Nebezpečí na Internetu

Jan Soukal

https://security.ics.muni.cz/edu/bit/

Co se dozvíte

1) Co je to Phishing a jak se mu ubránit
2) Které jiné hrozby vás mohou na Internetu potkat
3) Jak správně pracovat s hesly
4) Jak je to s anonymitou v Internetu

Phishing

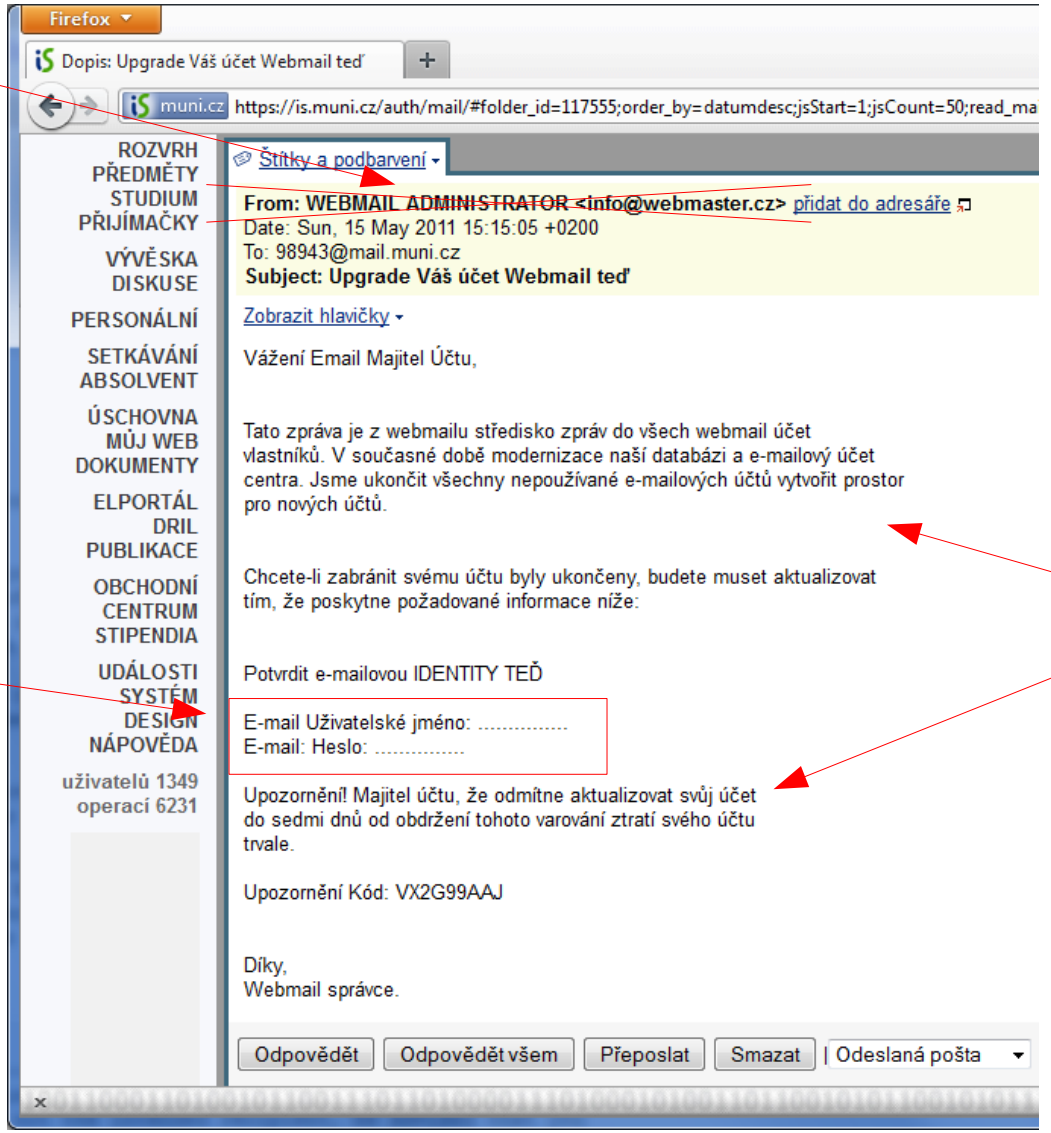
Co je phishing?

- Podvodná zpráva (nejčastěji e-mail)
- Snaží se z vás vytáhnout nějaké cenné údaje
  - Heslo k e-mailu, údaje k bankovnímu účtu, …

- V síti MU zaznamenáme nějaký phishingový útok téměř každý den!
- V rámci MU je každý měsíc několik účtů úspěšně napadeno!

Phishing I.

Padělaná hlavička zprávy!



