Inovace bakalářského studijního oboru Aplikovaná chemie

http://aplchem.upol.cz

CZ.1.07/2.2.00/15.0247

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Internet a zdroje

Elektronická pošta a její správa, bezpečnost

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
OKRESNÍ HOSPODÁŘSKÁ KOMORA OLOMOUC
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Úvod

- Elektronická pošta (**e-mail**) → internetový komunikační systém založený na protokolu **SMTP**
- Historie
  - Vznik v roce 1962 (aplikace starší než Internet!)
  - 1965 → První využití → komunikace mezi uživateli Mainframového počítace → MIT (systémy Q32, SDC)
  - 1966 → Síťový e-mail (Systém AUTODIN)
  - 1969 → ARPANET
  - 1972 → zavedení @

Technické zázemí

Výměna zpráv pomocí programu MTA (MUA)

↓

protokolem **SMTP** (**S**imple **M**ail **T**ransfer **P**rotokol)

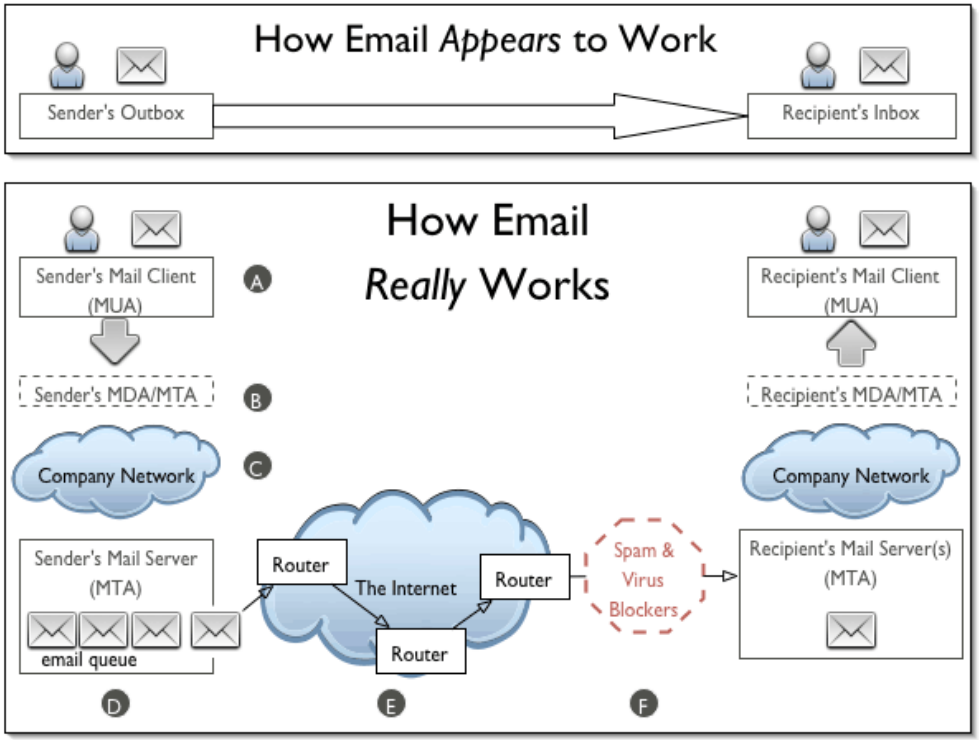
↓

Stahování zpráv z poštovního serveru pomocí **POP** × **IMAP**

↓

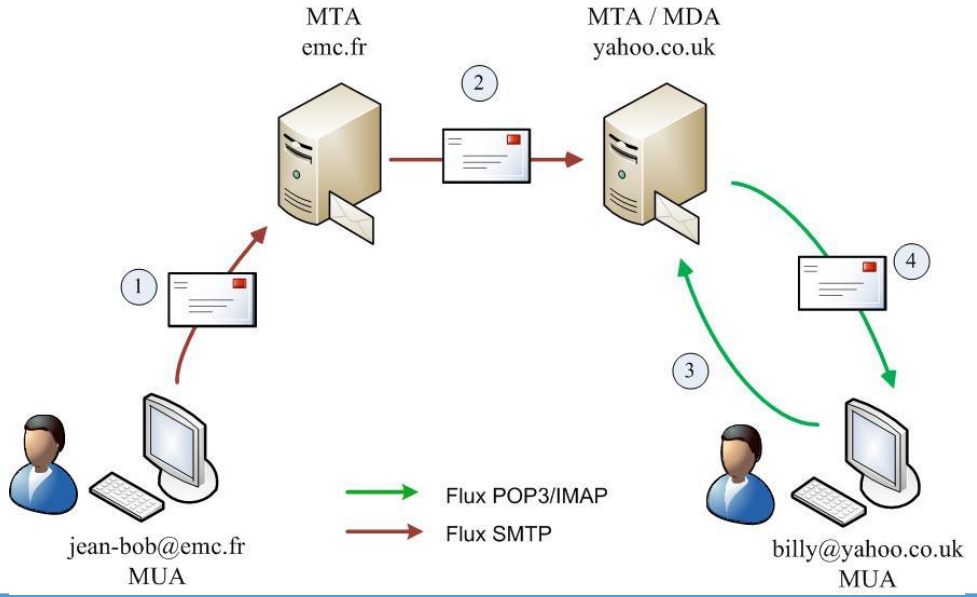
Prohlížení mailu

mailový klient vs. **web**



SMTP – Simple Mail Transfer Protocol

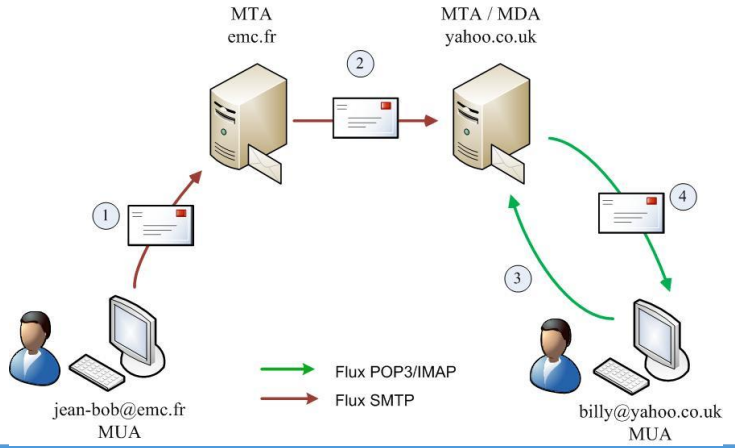
- Protokol určený pro přenos e-mailů mezi přepravci elektronické pošty (**MTA**)
- Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem
