CryptoParty
Základy počítačové bezpečnosti pro začátečníky

Ondřej Profant

Česká pirátská strana

18. května 2013

Osnova

Hesla

Zásady silného hesla:

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

Hesla

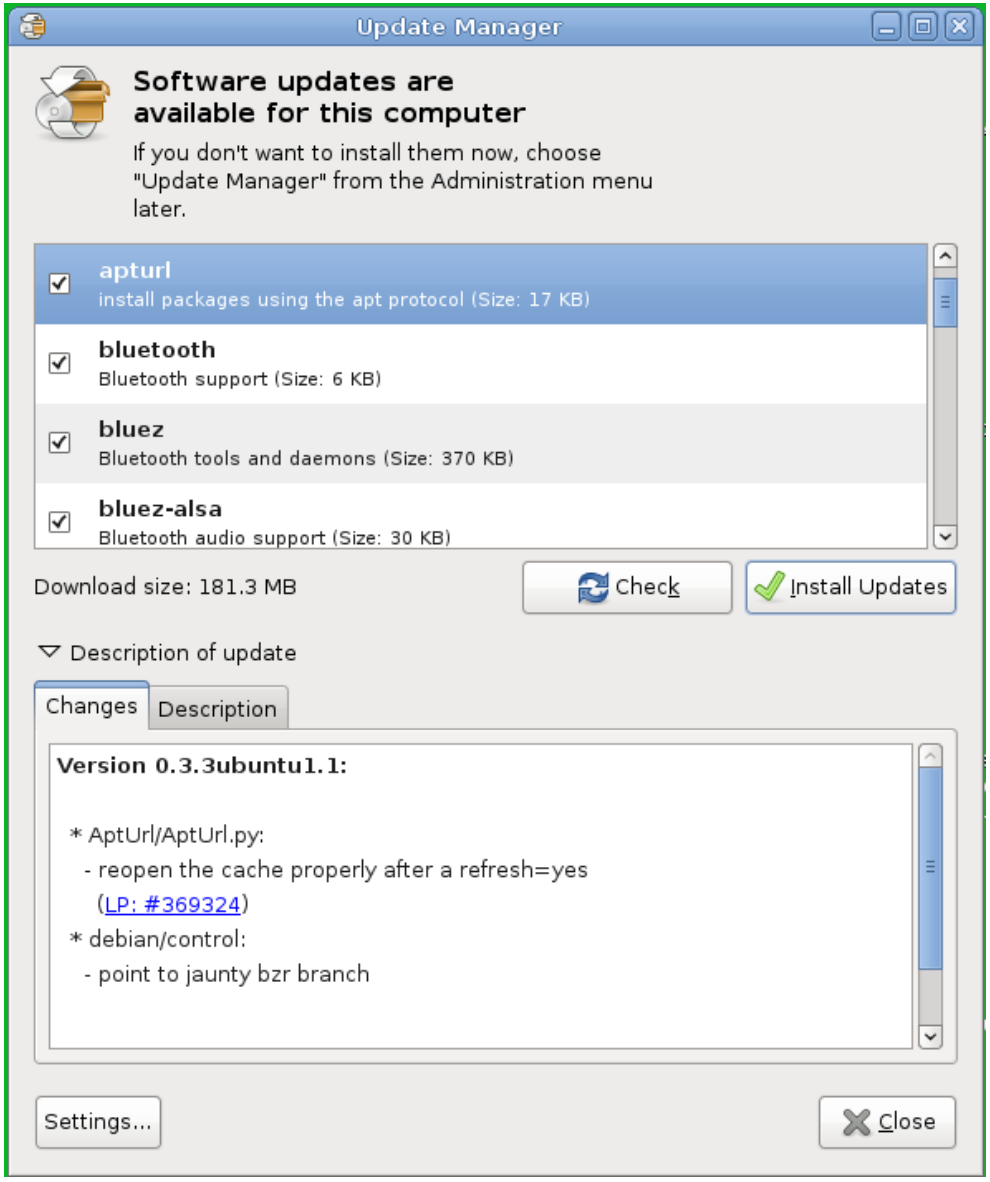
Jak to splnit:

- kombinovat, modifikovat
- prokládat
- vyhodnocovat riziko

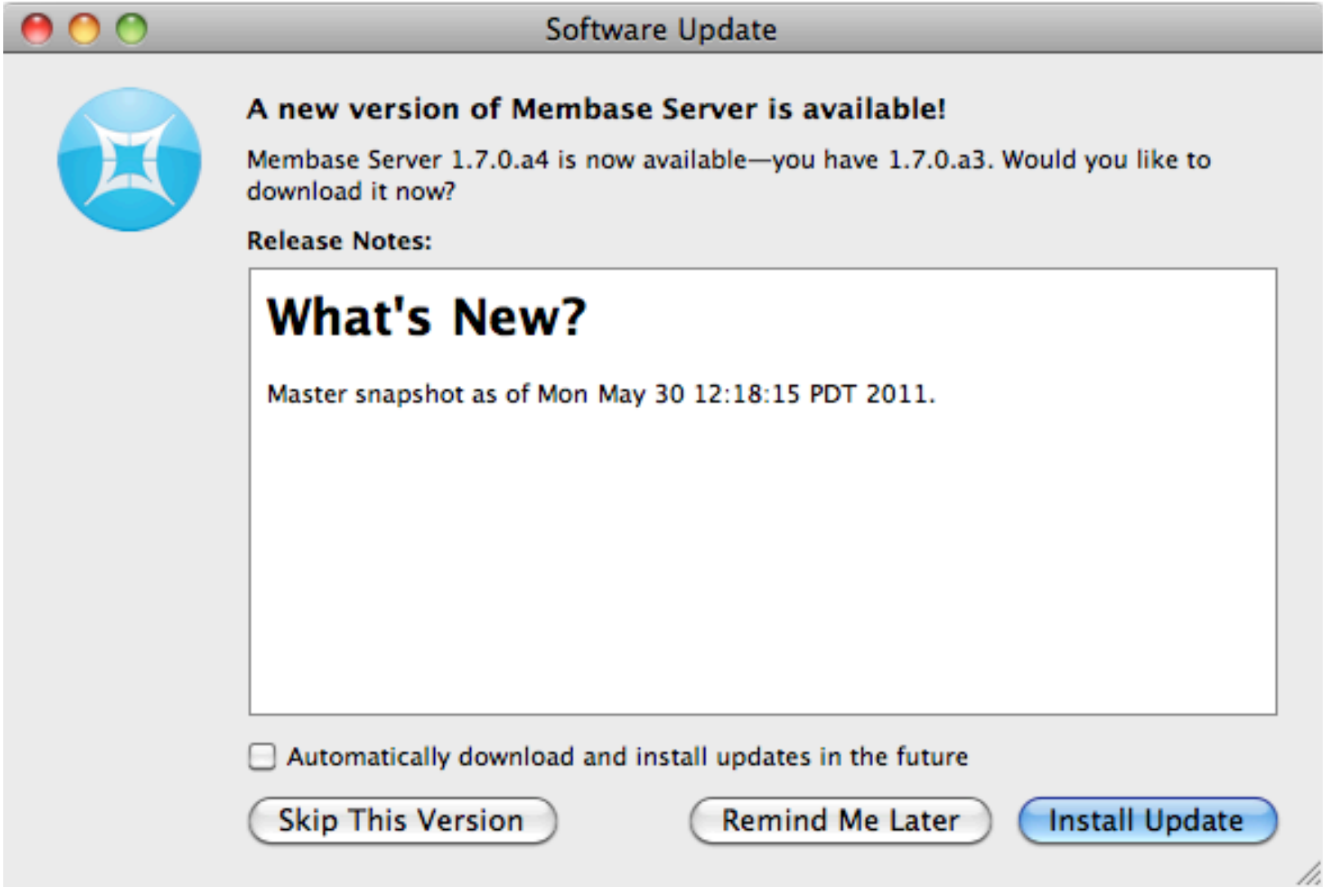
Pravidelné aktualizace

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

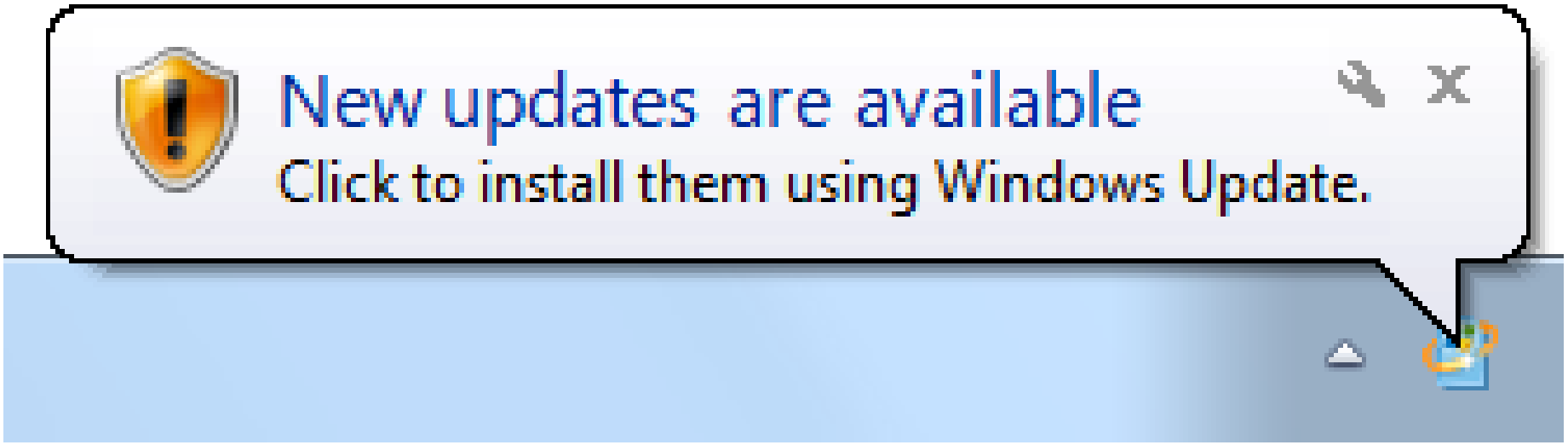