Podvodník se z uživatele snaží vylákat jméno a heslo

Text snažící se uživatele vystrašit

Často je „strojově“ přeložený

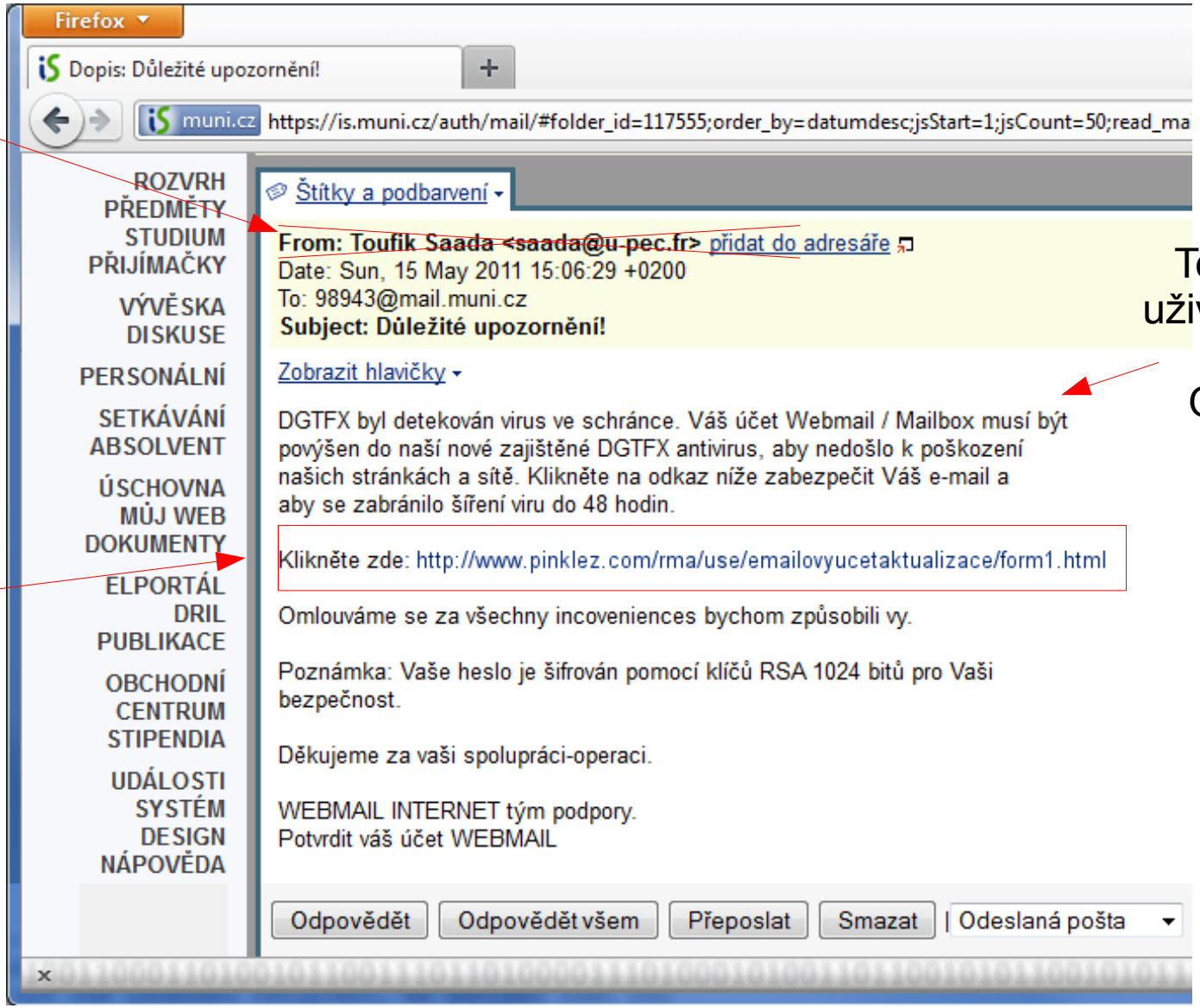
Jak odhalit phishing?

- Podvodník se vás snaží vystrašit
  - zrušením účtu, deaktivací platební karty, ...
- Často se jedná o „strojově“ přeložený text
- Tlačí vás k vyplnění hesla či podobných údajů
  - Přimo do mailu nebo prostřednictvím formuláře

- Poznámka: Nedůvěřujte políčku From (Od)
  - Lze je velmi snadno padělat

Phishing II.

