

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



Phishing I.

Padělaná hlavička zprávy!

ROZVRH
PŘEDMĚTY
STUDIUM
PŘIJÍMAČKY
VÝVĚSKA
DISKUSE
PERSONÁLNÍ
SETKÁVÁNÍ
ABSOLVENT
ÚSCHOVNA
MŮJ WEB
DOKUMENTY
ELPORTÁL
DRIL
PUBLIKACE
OBCHODNÍ
CENTRUM
STIPENDIA
UDÁLOSTI
SYSTÉM
DESIGN
NÁPOVĚDA
uživatelů 1349
operací 6231

Štítky a podbarvení

From: WEBMAIL ADMINISTRATOR <info@webmaster.cz> [přidat do adresáře](#)
Date: Sun, 15 May 2011 15:15:05 +0200
To: 98943@mail.muni.cz
Subject: Upgrade Váš účet Webmail teď

[Zobrazit hlavičky](#)

Vážený Email Majitel Účtu,

Tato zpráva je z webmailu středisko zpráv do všech webmail účtů vlastníků. V současné době modernizace naší databázi a e-mailový účet centra. Jsme ukončit všechny nepoužívané e-mailových účtů vytvořit prostor pro nových účtů.

Chcete-li zabránit svému účtu byly ukončeny, budete muset aktualizovat tím, že poskytne požadované informace níže:

Potvrdit e-mailovou IDENTITY TEĎ

E-mail Uživatelské jméno:
E-mail: Heslo:

Upozornění! Majitel účtu, že odmítne aktualizovat svůj účet do sedmi dnů od obdržení tohoto varování ztratí svého účtu trvale.

Upozornění Kód: VX2G99AAJ

Díky,
Webmail správce.

Odpovědět | Odpovědět všem | Přeposlat | Smazat | Odeslaná pošta

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

ROZVRH
PŘEDMĚTY
STUDIUM
PŘIJÍMAČKY
VÝVĚSKA
DISKUSE
PERSONÁLNÍ
SETKÁVÁNÍ
ABSOLVENT
ÚSCHOVNA
MŮJ WEB
DOKUMENTY
ELPORTÁL
DRIL
PUBLIKACE
OBCHODNÍ
CENTRUM
STIPENDIA
UDÁLOSTI
SYSTÉM
DESIGN
NÁPOVĚDA

Štítky a podbarvení

From: Toufik Saada <saada@u-pec.fr> přidat do adresáře
Date: Sun, 15 May 2011 15:06:29 +0200
To: 98943@mail.muni.cz
Subject: Důležité upozornění!

[Zobrazit hlavičky](#)

DGTFX byl detekován virus ve schránce. Váš účet Webmail / Mailbox musí být povýšen do naší nové zajištěné DGTFX antivirus, aby nedošlo k poškození našich stránek a sítě. Klikněte na odkaz níže zabezpečit Váš e-mail a aby se zabránilo šíření viru do 48 hodin.

Klikněte zde: <http://www.pinklez.com/rma/use/emailovyucetaktualizace/form1.html>

Omlouváme se za všechny incoveniencies bychom způsobili vy.

Poznámka: Vaše heslo je šifrován pomocí klíčů RSA 1024 bitů pro Vaši bezpečnost.

Děkujeme za vaši spolupráci-operaci.

