Základy bezpečného chování na Internetu, aneb jak se nenechat odposlouchávat

Viktor Ferus – WEBnet Incident Response Team

ferusvi@civ.zcu.cz
www.viktor-ferus.cz

Centrum Informatizace a výpočetní techniky

Motivace, aneb já nemám, co skrývat

- Časté reakce při debatách o bezpečnosti - „Já nemám, co skrývat, já s žádnými tajnými daty nedělám.“
  - A používáte Facebook / Instagram / WhatsApp / Signal…?
  - Co by se stalo, pokud by se Vašeho účtu zmocnil někdo, u koho byste si to rozhodně nepřáli?
    - Zveřejnění posměšného statusu je jen to nejmenší.
- Kybernetická bezpečnost se týká každého uživatele Internetu.

Základy

- Silná a unikátní hesla,
- šifrování,
- používání VPN,
- …ale především rozum. ☺

Hesla

Heslo

- Klíč k Vaší online identitě
  - Znalostí hesla prokazuji službě, že „já jsem já“ a že mi může zpřístupnit údaje, které jsou jen pro mě
- Kdo jej získá, může se za Vás vydávat
- Je zapotřebí si jej chránit „jako oko v hlavě“

Silná hesla

- Mluví se o nich již od nepaměti
- Doporučená podoba se v průběhu času mění v souvislosti s běžně dostupným výkonem počítačů
- Osmiznaková hesla dnes již nejsou považována za bezpečná, minimum je dnes 12 znaků
  - Dobrá jsou tzv. **frázová hesla,** např.: „trhat.fialky.BOOM.dynamitem“
  - Nejlepší jsou hesla typu **$kLKC{~A<BXh42:{**, ty si lze ale jen těžce pamatovat
- Do každé služby by mělo být jiné (unikátní) heslo

Správci hesel

- Programy, jež v šifrované podobě uchovávají Vaše hesla
  - Přistupujete k nim pomocí tzv. **master password**, jediného hesla, které si musíte pamatovat
- Umožňují používat do každé služby jiné (komplikované) heslo bez nutnosti si je všechny pamatovat
- Často umožňují i generování velmi silných hesel
- Správci hesel v prohlížečích nebývají nejspolehlivější
- Dobrý je **KeePass**, ten je ale celkem „old-school“ ☻
- Populární je také **LastPass**
- **Dobrý správce hesel je open-source!**

Správci hesel

Pro

- Do každé služby je jiné heslo
- Hesla mohou být velmi silná bez nutnosti pamatování
- Uchování dat v bezpečně zašifrovaném souboru

Proti

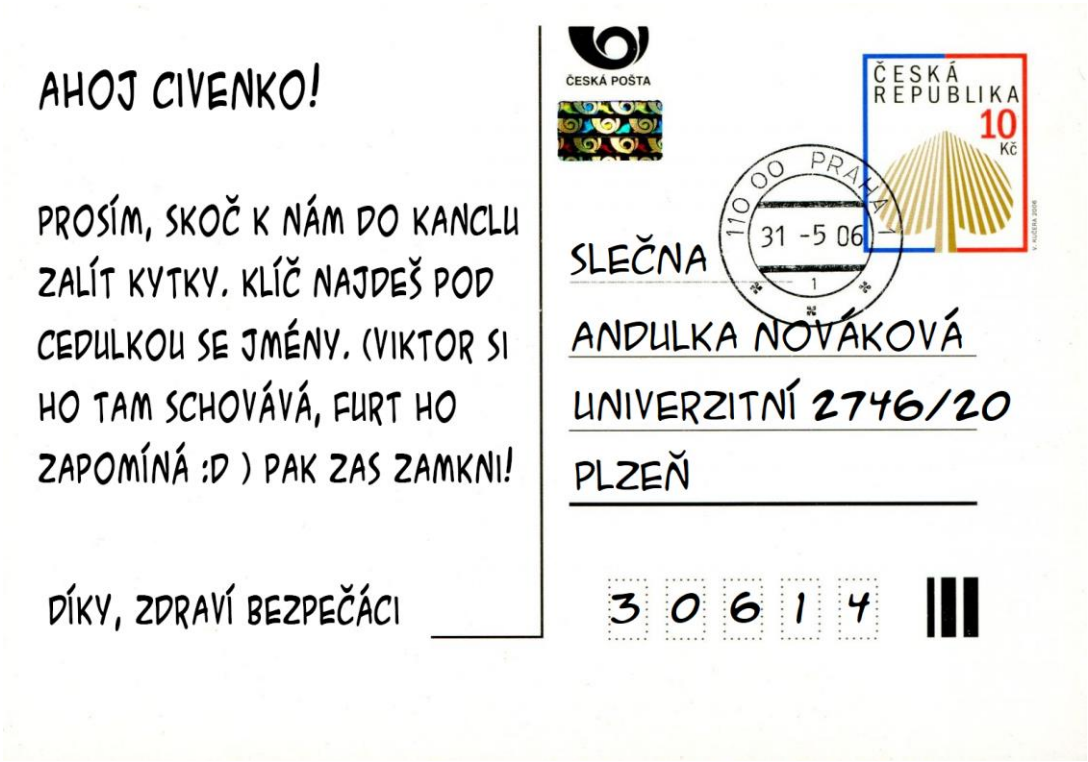
- Dáváte „všechna vajíčka do jednoho košíku“ – kdo zjistí master password, ten má přístup ke **všem heslům!**
  - Do nejkritičtějších služeb (E-mail, Facebook, bankovnictví) si hesla stále noste v hlavě.
- Mírné snížení uživatelského komfortu – nutnost instalace dalšího SW a interakce s ním.

Šifrování

„Dance like no one is watching. Encrypt like everyone is.“

Šifrování

- Silné heslo je důležité, ale schováním do správce hesel jeho ochrana nekončí.
- Odesláním hesla přes nešifrovaný protokol jej prakticky dáváme k dispozici každému, kdo se k datům po cestě Internetem dostane.
- Poslali byste snad takovou pohlednici…?

