ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

IT bezpečnost
Phishing

Školení pro uživatele sítě WEBnet

Jiří Čepák / úterý 10. 10. 2017

ÚVOD

Teroristický útok vs. Kybernetický útok

- Několik společných rysů
  - Útočník (terorista vs. hacker)
  - Cíl (skupina více osob 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 (skupina více osob 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 a zkouší, a pak se nestačí divit

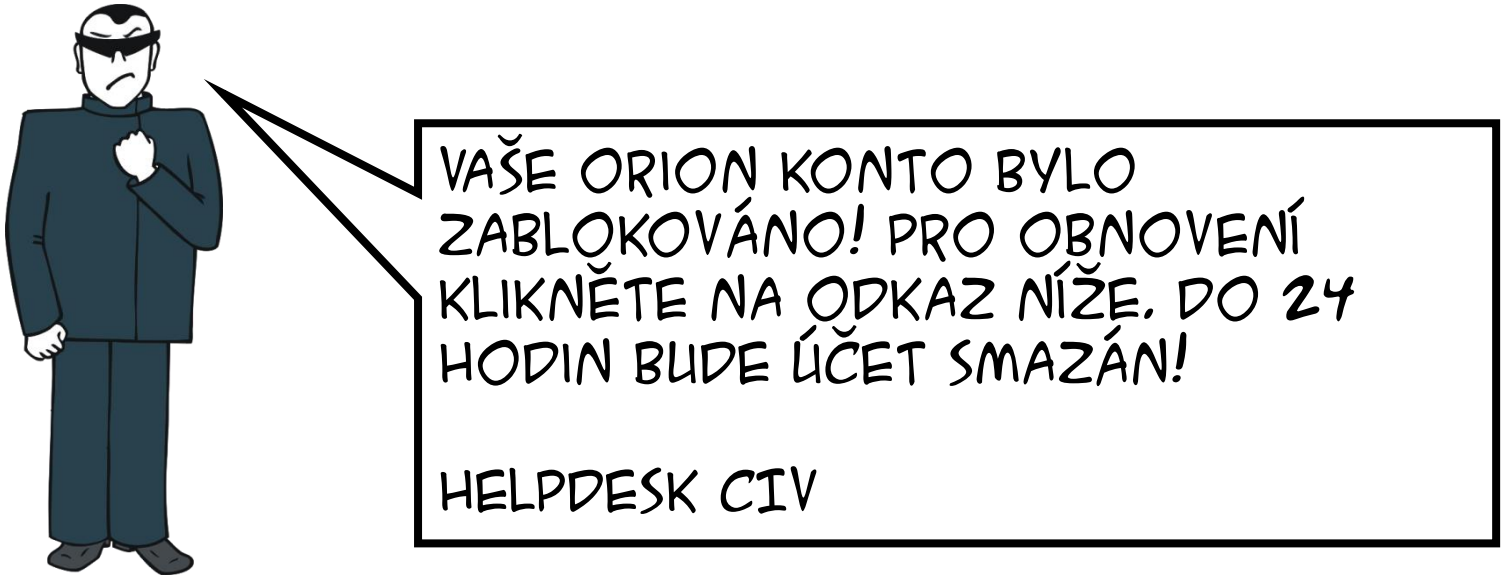
Co hrozí

- Ovládnutí počítače útočníkem
  - Odposlechnutí přihlašovacích údajů, další zneužití
  - V případě notebooku s integrovanou kamerou - přenos obrazu a zvuku, pořizování snímků, zvukových záznamů
  - Zneužívání počítače k dalším útokům
- Zašifrování souborů uložených na pevných i síťových discích

Co je to ten Phishing?

