

CryptoParty

Základy počítačové bezpečnosti pro začátečníky

Ondřej Profant

Česká pirátská strana

18. května 2013

Osnova

- 1 Hesla
- 2 Operační systém
 - Pravidelné aktualizace
 - Uživatelské účty
 - Výběr OS
- 3 Internetové prohlížeče
 - Anonymní mód
 - Certifikáty a zabezpečení stránek
 - Pluginy, addony
- 4 Šifrování
 - Archívy
- 5 Cloudy
- 6 Závěr

Hesla

Zásady silného hesla:

- přiměřeně dlouhé
- více druhů znaků (písmena, čísla, jiné znaky)
- nepoužívat existující slova
- nepoužívat všude stejné heslo (alespoň několik stupňů)

Hesla

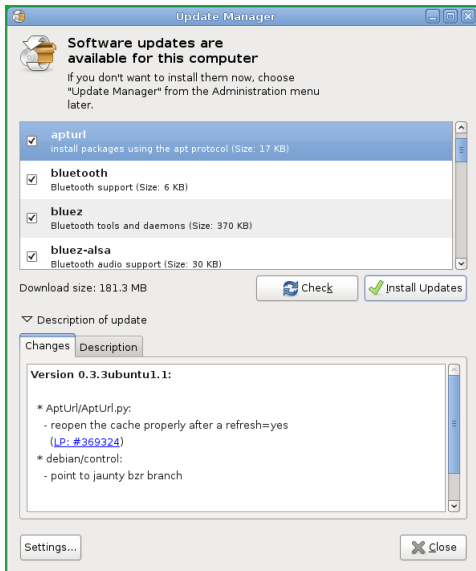
Jak to splnit:

- kombinovat, modifikovat
- prokládat
- vyhodnocovat riziko

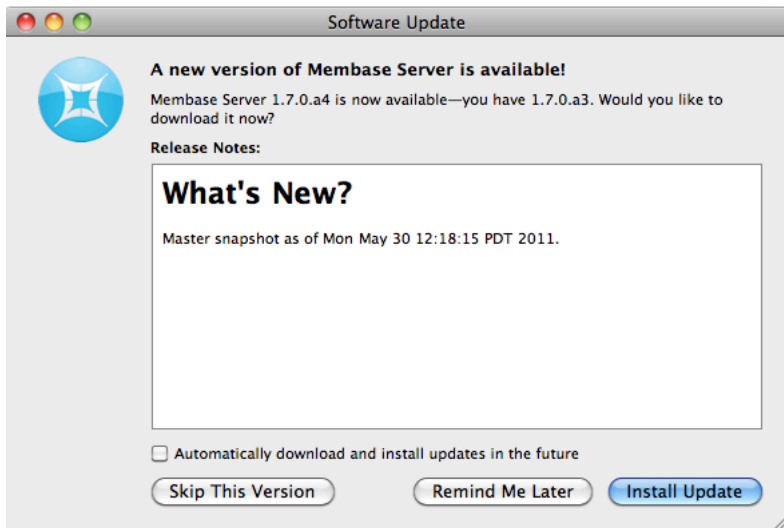
Pravidelné aktualizace

- Snad každý systém poskytuje bezpečnostní aktualizace.
- Tyto aktualizace se opravdu vyplatí nainstalovat.
- Tyto aktualizace jsou zpravidla zdarma.

Pravidelné aktualizace 2




Pravidelné aktualizace 3



The image shows a 'Software Update' dialog box with a title bar containing three colored window control buttons (red, yellow, green). The main content area features a blue circular icon with a white star-like shape on the left. The text reads: 'A new version of Membase Server is available!', 'Membase Server 1.7.0.a4 is now available—you have 1.7.0.a3. Would you like to download it now?', and 'Release Notes:'. Below this is a box titled 'What's New?' containing the text 'Master snapshot as of Mon May 30 12:18:15 PDT 2011.'. At the bottom, there is a checkbox for 'Automatically download and install updates in the future' and three buttons: 'Skip This Version', 'Remind Me Later', and 'Install Update'.

Software Update

 **A new version of Membase Server is available!**

Membase Server 1.7.0.a4 is now available—you have 1.7.0.a3. Would you like to download it now?

Release Notes:

What's New?