Padělaná hlavička zprávy

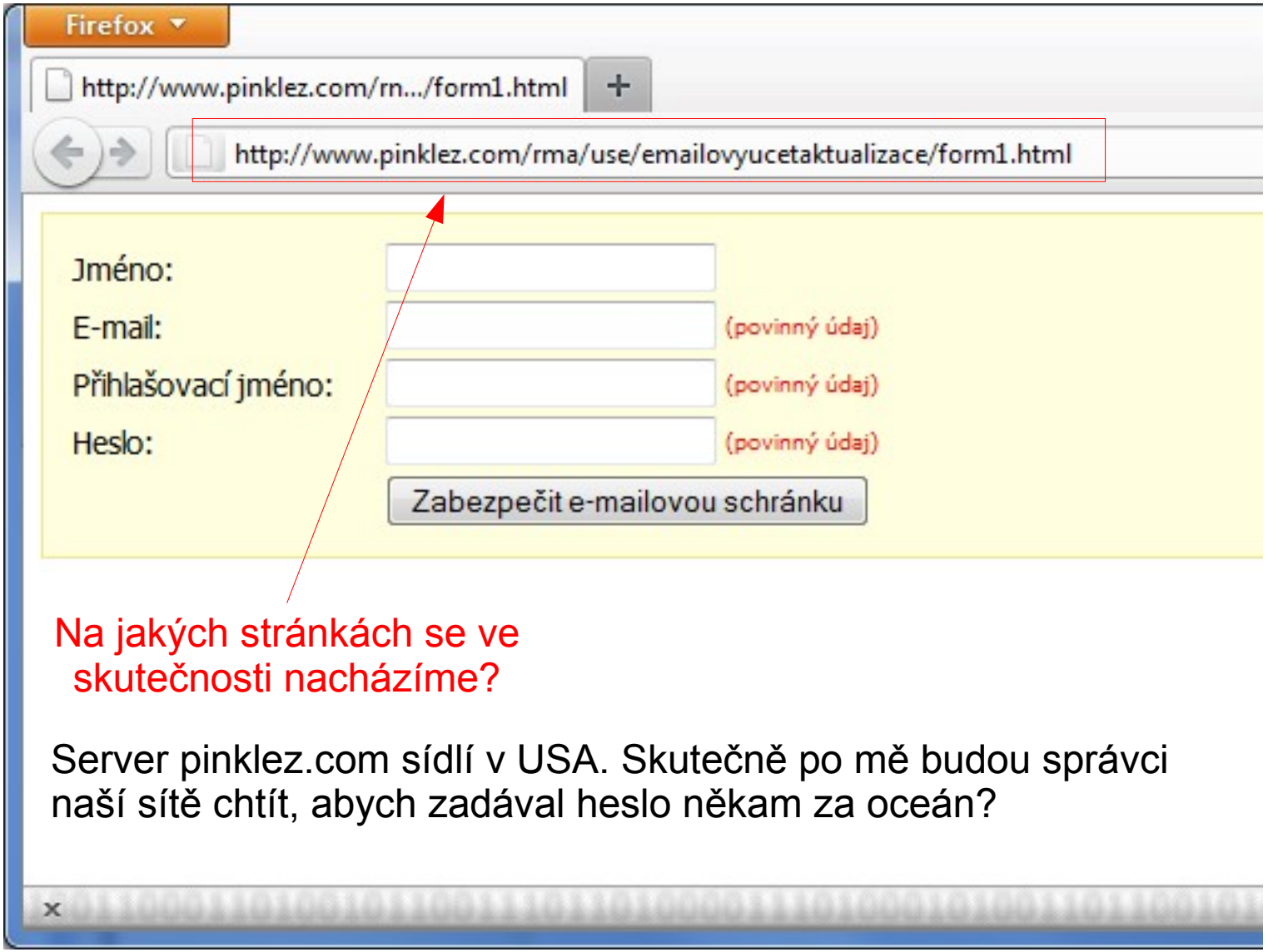


Text snažící se uživatele vystrašit.

Opět strojově přeložený

Podvodník se snaží přimět uživatele kliknout na odkaz

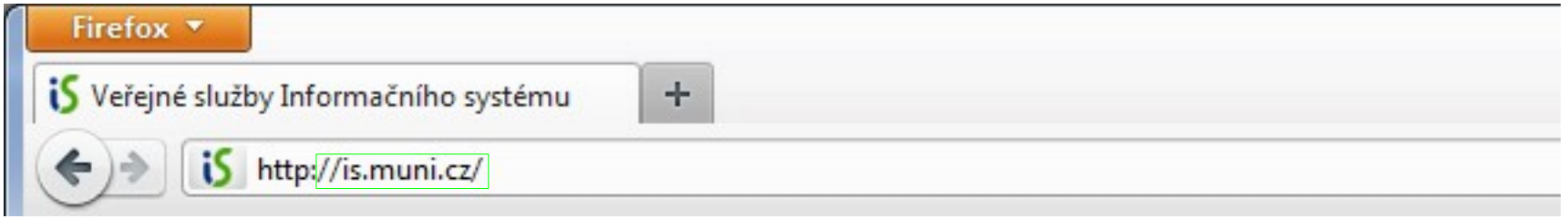
Phishing II - pokrač.