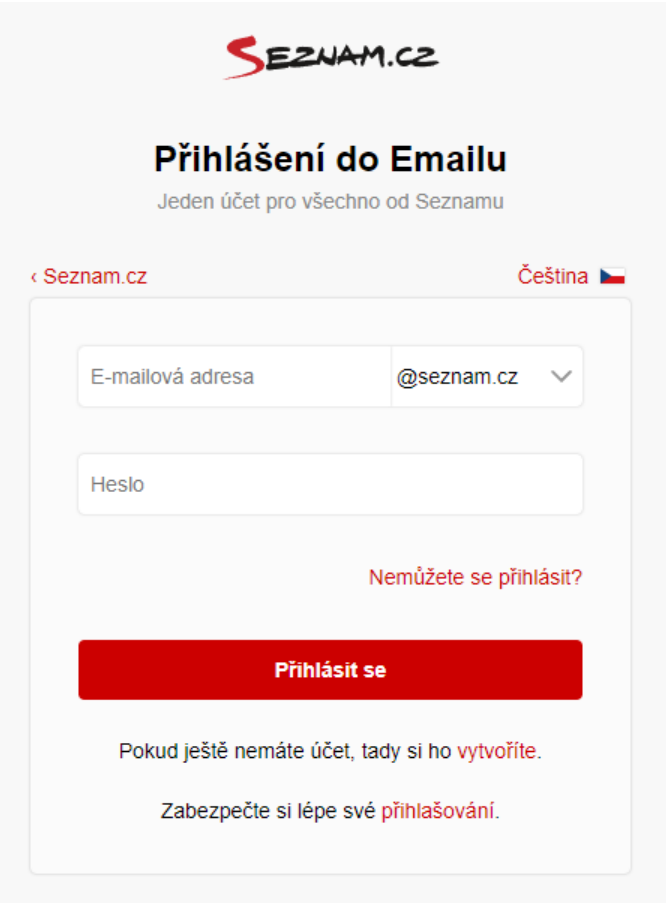


Šifrování

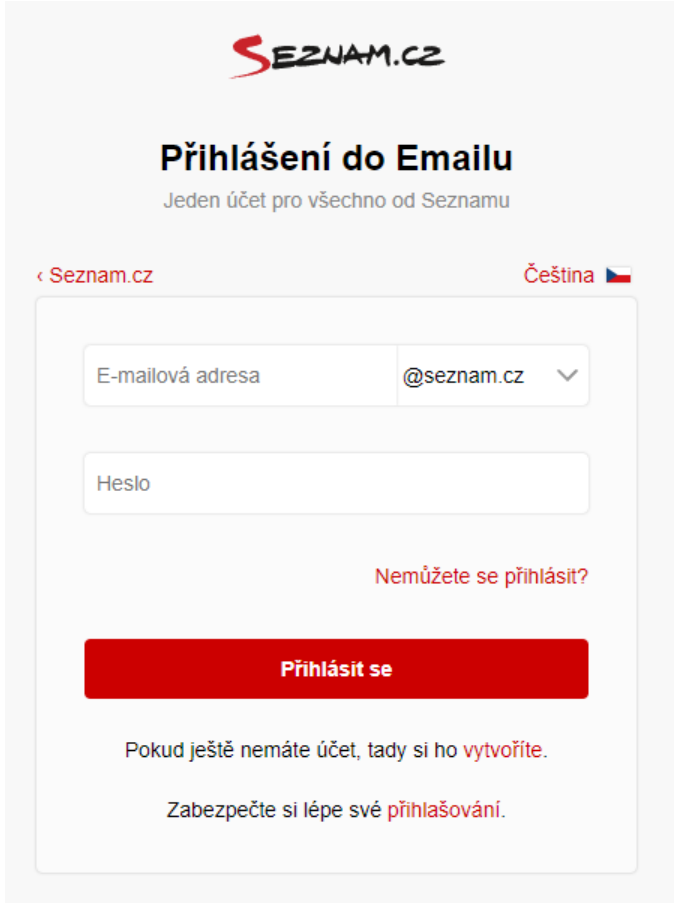
- = proces utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí. [Wiki]
- Dlouhá historie, vyvíjeno mj. zejména pro armádní účely
- Nejjednodušší je asi tzv. Caesarova šifra
  - *Klíč najdeš pod cedulkou se jmény.* => *Pqng seohix uth gihzqptz xi orisc.*
- V počítačích se dnes nejčastěji využívají šifrovací algoritmy **AES** a **RSA**, oba jsou využity při webové komunikaci přes **HTTPS**. *(HTTP over SSL)*

Šifrování

http://login.seznam.cz



https://login.seznam.cz



Šifrování

http://login.seznam.cz

```
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "username" = "pepik1997"
  > Form item: "password" = "tajneheslo"
  > Form item: "logon" = "Login"
```

```
0180  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm l,applic
0190  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
01a0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
01b0  71 3d 30 2e 39 2c 69 6d  61 67 65 2f 61 76 69 66   q=0.9,im age/avif
01c0  2c 69 6d 61 67 65 2f 77  65 62 70 2c 69 6d 61 67   ,image/w ebp,imag
01d0  65 2f 61 70 6e 67 2c 2a  2f 2a 3b 71 3d 30 2e 38   e/apng,* /*;q=0.8
01e0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 73 69 67   ,applica tion/sig
01f0  6e 65 64 2d 65 78 63 68  61 6e 67 65 3b 76 3d 62   ned-exch ange;v=b
0200  33 3b 71 3d 30 2e 39 0d  0a 52 65 66 65 72 65 72   3;q=0.9· ·Referer
0210  3a 20 68 74 74 70 3a 2f  2f 31 30 2e 31 30 39 2e   : http:/ /10.109.
0220  32 35 2e 32 2f 6c 6f 67  6f 6e 2f 4c 6f 67 6f 6e   25.2/log on/Logon
0230  52 70 6d 2e 68 74 6d 0d  0a 41 63 63 65 70 74 2d   Rpm.htm· ·Accept-
0240  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 20   Encoding : gzip,
0250  64 65 66 6c 61 74 65 0d  0a 41 63 63 65 70 74 2d   deflate· ·Accept-
0260  4c 61 6e 67 75 61 67 65  3a 20 63 73 2d 43 5a 2c   Language : cs-CZ,
0270  63 73 3b 71 3d 30 2e 39  0d 0a 0d 0a 75 73 65 72   cs;q=0.9 ····user
0280  6e 61 6d 65 3d 70 65 70  69 6b 31 39 39 37 26 70   name=pep ik1997&p
0290  61 73 73 77 6f 72 64 3d  74 61 6a 6e 65 68 65 73   assword= tajnehes
02a0  6c 6f 26 6c 6f 67 6f 6e  3d 4c 6f 67 69 6e         lo&logon =Login
```

