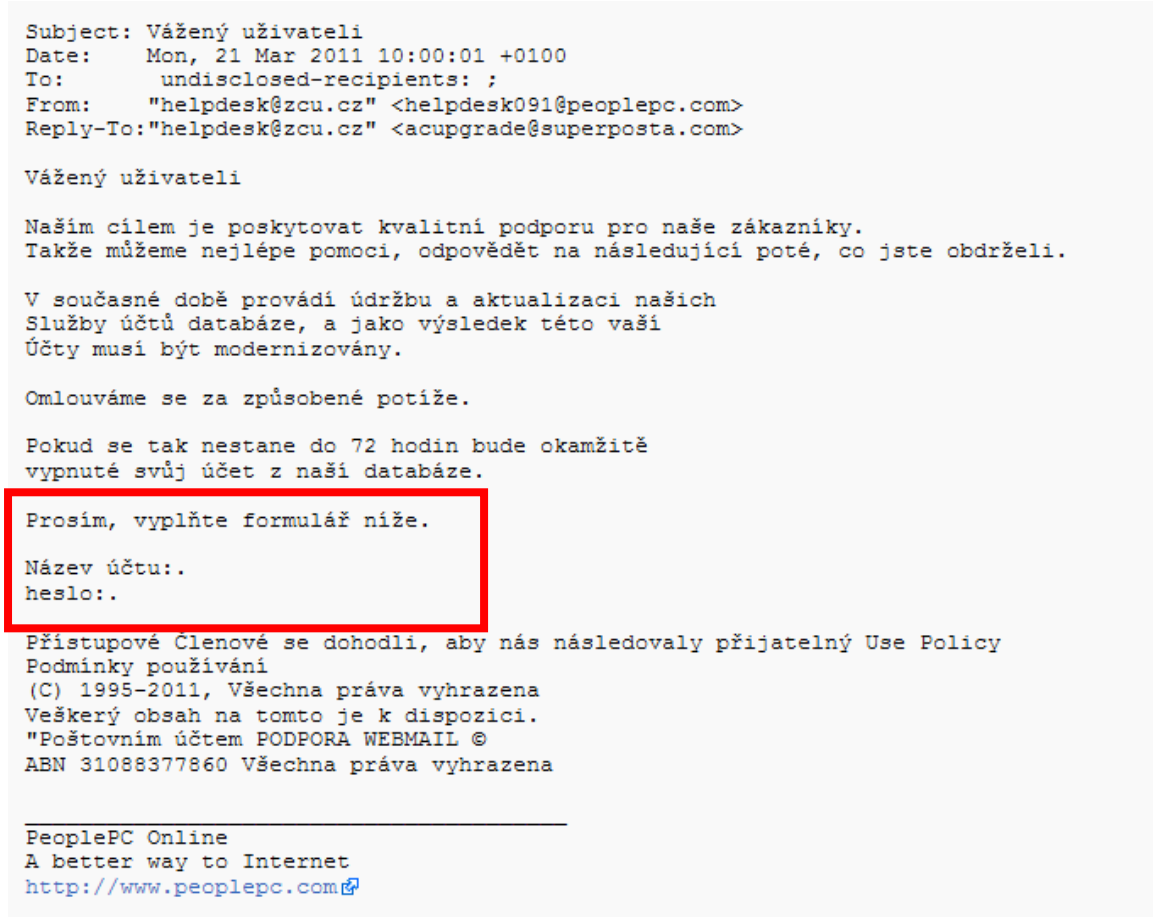
Phishing

- škodlivá aktivita využívající „sociální inženýrství“ k získání citlivých údajů
- Útočník se vydává za „autoritu“ a snaží se oběť přesvědčit o tom, že mu údaje poskytnout musí, často také omezuje čas, nabízí pomoc atd.