Server pinklez.com sídlí v USA. Skutečně po mě budou správci naší sítě chtít, abych zadával heslo někam za oceán?

Jak na adresu stránky (URL) - I.

- Kde se uživatel nachází?

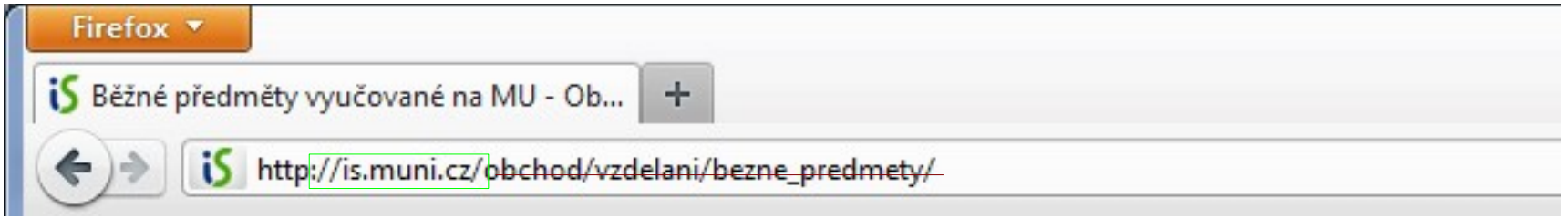


na stránkách IS MU

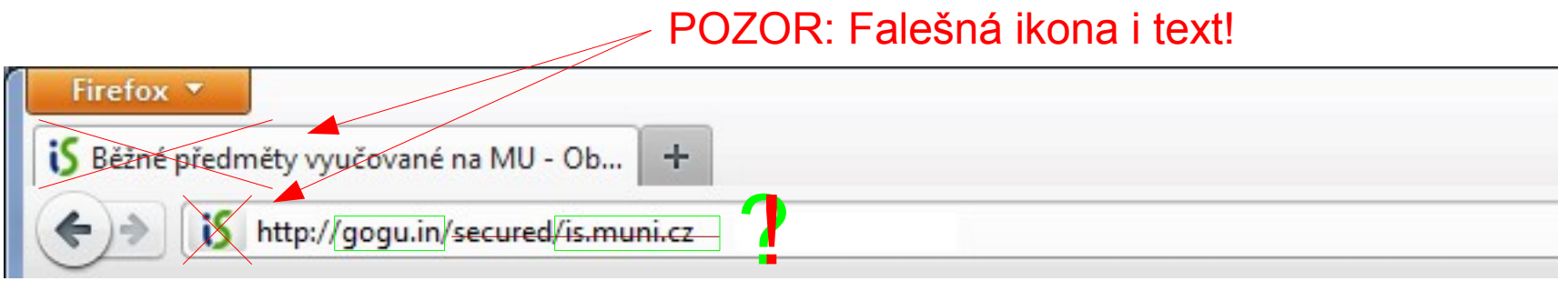
na stránkách www.pinklez.com

Jak na adresu stránky (URL) - II.

- Kde se uživatel nachází?