https://login.seznam.cz

```
> Transmission Control Protocol, Src Port: 58489, Dst Port: 443, Seq: 698, Ack: 5098, Len
v Transport Layer Security
  v TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 931
      Encrypted Application Data: d12dac9da1e4be6e564ed4972b760a72ecb94b3e9440a8fd0004e6
      [Application Data Protocol: http-over-tls]
```

```
0020  4c 37 e4 79 01 bb 99 80  85 22 b1 6a 68 59 50 18   L7·y···· ·"·jhYP·
0030  04 02 32 ab 00 00 17 03  03 03 a3 d1 2d ac 9d a1   ··2····· ····-···
0040  e4 be 6e 56 4e d4 97 2b  76 0a 72 ec b9 4b 3e 94   ··nVN··+ v·r··K>·
0050  40 a8 fd 00 04 e0 4d a8  34 b7 41 7c fd 48 8b 14   @·····M· 4·A|·H··
0060  7d 93 d5 d4 c0 2c 63 dc  c9 91 ed 7d 82 48 08 46   }····,c· ···}·H·F
0070  a7 a2 c1 9a b5 17 a5 42  b4 b1 92 68 4d 48 05 79   ·······B ···hMH·y
0080  47 40 c8 a5 a0 2a 38 c9  99 89 5a 9d c6 60 9c 1a   G@···*8· ··Z··`··
0090  8f 7c 0a 49 ad 9c 41 fc  6e 10 4d d0 66 17 f0 9c   ·|·I··A· n·M·f···
00a0  39 6a 94 03 4b ca 2d 0f  d6 dd 8b c7 b8 02 59 db   9j··K·-· ·····Y·
00b0  84 e8 fd 0d 96 63 b5 ff  ef 38 6a ad 57 52 e6 1f   ·····c·· ·8j·WR··
00c0  e7 e6 cc 4f 7a 28 a7 c5  fe c2 ed 22 f7 c2 af 72   ···Oz(·· ···"···r
00d0  43 46 09 19 10 5e 27 94  34 b6 6a 31 de 43 bf 60   CF···^'· 4·j1·C·`
00e0  f1 58 bf 13 f0 1b 87 30  3c 77 91 2c f0 6c 19 a4   ·X·····0 <w·,·l··
00f0  0a f3 7e 62 db 34 46 a0  f8 04 43 92 dd 18 65 67   ··~b·4F· ··C···eg
0100  6b ec fc ff b9 53 50 8e  b8 85 6b 09 2f f3 be a3   k····SP· ··k·/···
0110  a8 be b7 e0 2e 96 12 35  07 97 88 31 af b1 80 d0   ····.··5 ···1····
0120  4e 50 8b 2c 37 79 41 3d  ef 5d 62 08 40 7e 3d a0   NP·,7yA= ·]b·@~=·
0130  e9 7d bb 48 be 8e 3b 73  db 28 c3 c5 78 10 97 08   ·}·H··;s ·(··x···
0140  8b 0b 03 d7 00 d2 0a b0  b8 4b 0a 22 a9 c2 d6 bd   ········ ·K·"····
0150  5c 0f 5f e5 aa 3f f9 7c  09 ee 87 b5 b0 12 b3 88   \·_··?·| ········
```

Co HTTPS zaručuje a co nikoliv?

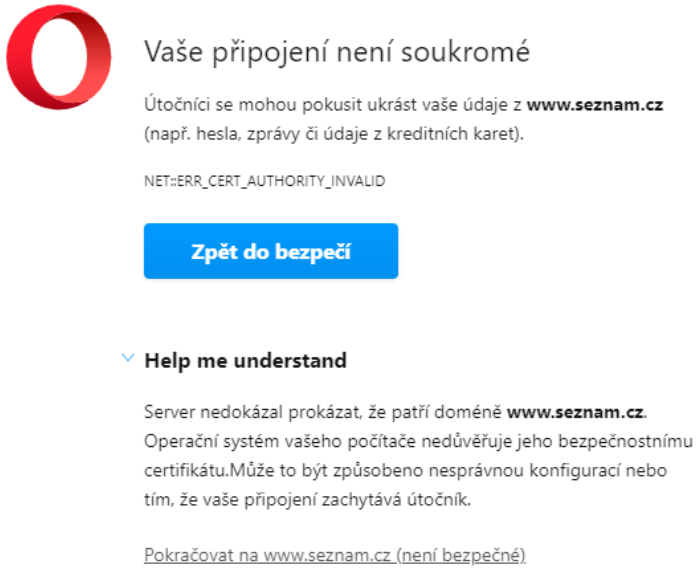
- HTTPS **zaručuje**, že data budou **po síti přenesena** v šifrované podobě.
- HTTPS **nezaručuje**, že stránka, na kterou data zadáváte, **není podvodná**.