Master snapshot as of Mon May 30 12:18:15 PDT 2011.

Automatically download and install updates in the future

[Skip This Version](#) [Remind Me Later](#) [Install Update](#)

Pravidelné aktualizace 4



New updates are available

Click to install them using Windows Update.



Uživatelské účty

- Uživatelské účty jsou praktická věc!
- Oddělují prostředí.
- Zabezpečují základní soukromí.

Operační systém

- Existuje více druhů operačních systémů
- S různým zaměřením a různým stylem používání

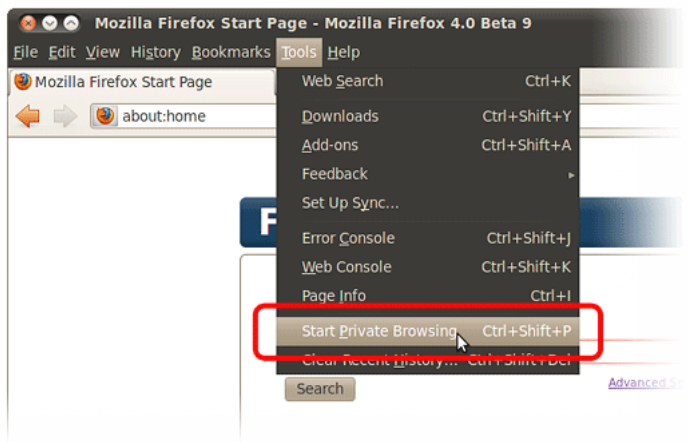
Internetové prohlížeče

- Existuje více prohlížečů
- Liší se kvalitou, rychlostí
- a mnohdy bezpečností a přístupem k ni

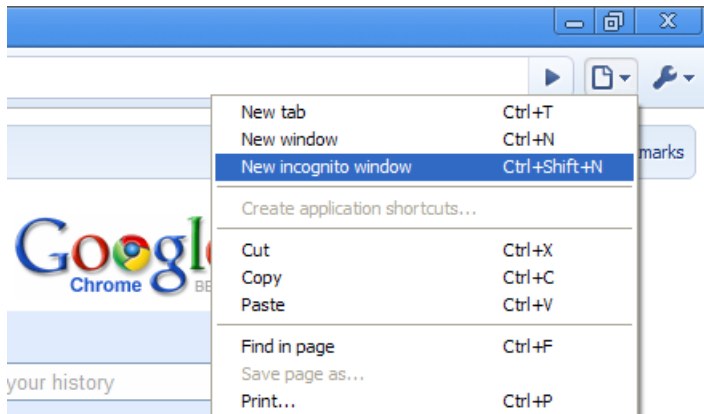
Anonymní mód

- Neukládá data do počítače.
- Nepoužívá data již uložená (např. cookies).
- Slouží k základní anonymizaci, ale ne moc podrobné.
- Nejedná se o anonymizér.