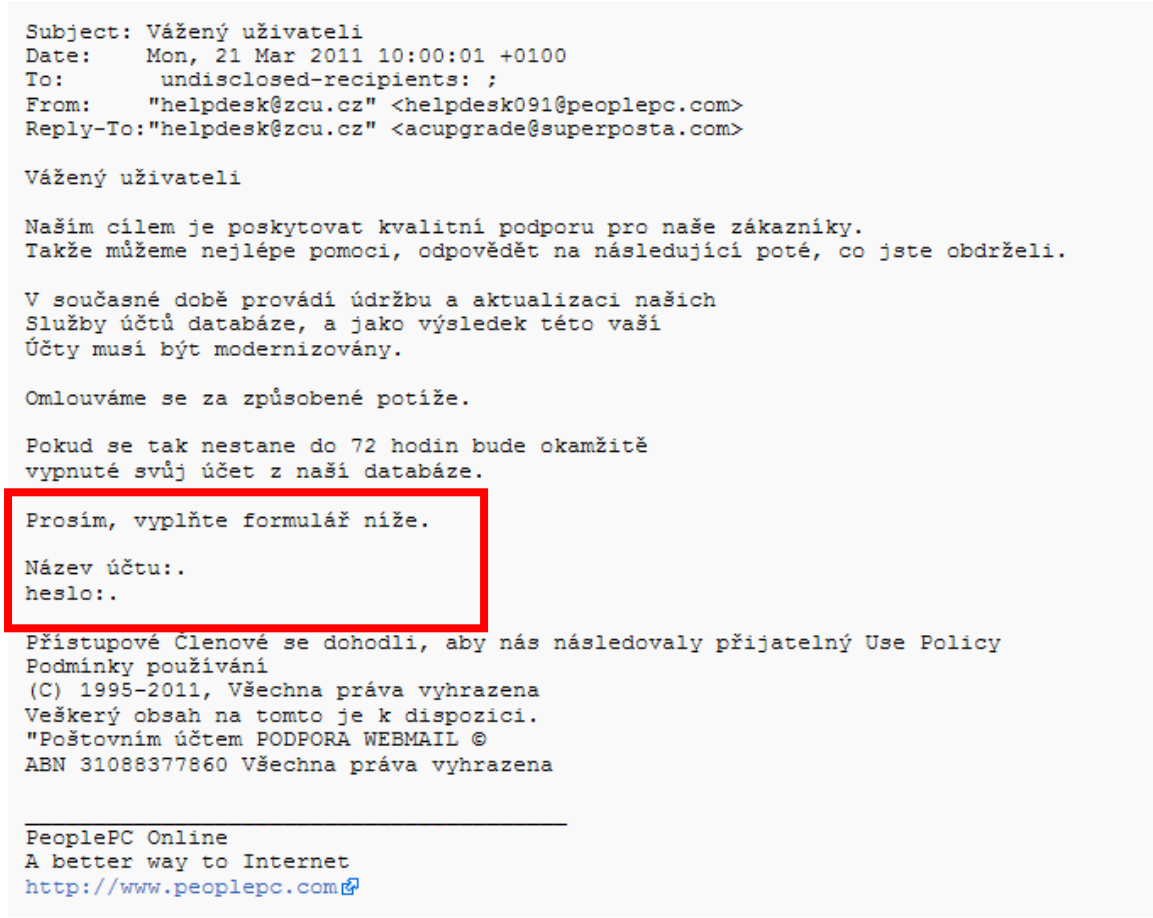
Phishing

- 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

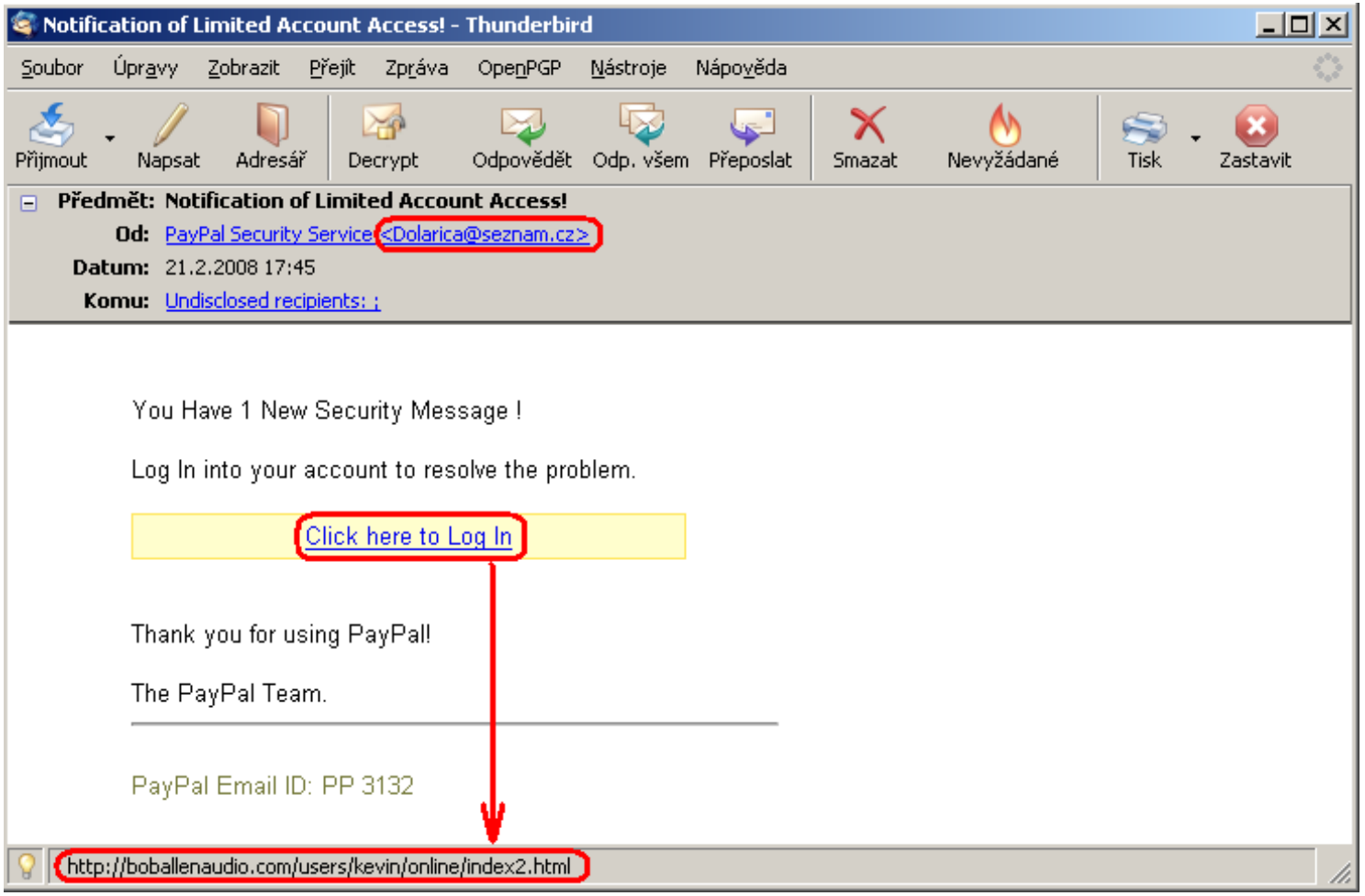
- email s požadavkem o heslo
  - hlavní zásada – nikdy nikomu jakýmkoli způsobem nesdělujte heslo!



```
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

