# Bezpečnost Internetu

### M. Indra, SSČ AV ČR, v.v.i.

- ☐ Úvod: Bezpečnost přenosu dat v Internetu
- ☐ Bezpečnostní incidenty v Internetu
- ☐ Ochrana soukromí na internetu

# Bezpečnost přenosu dat v Internetu

## Přenos dat po Internetu zajišťují protokoly TCP/IP

**První komunikační testy mezi dvěma různými sítěmi Standfordovou a londýnskou univerzitou využívající protokoly TCP/IP se uskutečnily již v roce 1975.**

**Základní, stále používané přenosové protokoly, např. Telnet, FTP, HTTP přenáší data v nechráněné podobě, teoreticky je možné je odposlechnout a zneužít.**

# Bezpečnost přenosu dat v Internetu

## Přenosové mechanismy založené na šifrování

**VPN** (virtuální privátní síť). Bezpečnost přenosu dat zaručuje šifrovaný tunel mezi stanicemi účastníků přenosu.

- Připojení vzdáleného uživatele do sítě pracoviště
- Připojení vzdálené pobočky k hlavnímu pracovišti
- Komunikace uživatele přes veřejný VPN server

**HTTPS** (protokol umožňující zabezpečenou komunikaci).

- Webmail
- Internetové bankovnictví
- E-shop

# Bezpečnost přenosu dat v Internetu

## Bezpečnostní aplikace založené na šifrování

**Elektronický podpis (digitální podpis) plně nahrazuje vlastnoruční podpis při elektronické komunikaci. Vytváří se vždy pro konkrétní data a proto umožňuje ověřit nejen identitu odesílatele, ale i integritu podepsaného dokumentu.**

**K vytvoření důvěryhodného elektronického podpisu je třeba kvalifikovaný digitální certifikát vydaný důvěryhodnou (kvalifikovanou) Certifikační autoritou.**

# Bezpečnost přenosu dat v Internetu

## Certifikační autority dostupné v ČR

**Kvalifikované certifikační autority:**
**První certifikační autorita, a.s. (www.ica.cz)**
**Česká pošta, s.p. (www.postsignum.cz)**
**EIdentity, a.s. (www.eidentity.cz)**

**Certifikáty (kvalifikované) vydané těmito organizacemi jsou určené pro běžné použití i pro zabezpečenou komunikaci se státní správou.**

**CESNET CA:** **www.cesnet.cz/sluzby/**

**Certifikáty vydané CESNET CA nejsou určené pro komunikaci se státní správou, ale např. pro komunikaci při řešení vědeckovýzkumných projektů mezi členy sdružení CESNET z.s.p.o.**

# Bezpečnost přenosu dat v Internetu

## Shrnutí

- **Základní stále používané přenosové protokoly sítí Internet (HTTP, Telnet, FTP,…) řeší bezpečnost přenášených dat nedostatečně, např. nebrání jejich neoprávněnému získání (odposlechu).**
- **Pro bezpečný přenos dat v síti Internet je třeba používat přenosové mechanismy (protokoly) založené na šifrování (VPN, HTTPS, SSH, FTPS, …).**
- **Pro ověření identity odesílatele a integrity dokumentu je třeba použít elektronický podpis.**

# Bezpečnostní incidenty v Internetu

**Kybernetické bezpečnostní incidenty (ZKB): kybernetické události, které představují narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí v elektronických komunikacích.**

**K bezpečnostním incidentům řadíme i neoprávněné šíření a sdílení autorských děl.**

**Cílem většiny bezpečnostních incidentů je přímý nebo zprostředkovaný zisk**

# Bezpečnostní incidenty Internetu

## Kategorie bezpečnostních incidentů vychází z Vyhlášky o kybernetické bezpečnosti z 15.12.2014

- **Neoprávněná činnost v síti - hacking (packet sniffing, port scanning, password cracking), DoS, DDoS…**
- **Šíření škodlivých kódů (malware, infikované webové stránky, …)**
- **Šíření podvržených stránek (phishing)**
- **Šíření spamů a hoaxů**
- **Porušování autorských práv (neoprávněné šíření multimediálních dat)**

# Bezpečnostní incidenty v Internetu

## Neoprávněná činnost v počítačové síti - hacking

**Bezpečnostní incidenty využívající bezpečnostní slabiny síťových zařízení, nedostatečně zabezpečená uživatelská data a nedostatečně zabezpečenou síťovou infrastrukturu.**

**Kevin Mitnick: pravděpodobně nejznámější hacker**
**(používal metody sociálního inženýrství)**

**Hackerské skupiny: Anonymous (ACTA), LulzSec (CIA)**

---

**RFC 1392: Internet Users' Glossary**

**The „hacker“ is a person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where „cracker” would be the correct term☺**

# Bezpečnostní incidenty v Internetu
## Neoprávněná činnost v počítačové síti - hacking

### Motivace hackerů

- Osobní obohacení (útočníka nebo třetí strany)
- Forma zábavy
- Výzva pokořit složitou bezpečnostní ochranu

- Forma protestu
- Prezentace osobních postojů, poselství, …

# Bezpečnostní incidenty v Internetu

## Neoprávněná činnost v počítačové síti - hacking

### Nejčastější metody hackerů, které mohou vést k napadení síťového zařízení

- Skenování portů (hledání otevřených portů - backdoors)
- Hledání bezpečnostních „děr“ systémů a aplikací
- Nelegální získávání hesel (odposlech, phishing, cracking, keylogger, …)

### Po úspěšném průniku do síťového zařízení většinou následuje

- Převzetí kontroly nad zařízením, zcizení všech uložených hesel, kontaktů, osobních dat, fotografií …
- Vložení škodlivého kódu (typické např. pro webové servery)
- Využití napadeného zařízení pro další nelegální činnost

# Bezpečnostní incidenty v Internetu
## Neoprávněná činnost v počítačové síti - hacking

**Příklady využití napadeného zařízení k nelegální činnosti:**

- Zařazení do botnetu za účelem
  - Omezování přístupu k informačním zdrojům (DDoS)
  - Masivního šíření škodlivých kódů nebo spamů
  - cíleného šíření škodlivých kódů, např. na konkrétní OS, síť, organizaci …