na stránkách IS MU

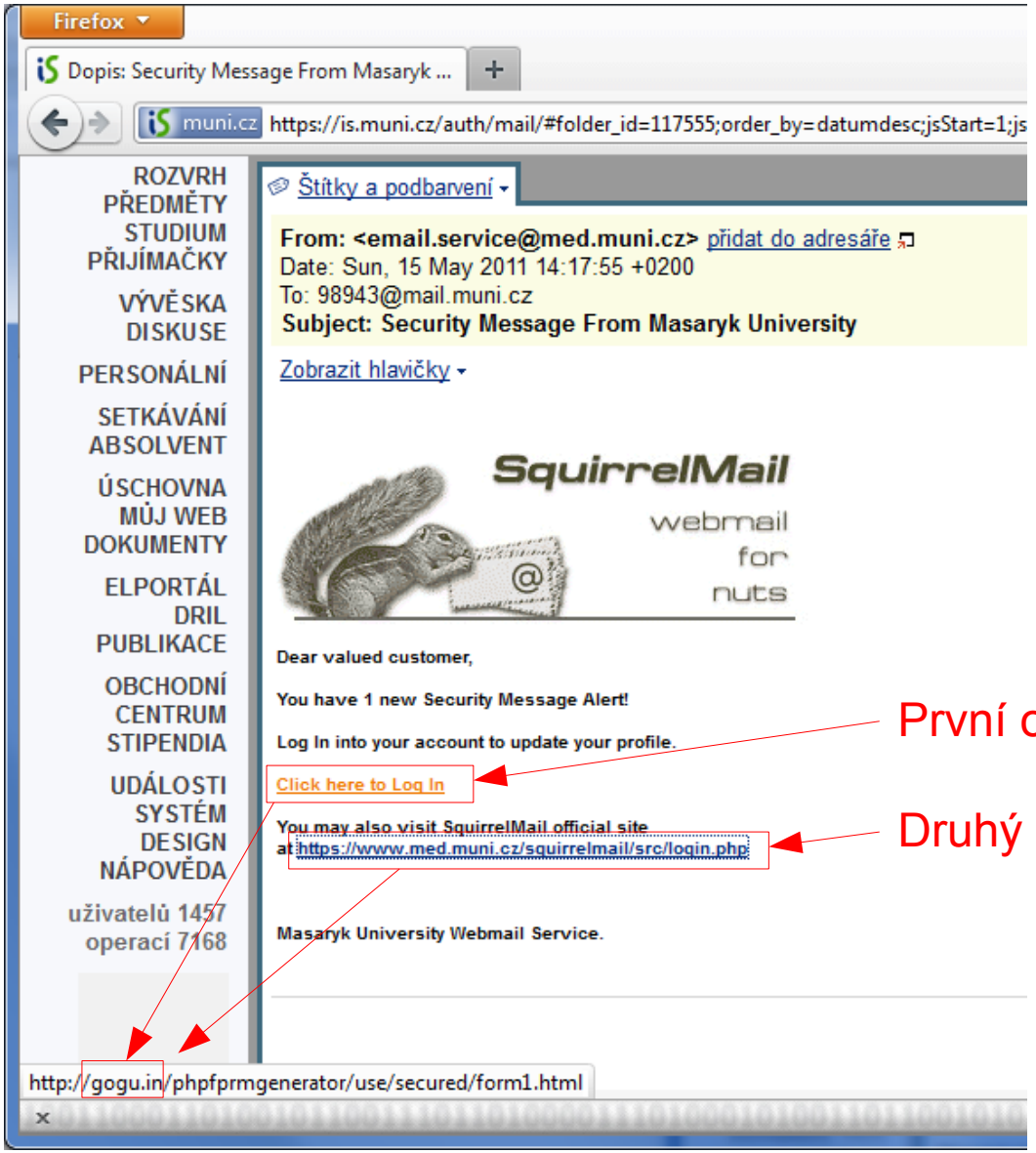


na stránkách gogu.in, nikoliv na IS MU!

Phishing III.

Opět vidíme padělanou hlavičku

Oficiální a známý obrázek zvyšuje falešný pocit důvěryhodnosti



Opět snaha uživatele zaujmout a přimět jej kliknout na přiložený odkaz

(kam ale odkaz ve skutečnosti směřuje?)

První odkaz směřuje do Indie!

Druhý odkaz taktéž!

Phishing III. - pokrač.

Jak se bránit?

- Většinou stačí „selský“ rozum
  - Odevzdali byste klíče od domu nebo kreditní kartu jen tak někomu, kdo by vás o to požádal?
- Správci sítě nikdy nebudou chtít vaše heslo
  - To slouží pouze vám k přihlašování na známých stránkách
- Myslet na 3 NE
  - **NEvyplňovat** údaje, **NEklikat** na odkazy a **NEstahovat** soubory
- Když si nebudete jisti, požádejte správce o radu
  - Ale až v posledním případě (správci mají i vlastní práci)

Co dalšího nás může na Internetu potkat?