- Zpráva je doručena do poštovní schránky adresáta, ke které potom může uživatel kdykoli (off-line) přistupovat (vybírat zprávy) pomocí protokolů **POP3** nebo **IMAP**



MTA, MDA, MUA...

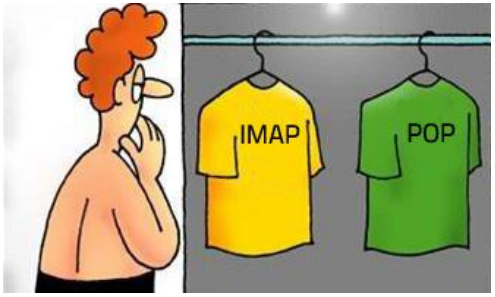
Architektura pošty

- **MUA** – Mail User Agent, poštovní klient, který zpracovává zprávy u uživatele
- **MTA** – Mail Transfer Agent, server, který se stará o doručování zprávy na cílový systém adresáta
- **MDA** – Mail Delivery Agent, program pro lokální doručování, který umísťuje zprávy do uživatelských schránek, případně je může přímo automaticky zpracovávat (ukládat přílohy, odpovídat, spouštět různé aplikace pro zpracování apod.)



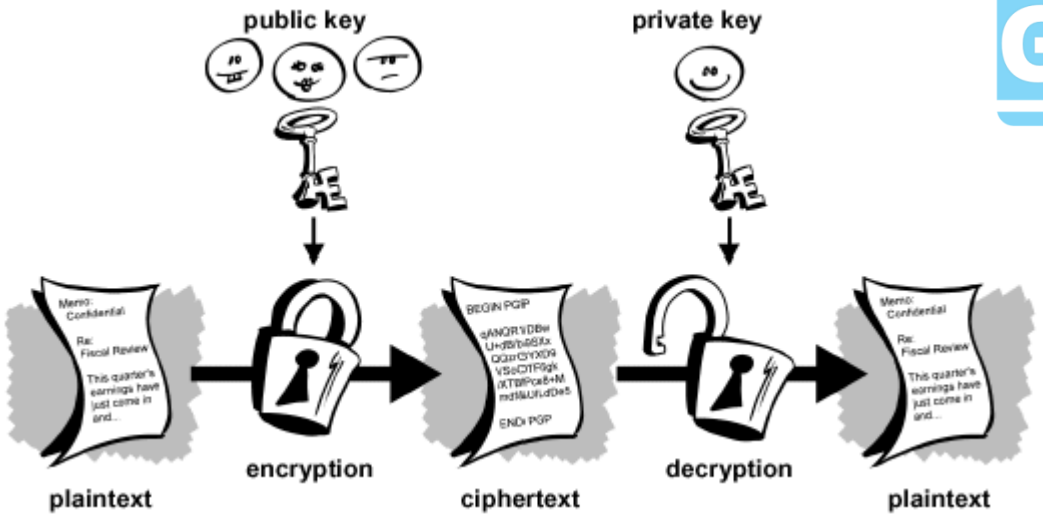
POP3 vs. IMAP

- **POP3** (**P**ost **O**ffice **P**rotocol version **3**)
  - Pracuje pouze v **off-line** režimu (port 110)
  - Protokol POP3 dovoluje připojení pouze jednoho uživatele ke schránce
- **IMAP** (**I**nternet **M**essage **A**ccess **P**rotocol)
  - umí pracovat v tzv. **on-line** i **off-line** režimu (port 143)
  - pokročilé možnosti vzdálené správy (práce se složkami apod.)
  - IMAP dovoluje současné připojení více uživatelů k jedné schránce
  - využití příznaků → přehled o stavu zprávy (jestli byla přečtena, smazána atd.)
  - podpora více schránek na serveru