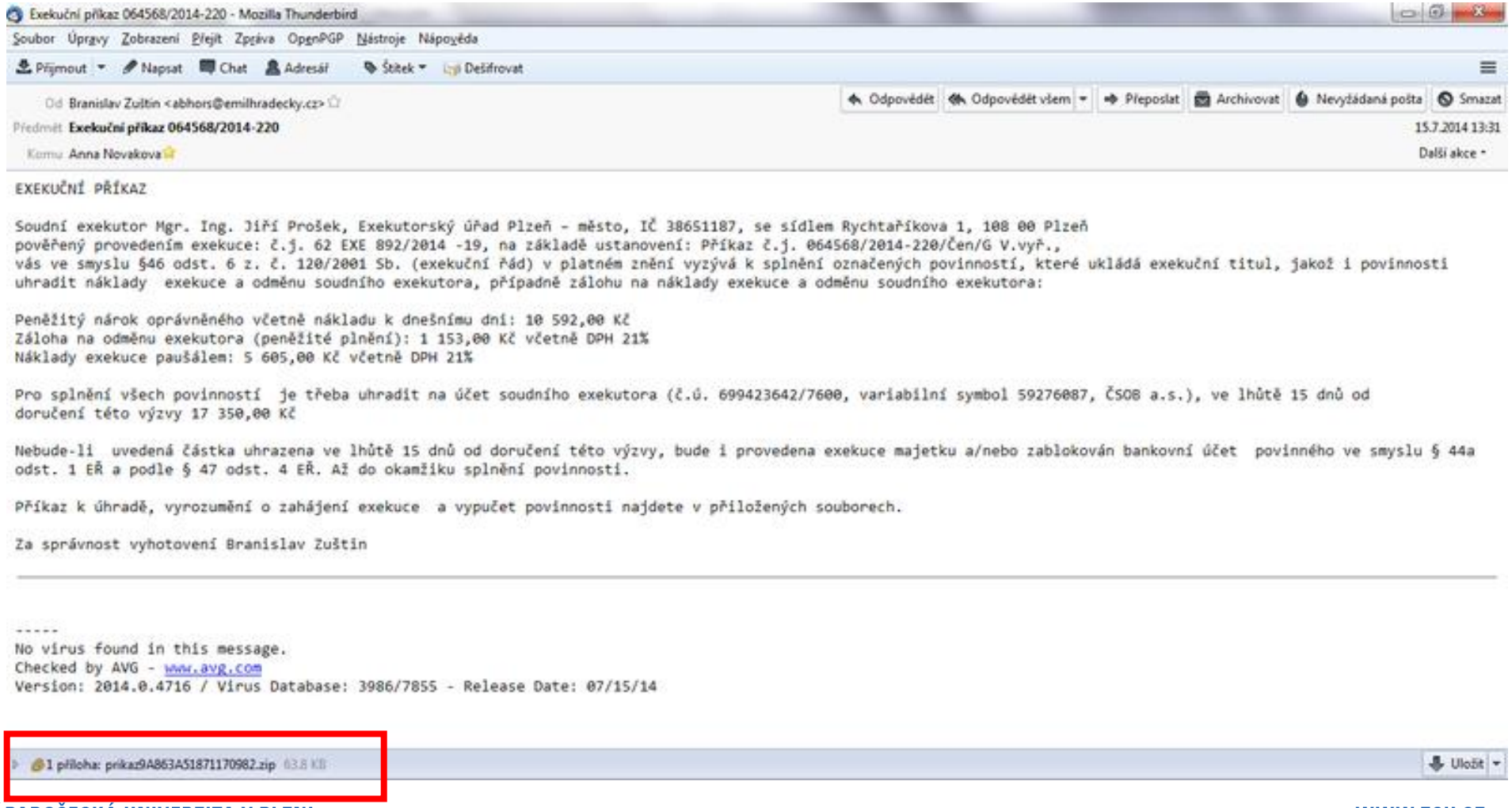
- email s odkazem na vizuálně podobné nebo jiné podvodné stránky



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

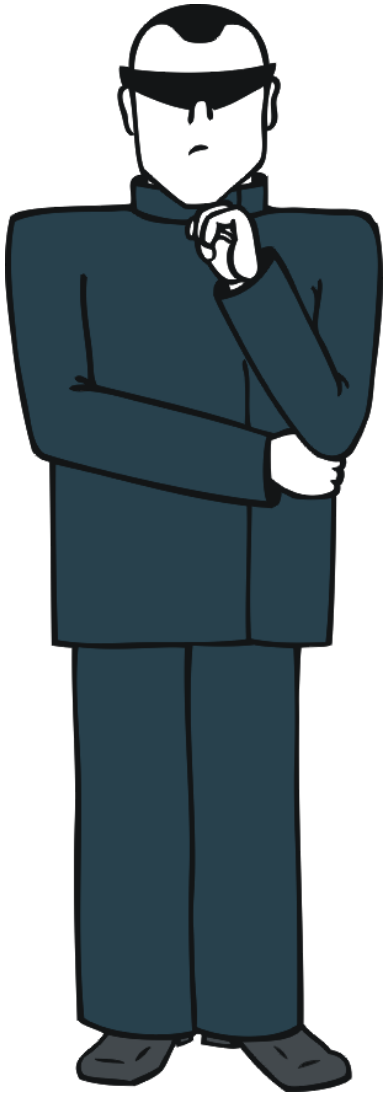
No virus found in this message.
Checked by AVG - www.avg.com
Version: 2014.0.4716 / Virus Database: 3986/7855 - Release Date: 07/15/14

