Kryptografie a bezpečnost

Úvodní otázka: Co se o nás dá zjistit jen pomocí polohy?

- Kde pracujeme/studujeme
- Kde bydlíme
- Náš socio-ekonimický status (co navštěvujeme za obchody, podniky,…)
- Naše zájmy
- S kým se pravděpodobně stýkáme (porovnání dat s jinými uživateli)
- Do jisté míry naše politické názory (shromáždění, demonstrace)
- Co používáme za dopravní prostředky
- Jak často a kam cestujeme za hranice (jak to třeba souvisí s naší prací ?)

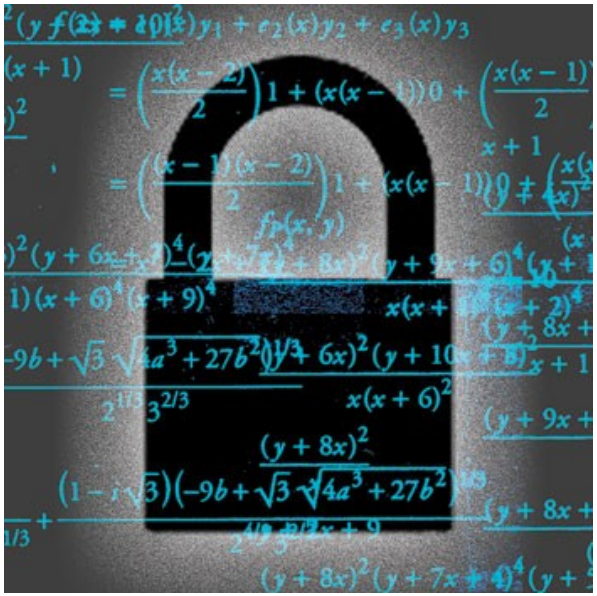
…a to je „jen“ poloha

- Jen přes telefon se dá sledovat mnoho dalších věci:
  - Komu voláme
  - Jaké stránky navštěvujeme
  - Celý aparát soc. sítí (který sleduje milion svých metrik)
  - Odposlech přes mikrofon
  - Apps které používáme a dáváme jim pı
  - Prakticky cokoliv co děláme na interne

  - …a to nepočítáme vyložený mallware

Kryptografie

- věda zabývající se zajištěním utajené a důvěryhodné komunikace – tedy tvorbou šifer pro lepší zabezpečení nás na síti



Proč kryptografie?

- Stále větší část našich dat je na síti
- Prostřednictvím internetu děláme i důležité úkony (el. Podpis, žádosti o práci, platby…)
- Kryptografie na síti je stejně logická jako to, že zamykáme svoje domy nebo auta
- S kryptografií se setkáváme každý den, i když si to ani neuvědomujeme -> třeba při přihlašování do IS MU