- Nástroj k napadání dalších síťových zařízení

**K útokům dochází kontinuálně s různou intenzitou**

# Bezpečnostní incidenty v Internetu

## Neoprávněná činnost v počítačové síti – hacking

## Shrnutí

**Pravděpodobnost napadení síťových zařízení nelze nikdy zcela vyloučit, ale lze ji výrazně snížit:**

- **Dostatečným zabezpečením (firewall, silné heslo, aktualizovaný software, …)**
- **Průběžnou kontrolou (Windows Sysinternals)**
- **Dodržováním standardních bezpečnostních zásad (opatrnost při otevírání příloh, návštěvách webových stránek, přístupu ke sdíleným adresářům,…)**

**ShieldsUP!: https://grc.com/stevegibson.htm#projects**

# Bezpečnostní incidenty Internetu

## Kategorie bezpečnostních incidentů vychází z Vyhlášky o kybernetické bezpečnosti z 15.12.2014

- **Neoprávněná činnost v síti – hacking (Packet Sniffing, Port Scanning, Password Cracking, DoS… )**
- **Šíření škodlivých kódů (malware, infikované webové stránky, …)**
- **Šíření spamů a hoaxů**
- **Šíření podvržených stránek (phishing, …)**
- **Porušování autorských práv (neoprávněné šíření multimediálních dat)**

# Bezpečnostní incidenty v Internetu

## Šíření škodlivých kódů

www.govcert.cz, www.symantec.com

**Klasické počítačové viry z 90.let odstranitelné jednoduše a bez následků jednoúčelovým „odvirovacím“ programem se dnes prakticky již nevyskytují. Nahradily je sofistikované škodlivé kódy – malware (viry, červy, trojské koně, spyware, adware).**

**K jejich odstranění je většinou nutná reinstalace počítače.**

**Škodlivé kódy jsou vytvářeny hlavně za účelem zisku, často obsahují prvky sociálního inženýrství.**

# Bezpečnostní incidenty v Internetu

## Šíření škodlivých kódů

www.viry.cz

**Ransomware (kryptovirus):** **blokuje přístup k infikovanému PC nebo k běžícím aplikacím. Za odblokování vyžaduje zaplacení výkupného (*ransom*). Některé formy ransomware šifrují soubory na pevném i připojeném sdíleném disku.**

**WannaCry**

Ooops, your files have been encrypted!

**What Happened to My Computer?**

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

# Bezpečnostní incidenty v Internetu

## Šíření škodlivých kódů

press.avast.com

**Ransomware může být směrován na:**

- **Koncové uživatele a menší podniky (e-mail, ilegální software)**
- **Konkrétní významné cíle, např. velké společnosti, doprava, zdravotnictví (FN Brno, březen 2020 - RDP)**

**Během pandemie – březen a duben nárůst o 40%**

# Bezpečnostní incidenty v Internetu

## Šíření škodlivých kódů

www.viry.cz

### Škodlivé kódy určené pro PC se šíří

- V přílohách e-mailů
- Prostřednictvím přenosových médií (USB flash)
- Prostřednictvím sdílených adresářů (Dropbox, OneDrive, Google Drive, uloz.to, …)
- Zneužitím Vzdálené plochy

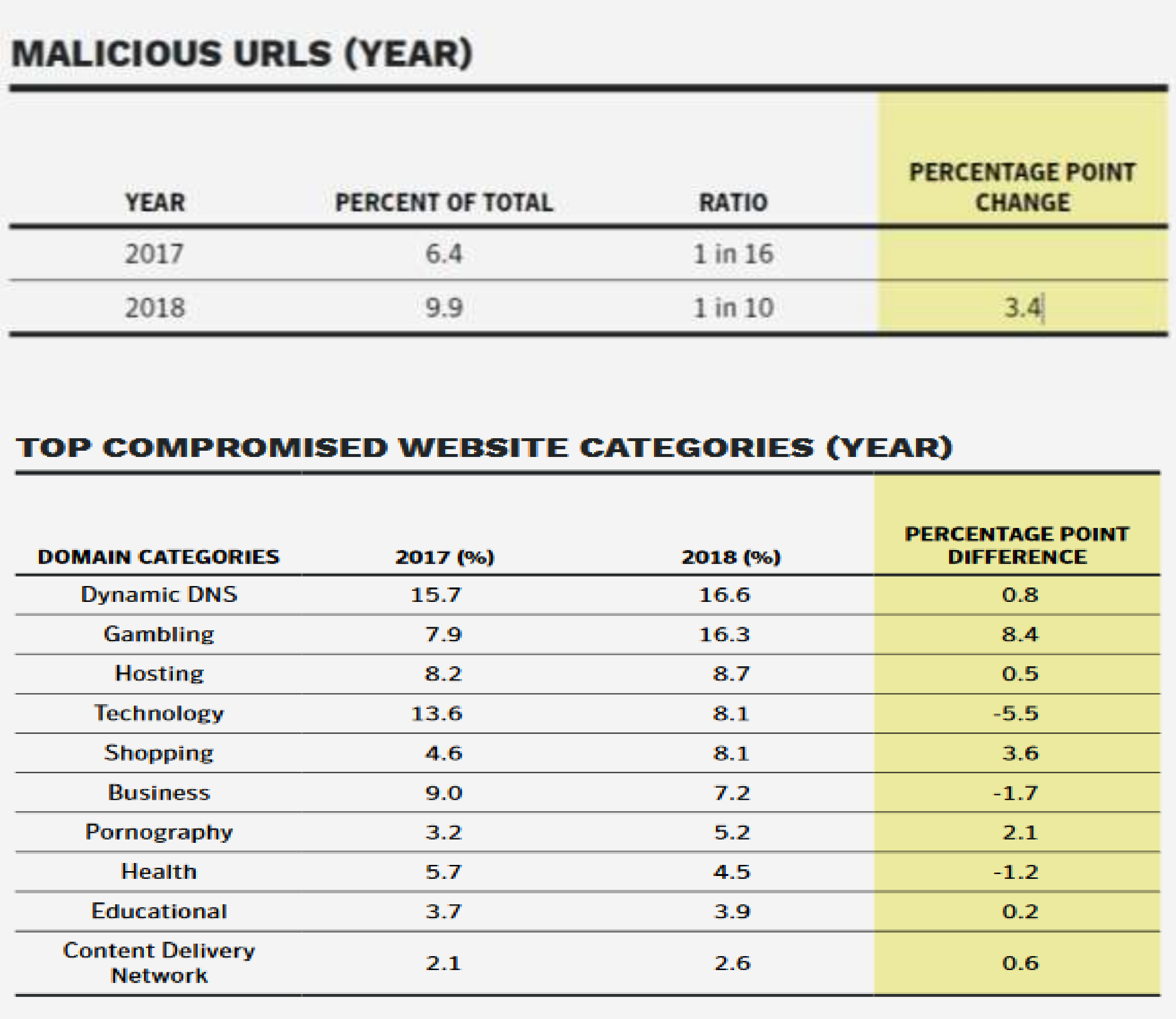
### Škodlivé kódy určené pro mobilní zařízení se šíří