WEBMAIL INTERNET tým podpory.
Potvrdit váš účet WEBMAIL

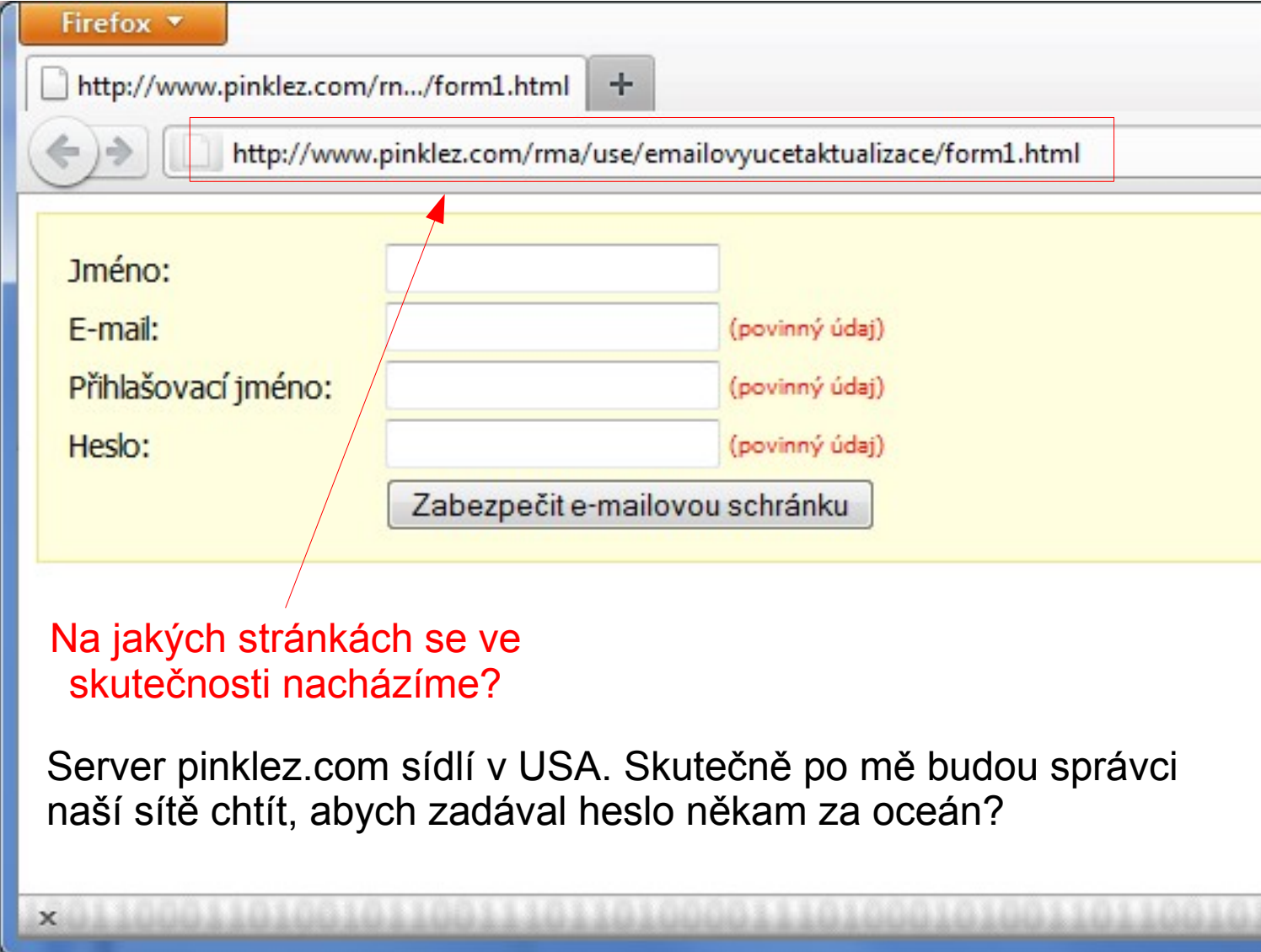
Odpovědět | Odpovědět všem | Přeposlat | Smazat | Odeslaná pošta

Text snažící se
uživatele vystrašit.

Opět strojově
přeložený

Podvodník se
snaží přimět
uživatele
kliknout
na odkaz

Phishing II - pokrač.



Firefox

http://www.pinklez.com/rn.../form1.html

http://www.pinklez.com/rma/use/emailovyucetaktualizace/form1.html

Jméno:

E-mail: (povinný údaj)

Přihlašovací jméno: (povinný údaj)

Heslo: (povinný údaj)

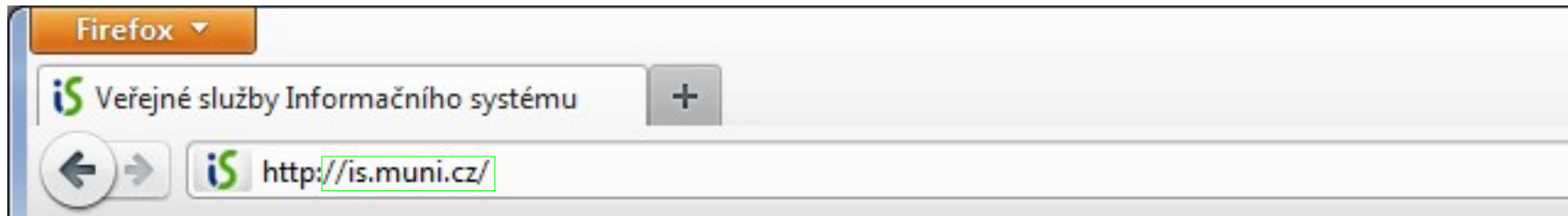
Zabezpečit e-mailovou schránku

Na jakých stránkách se ve skutečnosti nacházíme?