Pravidelné aktualizace 2



Pravidelné aktualizace 3



Pravidelné aktualizace 4



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

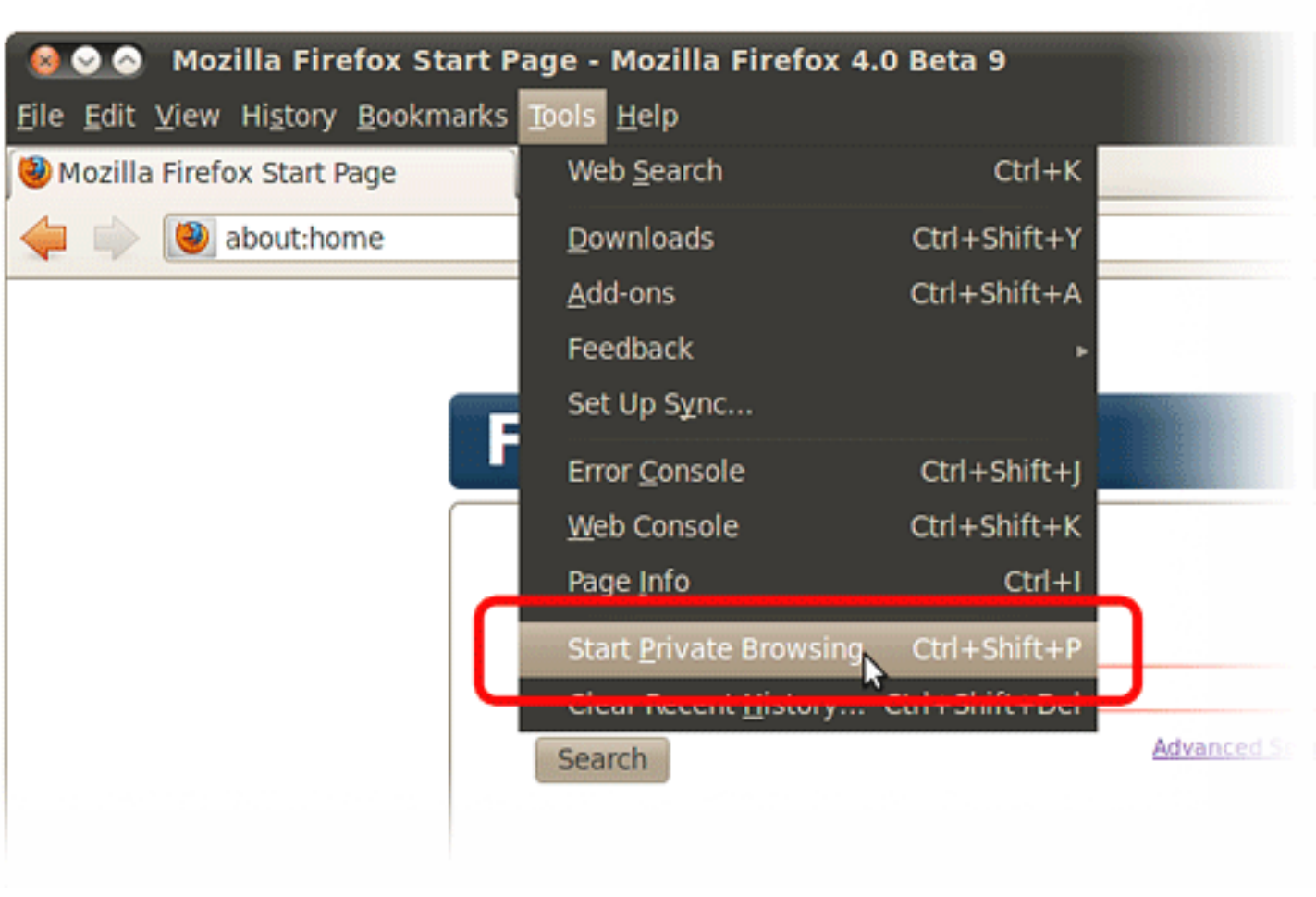
Internetové prohlížeče

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