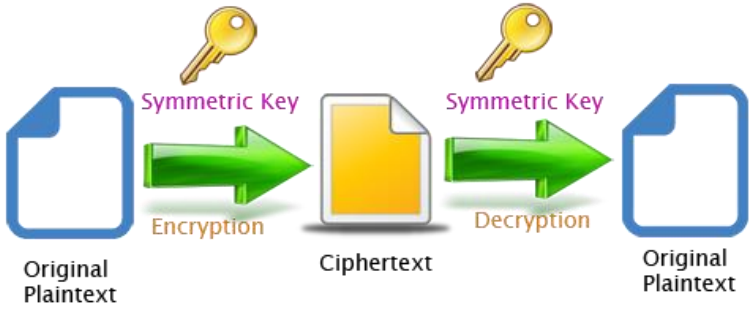
E-mail a bezpečnost

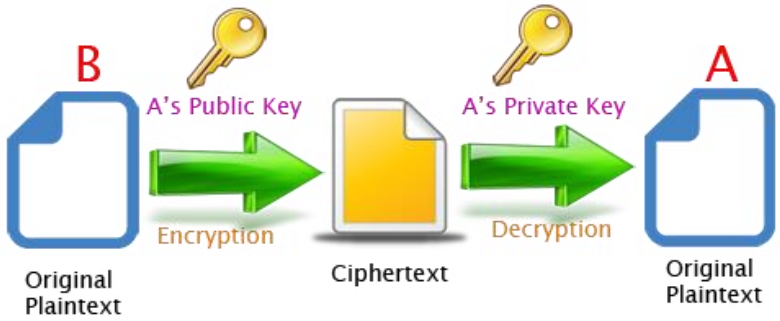
- e-mailové zprávy obecně nejsou šifrované
- Nutnost tvorby kopií e-mailů + Nutnost zapojení šifrování
  - **S/MIME**
  - **PEM**
  - **PGP**
  - **GPG**
  - TLS (SSL)
  - VPN
  - TOR



S/MIME, PEM, PGP, GPG

- **S/MIME (Secure/Multipurpose Internet Mail Extensions)**
  - Šifrování zpráv + digitální podpis
  - Obsah zprávy – symetrická šifra
  - Klíč se následně šifruje asymetricky
  - Autentizace: otisk zprávy + digitální podpis
- **PEM (Privacy-Enhanced Mail)**
  - Obsah zprávy – symetrická šifra
  - Klíč se následně šifruje asymetricky
- **PGP (Pretty Good Privacy)**
  - Obsah zprávy – symetrická bloková šifra (náhodně generovaný klíč: 128 bit)
  - Klíč se následně šifruje asymetricky
  - Autentizace: digitální podpis
- **GPG (GNU Privacy Guard)**
  - Open alternativa k PGP

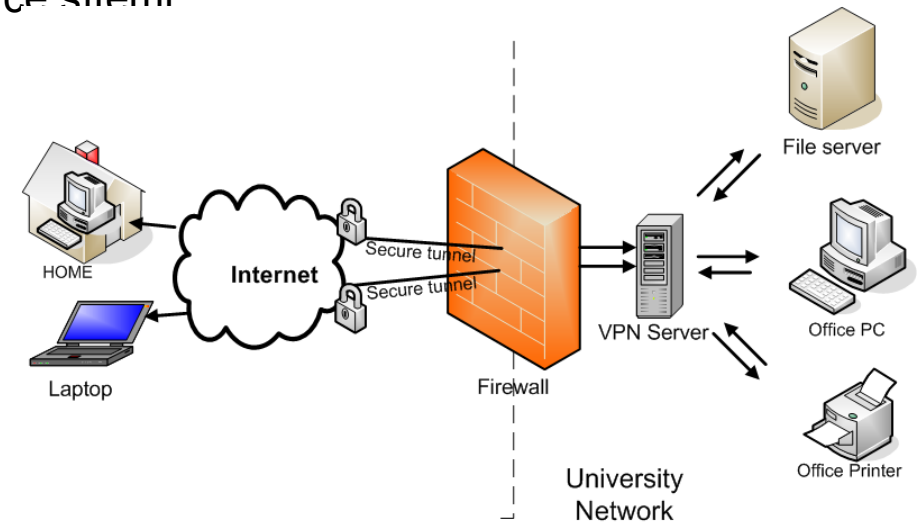




VPN

VPN (virtual private network)

- Propojení PC prostřednictvím nedůvěryhodné sítě (Internet)
  - bezpečné spojení mezi dvěma či více sítěmi
- využití dig. podpisů + šifrování



Aplikace:

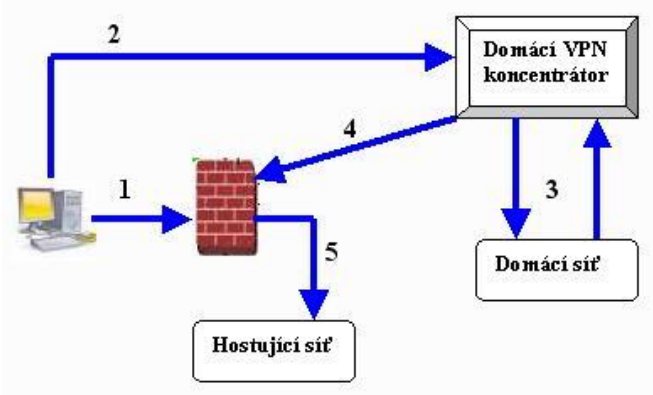
1. Zprovoznit VPN server
2. Připojit PC k Internetu
3. Připojit klienty k VPN serveru

Úloha VPN serveru:

1. Síťová brána (zprostředkovává spojení)
2. Šifrování komunikace

Princip fungování:

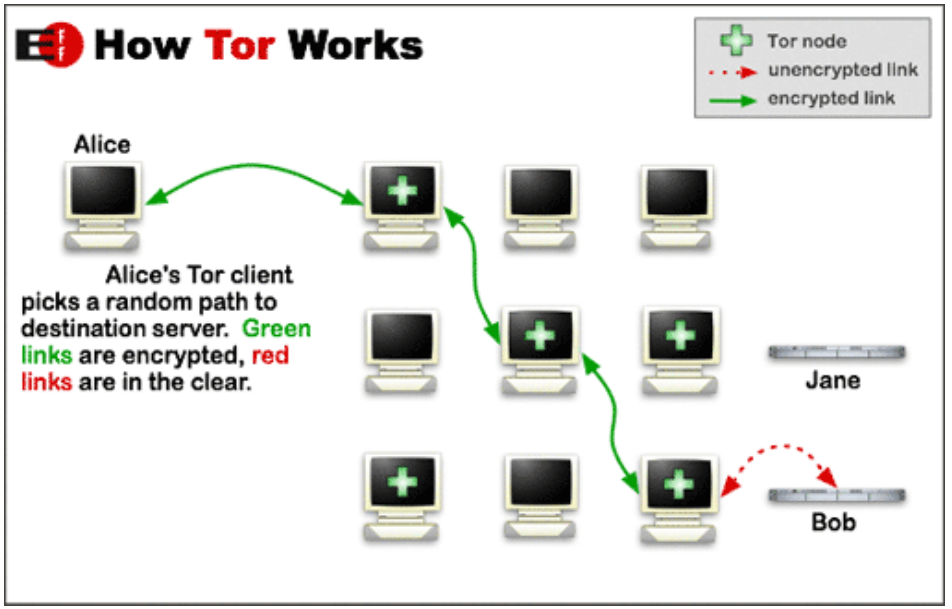
1. Uživatele blokuje firewall
2. proto se hlásí na Domácí VPN koncentrátor
3. Který ověří jeho důvěryhodnost (domácí síť)
4. Pokud je známý, povolí komunikaci
5. A konečně se může připojit do hostující sítě

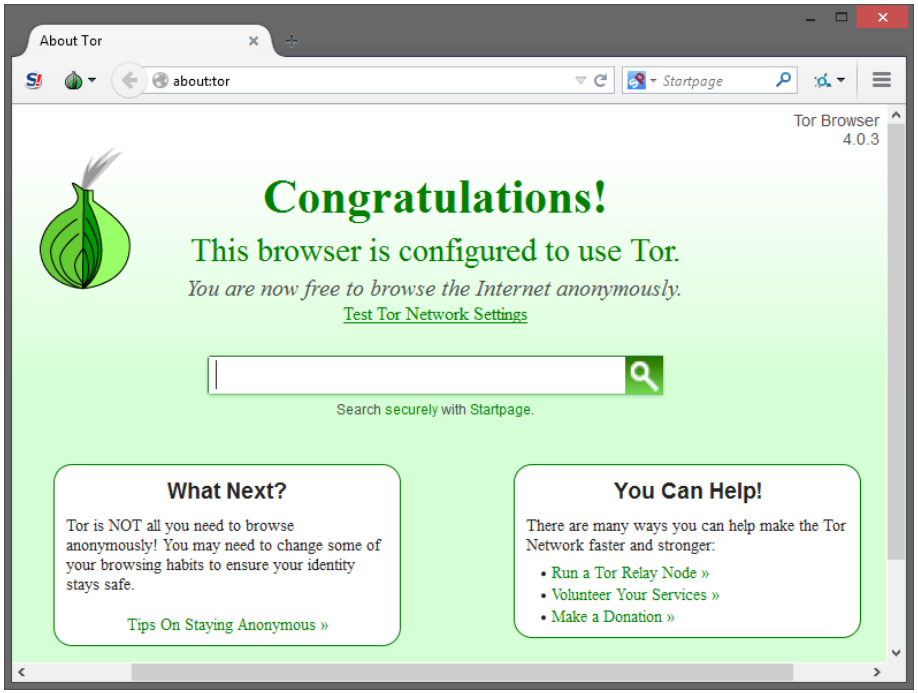


TOR

TOR (**T**he **O**nion **R**outing)

- Softwarový systém zajišťující anonymitu
- Open Source
- Ochrana osobních údajů
- Ochrana obchodní aktivit





Bezpečnostní rizika

- **Spam, Scam, Phishing, Hoaxy**
  - **Scam 419** – Nigerijské dopisy (podvody s převodem peněz)
  - **Spam** = nevyžádaná reklamní pošta (přetěžování serverů)
  - **Phishing** = internetový podvod (př. snaha získat přístup k bankovním účtům)
    - Příklady:
      - Facebook – podvodná žádost o přátelství
      - Překročení kóty e-mailu
      - Bankovní zprávy
  - **Hoax** = nesmyslné a poplašné zprávy putující Internetem
    - http://www.hoax.cz/cze/

- **Nigerijské dopisy:**

Salutations,

I am Vicky Stamatis the wife of the former Minister of Defense, Akis Tsochatzopoulos. I have been thrown into a state of utter confusion, frustration and hopelessness following the recent imprisonment of my husband.

On March 4th this year, my husband was sentenced to eight years in prison and since then, I have been living a life of no hope. I have been subjected to psychological torture and I have been abandoned by people who were our family friends when my husband was a free man, people that we trusted.

I have lost confidence in everybody here in Greece for the way my husband was treated after devotedly serving the country for over two decades and where the people that pretended to be loyal to my husband have now abandoned us.