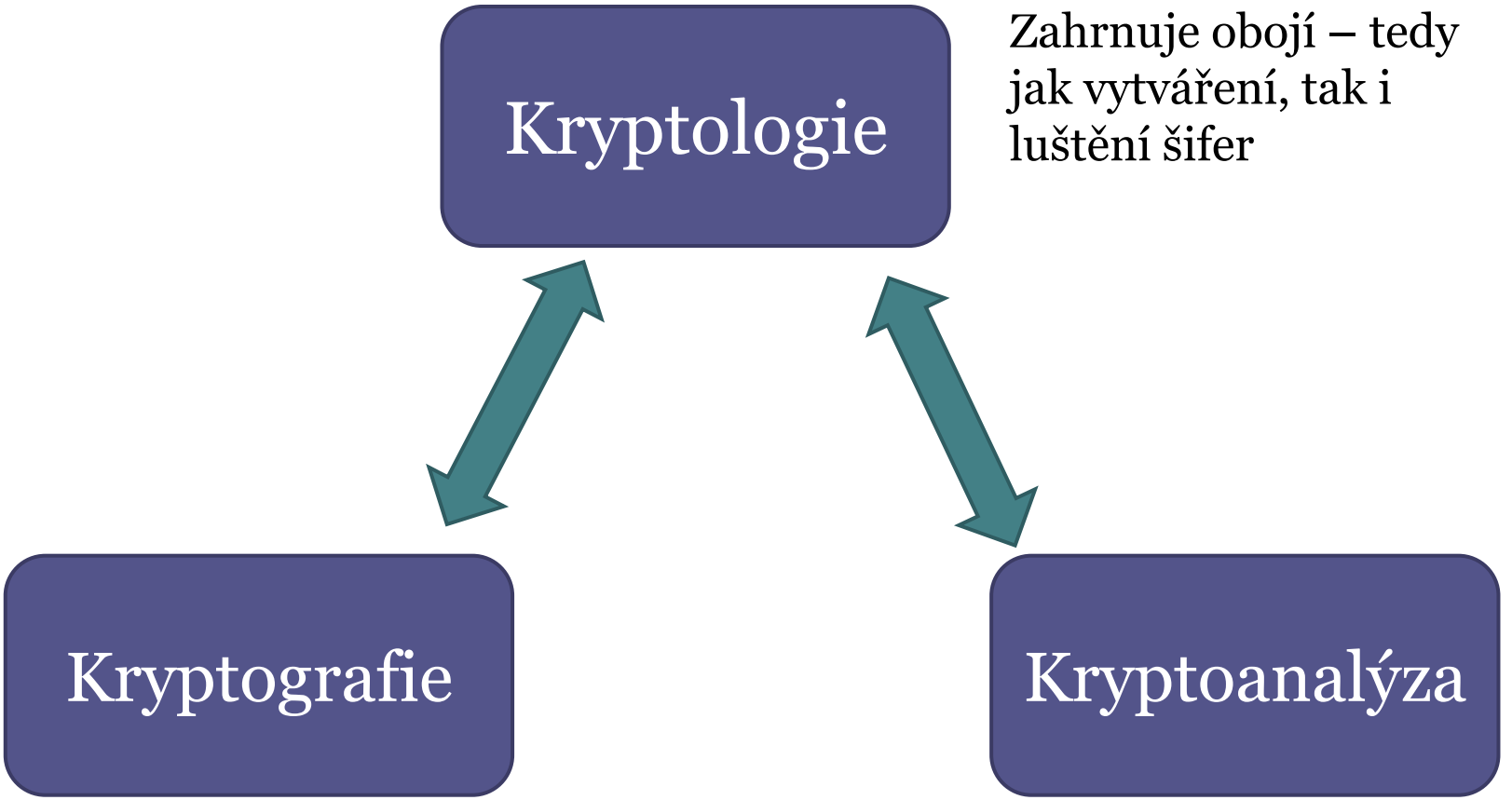
Něco z historie

- Lidé šifrovali svoji komunikaci již od starověku
- Šifrovali se rozkazy pro vojska, deníky politiků, depeše diplomatů…
- Kryptografie nebyla tedy vědou spojenou s IT, ale obecně s šifrováním zpráv

Skytalé - šifrování, který se skládá z válce a na něm navinutém pergamenu na kterém je napsaný vzkaz. Používali je Řekové, kteří ji využívali během válek.

Enigma - šifrovací stroj používaný za války německou armádou

Kryptografie vs. Kryptoanalýza



Cíle kryptografie

- zabezpečit komunikaci citlivých dat mezi uživatelem a internetovou službou
- zajistit důvěryhodnost komunikace mezi uživateli (např. email)
- autorizace závažných úkolů (ebanking, el. obchody, …)
- omezit přístup k určitým službám jen pro určené jedince (zabezpečená wi-fi)

Časté omyly uživatelů

- „V tom e-mailu stejně nemám nic co by stálo za to ukrást.“ – chyba. Stačí i to, že znají vaše e-mailové heslo, které může být stejné/podobné jako heslo k e-bankingu, pracovním datům a podobně
- „Jaká je pravděpodobnost, že se to stane zrovna mě?“ – docela slušná. Data o uživatelích dnes kradou často autonomní programy. Pokud odhalí že máte slabé zabezpečení zaměří se na vás.
- I když vy sami nejste pro hackera zajímavý, může z vašich dat získat informace třeba o vašem zaměstnavateli

Co tedy napomáhá k naší ochraně?

- Dobré heslo
- Certifikační systém
- Šifrované spojení
- Zdravá paranoia ☺

Autentizace

- … je ověření identity uživatele, který se pokouší přihlásit do služby, systému apod. (od slova autentický)

Autentizace – jak se provádí?

❖podle toho, co uživatel zná (zná správnou kombinaci uživatelského označení a hesla nebo PIN)

❖podle toho, co uživatel má (nějaký technický prostředek, který uživatel vlastní – hardwarový klíč, smart card, privátní klíč apod.)

❖podle toho, čím uživatel je (uživatel má biometrické vlastnosti, které lze prověřit – otisk prstu, snímek oční duhovky či sítnice apod.)