- Prostřednictvím aplikací např. Qrecorder, Blockers call, Word Translator (Google Play) – cílí na internetové bankovnictví

# Bezpečnostní incidenty v Internetu

## Infikované webové stránky (stránky se škodlivým kódem)

**www.symantec.com**



### MALICIOUS URLS (YEAR)

| YEAR | PERCENT OF TOTAL | RATIO | PERCENTAGE POINT CHANGE |
|---|---|---|---|
| 2017 | 6.4 | 1 in 16 | |
| 2018 | 9.9 | 1 in 10 | 3.4 |

### TOP COMPROMISED WEBSITE CATEGORIES (YEAR)

| DOMAIN CATEGORIES | 2017 (%) | 2018 (%) | PERCENTAGE POINT DIFFERENCE |
|---|---|---|---|
| Dynamic DNS | 15.7 | 16.6 | 0.8 |
| Gambling | 7.9 | 16.3 | 8.4 |
| Hosting | 8.2 | 8.7 | 0.5 |
| Technology | 13.6 | 8.1 | -5.5 |
| Shopping | 4.6 | 8.1 | 3.6 |
| Business | 9.0 | 7.2 | -1.7 |
| Pornography | 3.2 | 5.2 | 2.1 |
| Health | 5.7 | 4.5 | -1.2 |
| Educational | 3.7 | 3.9 | 0.2 |
| Content Delivery Network | 2.1 | 2.6 | 0.6 |

**Formjacking**

# Bezpečnostní incidenty v Internetu

## Nutnou (ne postačující) podmínkou pro bezpečné surfování po internetu je bezpečný webový prohlížeč

**Vybraných 5 TOP prohlížečů roku 2020 (www.2-spyware.com):**

- **Mozilla Firefox**
- **Microsoft Edge**
- **Google Chrome**
- **Opera**
- **Vivaldi**

**Žádný prohlížeč není dokonalý ve všech parametrech**

- **Úrovní bezpečnosti před malwarem**
- **Úrovní ochrany osobních údajů**
- **Množstvím Informací poskytovaných třetím stranám**
- **Uživatelským komfortem**

# Bezpečnostní incidenty v Internetu

## Šíření škodlivých kódů

### Jak poznáte, že Váš PC, notebook byl napaden, obsahuje aktivní škodlivý kód

- Podezřele pomalý chod PC, notebooku
- Samovolně vyskakující okna s reklamou
- Mizení souborů a ikon

- "Falešný antivirus" brání instalaci jiných antivirů
- Nejsou dostupné stránky antivirových programů
- Po přihlášení je Váš počítač "blokován"

# Bezpečnostní incidenty v Internetu

## Malware v mobilních zařízeních

- Vynucuje „klik“ na reklamní banner (HummingBad)
- Odesílá prémiové SMS
- Získává lokalizační a přihlašovací údaje (Blockers call2019)
- Existuje i mobile ransomware
- Umožňuje útočníkovi převzít kontrolu nad napadeným přístrojem (CopyCat)

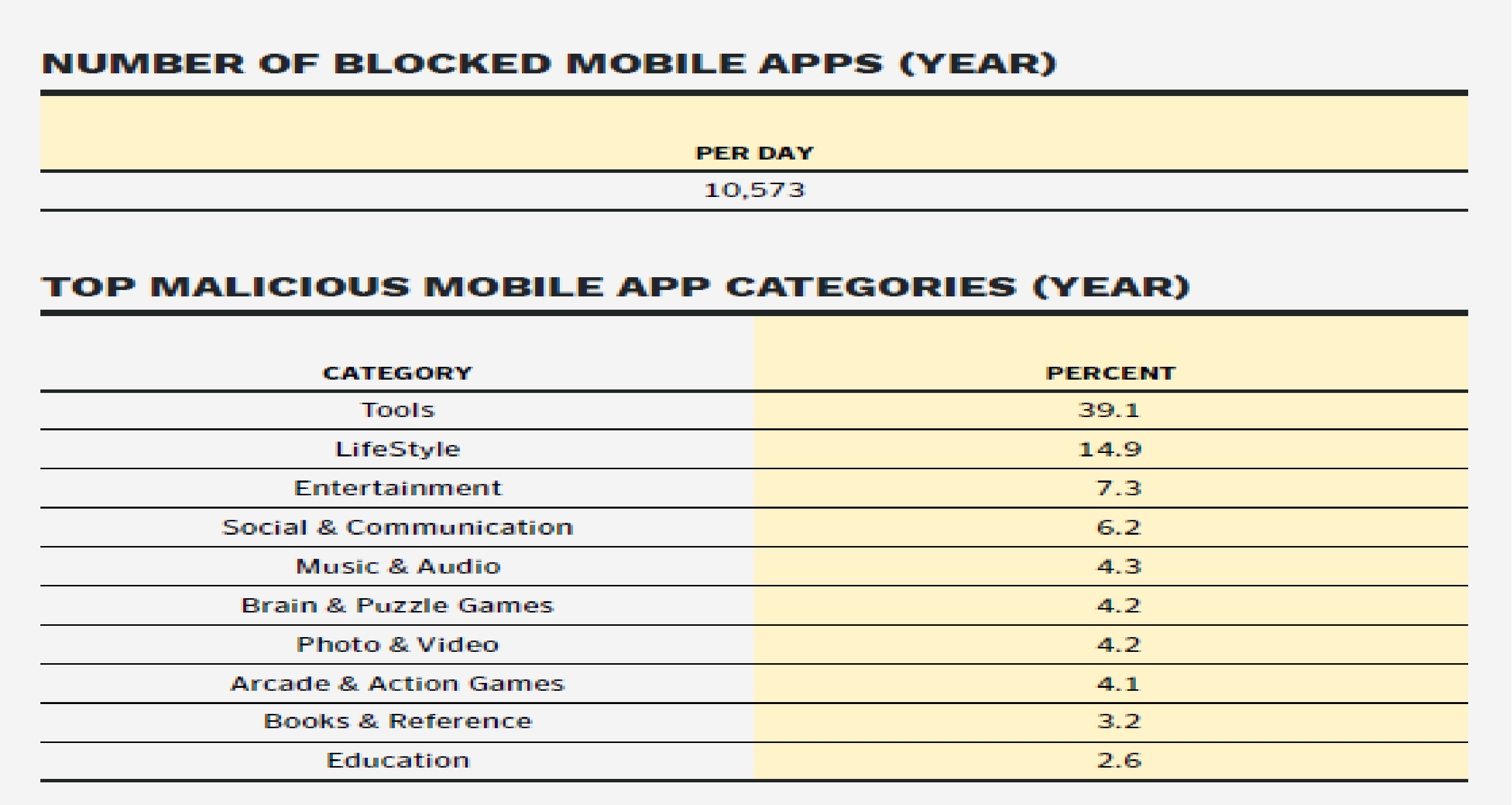
**Bezpečnostní riziko napadení se výrazně zvyšuje v případě používání aplikací stažených z neověřených zdrojů, nebo neodborným používáním jailbreak (IOS), root (Android)** !