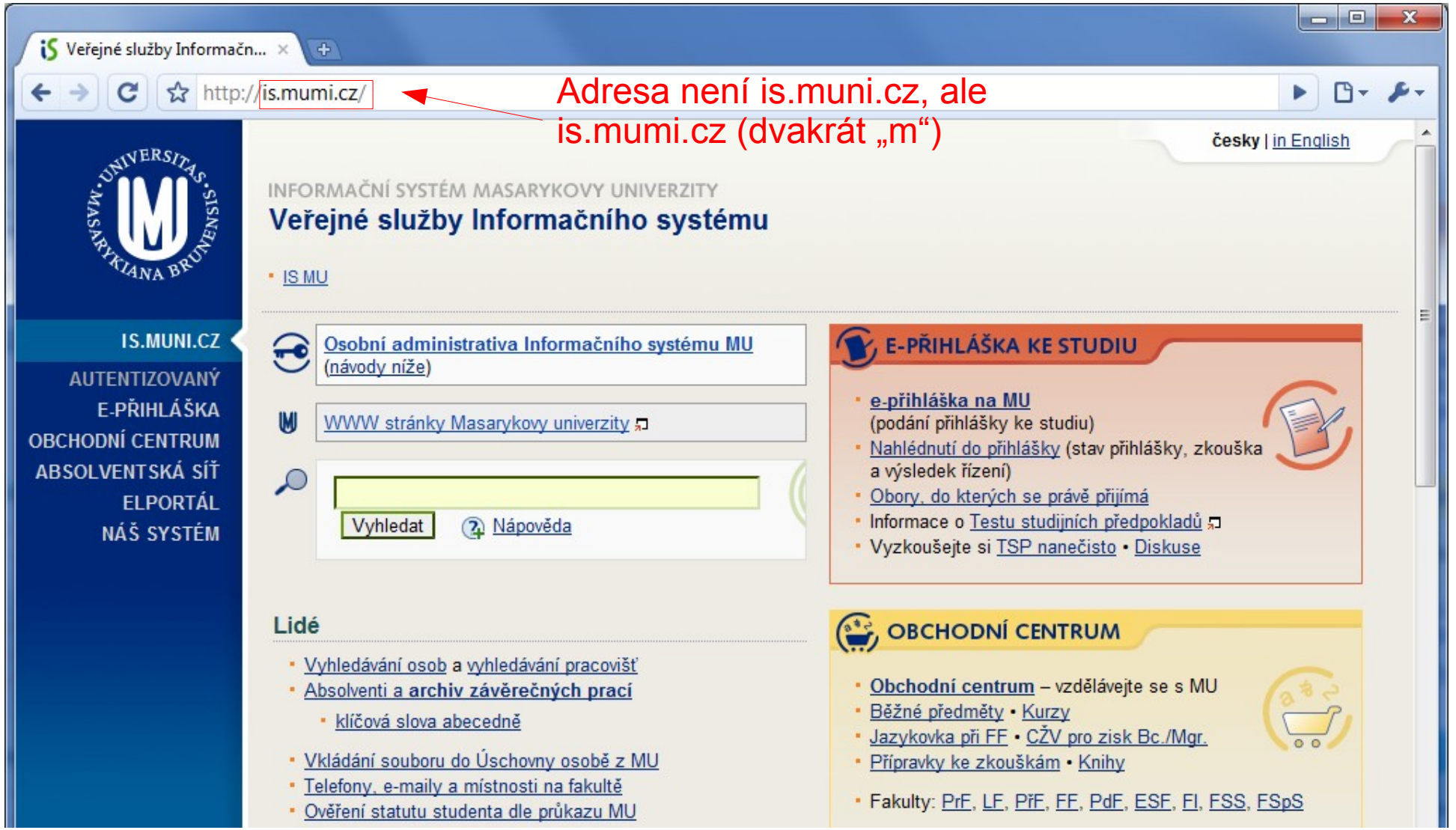
Podvodné anitiviry

- Tváří se jako profesionální software
  - Snaží se napodobit existující antivirové programy
- Nacházejí „neexistující“ viry a nutí uživatele zakoupit licenci
  - Případně samotný software obsahuje virus
- Často se šíří interneto-vou reklamou

Tabnapping

- Doslova „únos záložky“
- Jakmile uživatel pracuje v jiném okně, infikovaná stránka se „překreslí“ a zobrazí přihlašovací okno do některé populární aplikace
  - (Facebook, G-mail, …)
- Uživatel není překvapený (občas vás systém odhlásí) a zadá své údaje
- Podvodník si údaje uloží a přesměruje uživatele do dané aplikace

Typosquatting



Podvod vaším jménem (CSRF)

- Uživatel je přihlášen do nějaké aplikace

  (např. e-banking) a souběžně otevře infikova-nou stránku
- Infikovaná stránka potají pošle z vašeho počítače požadavek (např. převod peněz)
- E-banking provede převod a uživatel nic netuší
- Rada: Kritické aplikace (e-banking) vždy pouštět samostatně v prohlížeči a na závěr prohlížeč zavřít!

Hesla

Hesla

- Heslo je jako klíč k zámku od domu
- Musí být dostatečně těžké na uhádnutí (tzv. silné) a současně dobře zapamatovatelné
- Většina aplikací výslovně zakazuje sdělovat heslo
- Špatný příklad:
  - Uživatelské jméno: novak
  - Heslo: novak

Co radí Microsoft?