❖podle toho, co uživatel umí (umí správně odpovědět na náhodně vygenerovaný kontrolní dotaz)

Heslo – vaše osobní šifra

Co je to „dobré heslo“

- …je takové, co půjde špatně odhalit ☺
- 1) Heslo by se neměl tvořit nějaký snadno dohádatelný údaj o uživateli. – tedy ne vaše jméno, jména vašich dětí apod.
- 2) Mělo by být dostatečně dlouhé – čím delší tím déle trvá jeho odhalení. S každým dalším znakem se násobí časová délka nutná k jeho odhalení
- 3) Mělo by obsahovat velká a malá písmena, čísla a speciální znaky (@, ?). Nejdůležitější je ale jeho délka

Jak s heslem zacházet

- hesla k důležitým službám (ebanking, IS, email, ...) nesmí být stejná
- heslo nikdy nikomu nesdělujte
- důležitá hesla neukládejte v prohlížeči, ani je nikam nezapisujte
- po zadání hesla na nedůvěryhodném stroji (např. na cestách) jej při nejbližší příležitosti změňte

Klikni zde

Něco více o heslech

Útoky na hesla

- **Sociální inženýrství** - patří mezi nejúčinnější metody útoků . Útočník se snaží zjistit buď přímo zjistit heslo, nebo informace, které ho k heslu dovedou. Prostě se vás zeptá. Druhá varianta je zjistit si základní informace o daném člověku a potom zkusit zmiňované jméno partnera, dětí, dalších rodinných příslušníků, nebo domácích zvířat.

- **Odchycení hesla-** používají se například keyloggery (programy pro snímání stisknutých kláves na klávesnici).

- **Slovníkový útok -** Útočník má slovník slov daného jazyka a zkouší zadat jako heslo jednotlivá slova z tohoto slovníku. Nezadává ručně, ale automaticky pomocí počítačového programu. Takovým způsobem pak může vyzkoušet mnoho hesel za sekundu.

- **Útok hrubou silou -** Nejprimitivnější varianta útoku, útočník zkouší postupně zadávat všechny kombinace, například: aaa, aab, aac, aad,...