Typy phishingu

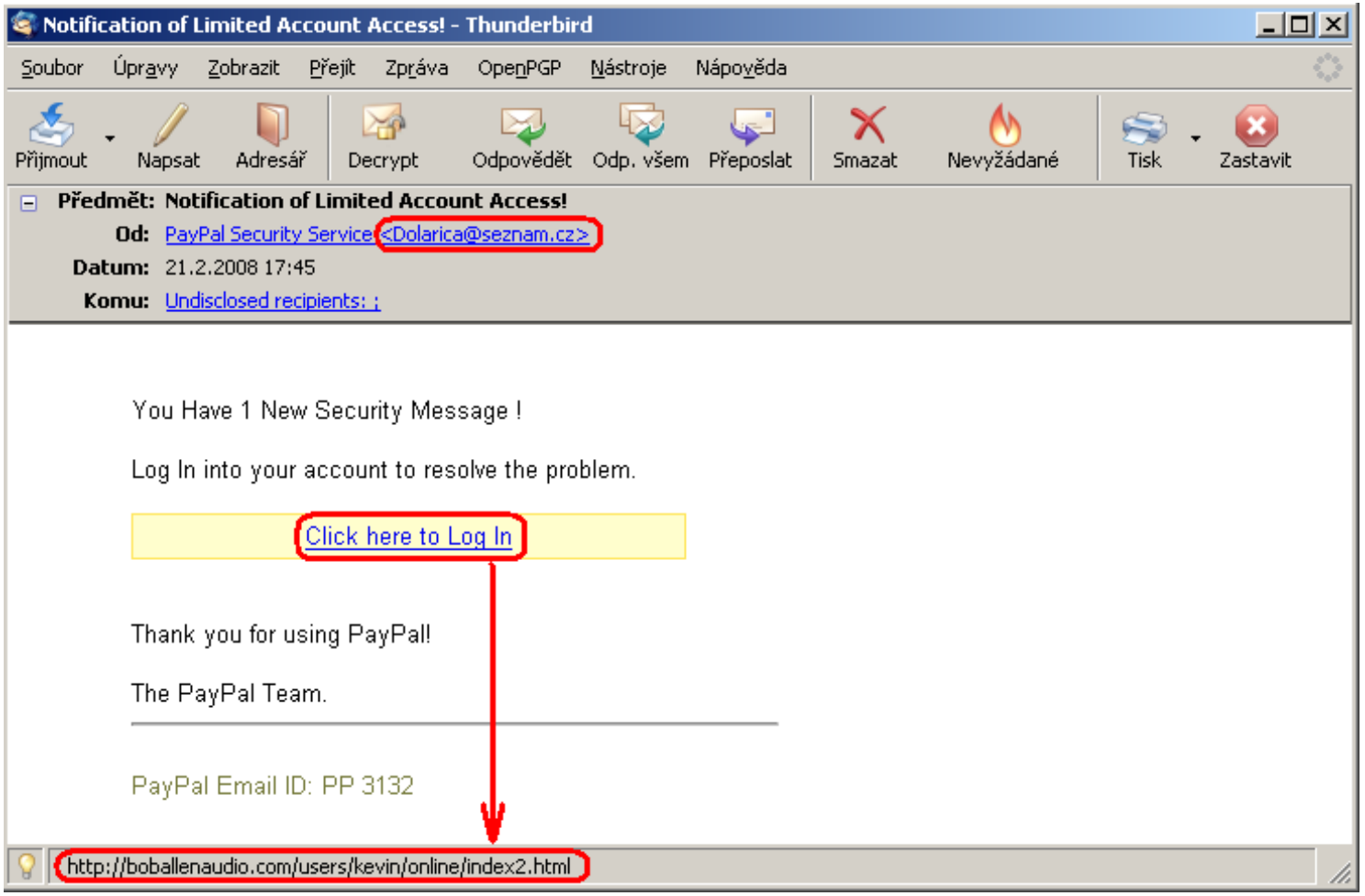
- email s požadavkem o heslo
  - hlavní zásada – nikdy nikomu jakýmkoli způsobem nesdělujte heslo!