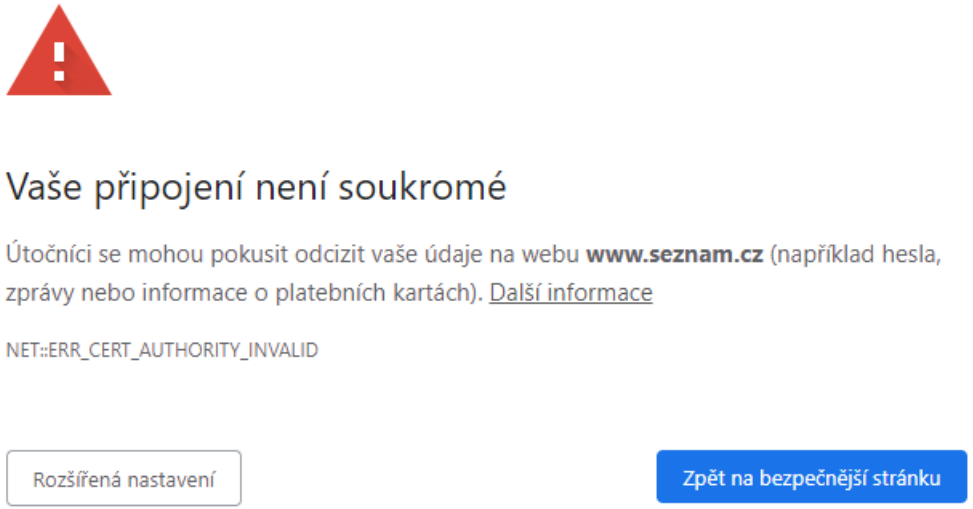
www.seznam.cz X www.seznam.cz.blogger.com/dG90byBqZSBwb2R2b2Q=

- Certifikát pro používání HTTPS si dnes může nechat vystavit každý.

Šifrování

- **NEIGNOROVAT:**





Šifrování e-mailu

- Používáte-li e-mailového klienta, věnujte pozornost zabezpečení jeho komunikace se serverem.
- Drtivá většina běžně používaných e-mailových serverů dnes nabízí šifrování přes SSL – tedy stejnou metodou, jako u HTTPS.
- **V případě nešifrování je riziko krádeže hesla násobně vyšší, než u procházení webu** – e-mailový klient provádí pravidelnou synchronizaci, př níž **pokaždé** pošle heslo.

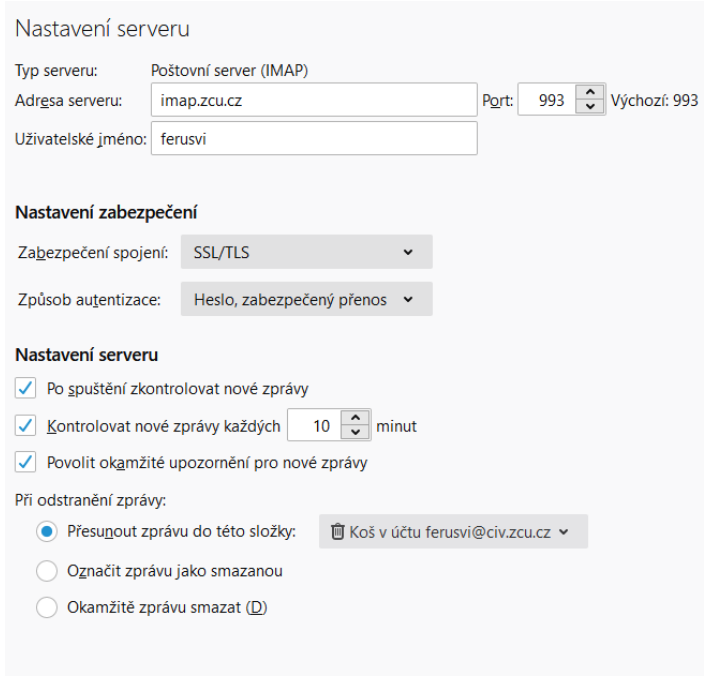
Jak to nastavit?

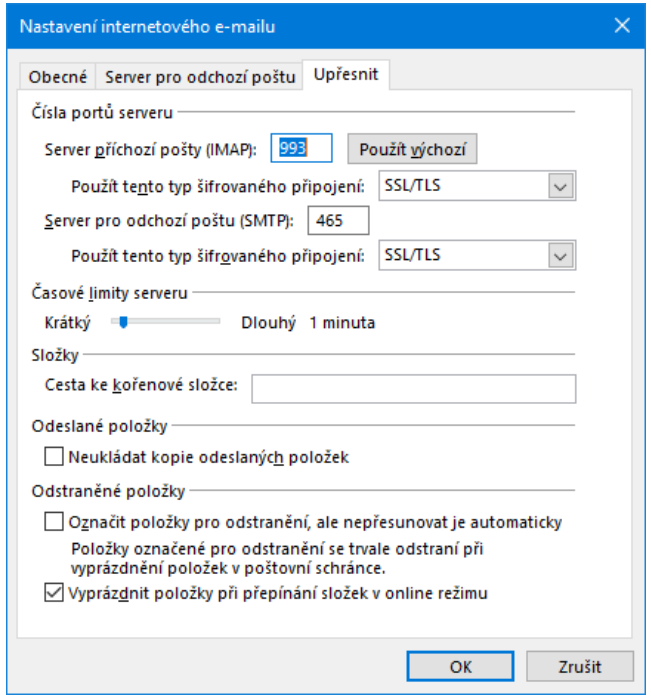
- Obecně, vyžadujte protokoly, co používají SSL.
- Pro příjem pošty – ~~protokol IMAP na portu 143~~ => protokol IMAPS na portu 993

  …nebo…
- Pro příjem pošty – ~~protokol POP3 na portu 110~~ => protokol POP3S na portu 995
- Pro odesílání pošty – ~~protokol SMTP na portu 25~~ => protokol SMTPS na portu 465
- STARTTLS se obecně NEDOPORUČUJE.

Kde to nastavit?