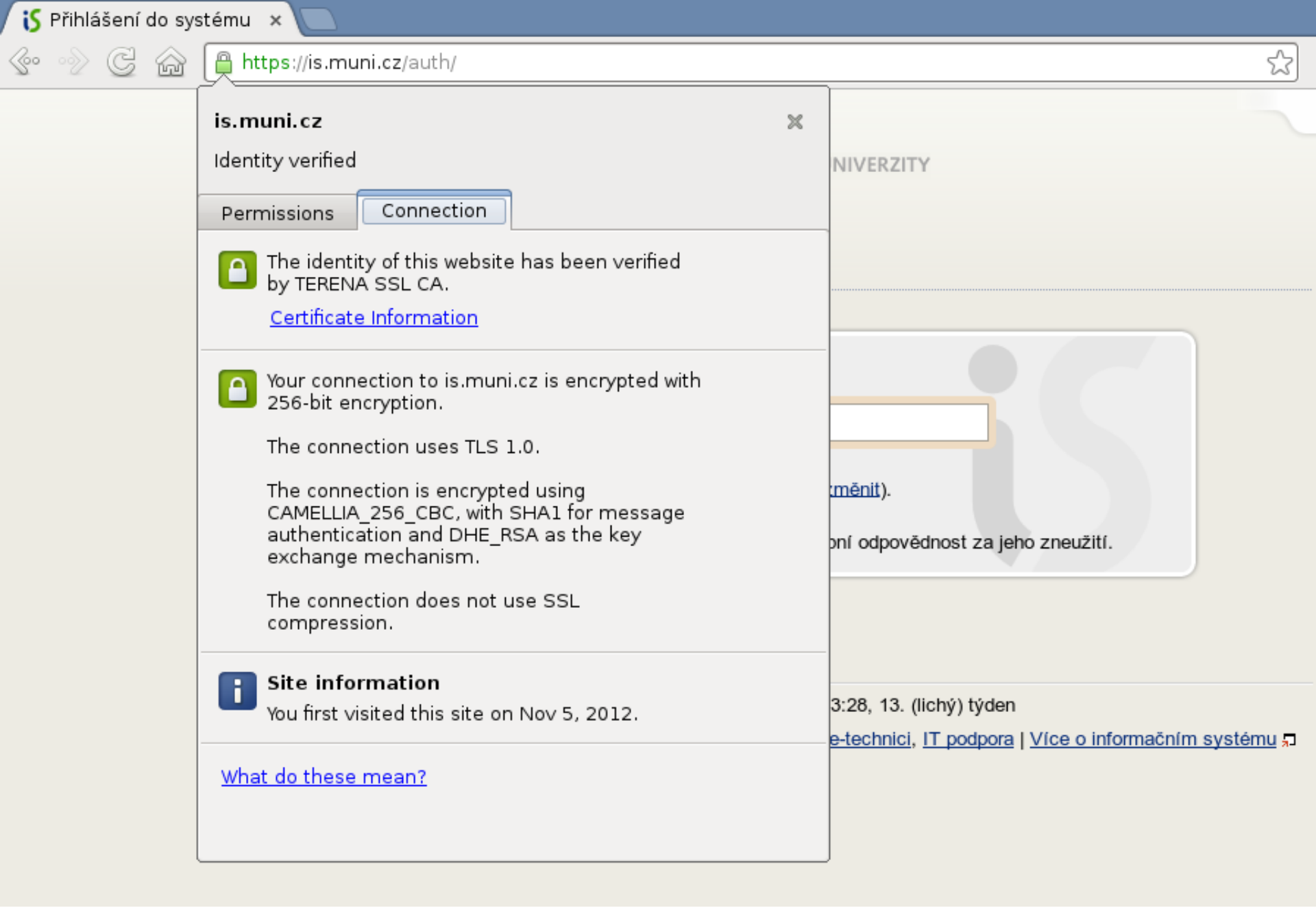
Elektronický podpis

- Vychází z principů asymetrického šifrování

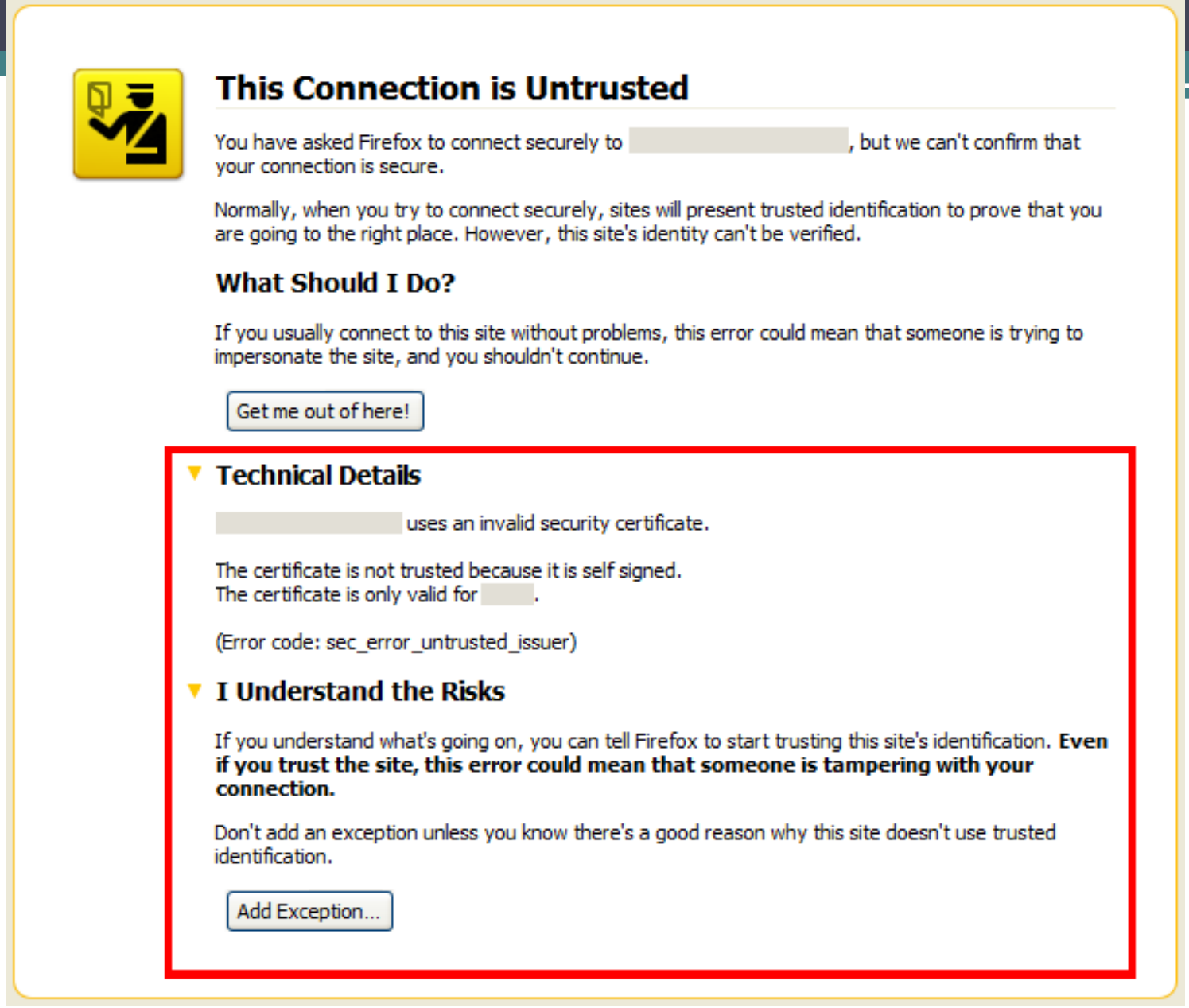
- El. podpis je potvrzení, že zpráva byla vytvořena daným autorem
- realizován pomocí asymetrické kryptografie:
  - pomocí soukromého klíče je k dané zprávě vytvořen podpis
  - příslušný veřejný klíč umožňuje ověřit pravost podpisu