```
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

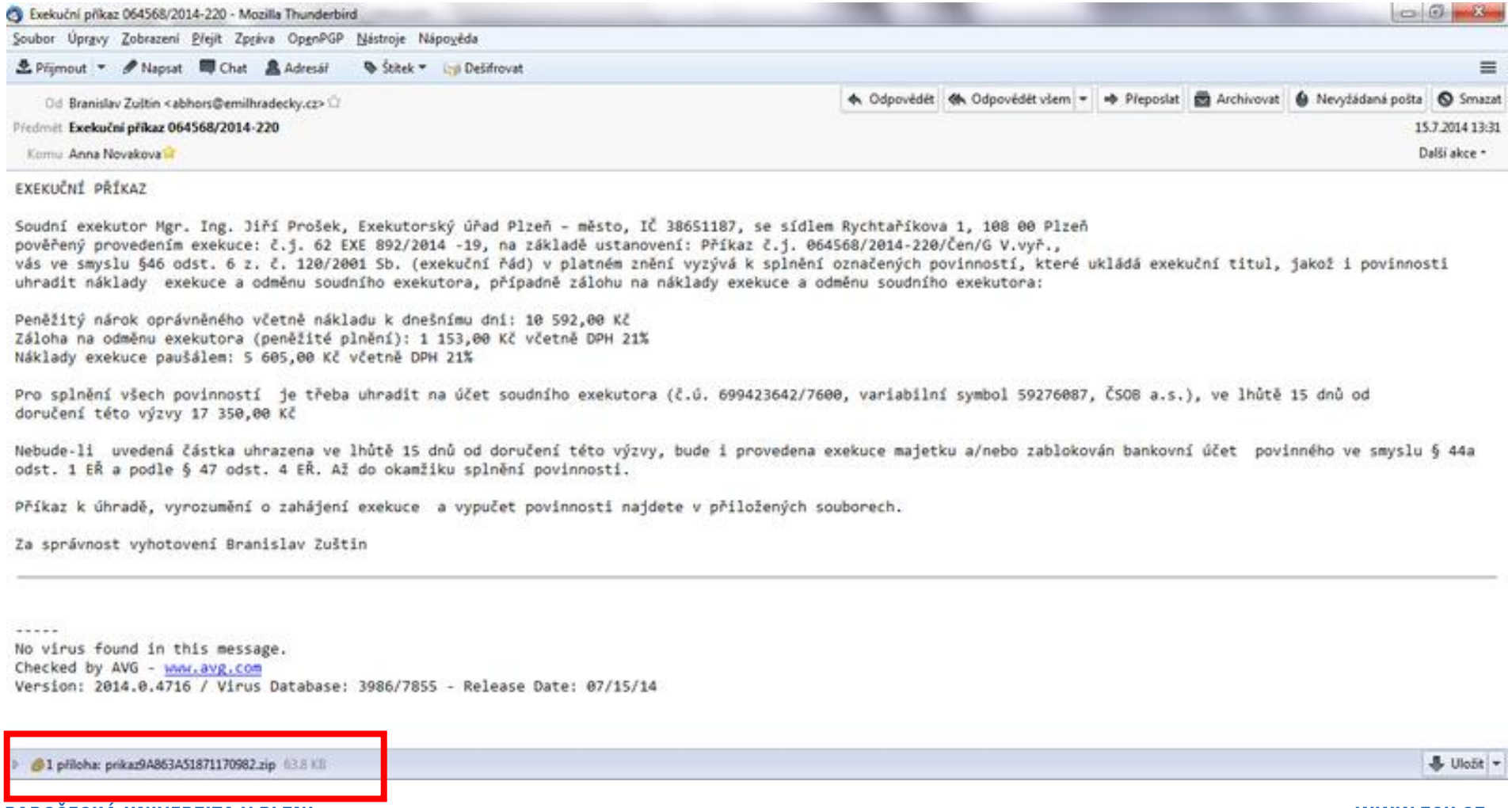
- email s odkazem na vizuálně podobné nebo jiné podvodné stránky



Typy phishingu

Typy phishingu

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



Exekuční příkaz 064568/2014-220 - Mozilla Thunderbird

Soubor Úpravy Zobrazení Přejít Zpráva OpenPGP Nástroje Nápověda

Přijmout Napsat Chat Adresář Štítek Dešifrovat

Od Branislav Zuštin <abhors@emilhradecky.cz>

Odpovědět Odpovědět všem Přeposlat Archivovat Nevyžádaná pošta Smazat

Předmět **Exekuční příkaz 064568/2014-220**

15.7.2014 13:31

Komu Anna Novakova

Další akce

EXEKUČNÍ PŘÍKAZ

Soudní exekutor Mgr. Ing. Jiří Prošek, Exekutorský úřad Plzeň - město, IČ 38651187, se sídlem Rychtaříkova 1, 108 00 Plzeň
pověřený provedením exekuce: č.j. 62 EXE 892/2014 -19, na základě ustanovení: Příkaz č.j. 064568/2014-220/Čen/G V.vyř.,
vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění označených povinností, které ukládá exekuční titul, jakož i povinnosti