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

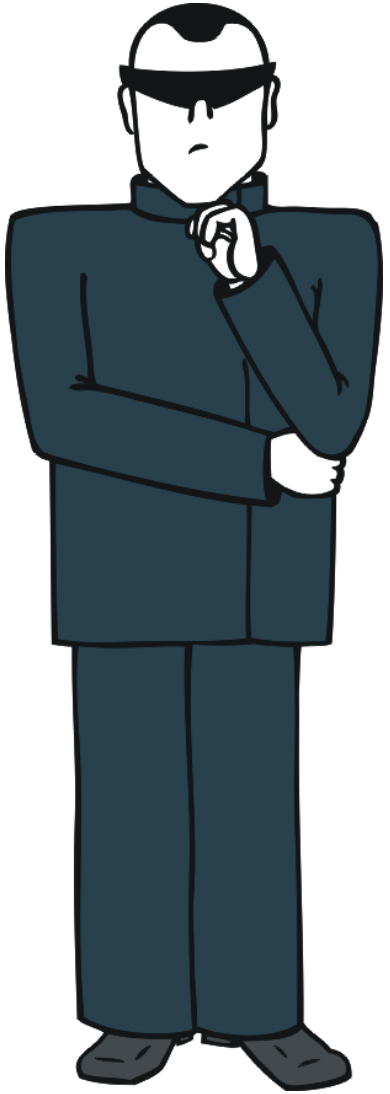
Kvíz - 1

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

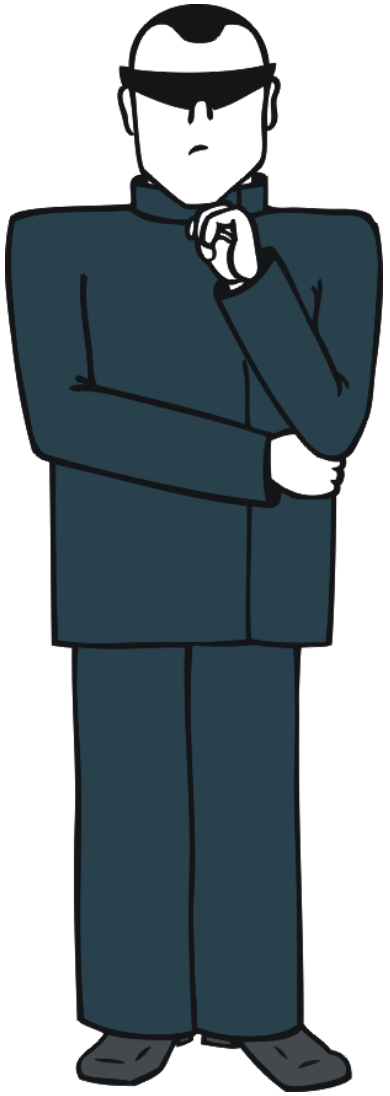
Kvíz - 3

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

Co dělat?