# Bezpečnostní incidenty v Internetu

## Malware pro mobilní zařízení

## www.symantec.com

**99.9 % detekovaného malware pro mobilní zařízení pochází z aplikací třetích stran**



### NUMBER OF BLOCKED MOBILE APPS (YEAR)

| PER DAY |
|---|
| 10,573 |

### TOP MALICIOUS MOBILE APP CATEGORIES (YEAR)

| CATEGORY | PERCENT |
|---|---|
| Tools | 39.1 |
| LifeStyle | 14.9 |
| Entertainment | 7.3 |
| Social & Communication | 6.2 |
| Music & Audio | 4.3 |
| Brain & Puzzle Games | 4.2 |
| Photo & Video | 4.2 |
| Arcade & Action Games | 4.1 |
| Books & Reference | 3.2 |
| Education | 2.6 |

# Bezpečnostní incidenty v Internetu

## Šíření škodlivých kódů

## Shrnutí

**Chránit se  před škodlivými kódy znamená**

- **Používat aktualizovaný antivirový program (i na mobilu)**
- **Používat aktualizovaný webový prohlížeč**
- **Uváženě otevírat e-mailové přílohy**
- **Opatrně přistupovat k datovým úložištím (usb, sdílené disky)**
- **Z rozmyslem stahovat bezplatný software, aplikace**
- **Vyhýbat se nedůvěryhodným webovým stránkám (QR)**
- **„Nevylepšovat“ mobilní telefony (jailbreak, root)**

- **Sledovat informace např. www.viry.cz, www.govcert.cz**

# Bezpečnostní incidenty Internetu

## Kategorie bezpečnostních incidentů vychází z Vyhlášky o kybernetické bezpečnosti z 15.12.2014

- **Neoprávněná činnost v síti – hacking (Packet Sniffing, Port Scanning, Password Cracking, DoS… )**
- **Šíření škodlivých kódů (malware, infikované webové stránky, …)**
- **Šíření podvržených stránek (phishing, …)**
- **Šíření spamů a hoaxů**
- **Porušování autorských práv (neoprávněné šíření multimediálních dat)**

# Bezpečnostní incidenty v Internetu

## Podvržené stránky

https://www.hoax.cz/phishing/co-je-to-phishing

**Phishing (Pharming):** metoda využívající kopie webových stránek, falešné e-maily nebo zprávy programů pro instant messaging s cílem zneužít identitu jejich příjemce.

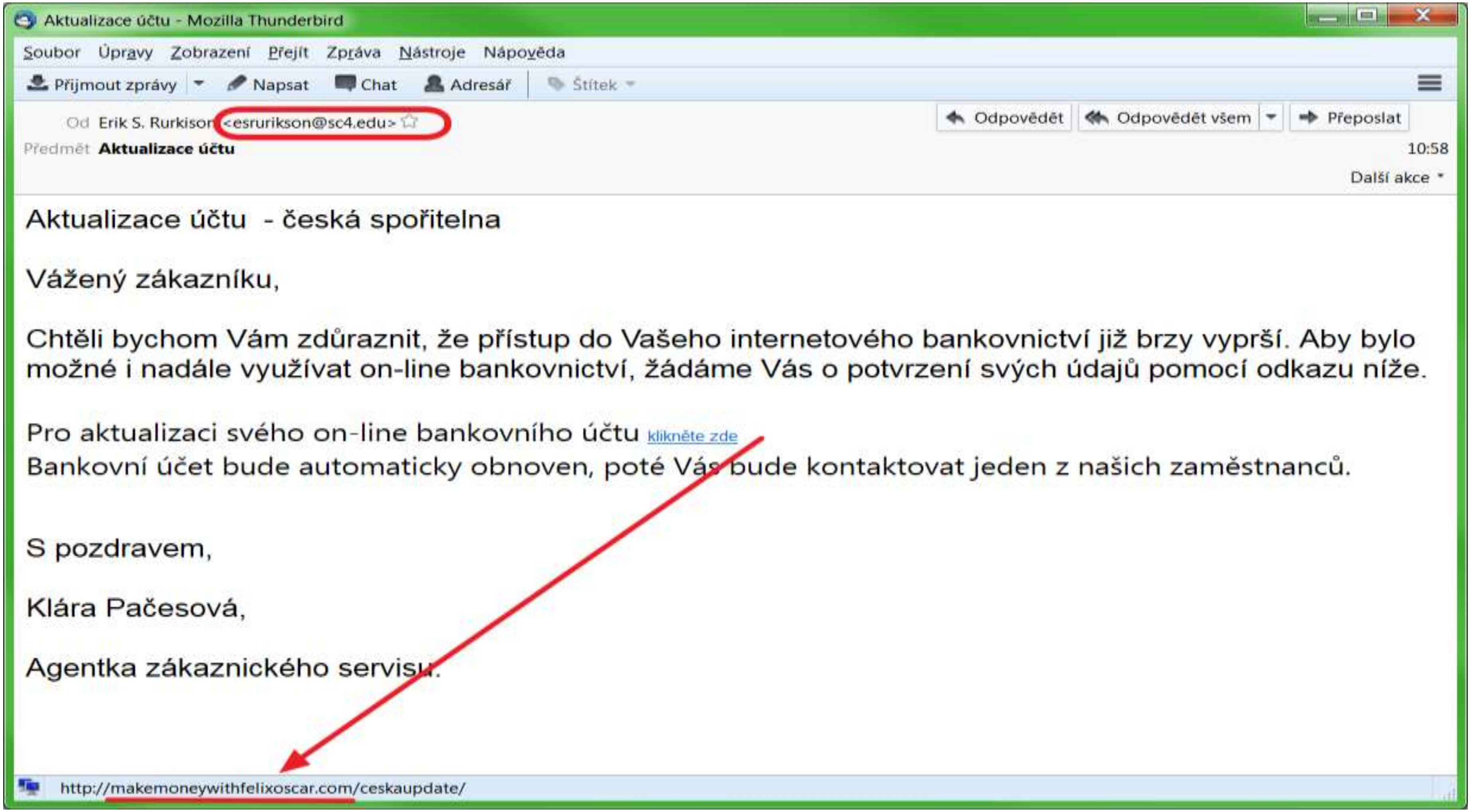
**Nejrozšířenější forma:** e-mailem doručená zpráva vyzývající (např. zákazníka banky) ke změně identifikačních údajů svého účtu prostřednictvím **podvržené webové stránky**

