

Jak zjistit, jestli nejsme obětí kybernetické kriminality

Šárka Vavrečková

Ústav informatiky, FPF SU Opava

sarka.vavreckova@fpf.slu.cz

Poslední aktualizace: 20. listopadu 2014

Dvoufaktorová autentizace

Co to je?

- účel: co nejvíc ztížit „cracknutí“ účtu, bezpečná možnost důkazu, že „jsem to já“
- nestačí dvojice jméno+heslo (jméno určuje, heslo autentizuje)
- dvoufaktorová: kromě hesla autentizujeme ještě jinak, nezávisle na hesle

Základní metody autentizace

- **něco vím a jen já to vím** (bez této znalosti se dál nedostanu) – heslo, PIN, odpověď na bezpečnostní otázku
- **něco mám a jen já to mám** (bez této věci se dál nedostanu) – průkaz, klíč (fyzický), karta, hardwarový token, smartphone
- **něčím jsem a jen já tím jsem** (souvisí to s mou fyzickou existencí) – biometrie (otisk prstu, rohovka oka, identifikace hlasu, chůze, apod.)

Typická dvoufaktorová autentizace

- musím kombinovat alespoň dvě z těchto kategorií (multifaktorová: více než dvě)
- většinou: heslo a autentizační řetězec zaslaný v SMS na smartphone (něco vím + něco mám)

Základní metody autentizace

- **něco vím a jen já to vím** (bez této znalosti se dál nedostanu) – heslo, PIN, odpověď na bezpečnostní otázku
- **něco mám a jen já to mám** (bez této věci se dál nedostanu) – průkaz, klíč (fyzický), karta, hardwarový token, smartphone
- **něčím jsem a jen já tím jsem** (souvisí to s mou fyzickou existencí) – biometrie (otisk prstu, rohovka oka, identifikace hlasu, chůze, apod.)

Typická dvoufaktorová autentizace

- musím kombinovat alespoň dvě z těchto kategorií (multifaktorová: více než dvě)
- většinou: heslo a autentizační řetězec zaslaný v SMS na smartphone (něco vím + něco mám)

Problémy

- problém mezi židlí a klávesnicí (uživateli se nedaří, uživatel protestuje, uživatel odmítá, uživatel zahlučuje servisní podporu)
- není až tak neprůstředná, jak by se mohlo zdát
- mohou nastat technické problémy (např. u biometrie), nebo u podmínky „něco mám“ to „zrovna nemám“
- může přestat být dvoufaktorovou (např. když přes smartphone přistupujeme tam, kde je druhým faktorem „něco mám“ právě smartphone)

U mnoha služeb je volitelná (Google, Facebook, atd.).

Zdroje

- <http://www.systemonline.cz/it-security/dvoufaktorova-autentizace-myty-a-realita.htm>
- <http://www.cleverandsmart.cz/vicefaktorova-autentizace/>

Facebook

- dá se zjistit, ze kterých zařízení se připojuji (lokalizace, také IP po najetí myší)
- když vidím jiné zařízení (lokalizaci) než co patří mně, klepnu na „Ukončit aktivitu“ (zobrazí se jen u jiného záznamu, než je ten můj) a okamžitě měním heslo
- dá se zapnout druhý faktor pro autentizaci v případě, že se přihlašuji z netypického zařízení