Certifikace pomocí https

- Nástavba běžného http protokolu, který není šifrován
- U https jsou využívány certifikáty důvěryhodnosti, které vydává nějaká velká certifikační autorita
- Dnešní prohlížeče s certifikáty umí běžně pracovat a pokud web žádnou certifikaci nemá (nebo ji jen předstírá) snaží se vás většinou varovat



- Certifikát v Google Chrome



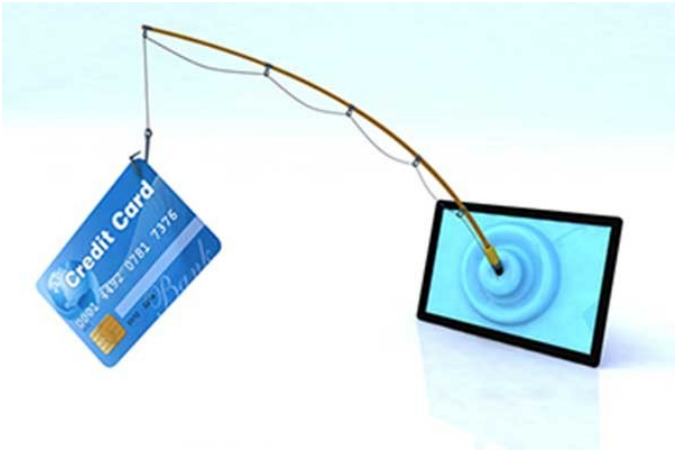
- Odhalení nedůvěryhodného certifikátu

Některé formy útoku

- **Phising** – podvržené stránky a zahrávání si s psychologií uživatele
- **Útoky na hesla** – různé metody jak odhalit vaše heslo. Viz. kapitola o heslech
- **Odposlech bezdrátové komunikace**
- **Malware** – různé druhy škodlivého softwaru, které mohou získat vaše hesla, nebo přímo data

Psychologie v útoku - phishing

- *Only amateurs attack machines; professionals target people.*
  - *— Bruce Schneier*



Phishing

- Pro útočníka je jednodušší využít neopatrnosti cíle (vás) a jeho oklamání, než složitě nabourávat šifrované stroje

- Evolučně jsme si vytvořili poznávací mechanismy, proti podvodům z očí do očí, teď se musíme naučit mechanismy pro odhalení podvodů skrze monitor.

Phishing – jak funguje

- Vytvoření návnady (falešná stránka vaší banky)
- Rozeslání e-mailů uživatelům (výzva ke změně hesla, kontrole údajů…)
- Uložení vašich údajů u útočníka
- …poté proběhne standardní přihlášení do běžné služby, aby se nevytvořilo podezření


THE NIGERIAN PRINCE NEEDS MY HELP?
I'LL GET MOM'S CREDIT CARD!