Various huge sums of money deposited by my husband in different banks and firms abroad have been traced and confiscated; some companies willingly gave up their secrets, disclosing our monetary transactions with them for robust reward from the Greek government. In fact lots of cash deposits and properties have been seized from us by the Greek government and they are not relenting in their effort in making me and my family poor for life. This is purely a political witch hunting to bring my husband and our family down.

There is a certain amount of money kept securely by my husband in Europe in my name and I am the only person that is privy to the location. I am writing to you out of desperation and I want you to assist me in moving this money out of its present location to anywhere you deem safe for a percentage.

I repose great confidence in you hence my approach to you through email. I cannot afford to do anything on my own, so, I decided to contact someone who is not in any way connected to my family. I will give you more information as to this regard as soon as you reply.

I will appreciate your timely and favourable response.

Best Regards,
Vicky Stamatis

Bezpečnostní rizika

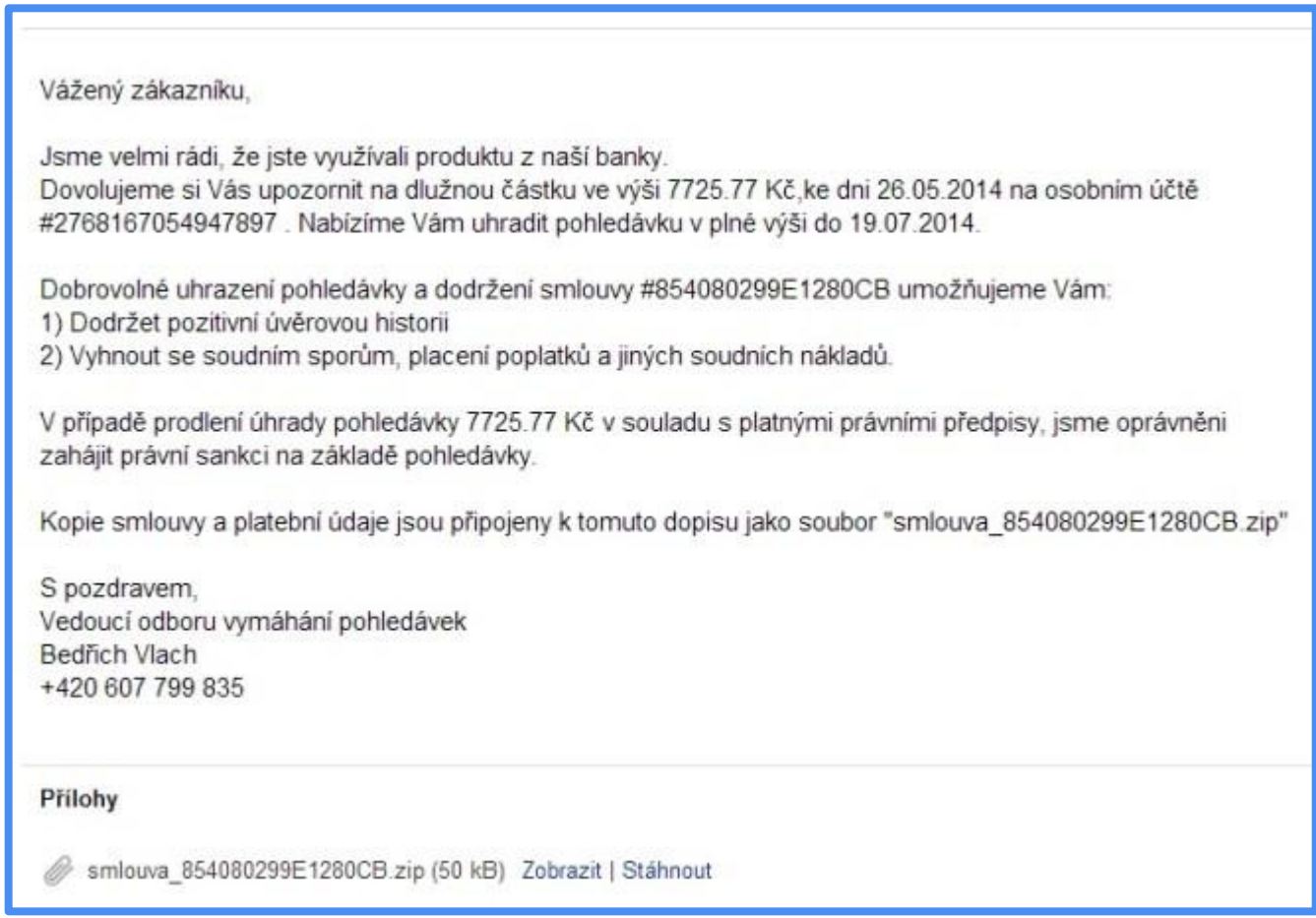
Policejní virus

- Využití JavaScriptu
- Platforma
  - Windows
  - Linux
  - OS X
- Obrana:

  Vymazání cash a cookies

Bezpečnostní rizika – exekuční příkaz

- **Výše pohledávky na vašem účtu…**
- Příloha emailu
- Platforma
  - Windows



Vážený zákazníku,

Jsme velmi rádi, že jste využívali produktu z naší banky.
Dovolujeme si Vás upozornit na dlužnou částku ve výši 7725.77 Kč,ke dni 26.05.2014 na osobním účtě #2768167054947897 . Nabízíme Vám uhradit pohledávku v plné výši do 19.07.2014.