**Sociální inženýrství:** způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace.

# Bezpečnostní incidenty v Internetu

## Podvržené stránky

## https://www.hoax.cz/phishing/co-je-to-phishing



Od Erik S. Rurkison <esrurikson@sc4.edu>

Předmět **Aktualizace účtu**

10:58

Aktualizace účtu - česká spořitelna

Vážený zákazníku,

Chtěli bychom Vám zdůraznit, že přístup do Vašeho internetového bankovnictví již brzy vyprší. Aby bylo možné i nadále využívat on-line bankovnictví, žádáme Vás o potvrzení svých údajů pomocí odkazu níže.

Pro aktualizaci svého on-line bankovního účtu klikněte zde
Bankovní účet bude automaticky obnoven, poté Vás bude kontaktovat jeden z našich zaměstnanců.

S pozdravem,

Klára Pačesová,

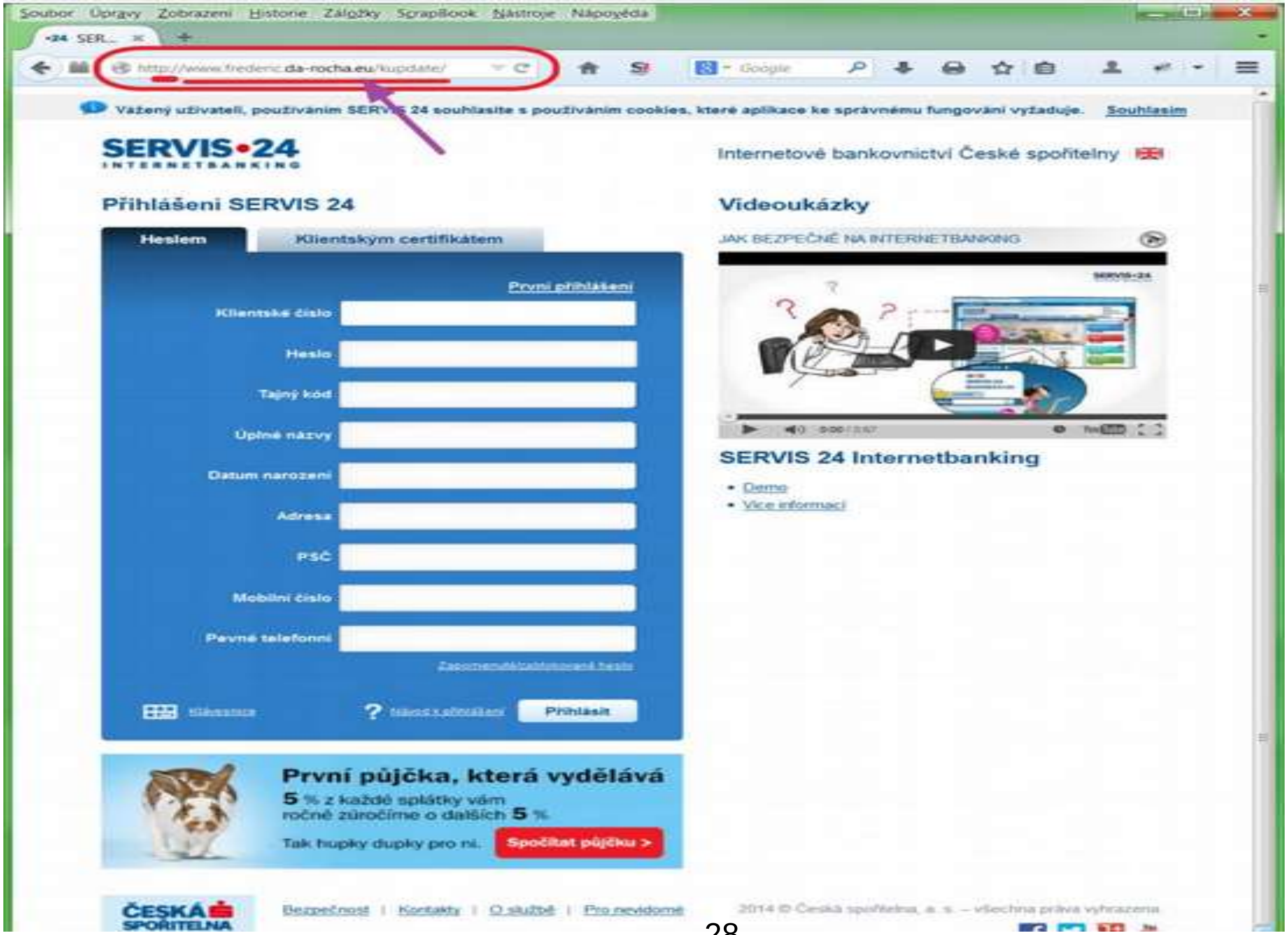
Agentka zákaznického servisu.