Není to jednoduché

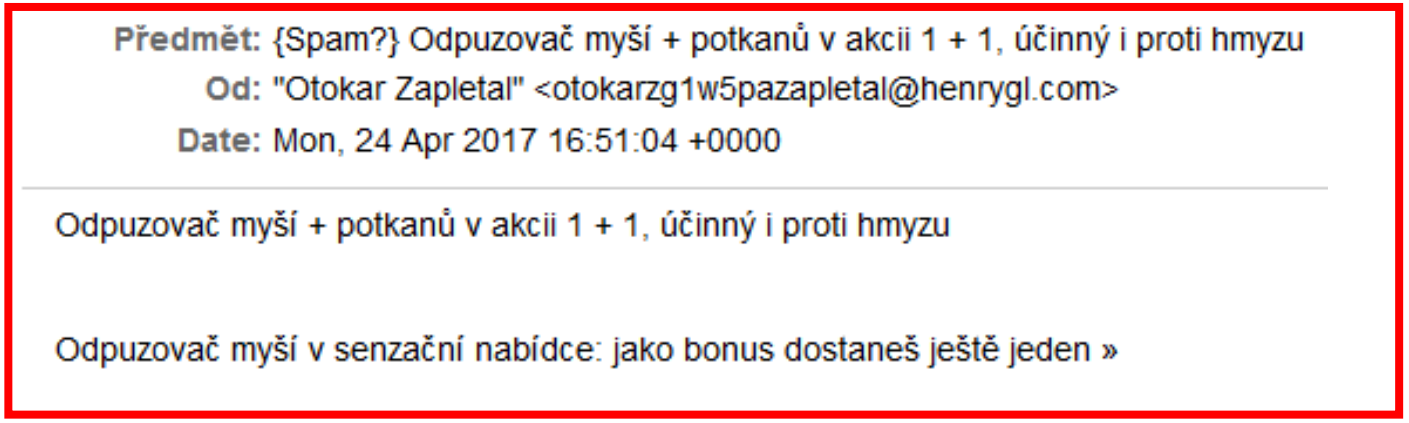
- Těžko se hledá pravidlo, které by s jistotou definovalo, co je a co není nebezpečné.
- Při podezření na útok je třeba se správně zachovat!

Jste důležití!

- Technické prostředky aplikovány
- 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

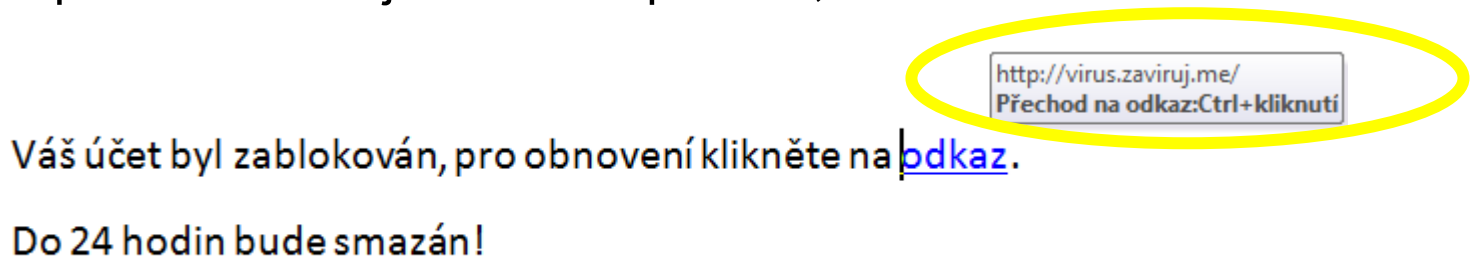
Co byste měli poznat sami

- Podezřelého odesílatele
  - Znám odesílatele nebo alespoň doménu, ze které email přišel?
    - Jméno před adresou nemusí skutečně odpovídat emailové adrese! např. Jan Novák virus@zaviruj.me.