- MS Outlook: Nastavení účtu -> Správa profilů -> E-mailové účty -> *Váš účet* -> Další nastavení -> Upřesnit
- Mozilla Thunderbird: Pravé tlačítko na Vaši schránku -> Nastavení -> Nastavení serveru / Server pro odchozí poštu (SMTP)





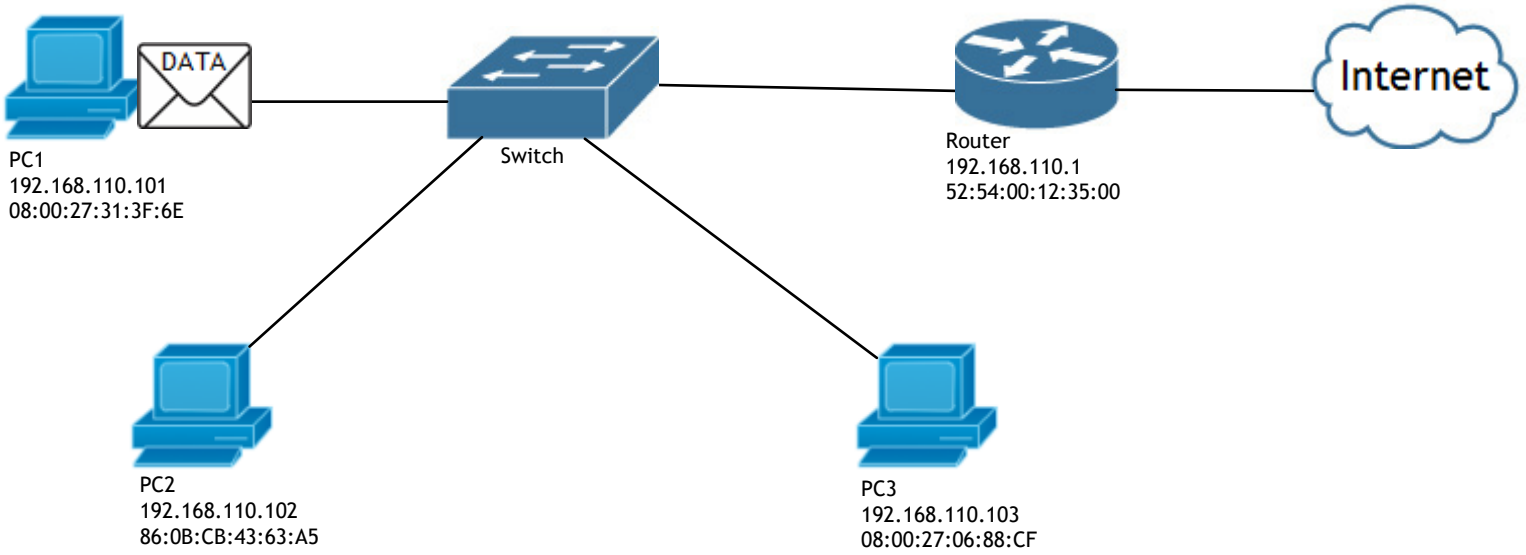
VPN 

VPN

- V dnešní době je již většina síťové komunikace šifrovaná
- Přesto může případný útočník v síti zjistit podstatné množství informací:
  - IP adresy, se kterými Vaše zařízení komunikovalo, včetně časových značek a množství přenesených dat,
  - domény, které jste si překládali,
  - další drobná data, která šla po nešifrovaných protokolech.
- V důvěryhodných sítích to nemusí být tak velký problém, ve veřejných sítích je to ale podstatná věc.