Dobrovolné uhrazení pohledávky a dodržení smlouvy #854080299E1280CB umožňujeme Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení úhrady pohledávky 7725.77 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základě pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_854080299E1280CB.zip"

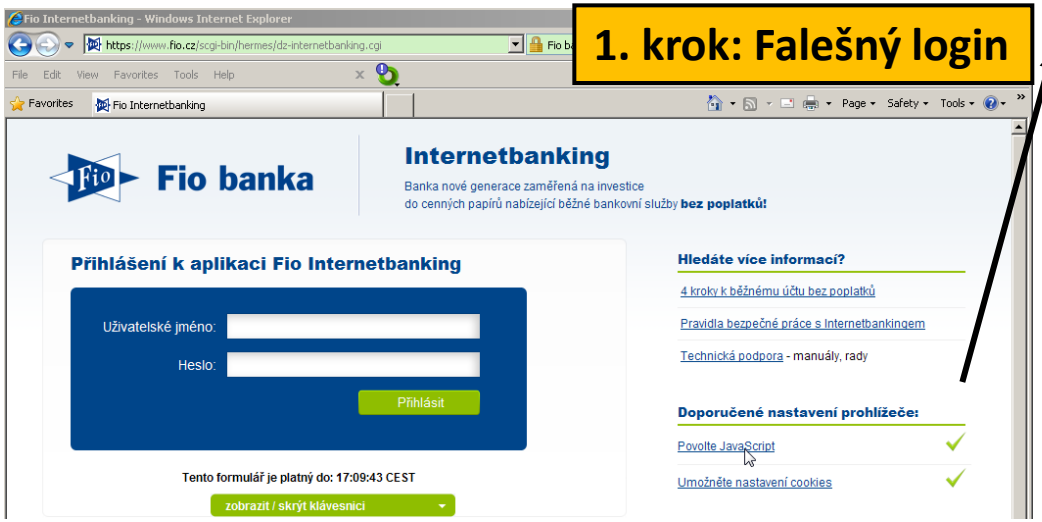
S pozdravem,
Vedoucí odboru vymáhání pohledávek
Bedřich Vlach
+420 607 799 835

Přílohy

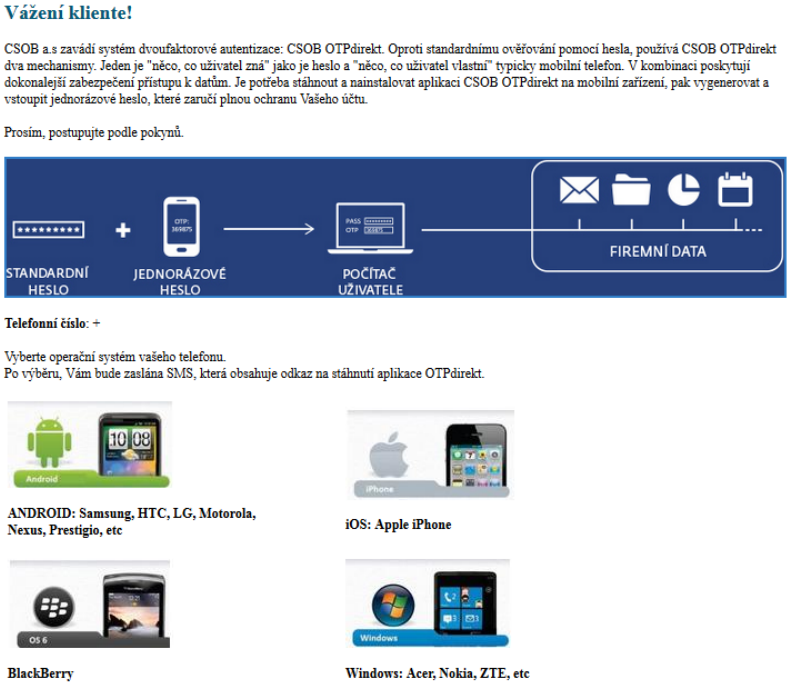
smlouva_854080299E1280CB.zip (50 kB) Zobrazit | Stáhnout

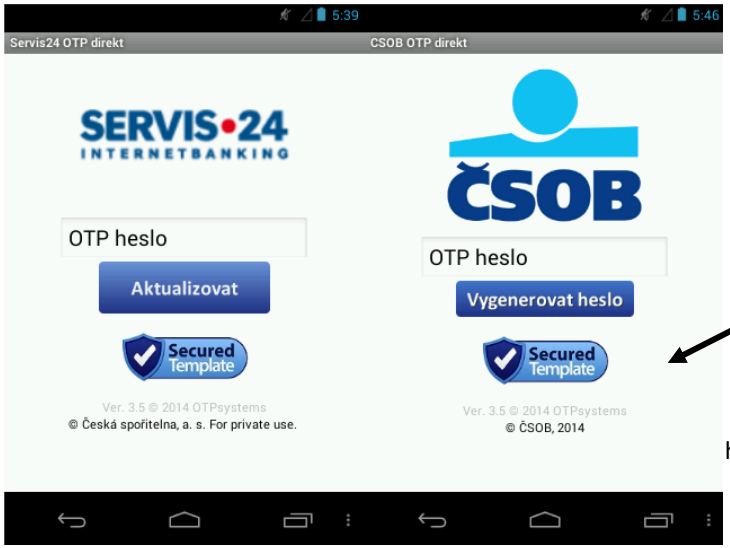
Win32/TrojanDownloader.Tiny.NKK, Win32/Tinba.AX Trojan ⇨ Zbot, Win32/Injector.BSCO