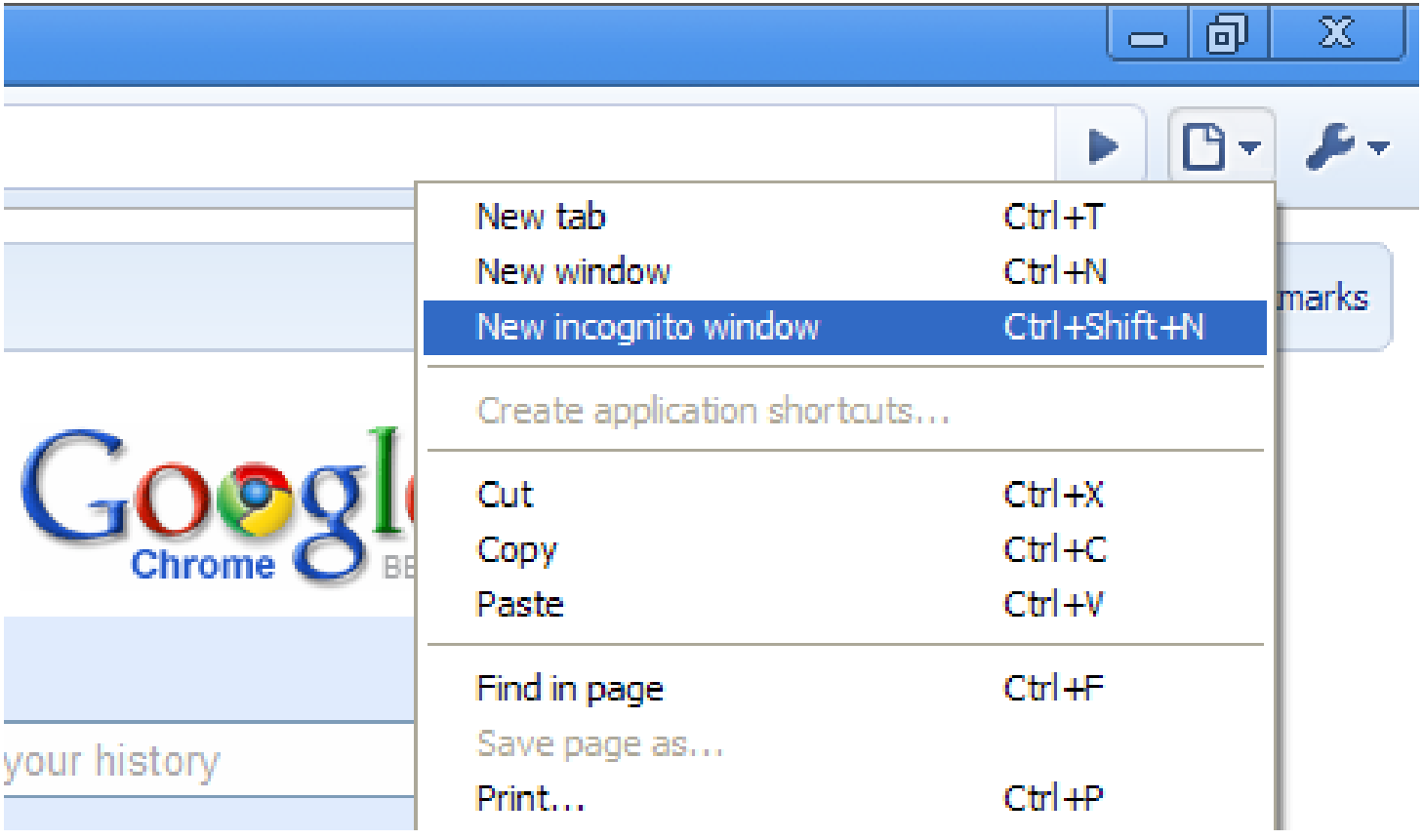
Anonymní mód

- 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



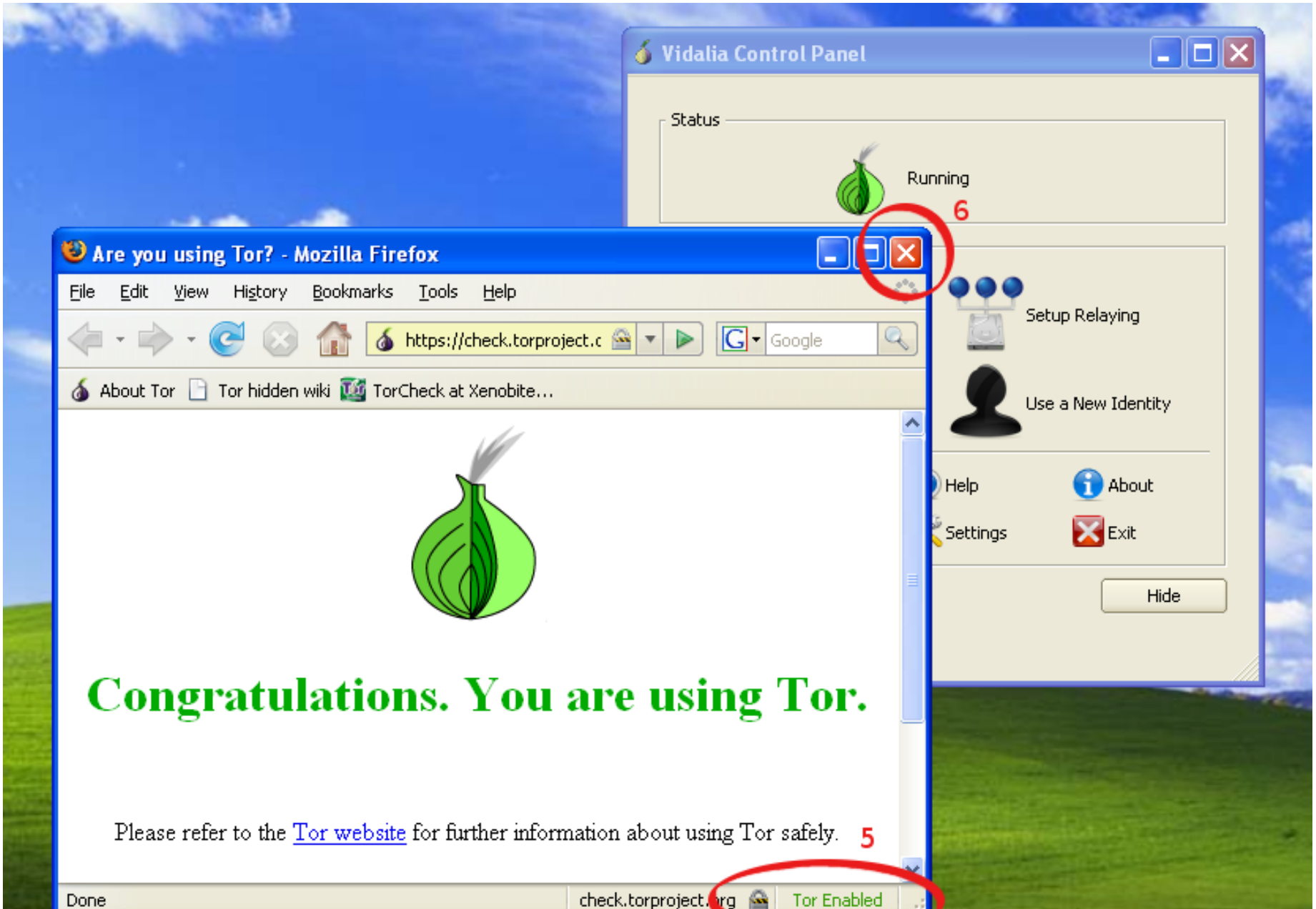
Anonymní mód – Chrome



Anonymizéry

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