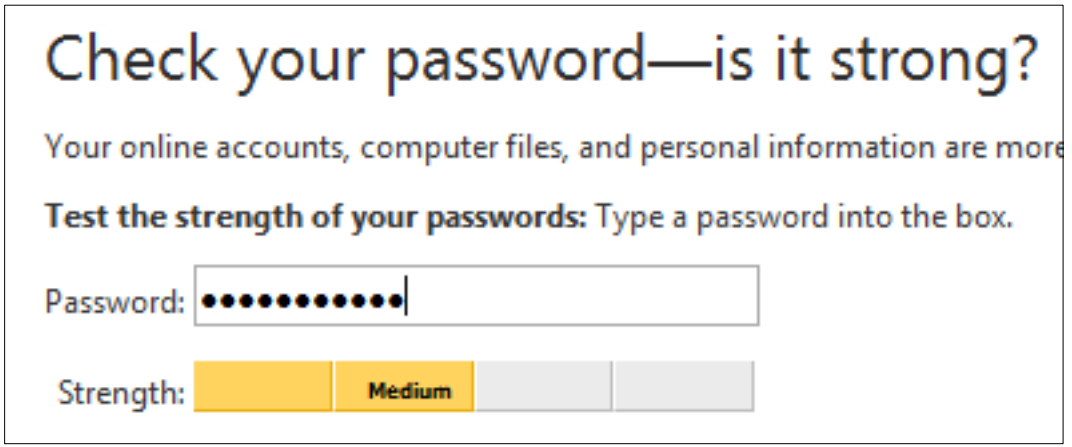
What to do	Suggestion	Example
Start with a sentence or two (about 10 words total).	Think of something meaningful to you.	Long and complex passwords are safest.
Turn your sentences into a row of letters.	Use the first letter of each word.	lacpasikms (10 characters)
Add complexity.	Make only the letters in the first half of the alphabet uppercase.	lACpAsIKMs (10 characters)
Add length with numbers.	Put two numbers that are meaningful to you between the two sentences.	lACpAs56IKMs (12 characters)
Add length with punctuation.	Put a punctuation mark at the beginning.	?lACpAs56IKMs (13 characters)
Add length with symbols.	Put a symbol at the end.	?lACpAs56IKMs" (14 characters)

Zdroj: www.microsoft.com

Hesla – tipy a triky

- Nepoužívejte opakující se znaky a sekvence
  - „asdf“, „1111“, „qwerty“, „12345678“, …
- Heslo si noste v hlavě, a občas změňte :-)
- Ověřte si sílu hesla:

  https://www.microsoft.com/security/pc-security/password-checker.aspx



Anonymita v kyberprostoru

Internet není bezpečné místo

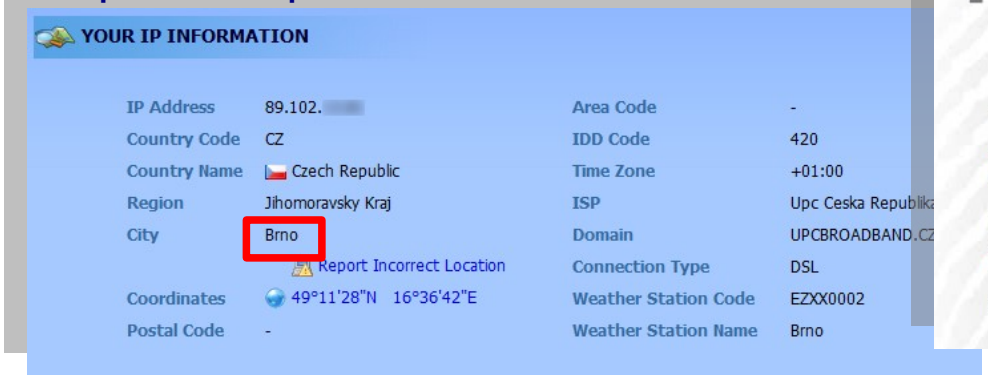
- Jen proto, že Internet nevidíme, neznamená to, že je bezpečný
  - Elektřinu taky nevidíme, ale nestrkáme vidličku do zásuvky

- Internet je prostor jako každý jiný
  - S pocitem anonymity se ale lidé chovají méně ostražitě
  - A proto je cílem mnoha podvodníků

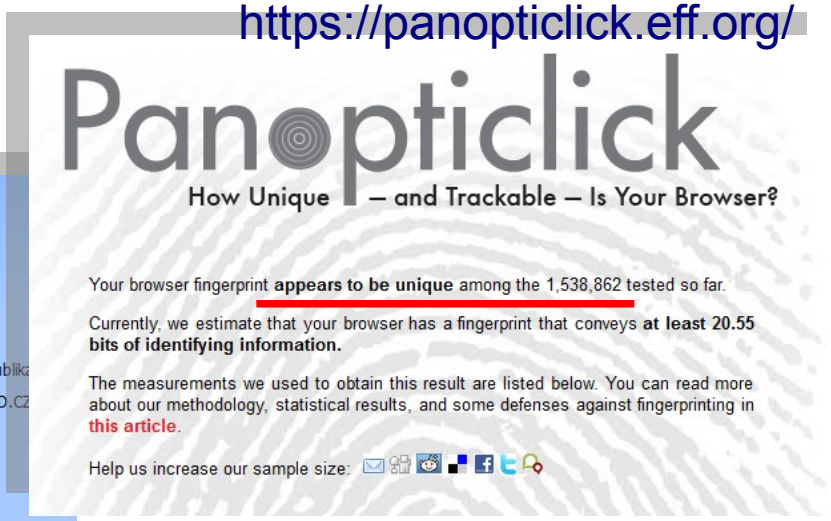
Co o mně ví Internet

- Ačkoliv má uživatel pocit anonymity, opak je pravdou
  - Veřejně dostupné služby (otisk prohlíž., geolokace, Google Analyt., ...)
  - V rámci MU logování provozu (ne obsahu) na síti