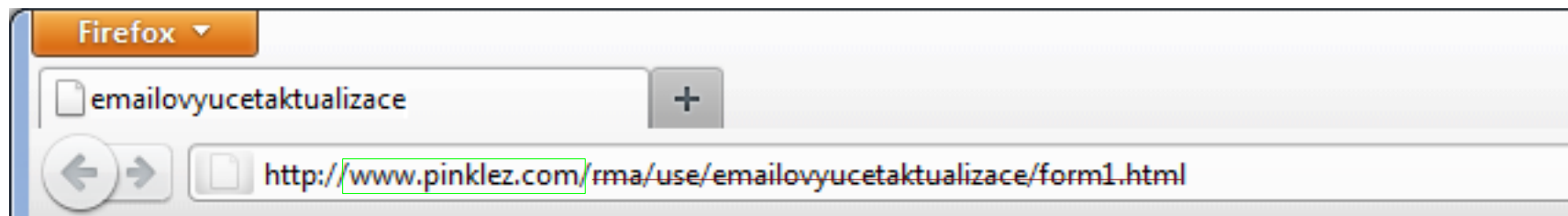
Server pinklez.com sídlí v USA. Skutečně po mě budou správci naší sítě chtít, abych zadával heslo někam za oceán?

Jak na adresu stránky (URL) - I.

- Kde se uživatel nachází?

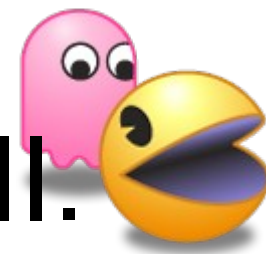


na stránkách IS MU

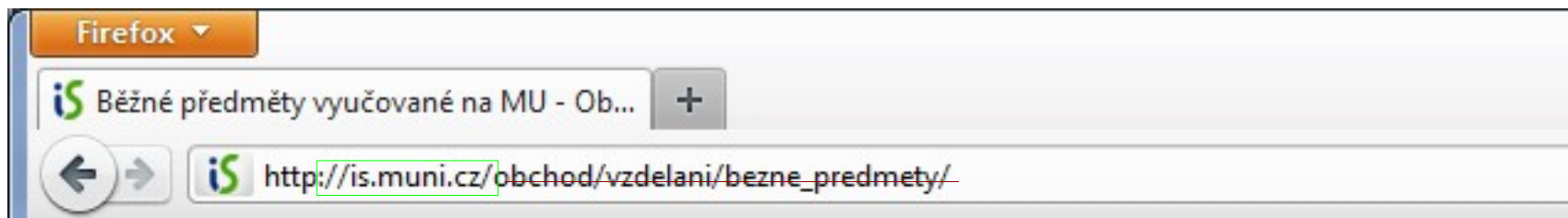


na stránkách www.pinklez.com

Jak na adresu stránky (URL) - II.

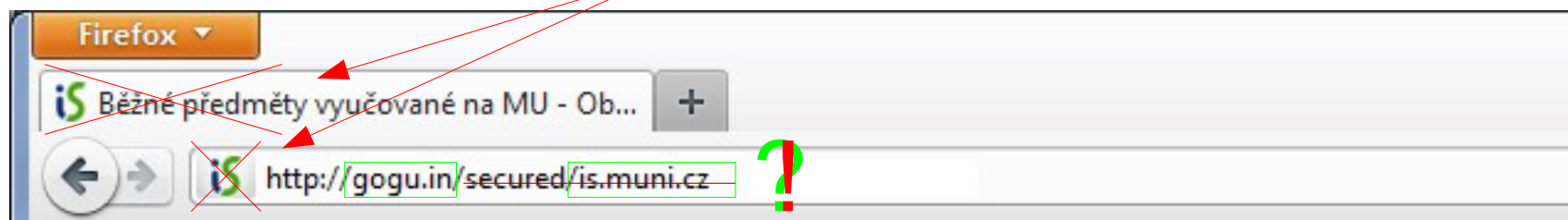


- Kde se uživatel nachází?



na stránkách IS MU

POZOR: Falešná ikona i text!



na stránkách gogu.in, nikoliv na IS MU!



Phishing III.

Opět vidíme
padělanou hlavičku

Oficiální a známý
obrázek zvyšuje
falešný pocit
důvěryhodnosti

Firefox

Dopis: Security Message From Masaryk ...

Štítky a podbarvení

From: <email.service@med.muni.cz> [přidat do adresáře](#)

Date: Sun, 15 May 2011 14:17:55 +0200

To: 98943@mail.muni.cz

Subject: Security Message From Masaryk University

[Zobrazit hlavičky](#)

SquirrelMail
webmail
for
nuts

Dear valued customer,

You have 1 new Security Message Alert!

Log In into your account to update your profile.

[Click here to Log In](#)

You may also visit SquirrelMail official site
at: <https://www.med.muni.cz/squirrelmail/src/login.php>

Masaryk University Webmail Service.

uživatelů 1457
operací 7168

<http://gogu.in/phpfprmgenerator/use/secured/form1.html>

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.

ALE jsme na stránkách „gogu“ v Indii!

Skutečně tam chcete zadávat vaše jméno a heslo?