Šifrování wifi vs. odposlech

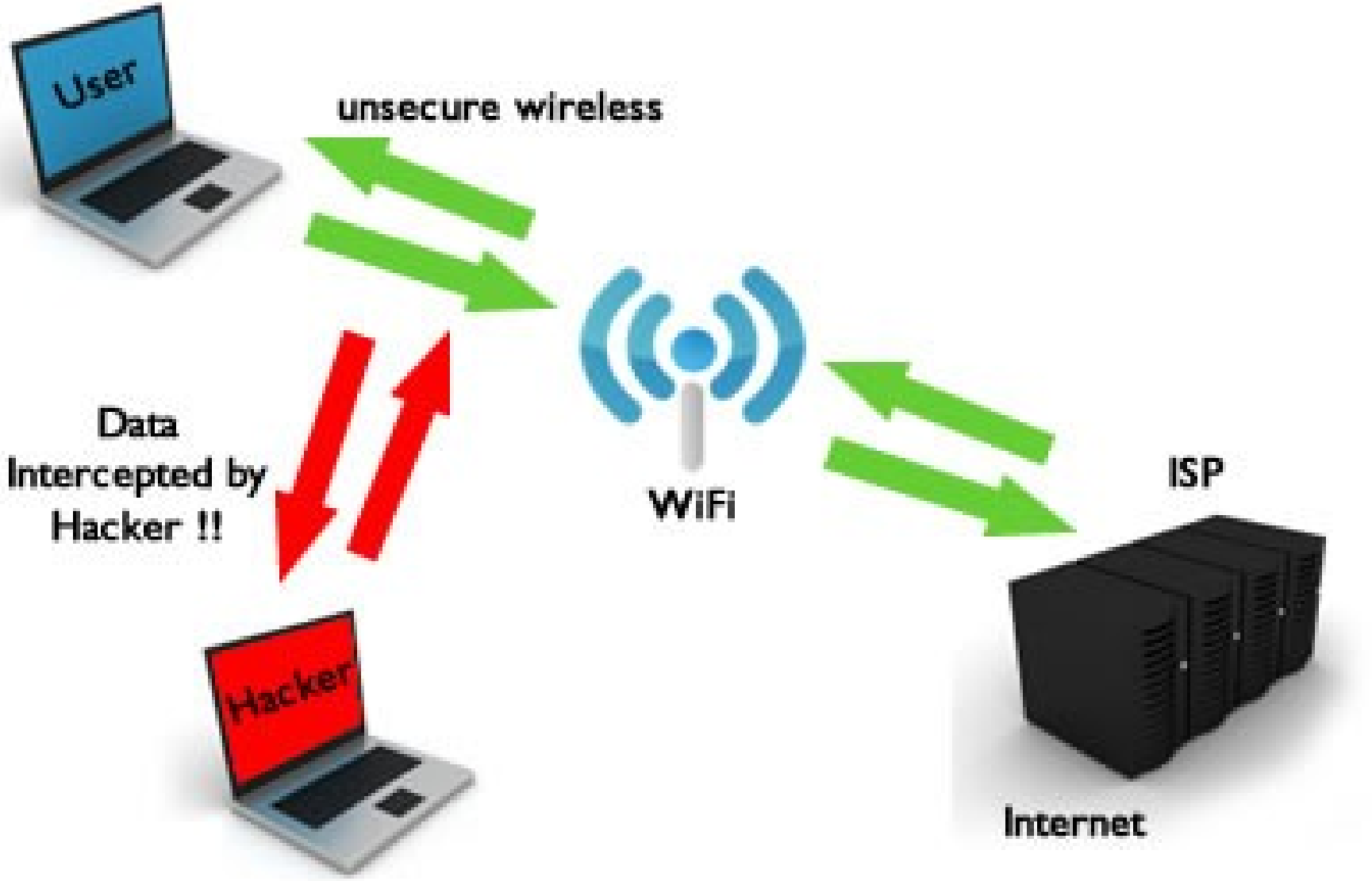
- Na rozdíl od pevné (drátové) sítě nelze fyzicky omezit přístup k bezdrátové síti. U wifi není možné zjistit, zda probíhající komunikaci někdo nesleduje (a nenahrává). Z těchto důvodů se zavádí autentizace (přihlašování) při připojení síti a šifrování provozu přihlášených uživatelů

- Pozor tedy na wifi zdarma! ☺

Útok na wifi

- **Odposlech**
- není možné jeho aktivitu zjistit
- v případě nešifrované (nebo slabě šifrované — WEP) vidí veškerou komunikaci vedenou mimo zabezpečené protokoly (např. https)
- může sledovat například osobní údaje, stahované dokumenty a další data putující sítí, které mu umožní vést přímé útoky: vydávání se za uživatele (krádež identity), získání přístupu přes fingovanou ztrátu hesla a pod.

- **Ofenzivní útočník**
- v případě slabého šifrování může získat klíč pro vstup do sítě (WEP)
- může získat přístup k nastavení přípojného bodu (a využít jej např. ke sledování aktivity na síti)
- po získání přístupu do sítě útočit na jednotlivé počítače (i tak jednoduše, jako vyhledávání nevědomky sdílených složek)
- vytvořit volně přístupný přípojný bod, na kterém bude sledovat veškerou komunikaci


User
unsecure wireless
Data
Intercepted by
Hacker !!
WiFi
ISP
Hacker
Internet

Jak se tedy bránit?

- **jako uživatel**
  - nepřipojujte se k nedůvěryhodným přípojným bodům
  - používejte zabezpečený protokol https
  - mějte zapnutý firewall
- **při nastavení domácí sítě**
  - změňte výchozí hodnoty pro název sítě a heslo pro administraci
  - vyberte šifrování provozu pomocí WPA (WPA-2), **WEP varianta je dnes již považována za slabou**
  - zvolte dostatečně silné heslo (viz výše)

Malware

- = škodlivý software, jehož účelem je poškození, nebo infiltrace počítačového systému

- Řadí se sem různé viry, trojské koně, keylogery, atp.

- Pomocí malwaru je možné:
  - Získávat data a údaje z postiženého PC (třeba hesla, soukromá data…)
  - Použít ovládnutý počítač k nelegální aktivitě (rozesílání dalších virů, útokům na velké cíle…)

Některé druhy malwaru

- Trojský kůň – vydává se za užitečný SW, po instalaci uživatelem provádí svoji pravou funkci
- Keylogger – program který snímá stisknuté klávesy (odposlech hesel)
- Adware – méně škodlivý, způsobuje časté zahlcování reklamou

Ransomware

- Vyděračský software neboli *ransomware* je druh škodlivého softwaru, který zabraňuje přístupu k počítači, který je infikován.
- Tento program zpravidla vyžaduje zaplacení výkupného (anglicky *ransom*) za zpřístupnění počítače.
- Některé formy ransomware šifrují soubory na pevném disku (kryptovirální vydírání), jiné jen zamknou systém a výhrůžnou zprávou se snaží donutit uživatele k zaplacení.