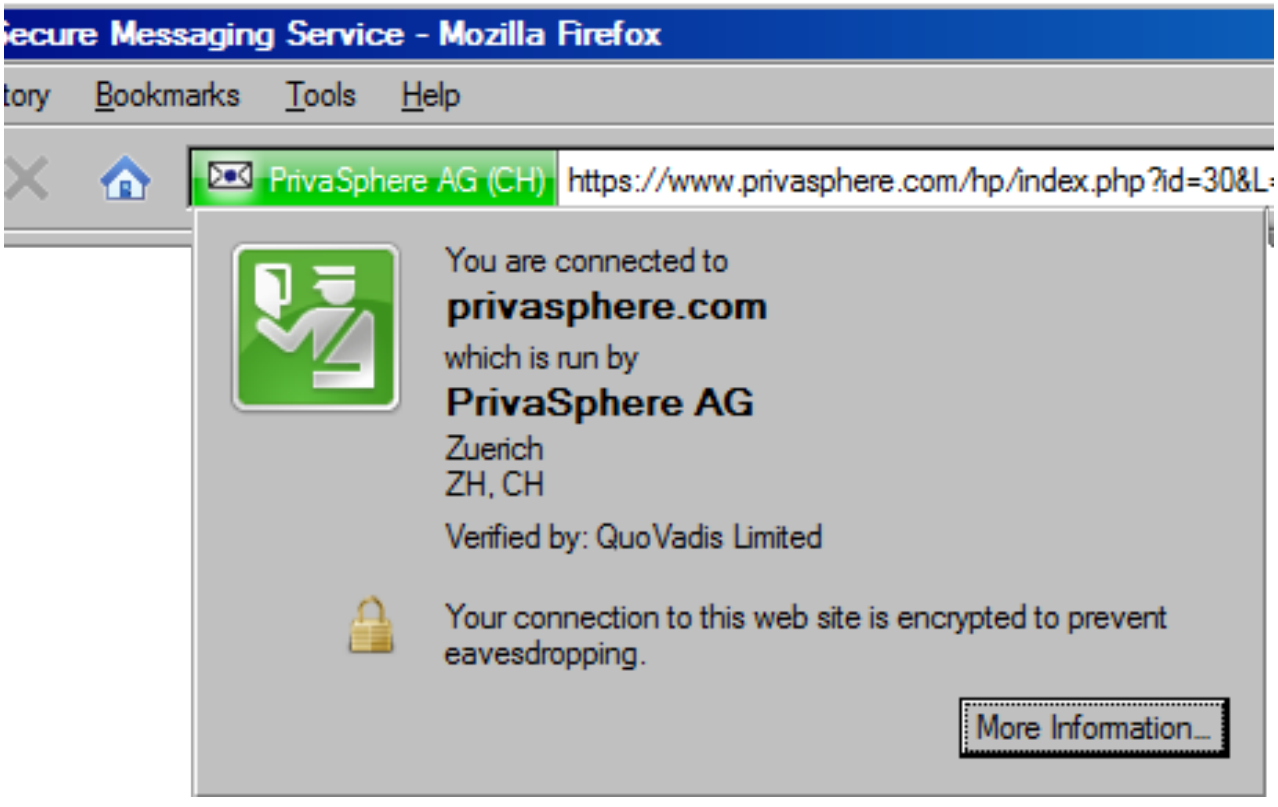
Anonymizéry



Certifikáty a zabezpečení stránek

- neodklikávajte bez rozmyslu

Certifikáty a zabezpečení stránek



Prohlížeče – pluginy, addony