 Vyhledávání přátel 

 Šárka [Hlavní stránka](#) [Vyhledat přátele](#)      **Nastavení**

 Obecně

 **Zabezpečení**

 Soukromí

 Timeline a označování

 Blokování

 Upozornění

 Mobile

 Sledující

 Aplikace

 Reklamy

 Platby

 Panel podpory

 Video

Nastavení zabezpečení

Upozornění na přihlášení	Nechte si zasílat upozornění, když se někdo pokusí dostat k vašemu účtu.	Upravit
Schválení přihlášení	Použijte telefon jako další vrstvu zabezpečení, aby se k vašemu účtu nemohl nikdo přihlásit neoprávněně.	Upravit
Generátor kódů	Použijte aplikaci Facebook k získání bezpečnostních kódů, když je budete potřebovat.	Upravit
Hesla k aplikacím	Do aplikací se můžete přihlašovat pomocí speciálních hesel místo použití hesla k Facebooku nebo kódů pro schválení přihlášení.	Upravit
Důvěryhodné kontakty	Vyberte přátele, na které se můžete obrátit, aby vám pomohli dostat se zpět k účtu, když k němu někdy ztratíte přístup.	Upravit
Důvěryhodné prohlížeče	Podívejte se, které prohlížeče jste si uložili jako často používané.	Upravit
Kde jste přihlášení	Stávající relace Lokalita Opava, Moravskoslezský kraj, Česká republika (přibližně) Typ zařízení Firefox v systému Windows 7 Zavřít	

[Deaktivujte svůj účet.](#)

 Vyhledávání přátel 

 Šárka [Hlavní stránka](#) [Vyhledat přátele](#)    

Obecně

Zabezpečení

Soukromí

Timeline a označování

Blokování

Upozornění

Mobile

Sledující

Aplikace

Reklamy

Platby

Panel podpory

Videa

Nastavení zabezpečení

Upozornění na přihlášení	Nechte si zasílat upozornění, když se někdo pokusí dostat k vašemu účtu.	Upravit
Schválení přihlášení	☐ Vyžadovat bezpečnostní kód pro přístup k mému účtu z neznámých prohlížečů [?]	
Uložit změny Storno		
Generátor kódů	Použijte aplikaci Facebook k získání bezpečnostních kódů, když je budete potřebovat.	 Upravit
Hesla k aplikacím	Do aplikací se můžete přihlašovat pomocí speciálních hesel místo použití hesla k Facebooku nebo kódů pro schválení přihlášení.	Upravit
Důvěryhodné kontakty	Vyberte přátele, na které se můžete obrátit, aby vám pomohli dostat se zpět k účtu, když k němu někdy ztratíte přístup.	Upravit
Důvěryhodné prohlížeče	Podívejte se, které prohlížeče jste si uložili jako často používané.	Upravit
Kde jste přihlášení	Zkontrolujte a nastavte, kde jste momentálně přihlášení k Facebooku.	Upravit

Google

Google

- můžeme zkontrolovat, ze kterých zařízení bylo realizováno připojení (Nastavení, Zabezpečení)
- můžeme zakázat, případně změníme heslo

The screenshot shows the Google Account security page for user sarka.vavreckova@gmail.com. The 'Zabezpečení' (Security) tab is selected and highlighted with a red box. A red arrow points to the user's profile picture in the top right corner. The 'Přihlášení' (Sign-in) section includes fields for username, password, and recovery information, with a large yellow redaction box covering the password and recovery details. The 'Nedávná činnost' (Recent activity) section shows a list of devices and activities, with a red box highlighting the 'Zobrazit' (View) link for the 'Zařízení a aktivity' (Devices and activity) section. The 'Upozornění' (Warnings) section shows a warning about phone calls, with a yellow redaction box covering the details. The 'Oprávnění účtu' (Account permissions) section shows a list of applications and websites, with a yellow redaction box covering the details. The 'Zobrazit aktivitu' (View activity) link is also highlighted with a red box.