RansomWare


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
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
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Kyberbezpečnost z pohledu žáka základní školy

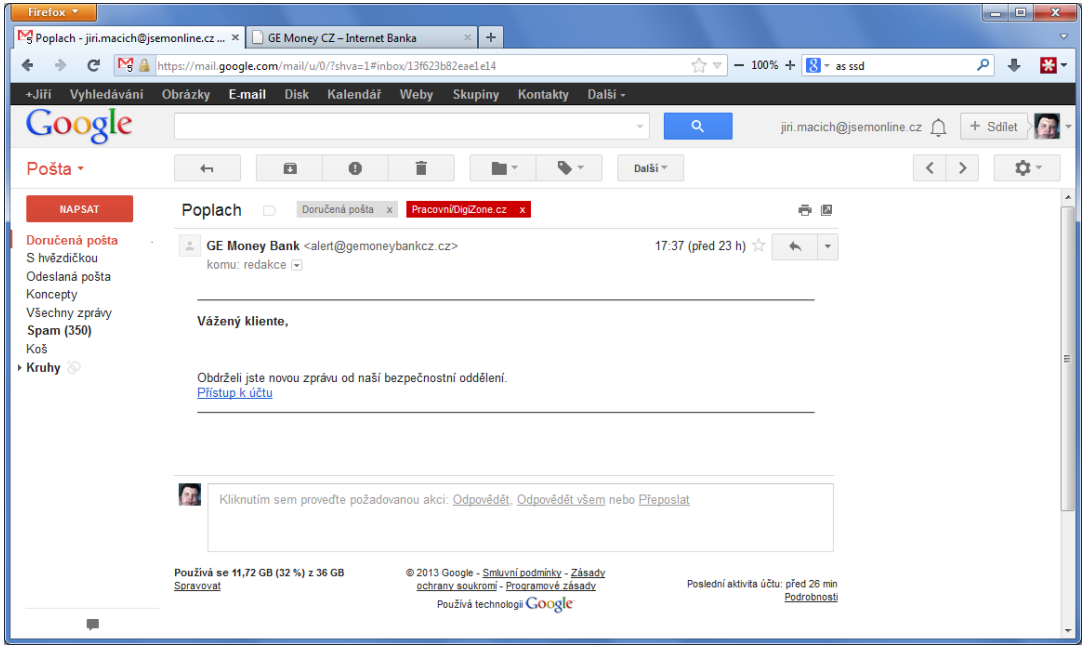
Žákovské prekoncepce – co žáci často slyšeli

- Nebezpečí sexuálních útoku přes internet
- Existuje malware (žáci spíše říkají viry)
- Fantaskní povědomí o hackerech (skrze optiku filmů, her, …)
- Viry často vnímají jako destruktivní
- Vágní představa o krádeži identity (často moc nevědí proč)
- Často až přehnaná důvěra v antivirové programy (potažmo i firewall)

Kde je nebezpečí?

- Sociální sítě
- Herní platformy
- „Náhodné klikání“
- Pornografie
- Phising

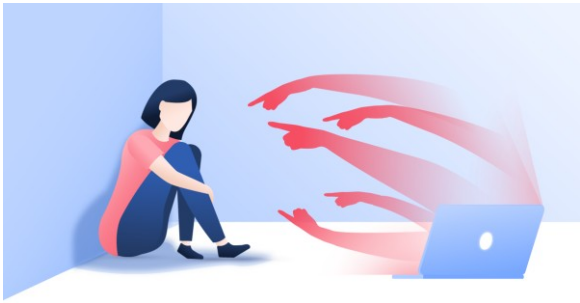
- ~~Bankovnictví~~
- ~~Pracovní maily~~
- ~~Datová uložiště~~



Rizikové chování v kyberprostoru

- Děti jsou samozřejmě cíle všech dosud zmíněných rizik (stejně jako dospělí)
- Více se jich ale dotýkají některá další rizika

Kyberšikana



- Kyberšikana je spjata s šikanou školní
- Kyberšikana sdílí základní rysy a projevy tradiční šikany, avšak ty nabývají v kyberprostoru jiných forem

  - *Kyberšikana je kolektivní označení forem šikany prostřednictvím elektronických médií, jako je internet a mobilní telefony, které slouží k agresivnímu a záměrnému poškození uživatele těchto médií. Stejně jako tradiční šikana zahrnuje i kyberšikana opakované chování a nepoměr sil mezi agresorem a obětí.*
  - (Price & Dalgeishe (2010))

Kyberšikana

- Základní prvky kyberšikany:
  - Probíhá prostřednictvím elektronických médií
  - Opakuje se
  - **Záměrnost agresivního** aktu ze strany útočníka (někdy se může plést jen s vrstevnickým popichováním a podobně)
  - Mocenská nerovnováha
  - Oběť vnímá toto jednání jako nepříjemné, ubližující