http://makemoneywithfelixoscar.com/ceskaupdate/

# Bezpečnostní incidenty v Internetu

## Podvržené stránky

**https://www.hoax.cz/phishing/co-je-to-phishing**



Vážený uživateli, používáním SERVIS 24 souhlasíte s používáním cookies, které aplikace ke správnému fungování vyžaduje. Souhlasím

SERVIS•24 INTERNETBANKING

Internetové bankovnictví České spořitelny

Přihlášení SERVIS 24

Heslem | Klientským certifikátem

První přihlášení

Klientské číslo
Heslo
Tajný kód
Úplné názvy
Datum narození
Adresa
PSČ
Mobilní číslo
Pevné telefonní

Zapomenuté/zablokované heslo

Klávesnice ? Návod k přihlášení Přihlásit

První půjčka, která vydělává

5 % z každé splátky vám ročně zúročíme o dalších 5 %

Tak hupky dupky pro ni. Spočítat půjčku >

Videoukázky

JAK BEZPEČNĚ NA INTERNETBANKING

SERVIS 24 Internetbanking

- Demo
- Více informací

ČESKÁ SPOŘITELNA

Bezpečnost | Kontakty | O službě | Pro nevidomé

2014 © Česká spořitelna, a. s. – všechna práva vyhrazena

# Bezpečnostní incidenty v Internetu

## Podvržené stránky (spear-phishing)

## www.cleverandsmart.cz

**Spear Phishing:** zatímco pro tradiční phishing je typické rozeslání velkého množství mailů, v případě spear phishingu je tomu přesně naopak.

Útočník zašle e-mail konkrétní osobě v organizaci, zpravidla vysoce postavenému manažerovi. Zaslaný e-mail nevykazuje žádné znaky typické pro phishing. Adresa odesílatele, ani adresa odesílacího serveru se nenachází na žádném blacklistu a z mailu nevedou žádné odkazy do internetu. E-mail může být odeslán také přímo z napadené organizace.

E-mail však obsahuje přílohu se škodlivým kódem

# Bezpečnostní incidenty v Internetu

## Podvodné maily (spear-phishing)

Vážený pane řediteli,

Omlouvám se za nežádoucí obtěžování a přeposílám Vám doklady ke smlouvě které asi mi byly zaslané omylem (předpokládám že přeposílám správně, jelikož Váš email byl uvedený ve smlouvě).

Doklady a smlouvu odesílám přílohou stejně jak jsem je dostal.

S pozdravem,

**Pozor na přílohy od neznámých (i známých) odesílatelů**

**www.govcert.cz/download/doporuceni/NUKIB_doporuceni-spear-phishing.pdf**

# Bezpečnostní incidenty v Internetu

## Podvržené stránky – mobilní telefony

UKÁZKA PODVODNÉ SMS ZPRÁVY

Vážený kliente České spořitelny,dosáhli jste maximálního možného počtu pokusů o přihlášení do služby Servis 24,pro odblokování Vašeho účtu se přihlašte zde:http://ceskasporitelna-servis24.cz.Vaše Česká spořitelny

UKÁZKA PODVODNÉ SMS ZPRÁVY

Vážený kliente, právě Vám na Váš účet dorazila neoprávněná platba. Zkontrolujte Váš účet na stránce http://ceskasporitelna-servis24.cz.

UKÁZKA PODVODNÉ SMS ZPRÁVY

Vazeny kliente Ceské sporitelny, z technickych duvodu jsme byli nuceni obnovit Vas Servis 14 ucet z internich zaloh. Zkontrolujte prosim spravnost vsech udaju zde: http://servis24-csas.cz. V pripade nalezeni nesrovnalosti nas kontaktuje telefonicky nebo na pobocce. Vase Ceska sporitelna.

# Bezpečnostní incidenty Internetu

## Kategorie bezpečnostních incidentů vychází z Vyhlášky o kybernetické bezpečnosti z 15.12.2014

- **Neoprávněná činnost v síti – hacking (Packet Sniffing, Port Scanning, Password Cracking, DoS… )**
- **Šíření škodlivých kódů (malware, infikované webové stránky, …)**
- **Šíření podvržených stránek (phishing, …)**
- **Šíření spamů a hoaxů**
- **Porušování autorských práv (neoprávněné šíření multimediálních dat)**

# Bezpečnostní incidenty v Internetu

## Šíření spamů

### Zastoupení spamů v celkové Internetové poště:

| | | |
|---|---|---|
| Konec roku | 2001: | 7 % |
| Průměr | 2010: | 89 % |
| Průměr | 2019: | 85 % |

- Inzerce prostřednictvím spamů je výhodná

- Více než 80% spamů se šíří z botnetů
  (Necurs: 6mil. PC, celkem asi 95mil. PC)

Malicious spam vede k napadení systému
- odkaz na infikované stránky
- infikovaná příloha

Pozor na přílohy inzertních zpráv

# Bezpečnostní incidenty v Internetu

## Šíření spamů

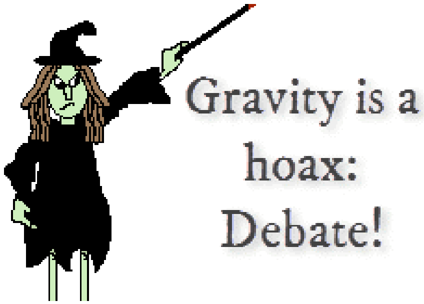
### Spamy podle země původu (Hospodářské Noviny, 24.6.2019)

| pořadí | stát | počet spamů za měsíc (mld) |
|---|---|---|
| 1. | Čína | 8,1 |
| 2. | USA | 6,5 |
| 3. | Brazílie | 5,1 |
| 4. | Rusko | 3,2 |
| 5. | Vietnam | 2,0 |
| 6. | Indie | 1,6 |
| 7. | Francie | 1,6 |
| 8. | Česko | 1,3 |
| 9. | Německo | 1,3 |
| 10. | Nizozemsko | 1,3 |