    - Odesílatele lze podvrhnout – jistotou je elektronický podpis
    - Při podezření podvrhu ověřit jiným kanálem (např. telefonicky)
- Očividný spam
  - např. odpuzovač myší a potkanů 1+1 zdarma



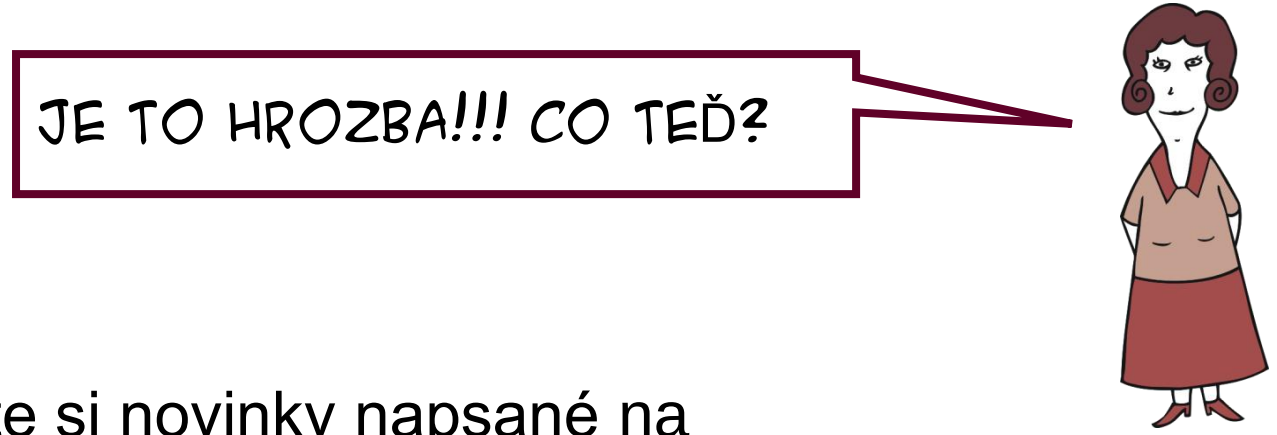
Co byste měli poznat sami

- Podezřelý obsah emailu
  - Očekáváte email podobného typu a z této emailové adresy?
  - Obsah zprávy neodpovídá mému zájmu – např. obdržím životopis od neznámé osoby, ale nejsem personalista ani vedoucí pracovník
  - Z adresy např. herrmann.muller@web.de dostanu email napsaný česky
  - Klikací odkazy
    - před kliknutím je nutno se podívat, kam vede



  - 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 VE SVÉ EMAILOVÉ SCHRÁNCE.

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, když si nevíte rady

Praktické ukázky

Praktické ukázky

Odpovědět Odpovědět všem Předat dál Rychlé zprávy

po 28. 4. 2014 10:59

Ambraa Jaroslav <debt@vlevy.cz>

Výše pohledávky na vašem účtu #1151215389217520

Komu [redacted]

Zpráva smlouva_943140E481F1215A.zip (24 kB)

Vážený zákazníku,

Jsme velmi rádi, že jste vyuziváli produktu z naší banky.
Dovolujéme Vás upozornit, že k 25.04.2014 dlužné částky na osobní účet ve vysi #1151215389217520 8438.92 Kč. Nabízíme vám dobrovolně uhradit pohledávku v plné výši do 16.05.2014.

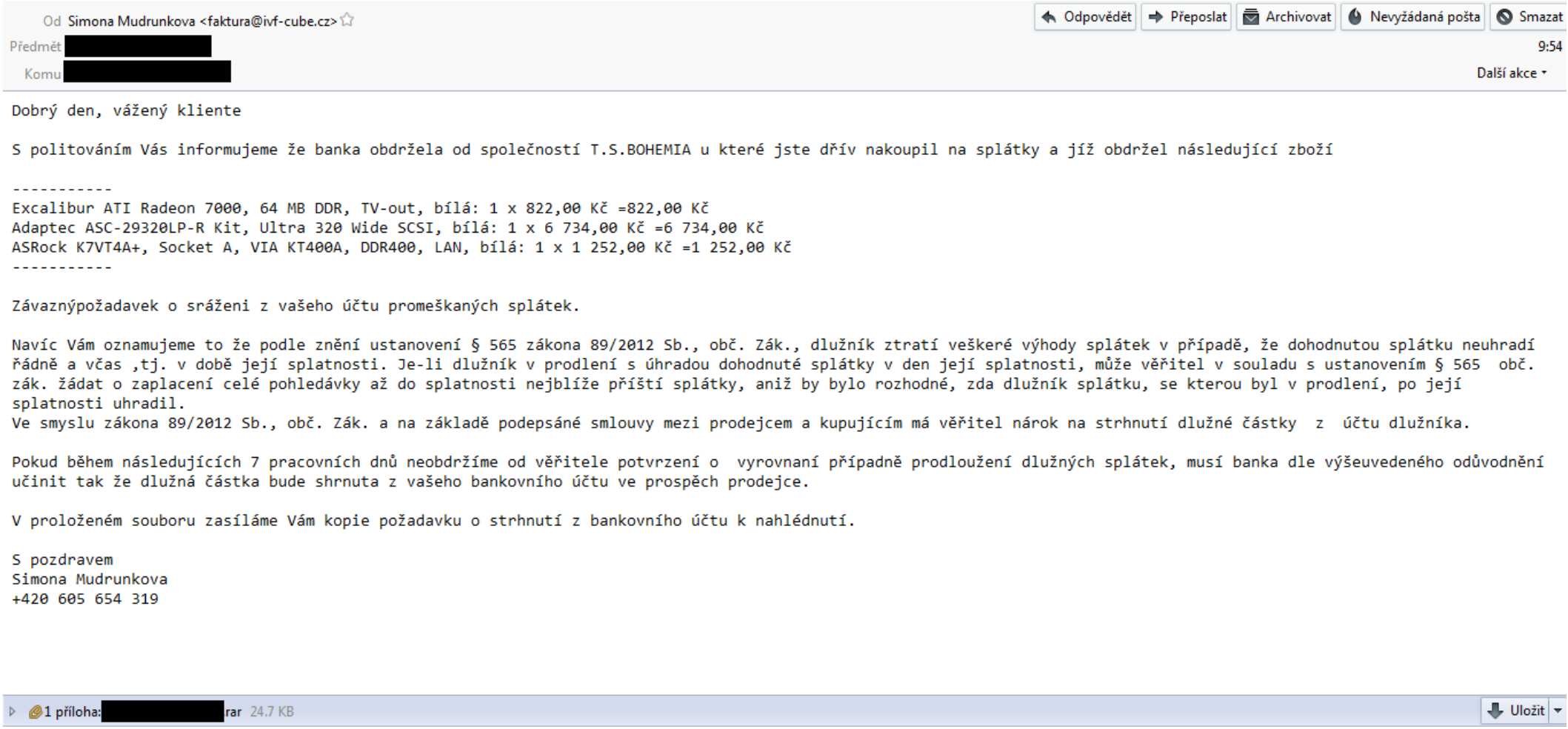
Dobrovolné uhrazeni pohledávky a dodrženi smlouvy #943140E481F1215A umožňuje Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení uhrady pohledávky 8438.92 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základe pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_943140E481F1215A.zip"

S pozdravem,
Vedoucí odboru vymahani pohledávek
Ambraa Jaroslav