uhradit náklady exekuce a odměnu soudního exekutora, případně zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 10 592,00 Kč
Záloha na odměnu exekutora (peněžité plnění): 1 153,00 Kč včetně DPH 21%
Náklady exekuce paušálem: 5 605,00 Kč včetně DPH 21%

Pro splnění všech povinností je třeba uhradit na účet soudního exekutora (č.ú. 699423642/7600, variabilní symbol 59276087, ČSOB a.s.), ve lhůtě 15 dnů od
doručení této výzvy 17 350,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a
odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku splnění povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

Za správnost vyhotovení Branislav Zuštin

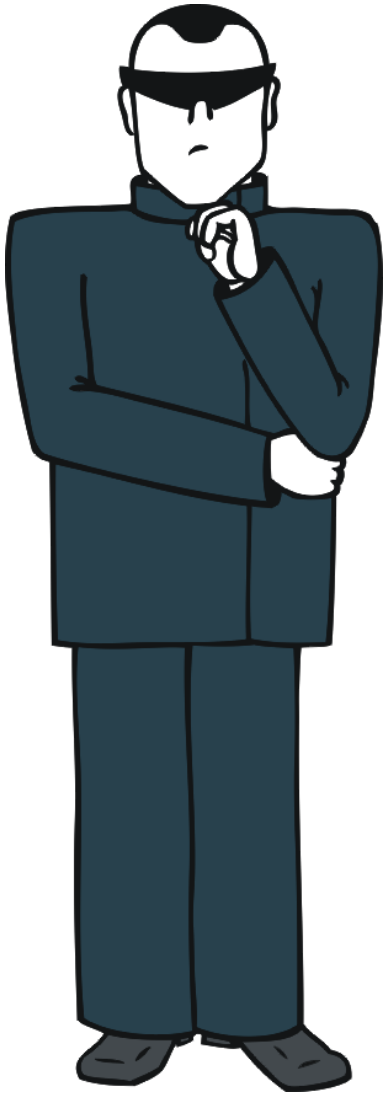
No virus found in this message.
Checked by AVG - www.avg.com
Version: 2014.0.4716 / Virus Database: 3986/7855 - Release Date: 07/15/14

1 příloha: prikaz9A863A51871170982.zip 63.8 KB

Uložit

Kvíz – rozpoznání závadných URL adres rozeslaných spamem

vs.