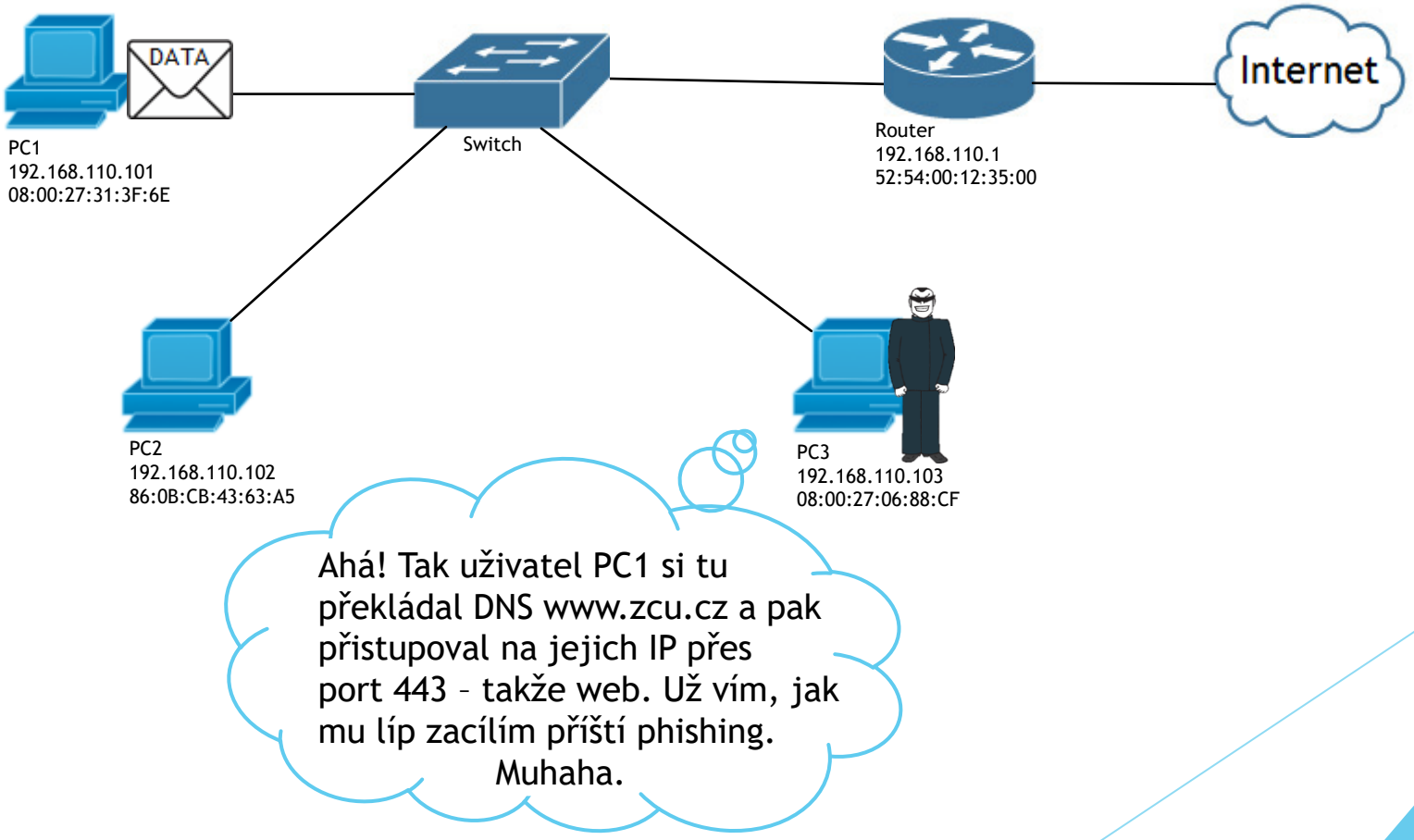
VPN

- Tok dat bez použití VPN



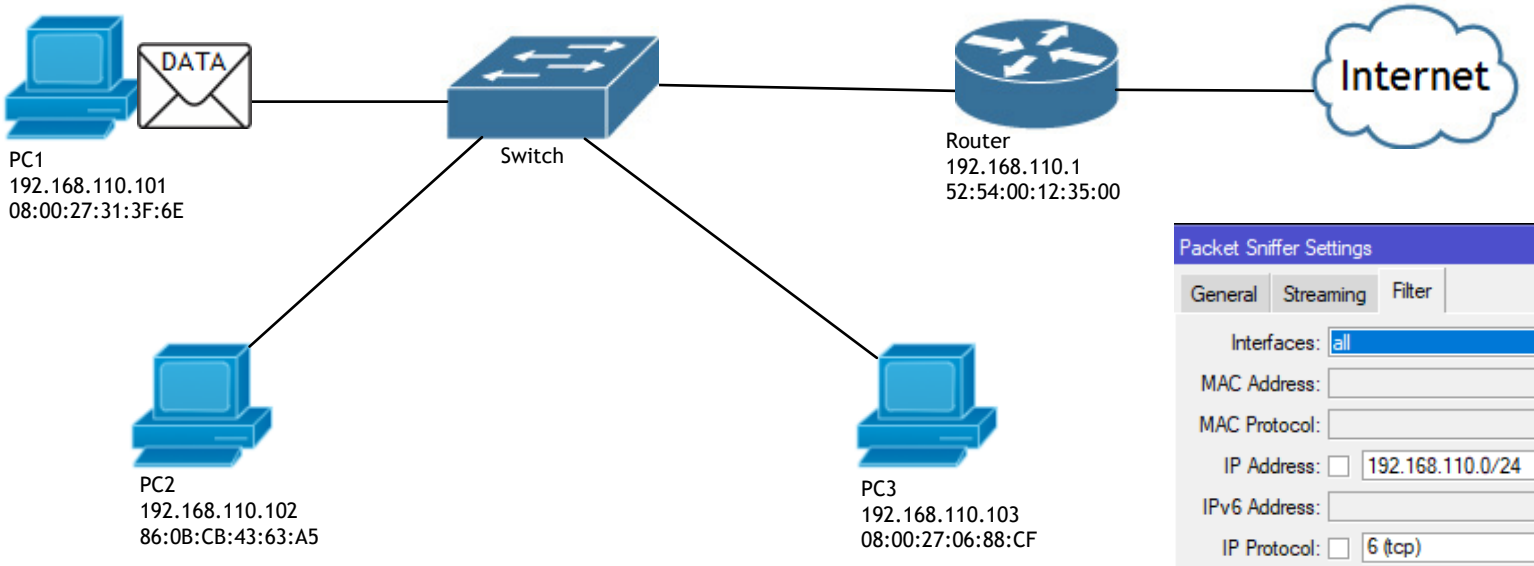
VPN

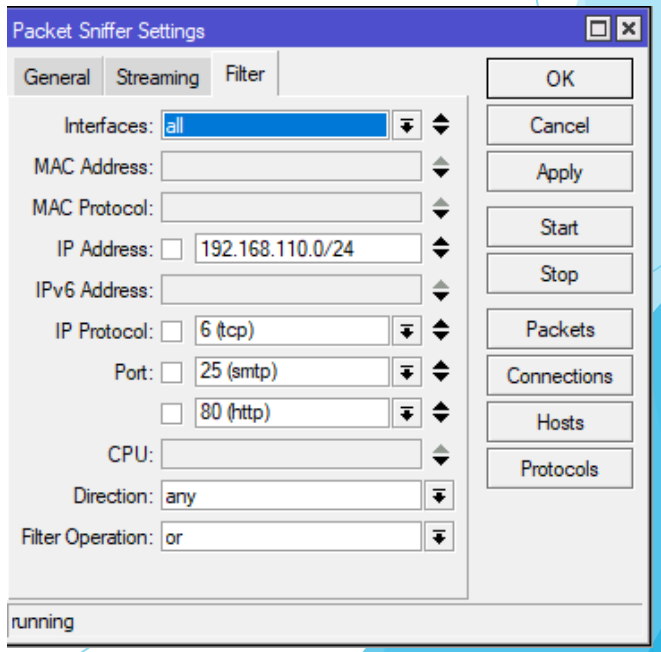
- Tok dat bez použití VPN



VPN

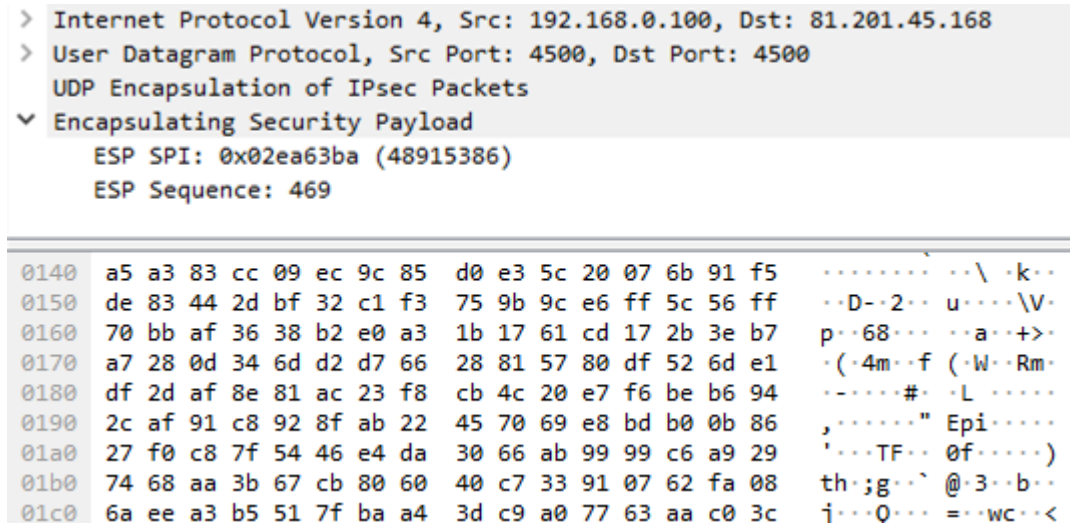
- Tok dat bez použití VPN



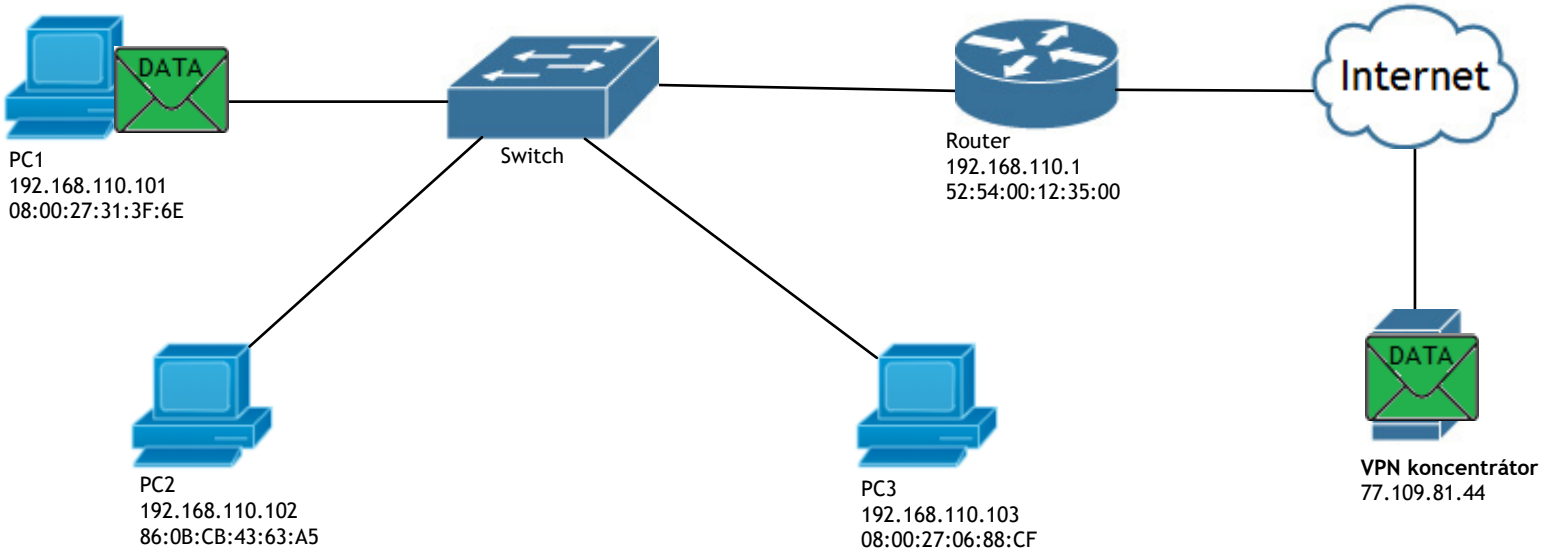


Co s tím?

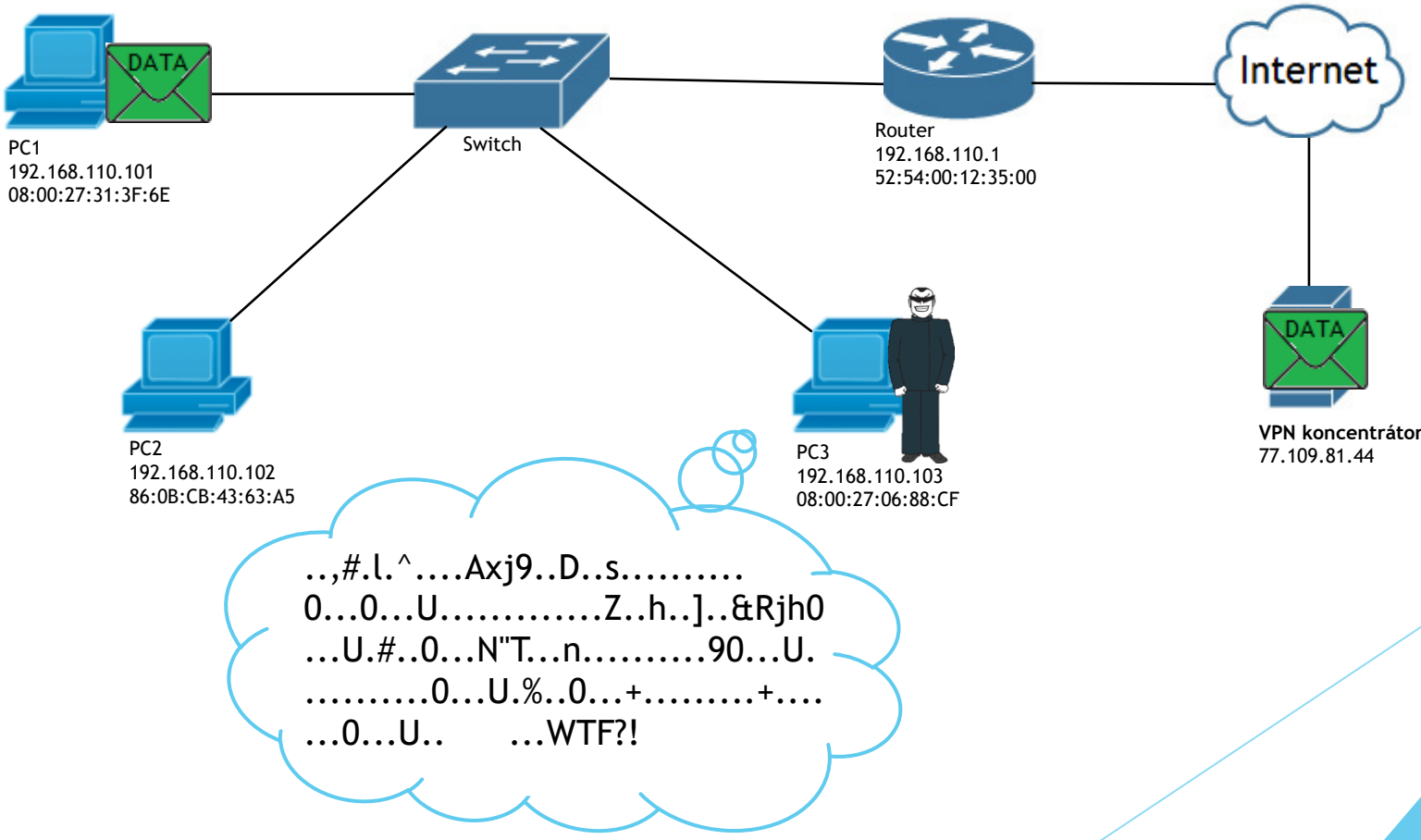
- Řešením je použití **VPN**.
- VPN (= Virtual private network) je technologie k propojování vzdálených sítí.
- Umožňuje Vám vytvořit si šifrovaný tunel mezi Vaším počítačem a jakoukoli vzdálenou sítí (přes její VPN koncentrátor) a všechna data posílat přes něj.
- Případný útočník tak uvidí pouze **komunikaci dvou IP adres a změť zašifrovaných dat.**