Google

sarka.vavreckova@gmail.com

Osobní údaje **Zabezpečení** Jazyk Datové nástroje Historie účtu Náповěda

Přihlášení

Uživatelské jméno sarka.vavreckova@gmail.com

Alternativní uživatelská jména [Upravit](#)

Heslo [Změnit heslo](#)

Telefon pro obnovení

Email pro obnovu

Bezpečnostní otázka

Dvoufaktorové ověření

Nedávná činnost

Zařízení a aktivity Všechna zařízení spojená s účtem Google [Zobrazit](#) [Přidat účet](#) [Odhlásit se](#)

Oznámení a upozornění Bezpečnostní události přivazované k vašemu účtu. [Zobrazit vše](#)

Upozornění

Odesílat telefonická upozornění

Oprávnění účtu

Aplikace a webové stránky

Přístup pro méně bezpečné aplikace

Šárka Vavrecková
sarka.vavreckova@gmail.com
[Účet](#) [Ochrana soukromí](#)
[Přidat se na Google+](#)

[Zobrazit aktivitu](#)

Google

Google



sarka.vavreckova@gmail.com ▾

Osobní údaje

Zabezpečení

Jazyk

Datové nástroje

Historie účtu

Nápověda

Všimli jste si něčeho podezřelého? [Zabezpečte svůj účet](#)

Zařízení a aktivita



Windows

Praha, Česká republika **AKTUÁLNÍ ZAŘÍZENÍ**

PMP7280C

Česká republika - 4. listopadu, 17:21

Google



 sarka.vavreckova@gmail.com ▾

Osobní údaje

Zabezpečení

Jazyk

Datové nástroje

Historie účtu

Nápověda

 Všimli jste si něčeho podezřelého? [Zabezpečte svůj účet](#)

←

Zařízení a aktivita

ⓘ

 Windows

Praha, Česká republika

AKTUÁLNÍ ZAŘÍZENÍ



PMP7280C

Naposledy synchronizováno: 4. listopadu 2014 v 17:21 ⓘ

[Najděte svá zařízení Android pomocí Správce zařízení Android](#)

Přístup

Úplný přístup k účtu ⓘ

Odstranit přístup

Naposledy použitá poloha ⓘ

Česká republika - 4. listopadu, 17:21

E-mail

- služba Institutu softwarových technologií Hassa Plattnera v Postupimi:
 - databáze ukradených identit
 - pokud se najdeme, máme problém
 - pokud se nenajdeme, nemusíme mít problém

<https://sec.hpi.uni-potsdam.de/leak-checker/search>

Hasso-Plattner-Institut

Identity Leak Checker
by Hasso Plattner Institut

Home Statistics FAQ Response E-mails

Is someone spying on you?

Everyday personal data is stolen in criminal cyber attacks. A large part of the stolen information is subsequently made public on Internet databases, where it serves as the starting point for other illegal activities.

With the HPI Identity Leak Checker, it is possible to check whether your e-mail address, along with other personal data (e.g. telephone number, date of birth or address), has been made public on the Internet where it can be misused for malicious purposes.

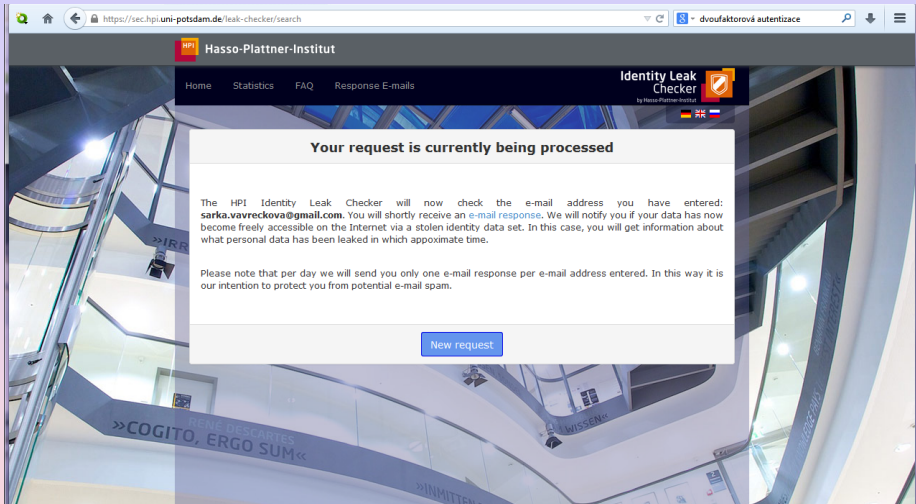
 sarka.vavreckova@gmail.com

The e-mail address you have entered will only be used for searching in our database and, when applicable, to subsequently send an e-mail notification. It will be saved in an obfuscated way to protect you from potential e-mail spam and is never given to a third party.