Rozbor URL


http://www.gjszlin.cz/gztgm/dispnews.php?idm=1&p=3
protokol
název serveru
cesta
název skriptu
parametry stránky

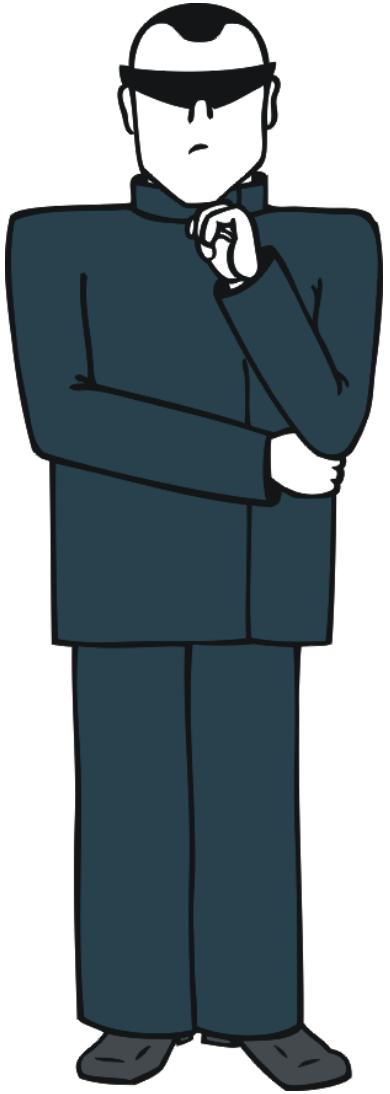
Kvíz - 1

http://xafylopaxwzwhcxwla.com

Kvíz - 1

http://xafylopaxwzwhcxwla.com

ADWARE



Kvíz - 2

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

Kvíz - 2

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

WEBOVÉ STRÁNKY OBCE V ANGLII, KTERÁ DRŽÍ SVĚTOVÝ REKORD V DÉLCE NÁZVU

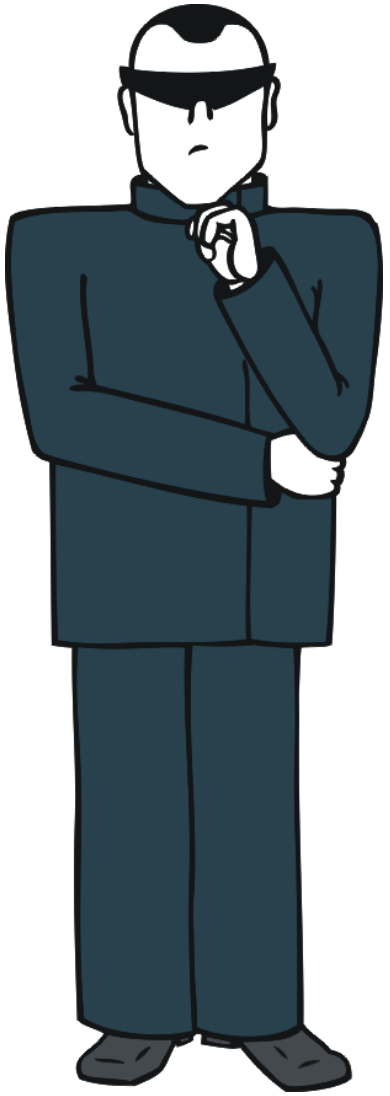
Kvíz - 3

http://apple.com-iphone7.com

Kvíz - 3

http://apple.com-iphone7.com

MALWARE



Kvíz - 4

http://apple.com

Kvíz - 4

http://apple.com

SPRÁVNÉ STRÁNKY VÝROBCE ELEKTRONICKÝCH ZAŘÍZENÍ ZNAČKY APPLE