# Bezpečnostní incidenty v Internetu

## Šíření hoaxů

www.hoax.cz



### Hoax (zpravidla poplašná zpráva)

- **Varuje před neexistujícím nebezpečným virem nebo jiným neexistujícím nebezpečím**
- **Obsahuje falešné prosby o pomoc, smyšlené informace**
- **Ve většině případů odkazuje na „důvěryhodné zdroje“**
- **Téměř vždy obsahuje výzvu k hromadnému rozeslán na další adresy**

**Na rozdíl od spamů Hoax šíří sami uživatelé internetu (email, whatsapp, sociální sítě)**

# Bezpečnostní incidenty Internetu

## Kategorie bezpečnostních incidentů vychází z Vyhlášky o kybernetické bezpečnosti z 15.12.2014

- ☐ **Neoprávněná činnost v síti – hacking (Packet Sniffing, Port Scanning, Password Cracking, DoS… )**
- ☐ **Šíření škodlivých kódů (malware, infikované webové stránky, …)**
- ☐ **Šíření podvržených stránek (phishing, …)**
- ☐ **Šíření spamů a hoaxů**
- ☐ **Porušování autorských práv (neoprávněné šíření multimediálních dat)**

# Bezpečnostní incidenty v Internetu

## Porušování autorských práv

**Je legální stažení filmu nebo hudby z internetu?**

**Dílo volně přístupné, tedy nechráněné autorskými zákony (například amatérské video) lze stahovat bez omezení. S takovým dílem lze nakládat zcela libovolně.**

**Dílo chráněné autorskými zákony (například hudba, film) lze stáhnout, přehrát a dokonce i ponechat na pevném (přenosném) disku pro další osobní použití (volné užití). Takové dílo však nelze nikomu dalšímu poskytnout (prodat, překopírovat ani půjčit) a nesmí být přehráváno veřejně.**

**Volné užití se nevztahuje na počítačový program, elektronickou databázi a záznam audiovizuálního díla pořízený při jeho provozování či přenosu (např. záznam pořízený v kině).**

# Bezpečnostní incidenty v Internetu

## Porušování autorských práv

**Evropský soudní dvůr v dubnu 2014 doporučil, aby členské státy zákonem zakázaly pořizování soukromých rozmnoženin z neoprávněného zdroje pro osobní potřebu. Zároveň by ale měly stanovit poplatky za prázdná média tak, aby jejich výše nezohledňovala nelegální kopírování děl.**

**I nadále musí být umožněno pořízení kopie pro vlastní potřebu, bude to však možné pouze z legálně šířené (získané) kopie díla nebo díla samotného, legálně pořízeného.**

# Bezpečnostní incidenty v Internetu

## Porušování autorských práv sdílením v sítích p2p (BitTorrent)

**K porušením autorského zákona při sdílení souborů dochází v případě, že:**

- **Obsahem sdíleného souboru je autorské dílo**
- **Sdílení je neoprávněné (bez souhlasu autora)**

**Naprostá většina souborů, které jsou šířeny v síti BitTorrent splňuje obě výše uvedené podmínky, a proto je možno toto šíření, resp. sdílení kvalifikovat jako trestný čin porušení autorského práva.**

**Wikipedie: https://cs.wikipedia.org/wiki/BitTorrent**

# Bezpečnostní incidenty v Internetu
## Porušování autorských práv

**Organizace zabývající se problematikou autorských práv**

**Česká národní skupina Mezinárodní federace hudebního průmyslu (www.ifpicr.cz)**

**Předmětem působnosti ČNS IFPI je ochrana práv výrobců zvukových a zvukově obrazových záznamů**

**BSA - Business Software Alliance (www.bsa.org)**

**Primárním cílem BSA je vzdělávání uživatelů softwaru v oblasti ochrany autorských práv a boj proti softwarovému pirátství**

# Ochrana soukromí na Internetu

## Digitální stopa

**Digitální stopa je informace zanechaná uživatelem internetu**

**Aktivní (vědomě zanechané stopy): profily a příspěvky zanechané na sociálních sítích, emaily, sms, historie chatu, různé úřední údaje …**

**Pasivní (bez zásahu uživatele): IP adresa počítače, vyhledávané výrazy na internetu, údaje o času stráveném na určité webové stránce (cookies), lokace …**

# Ochrana soukromí na Internetu

## Digitální stopa

**Pasivní i aktivní stopy mají určitou vypovídací hodnotu o uživateli, který je zanechal**

- **Lze je zneužít např. pro sledování návyků uživatelů**
- **Mohou zajímat zaměstnavatele (názory, postoje, záliby, rozdíly mezi uváděnými údaji v životopise a na sociálních sítích,  …)**
- **Digitální stopa se bere jako důkazní materiál při kriminalistickém vyšetřování**

# Ochrana soukromí na Internetu

## Digitální stopa

**Jediný způsob, jak za sebou nezanechávat žádnou digitální stopu, je nevyužívat moderní komunikační technologie a internet. Smazání všech digitálních stop je zatím prakticky nemožné.**

**Aktivní stopy lze však „rozmazat“ např. používáním více přihlašovacích jmen (e-mailových adres) k různým aplikacím nebo používáním speciálního prohlížeče TOR (www.torproject.org)**

**Pasivní stopy lze částečně omezit např. nastavením anonymního prohlížení (do not track) v prohlížeči nebo správou cookies…**

# Ochrana soukromí na Internetu

## Digitální stopa

### Svoje digitální stopy můžeme částečně kontrolovat

**Aktivní stopy** **např :**

- **People search engines (https://pipl.com)**
- **Google Dashboard (Hlavní panel Google)**
- **archive.org**

**Pasivní stopy** **např: Google Account (Účet Google)**

**www.forbes.cz/co-vsechno-o-vas-vi-google-10-odkazu-ktere-by-mel-znat-kazdy-kdo-je-na-internetu/**

# Ochrana soukromí na Internetu

## Digitální stopa

**Nejvíce aktivních digitálních stop zanechávají aktivní uživatelé sociálních sítí. Příklady zneužití digitálních stop:**