Check e-mail address!

Our other services and research on IT security

HPI-VDB	- Our database for IT attack analysis and self-diagnosis,
tele-TASK	- Lectures, not only on IT security,
openHPI	- Our interactive online educational program.



https://sec.hpi.uni-potsdam.de/leak-checker/search

Hasso-Plattner-Institut

Home Statistics FAQ Response E-mails

Identity Leak Checker
by Hasso-Plattner-Institut

»IRR«

»COGITO, ERGO SUM«

»WISSEN«

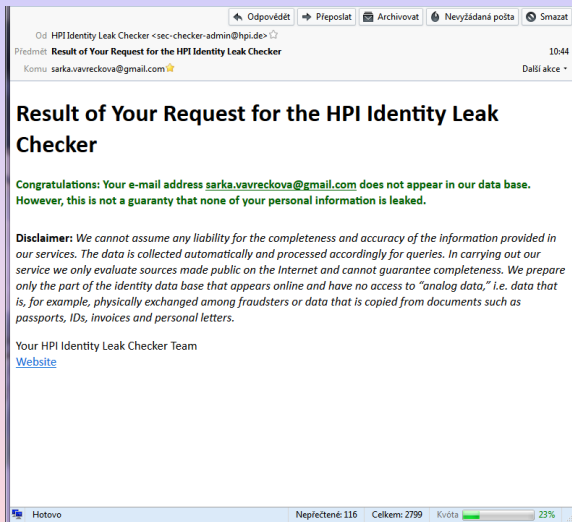
»INMITTEN«

Your request is currently being processed

The HPI Identity Leak Checker will now check the e-mail address you have entered: **sarka.vavreckova@gmail.com**. You will shortly receive an [e-mail response](#). We will notify you if your data has now become freely accessible on the Internet via a stolen identity data set. In this case, you will get information about what personal data has been leaked in which approximate time.

Please note that per day we will send you only one e-mail response per e-mail address entered. In this way it is our intention to protect you from potential e-mail spam.

New request



Na počítači

- základ: aktualizace, antivir, firewall
- aktualizace aplikací: Secunia PSI
http://secunia.com/vulnerability_scanning/personal/
- bezpečnostní kontrola prohlížeče:
http://www.check-and-secure.com/browsercheck/_en/

www.check-and-secure.com/browsercheck/_en/

STOP | THINK | CONNECT

HO
Hox-Slayer

Browser & Plugin-Check

1 Start 2 Check Internet Access 3 Browser & Plugin-Check 4 Cyber-Vaccination 5 Other Measures

 Your Firefox with version 33 is up to date.

83% of all malware infections could have been avoided, if the browser plugins had been updated in the first place. Please find below the scan results for your installed plugins:

PLUGIN-DETAILS	RESULT	ACTION
Silverlight Plug-In	5.1.30514.0	Latest i
Adobe Acrobat	11.0.9.29	Latest i
Java Deployment Toolkit 7.0.710.14	1.7.0.71	Latest i
Java(TM) Platform SE 7 U71	1.7.0.71	Latest i
Shockwave Flash Shockwave Flash 15.0 r0	15.0.0.223	Latest i

Router

- bezpečnostní nastavení (změnit administrátorské jméno a heslo, případně SSID a další, nastavit bezpečné šifrování), aktuální firmware
- xDSL router je pod stálou palbou, je vhodné ho otestovat
- <http://checkmyrouter.org/>
- <https://www.grc.com/shieldsup>