http://www.iplocationtools.com/

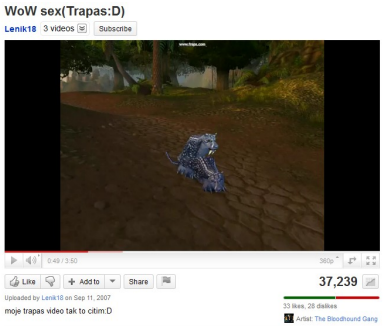


https://panopticlick.eff.org/



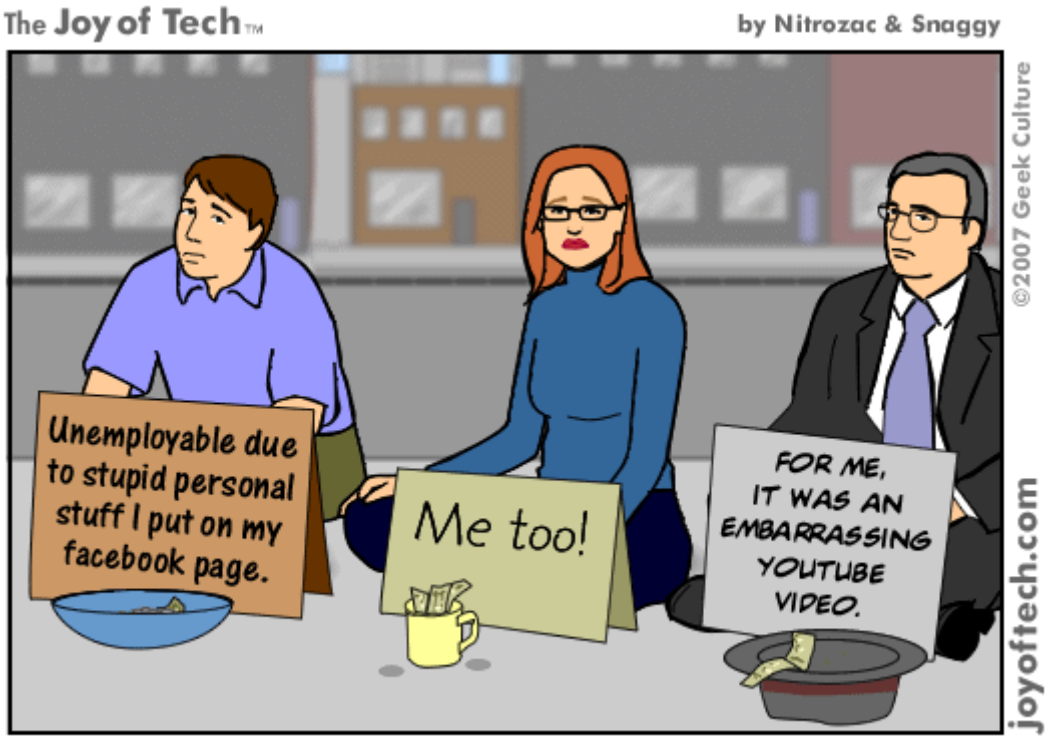
Jak si uživatel chrání soukromí?

- Většinou velmi málo nebo nijak
  - Kdyby vás někdo zastavil na ulici, řeknete mu, kde bydlíte, jaká je vaše e-mailová adresa?
  - Nejspíš ne. Ale na Internetu to většina lidí udělá!
- Uživatelé hojně sdělují informace i sami
  - Příklad, veřejné fotogalerie (Picasaweb, Rajče, …)
  - Facebook a jiné sociální sítě



  - Příklad (Youtube): http://www.youtube.com/watch?v=WS6aW4m4Apk
    - Komentář autorky: „moje trapas video tak to citim:D“

Jak to může dopadnout?



Signs of the social networking times.

Shrnutí

- Ostražitost se vyplácí
  - U phishingu dvojnásob
  - Nezadávat hesla jinam, než jsem zvyklý
- Používat zdravý rozum
- Nemyslet si, že je Internet bezpečné místo
  - Mít neustále „oči na stopkách“
- Rozumně přistupovat ke svému soukromí
  - Nesdělovat na Internetu to, co bych veřejně nesděloval ani běžným způsobem

Děkuji za pozornost
a přeji
žádné bezpečnostní incidenty