- **Co se děje při otevření přílohy?**
- Po spuštění .exe souboru instalace Win32/Tinba.AX Trojan
- Specializace na uživatele České spořitelny, ČSOB, Era a Fio banky



1. krok: Falešný login



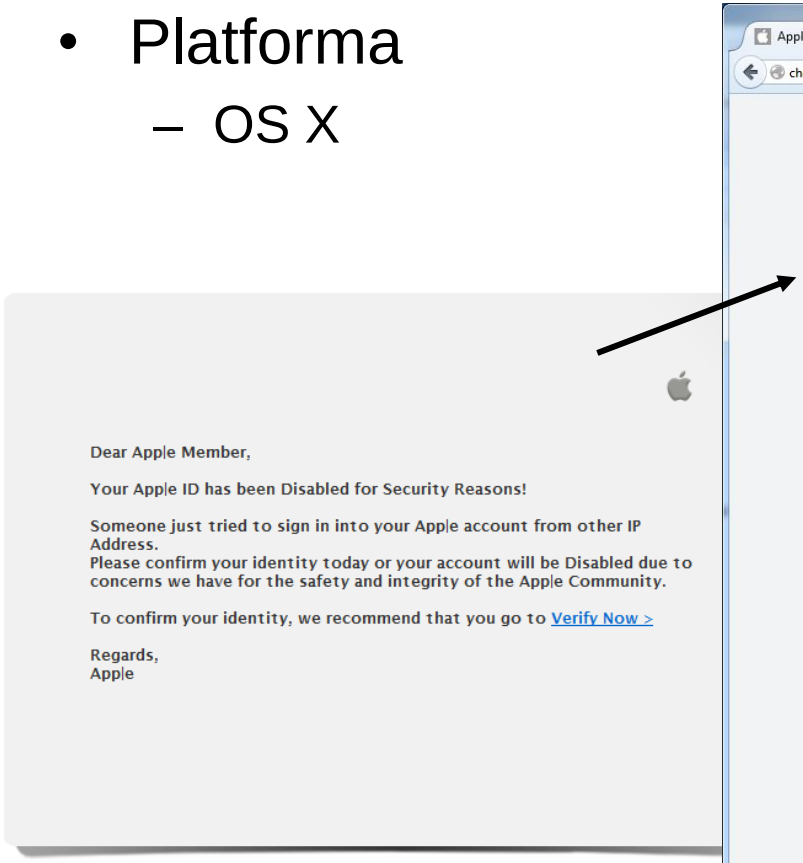


2. krok: Dvoufaktorová autentizace OTPdirekt = přímá cesta do pekla

http://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/

Bezpečnostní rizika

- **Zablokování Apple ID účtu**
- Platforma
  - OS X



Dear Apple Member,

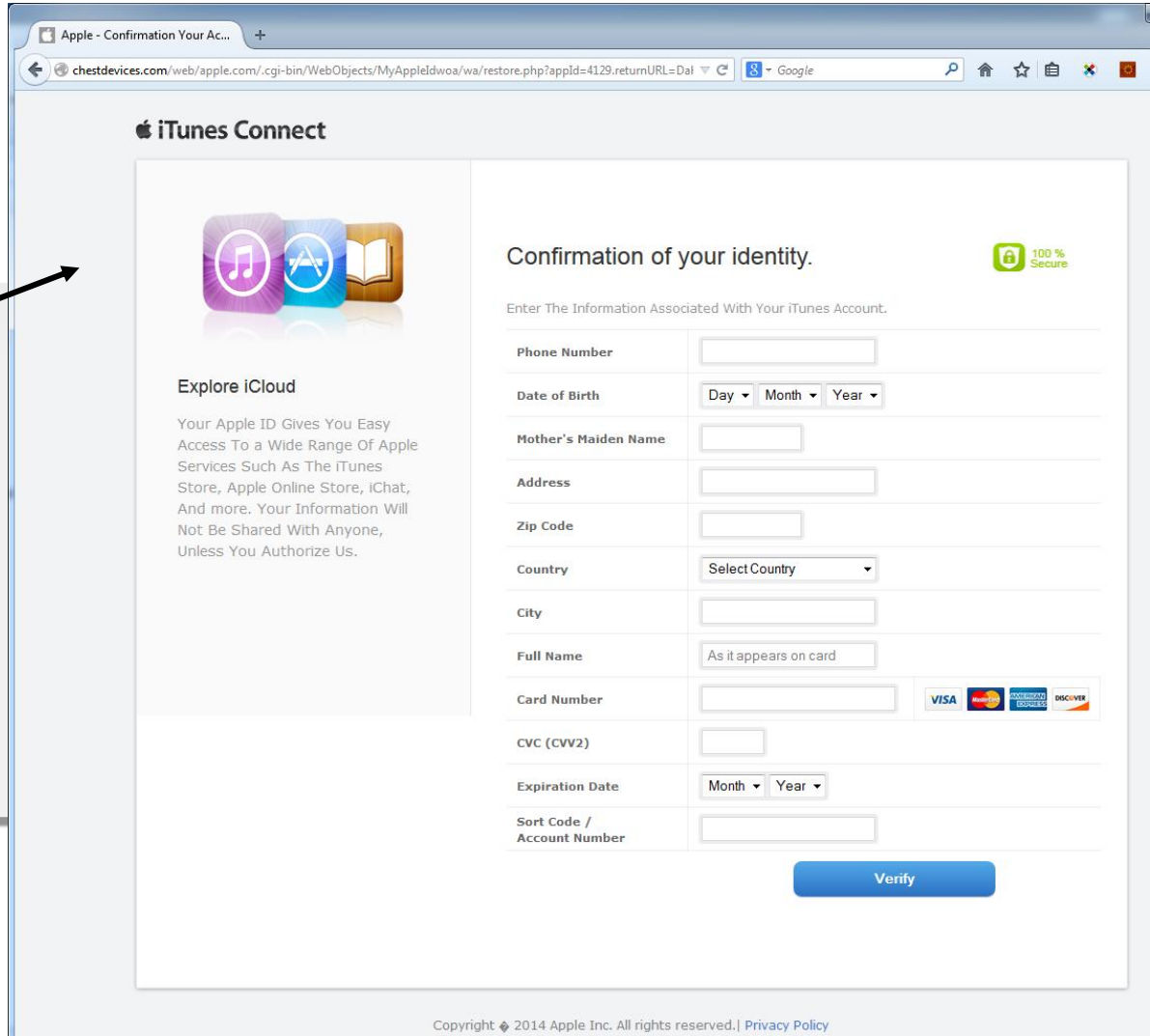
Your Apple ID has been Disabled for Security Reasons!