VPN


DATA
PC1
192.168.110.101
08:00:27:31:3F:6E
Switch
Router
192.168.110.1
52:54:00:12:35:00
Internet
DATA
VPN koncentrátor
77.109.81.44
PC2
192.168.110.102
86:0B:CB:43:63:A5
PC3
192.168.110.103
08:00:27:06:88:CF

VPN


DATA
PC1
192.168.110.101
08:00:27:31:3F:6E
Switch
Router
192.168.110.1
52:54:00:12:35:00
Internet
PC2
192.168.110.102
86:0B:CB:43:63:A5
PC3
192.168.110.103
08:00:27:06:88:CF
DATA
VPN koncentrátor
77.109.81.44
..,#.l.^....Axj9..D..s.....
0...0...U.....Z..h..]..&Rjh0
...U.#..0...N"T...n.....90...U.
.....0...U.%..0...+.....+....
...0...U.. ...WTF?!

Zřízení VPN

- VPN nabízí mnoho poskytovatelů (NordVPN, TunnelBear, ExpressVPN, …)
  - Většina z nich je ale placená, resp. jejich neplacené programy (pokud existují) jsou často nepoužitelné
- Pokud máte vlastní veřejnou IP a ten správný router, můžete si VPN koncentrátor zřídit sami doma.
  - Některé dražší routery Asus, nebo všechny Mikrotik
  - Základní účely plní, z podstaty věci však nenabídne vše, co komerční VPN

Komerční vs. domácí VPN

Komerční VPN

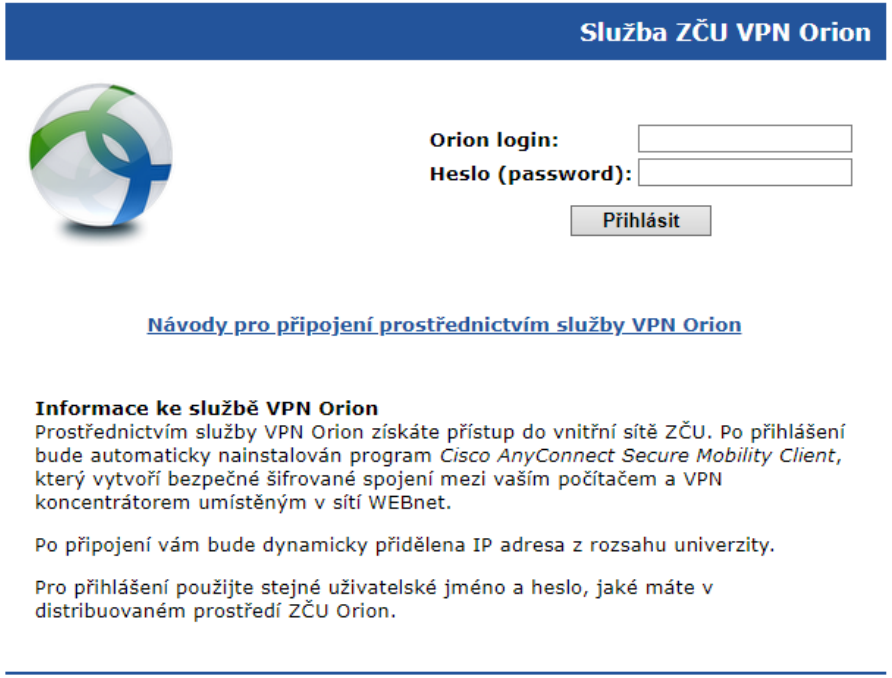
- 👍 Anonymizace v rámci místní sítě
- 👍 Anonymizace v Internetu
- 👍 Obvykle dobré šifrování
- 👎 Platí se za ni

Domácí VPN

- 👍 Anonymizace v rámci místní sítě
- 👍 Je zdarma
- ± Může mít dobré šifrování
- 👎 Anonymizace v Internetu schází
  - Přípojka, přes níž data posíláte, je u Vašeho ISP psána na Vaše jméno

Univerzitní VPN

- Specifikací podobná domácí VPN
- Potřebujete-li VPN jen na změnu IP (např. z důvodu geologických restrikcí českých služeb při cestě do zahraničí) a nechce se Vám za ni platit, je univerzitní VPN dobré řešení.
- https://vpn.zcu.cz



Děkuji za pozornost, prostor pro dotazy!

Viktor Ferus – WEBnet Incident Response Team

ferusvi@civ.zcu.cz
www.viktor-ferus.cz
https://www.youtube.com/nokia6085ful

Centrum Informatizace a výpočetní techniky, Západočeská univerzita v Plzni