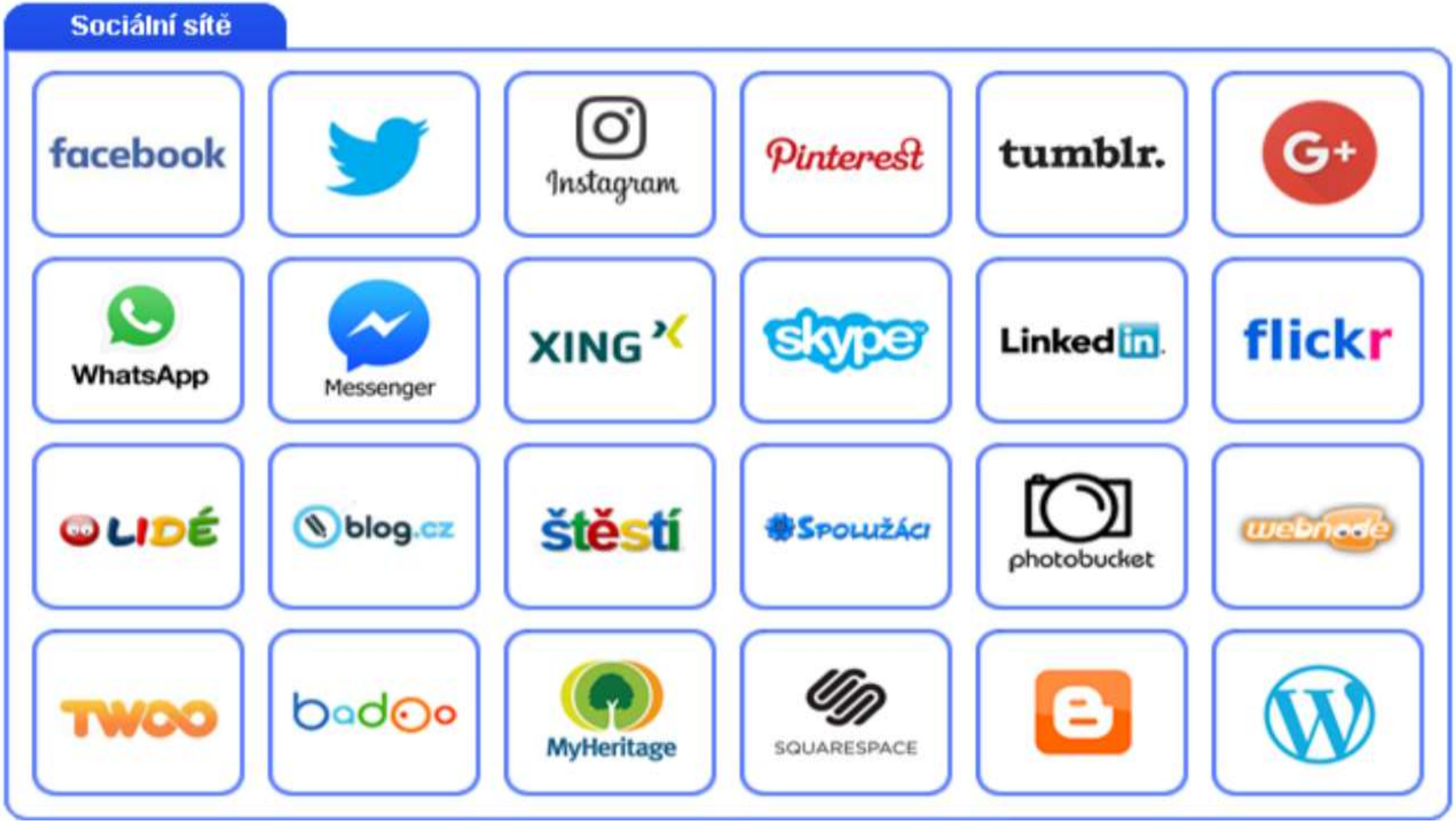
**Kybergrooming: psychická manipulace dítěte dospělým s cílem získat důvěru oběti, vylákat ji na osobní schůzku a zpravidla sexuálně zneužít.**

**Kyberšikana: (*cyberbullying*) obecné označení různých forem šikany (zesměšnění, zastrašení, ohrožení, …) prostřednictvím elektronických médií (internet, mobilní telefon).**

**Kyberstalking: pronásledování - opakované a stupňované kontaktování s cílem vyvolat u své oběti pocit strachu o své soukromí, zdraví nebo život.**

# Ochrana soukromí na Internetu

## Nejvíce aktivních stop je na sociálních sítích



# Ochrana soukromí na Internetu

## Bezpečnost na sociálních sítích:

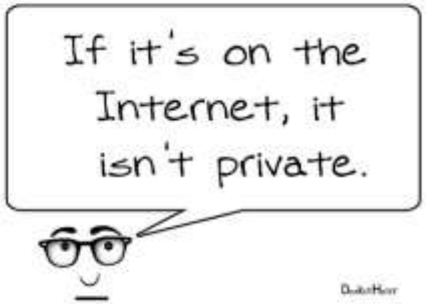
- **Neuvádějte na veřejném profilu svoje telefonní číslo nebo adresu**
- **Používejte fiktivní jméno**
- **Pozor na používání webové kamery**
- **Používejte sekundární e-mail**
- **Nepřidávejte si mezi přátele neznámé kontakty**
- **V žádném případě nezveřejňujte na sociálních sítích informace, jejichž případné zveřejnění by vám vadilo**

- **Přemýšlejte nad informacemi, které o sobě zveřejňujete, a nad tím, komu je sdělujete. Víte, kdo jsou přátelé vašich přátel …?**

# Ochrana soukromí na Internetu

## Digitální stopa - shrnutí

Osobní údaje jsou cenné zboží,
je třeba s nim zacházet obezřetně



**Pokud už někdy musíte zadat své osobní údaje, např. při registraci do e-shopu, k požadované službě, …**

- **Ověřte si, komu dáváte své údaje k dispozici**
- **Vytvořte si samostatnou e-mailovou adresu pro registrace do internetových služeb.**

- **Zadávejte jen nutné minimum osobních údajů**

# Závěr

**(Jiří Palyza, NCBI):**

**Bezpečný internet bohužel neexistuje,**

**ale největším nebezpečím pro uživatele bývá často sám uživatel**

**Děkuji za pozornost**

## Odkazy:

https://cs.wikipedia.org/wiki/Bezpečnost_na_internetu
https://cs.wikipedia.org/wiki/Sociální_síť
https://www.govcert.cz/
https://www.csirt.cz/
https://www.nic.cz/
https://wikisofia.cz/wiki/Digitální_stopa