Kvíz - 5

http://goo.gl/Qaloqr

Kvíz - 5

http://goo.gl/Qaloqr

ZKRÁCENÝ ODKAZ NA SUPPORT.ZCU.CZ

Není to jednoduché

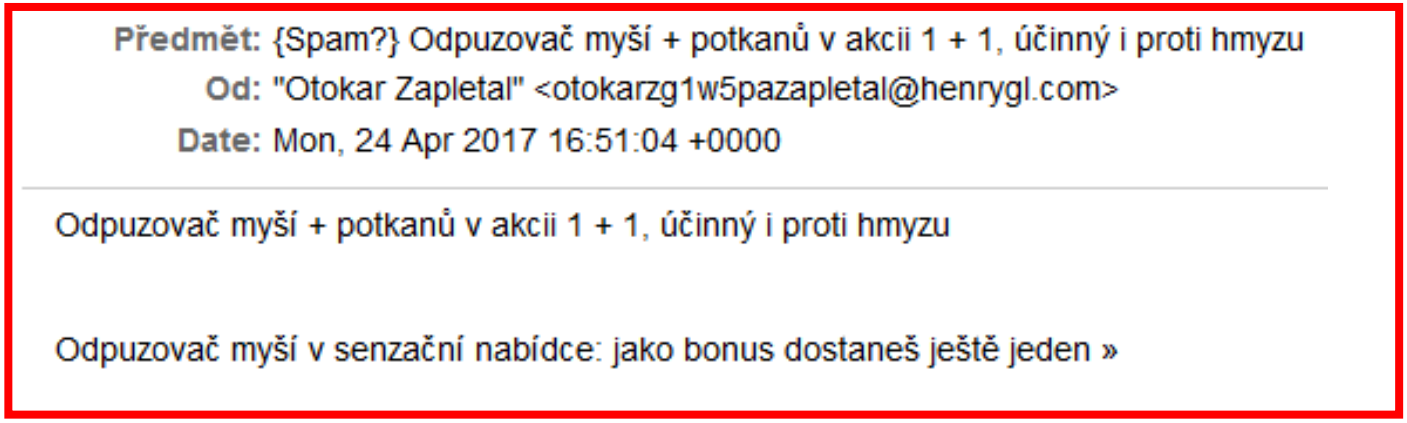
- Těžko se hledá pravidlo, které by s jistotou definovalo, co je a co není nebezpečné.
- Při podezření na útok je třeba se správně zachovat!

Jste důležití!

- Technické prostředky jsou aplikovány, ale většinou dokáží reagovat na nové hrozby až se zpožděním.
- Uživatel sítě WEBnet je nejúčinnější obrana vůči kybernetickým útokům, pokud je dostatečně poučen a s chladnou hlavou rozpozná hrozbu.

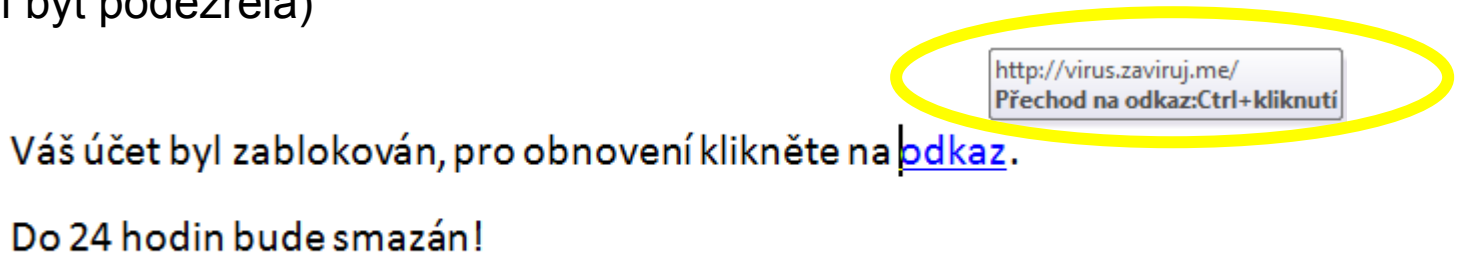
Co byste měli poznat sami

- Podezřelého odesílatele
  - znám odesílatele nebo alespoň doménu, ze které email přišel?