Známý design stránek

SquirrelMail
webmail
for
nuts

SquirrelMail verze 1.4.17
Vytvořeno týmem SquirrelMail

LF MU Brno - SquirrelMail Přihlásit

Jméno:

Heslo:

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
 - **NE**vyplňovat údaje, **NE**klikat na odkazy a **NE**stahovat 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 internetovou 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

Veřejné služby Informačn... x

← → ↻ ☆ http://is.mumi.cz/ Adresa není is.muni.cz, ale is.mumi.cz (dvakrát „m“)

česky | in English

UNIVERSITAS MASARYKIANA BRUNENSIS

IS.MUNI.CZ

AUTENTIZOVANÝ
E-PŘIHLÁŠKA
OBCHODNÍ CENTRUM
ABSOLVENTSKÁ SÍŤ
ELPORTÁL
NÁŠ SYSTÉM

INFORMAČNÍ SYSTÉM MASARYKOVY UNIVERZITY
Veřejné služby Informačního systému

- IS MU

Osobní administrativa Informačního systému MU
(návody níže)

[WWW stránky Masarykovy univerzity](#)

[Nápověda](#)

E-PŘIHLÁŠKA KE STUDIU

- [e-přihláška na MU](#)
(podání přihlášky ke studiu)
- [Nahlédnutí do přihlášky](#) (stav přihlášky, zkouška a výsledek řízení)
- [Obory, do kterých se právě přijímá](#)
- Informace o [Testu studijních předpokladů](#)
- Vyzkoušejte si [TSP nanečisto](#) • [Diskuse](#)

OBCHODNÍ CENTRUM

- [Obchodní centrum](#) – vzdělávejte se s MU
- [Běžné předměty](#) • [Kurzy](#)
- [Jazykovka při FF](#) • [CŽV pro zisk Bc./Mgr.](#)
- [Přípravky ke zkouškám](#) • [Knihy](#)
- Fakulty: [PrF](#), [LF](#), [PřF](#), [FF](#), [PdF](#), [ESE](#), [FI](#), [FSS](#), [FSpS](#)

Lidé

- [Vyhledávání osob a vyhledávání pracovišť](#)
- [Absolventi a archiv závěrečných prací](#)
 - [klíčová slova abecedně](#)
- [Vkládání souboru do Úschovny osobě z MU](#)
- [Telefony, e-maily a místnosti na fakultě](#)
- [Ověření statutu studenta dle průkazu MU](#)

Podvod vaším jménem (CSRF)

- Uživatel je přihlášen do nějaké aplikace (např. e-banking) a souběžně otevře infikovanou 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.	IACpAsIKMs (10 characters)
Add length with numbers.	Put two numbers that are meaningful to you between the two sentences.	IACpAs56IKMs (12 characters)
Add length with punctuation.	Put a punctuation mark at the beginning.	?IACpAs56IKMs (13 characters)
Add length with symbols.	Put a symbol at the end.	?IACpAs56IKMs" (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>

Check your password—is it strong?

Your online accounts, computer files, and personal information are more

Test the strength of your passwords: Type a password into the box.

Password:

Strength: Medium

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 prohlížeč., geolokace, Google Analyt., ...)
 - V rámci MU logování provozu (ne obsahu) na síti

<http://www.iplocationtools.com/>

YOUR IP INFORMATION

IP Address	89.102. [redacted]	Area Code	-
Country Code	CZ	IDD Code	420
Country Name	Czech Republic	Time Zone	+01:00
Region	Jihomoravsky Kraj	ISP	Upc Ceska Republika
City	Brno	Domain	UPCBROADBAND.CZ
	Report Incorrect Location	Connection Type	DSL
Coordinates	49°11'28"N 16°36'42"E	Weather Station Code	EZXX0002
Postal Code	-	Weather Station Name	Brno

<https://panopticlick.eff.org/>

Panopticlick

How Unique – and Trackable – Is Your Browser?

Your browser fingerprint **appears to be unique** among the 1,538,862 tested so far.

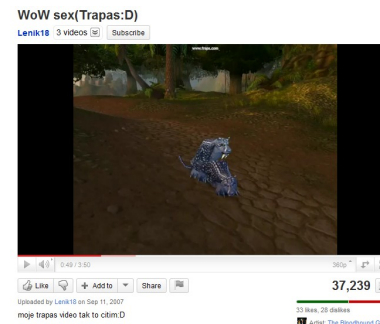
Currently, we estimate that your browser has a fingerprint that conveys **at least 20.55 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in [this article](#).

Help us increase our sample size:

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?

The Joy of Tech™

by Nitrozac & Snaggy



Signs of the social networking times.

Shrnutí

- Ostražitost se vyplácí
 - U phishingu dvojnásob
 - Nežadávat 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
 - Nездělovat na Internetu to, co bych veřejně nездěloval ani běžným způsobem

Děkuji za pozornost
a přeji
žádné bezpečnostní incidenty