Someone just tried to sign in into your Apple account from other IP Address.
Please confirm your identity today or your account will be Disabled due to concerns we have for the safety and integrity of the Apple Community.

To confirm your identity, we recommend that you go to Verify Now >

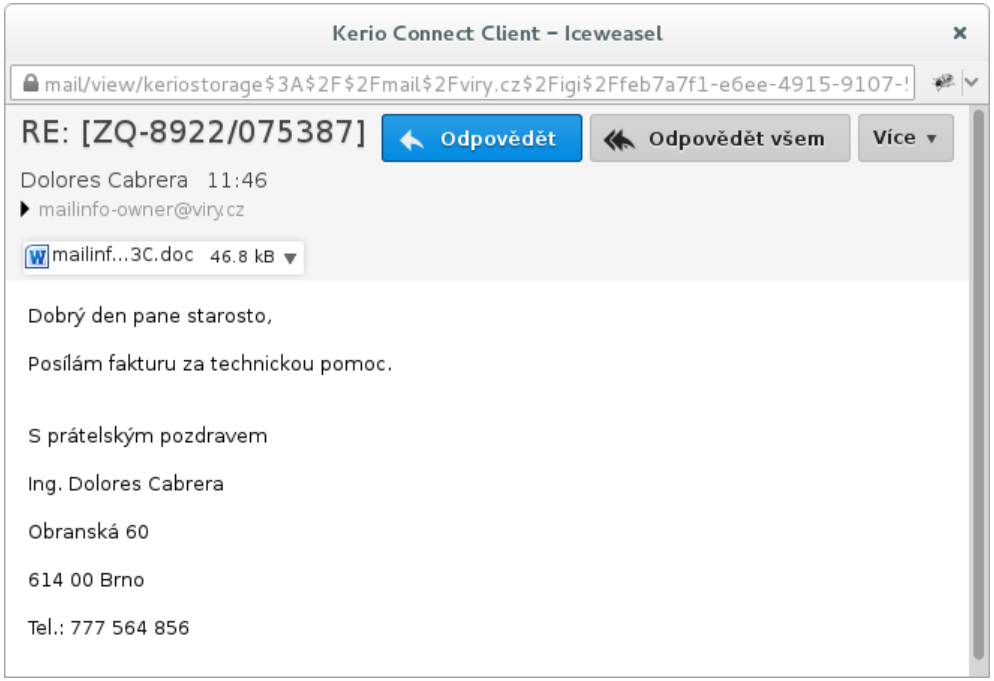
Regards,
Apple

TM and Copyright 2014 Apple Inc. 1 Infinite Loop, MS 96-DM, Cupertino, CA 95014, USA.
All rights reserved / Keep Informed / Privacy Policy / My Apple ID



Bezpečnostní rizika

- **Falešná faktura**
- Platforma
  - MS Windows
- Makrovirus (AutoOpen) → downloader: **Win32/Dridex (bankovní trojan)**



Bezpečnostní rizika

- **Droga Krokodil pohltila celé Česko a Slovensko! VIDEO ZDE!**
- Forma Clickjackingu
- Obrana: forma pluginu, např. FireFox ⇨ Clickjacking Reveal

Bezpečnostní rizika – sociální sítě

- **Heslo přes e-mail nikdy neobnovujte!**
- Podvodná zpráva vyzývající k resetu hesla z důvodu bezpečnosti → instalace trojského koně `Bredolab`
- Červ `Koobface` → stránky podobné YouTube → výzva k instalaci doplňku pro přehrání videa

Zásady bezpečnosti na sociálních sítích:

1. Uvádět o sobě jen nezbytné informace
2. Kontrola toho, kdo se může na co dívat
3. Používat jen prověřené aplikace

Bezpečnostní rizika – Facebook

- Vysoká koncentrace osobních údajů
- Absence mechanismů ověřování pravosti identity
- Problematická pravidla používání Facebooku
  - Práva na uploadovaný materiál
- Neexistence obchodního zastoupení
- Problematické blokace
- Nové funkce automaticky aktivní
- Nemožnost dokonalého smazání účtu
- Časté aktualizace licenčních podmínek a pravidel užívání služby

DESET DŮVODŮ, PROČ ODEJÍT Z FACEBOOKU:
http://www.root.cz/clanky/deset-duvodu-proc-odejit-z-facebooku/