Anonymní mód – Firefox



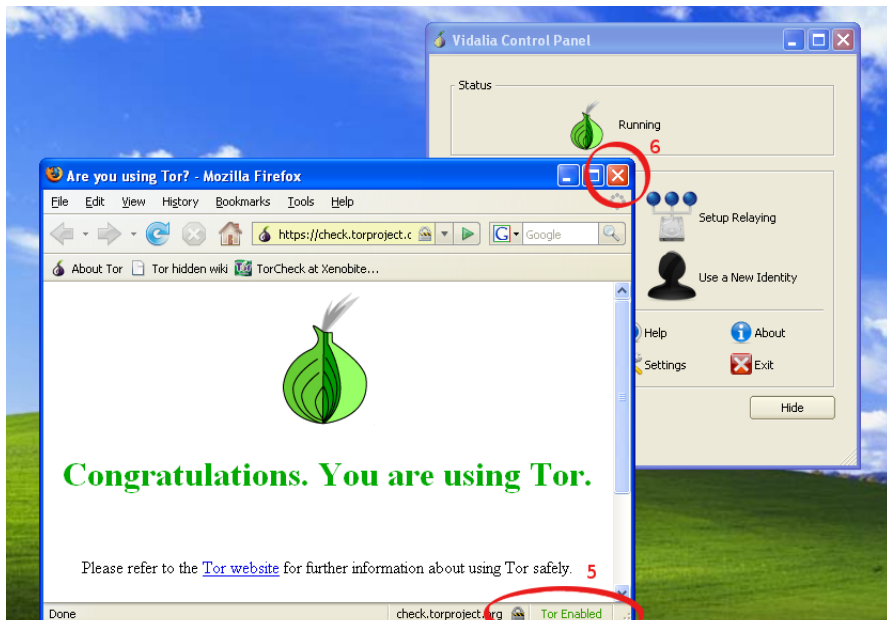
Anonymní mód – Chrome



Anonymizéry

- např. Tor
- ke stažení přímo předpřipravený prohlížeč:
<https://www.torproject.org/projects/torbrowser.html.en>
- jiné řešení může být např. VPN

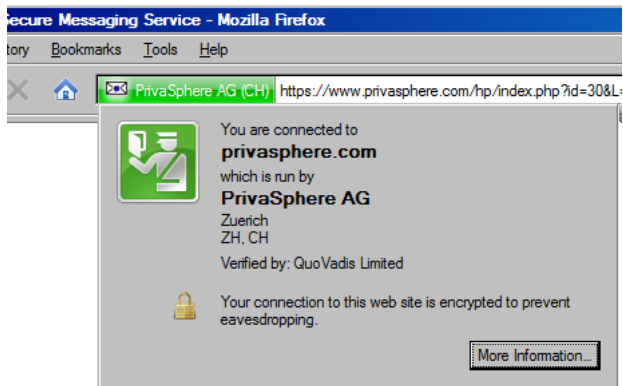
Anonymizéry



Certifikáty a zabezpečení stránek

- neodklikávejte bez rozmyslu

Certifikáty a zabezpečení stránek



Prohlížeče – pluginy, addony

- Nebezpečné.
- Ztráta výkonu.
- Odinstalujte, co nepoužíváte.

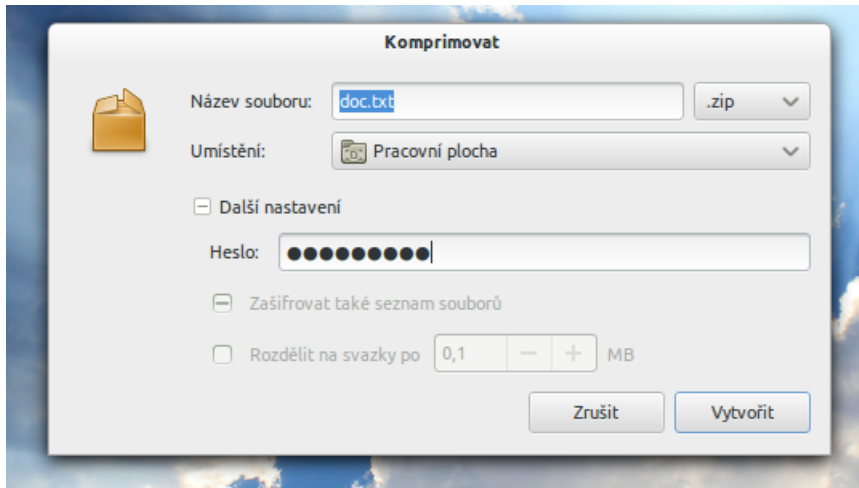
Archívy

- Archívy slouží primárně ke komprimaci (zmenšení) dat.
- Nicméně většinou dovolují i šifrovat.

Odbočka: šifrování vs. „heslování“

- Kvalitní šifrování je z podstaty bezpečné.
- „Heslování“ může znamenat pouze ochrana heslem.

Archívy



Cloudy

- Uložiště dat mimo váš počítač
- Obvykle mimo konkrétní počítač
- Již z principu založeno na důvěře poskytovateli
- Samozřejmě jsou lepší a horší řešení

Závěr

Děkuji za pozornost.

Doplňující otázky?

Další Cryptoparty?

Copyright Ondřej Profant, 2012. Všechna práva vyhlazena. Sdílejte, upravujte a nechte sdílet za stejných podmínek.

Prezentace v úplné formě¹ na vyžádání emailem: [ondrej.profant -at- pirati.cz](mailto:ondrej.profant-at-pirati.cz)

¹i se zdrojovými kódy