    - Pozor, jméno před adresou nemusí skutečně odpovídat emailové adrese! např. Jan Novák virus@zaviruj.me, důležité je znát, nebo alespoň poznat, odpovídající emailovou adresu
    - Odesílatele lze podvrhnout – jistotou je elektronický podpis
- Očividný spam
  - např. odpuzovač myší a potkanů 1+1 zdarma



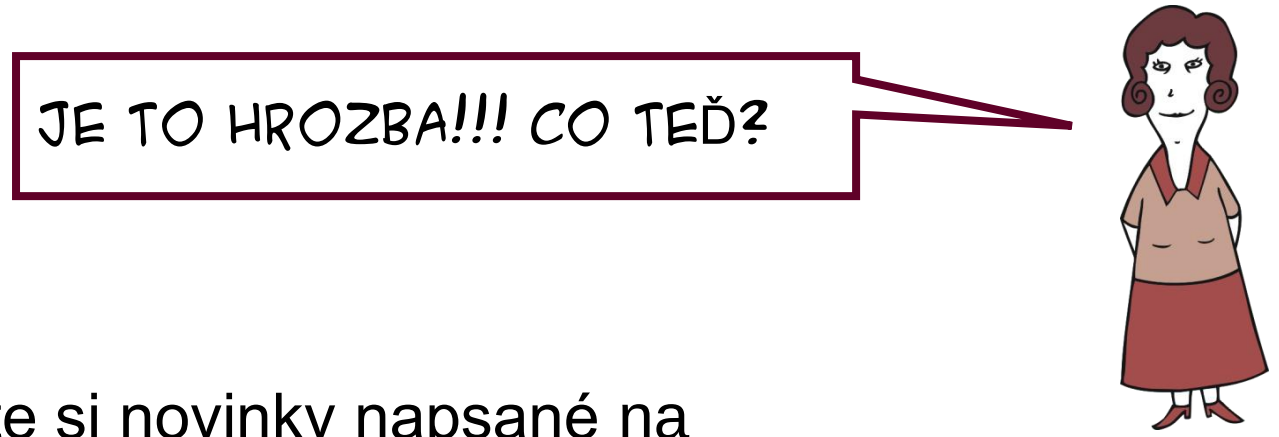
Co byste měli poznat sami

- Podezřelý obsah emailu
  - je odesílatel nebo celý email očekávatelný?
    - z adresy jmeno@domena.nl dostanu email napsaný česky
    - uvědomím si, na jaké pozici pracuji a zda email na oficiální adrese ZČU přísluší mé pozici, případně zda pochází ze zdroje, od kterého mohu email čekat (registroval jsem se, objednával jsem)
  - klikací odkazy
    - před kliknutím se na něm pozastavím myší a podívám se, kam odkazuje (adresa nesmí být podezřelá)



  - obsah zprávy neodpovídá mému zájmu – např. obdržím životopis od neznámé osoby, ale nejsem personalista ani vedoucí pracovník
  - přílohy
    - v textu najdu informaci, že další informace najdu v přiloženém souboru, očekávám soubor s příponou .doc, .pdf, .txt atp.
    - .zip, .rar atd. jsou podezřelé
    - ve výchozím stavu přípony skryty, lze zapnout

Jak se správně zachovat při podezření na hrozbu



- Ověřte si novinky napsané na http://support.zcu.cz/index.php/Novinky
  - hrozba je uvedena, email přepošlu z evidenčních důvodů na operator@service.zcu.cz
  - hrozba není uvedena, email přepošlu jako upozornění na hrozbu na operator@service.zcu.cz
  - NEKLIKÁM, NEOTVÍRÁM PŘÍLOHY, EMAIL PŘESUNU DO SLOŽKY SPAM NEBO NEVYŽÁDANÁ POŠTA.

Kdo mi pomůže?

- Pokud nejsem schopen s jistotou určit, zda je email nebezpečný, ale domnívám se, že jeho smazáním by mohlo dojít k nechtěné ztrátě, přepošlu jej s požadavkem na prověření na operator@service.zcu.cz
- Po prověření vám odepíšeme, zda něco hrozí nebo nikoli a doporučení dalšího postupu.

Shrnutí

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

ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

Děkuji za pozornost

Jiří Čepák / cepakj@civ.zcu.cz