+420 602 730 232

Praktické ukázky



Od Simona Mudrunkova <faktura@ivf-cube.cz>
Předmět [redacted]
Komu [redacted]

Odpovědět | Přeposlat | Archivovat | Nevyžádaná pošta | Smazat
9:54
Další akce

Dobrý den, vážený kliente

S politováním Vás informujeme že banka obdržela od společností T.S.BOHEMIA u které jste dřív nakoupil na splátky a jíž obdržel následující zboží

Excalibur ATI Radeon 7000, 64 MB DDR, TV-out, bílá: 1 x 822,00 Kč =822,00 Kč
Adaptec ASC-29320LP-R Kit, Ultra 320 Wide SCSI, bílá: 1 x 6 734,00 Kč =6 734,00 Kč
ASRock K7VT4A+, Socket A, VIA KT400A, DDR400, LAN, bílá: 1 x 1 252,00 Kč =1 252,00 Kč

Závaznýpožadavek o sráženi z vašeho účtu promeškaných splátek.

Navíc Vám oznamujeme to že podle znění ustanovení § 565 zákona 89/2012 Sb., obč. Zák., dlužník ztratí veškeré výhody splátek v případě, že dohodnutou splátku neuhradí řádně a včas ,tj. v době její splatnosti. Je-li dlužník v prodlení s úhradou dohodnuté splátky v den její splatnosti, může věřitel v souladu s ustanovením § 565 obč. zák. žádat o zaplacení celé pohledávky až do splatnosti nejblíže příští splátky, aniž by bylo rozhodné, zda dlužník splátku, se kterou byl v prodlení, po její splatnosti uhradil.
Ve smyslu zákona 89/2012 Sb., obč. Zák. a na základě podepsáné smlouvy mezi prodejcem a kupujícím má věřitel nárok na strhnutí dlužné částky z účtu dlužníka.

Pokud během následujících 7 pracovních dnů neobdržíme od věřitele potvrzení o vyrovnaní případně prodloužení dlužných splátek, musí banka dle výšeuvedeného odůvodnění učinit tak že dlužná částka bude shrnuta z vašeho bankovního účtu ve prospěch prodejce.

V proloženém souboru zasíláme Vám kopie požadavku o strhnutí z bankovního účtu k nahlédnutí.