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

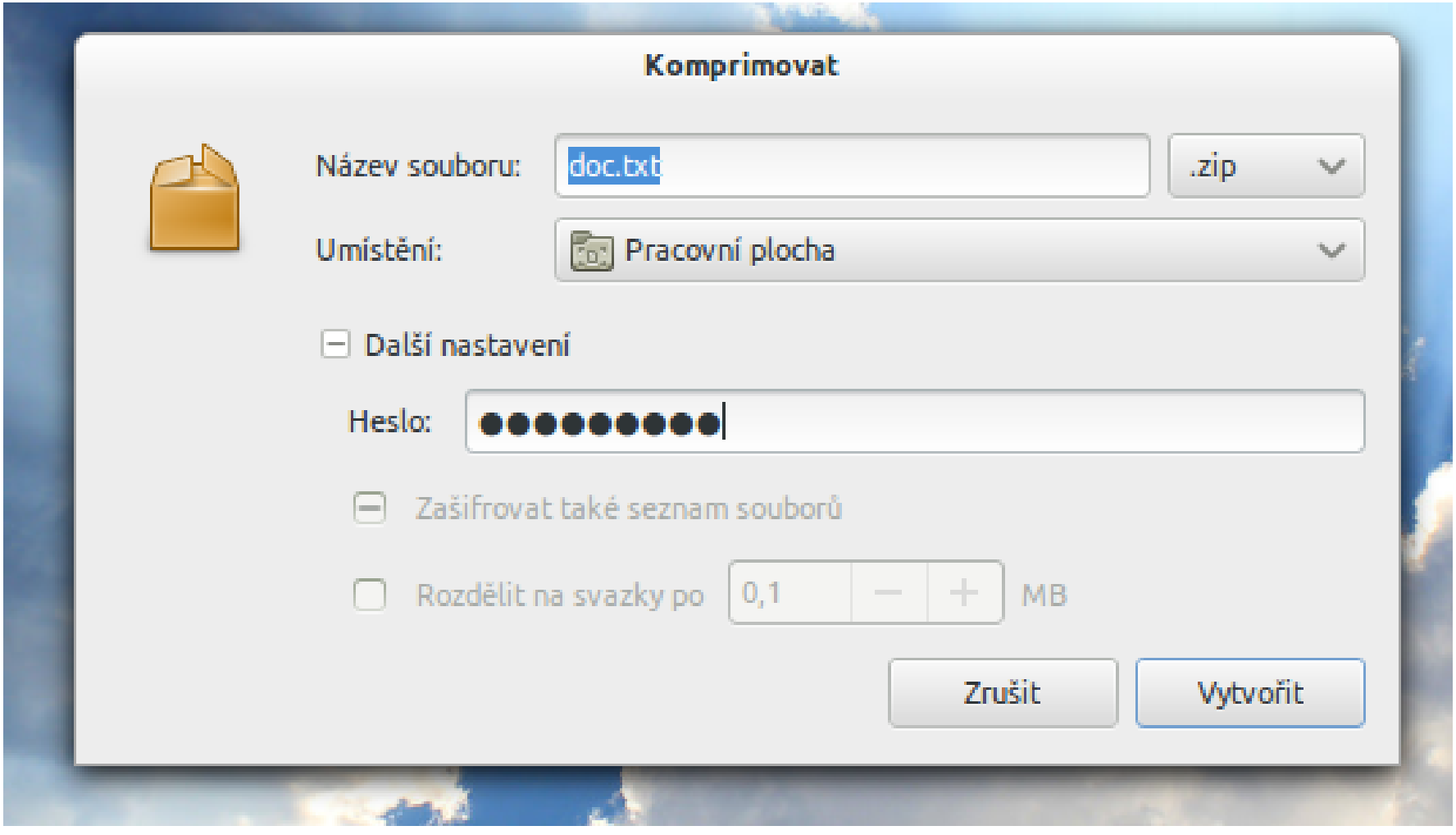
Archívy

- 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


Komprimovat
Název souboru:
doc.txt
.zip
Umístění:
Pracovní plocha
Další nastavení
Heslo:
Zašifrovat také seznam souborů
Rozdělit na svazky po
0,1
MB
Zrušit
Vytvořit

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?

Prezentace v úplné formě[1] na vyžádání emailem: ondrej.profant -at- pirati.cz

[1] i se zdrojovými kódy