S pozdravem
Simona Mudrunkova
+420 605 654 319

1 příloha: [redacted].rar 24.7 KB
Uložit

Praktické ukázky

Předmět: [redacted] Informace o Vaši zásilce
Datum: Thu, 27 Nov 2014 09:28:50 +0100
Od: Ceská pošta <tracktrace@cs-post24.com>
Společnost: cs-post24.com
Komu: [redacted].zcu.cz>

logo

[redacted]

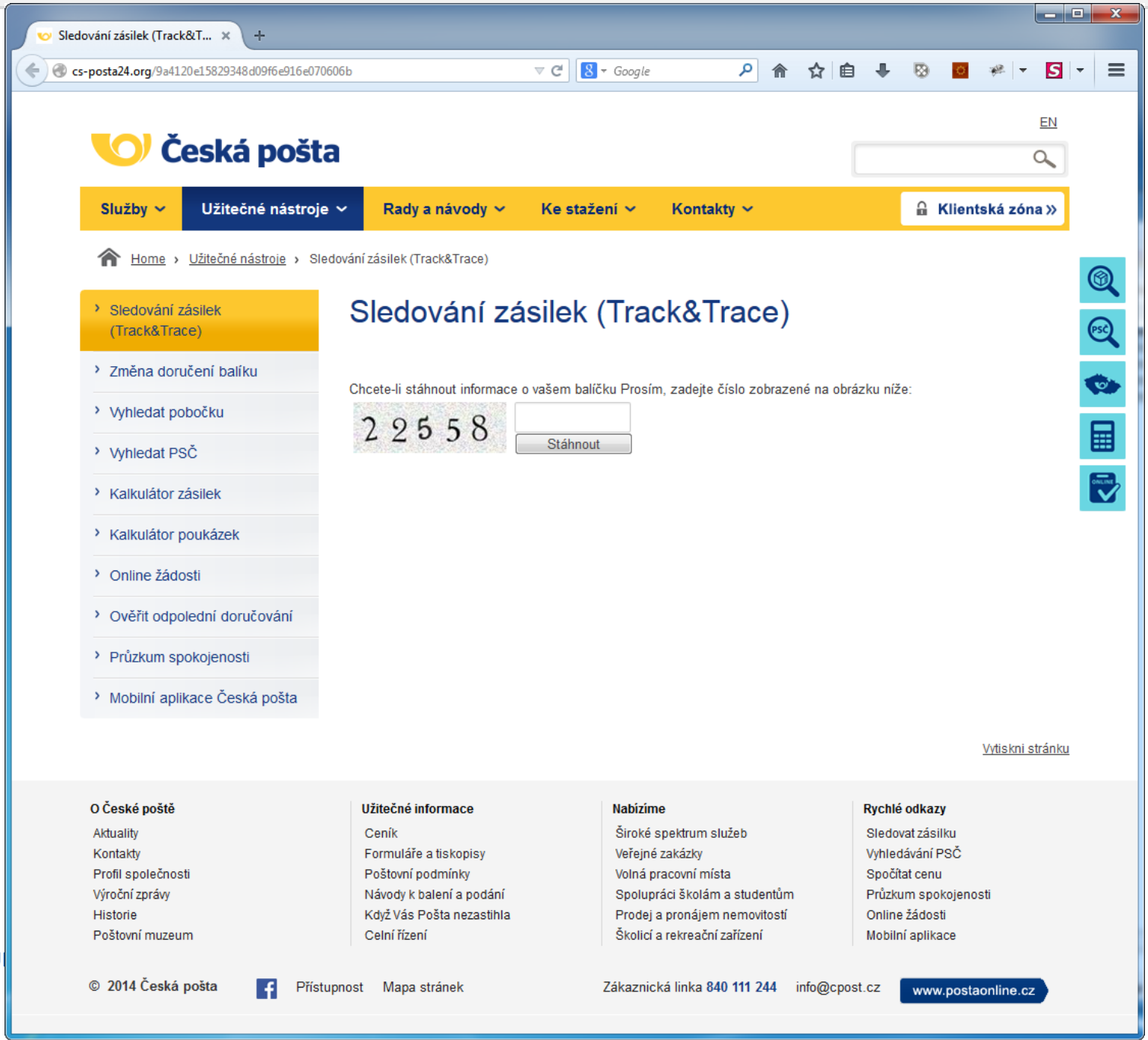
Vaše zásilka ***DR631396851C*** dorazila na 24. listopadu 2014. Courier nebyl schopen doru`eit zásilku pro vás. Vytisknout informace o Vaší zásilky a ukázat, že v nejbližší pošt`i, aby si zásilku.

Stáhn`ite si informace o zásilka
<http://cs-post24.com/service.php?id=027364718>

Pokud je zásilka neobdrží do 15 pracovních dn`u `Eeská pošta bude mít právo nárokovat odškodn`iní od si pro své udržení ve výši 52,5 K`e za každý den vedení.
M`užete si najít informace o postupu a podmínkách poi pozemku chov v nejbližší kanceláoi.

Toto je generován automaticky zprávu, pokud nechcete poijímat zprávy od nás prosím odhlásit <http://cs-post24.com/unsubscribe.php?id=625568844>

Praktické ukázky



ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

Děkuji za pozornost

Jiří Čepák / cepakj@civ.zcu.cz