Projevy kyberšikany

- **Vydávání se za někoho jiného** - vytvoření falešného profilu oběti, komunikace s kamarády z takového profilu, zveřejňování upravených a citlivých fotek,…
- **Vyloučení a ostrakizace**
- **Vytěžení osobních věcí a následné zveřejnění** (třeba v group chatu)
- **Pomlouvání, urážky, hrozby násilím, hecování ostatních na síti k násilí na oběti….**

Kybergrooming

- označuje chování internetových uživatelů (predátorů, kybergroomerů), které má vyvolávat falešnou důvěru a tím přinutit oběť k osobní schůzce
- Kybergrooming zahrnuje celou řadu trestných činů, jako jsou nebezpečné vydírání, sexuální nátlak, navazování nedovolených kontaktů s dítětem apod.

Kybergroomingem se zabýval třeba film "V síti"

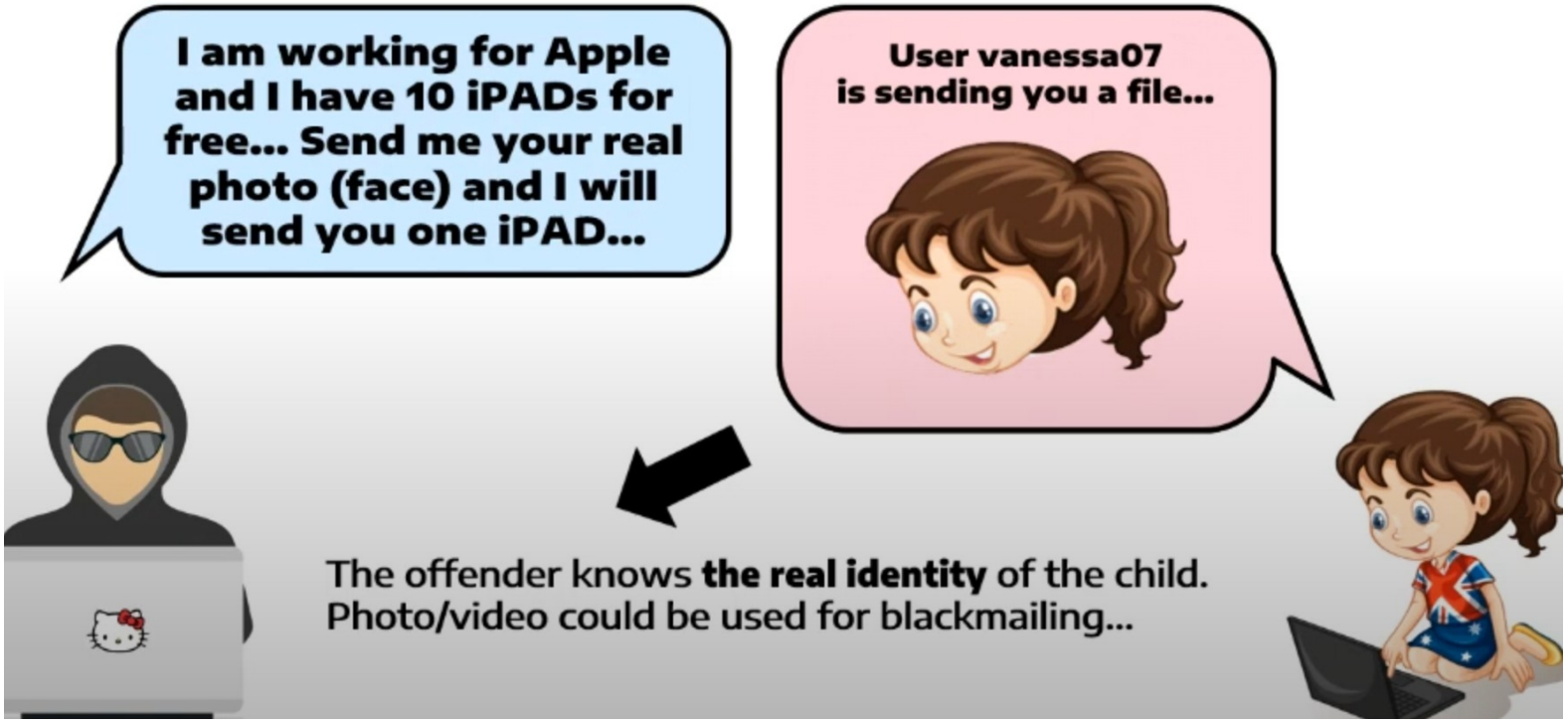
Příklady manipulace oběti - Mirroring

The attacker communicates mirror imitating child communication... for example in chat (-> trust, interest).

Převzato od Kamil Kopecký, e-bezpečí

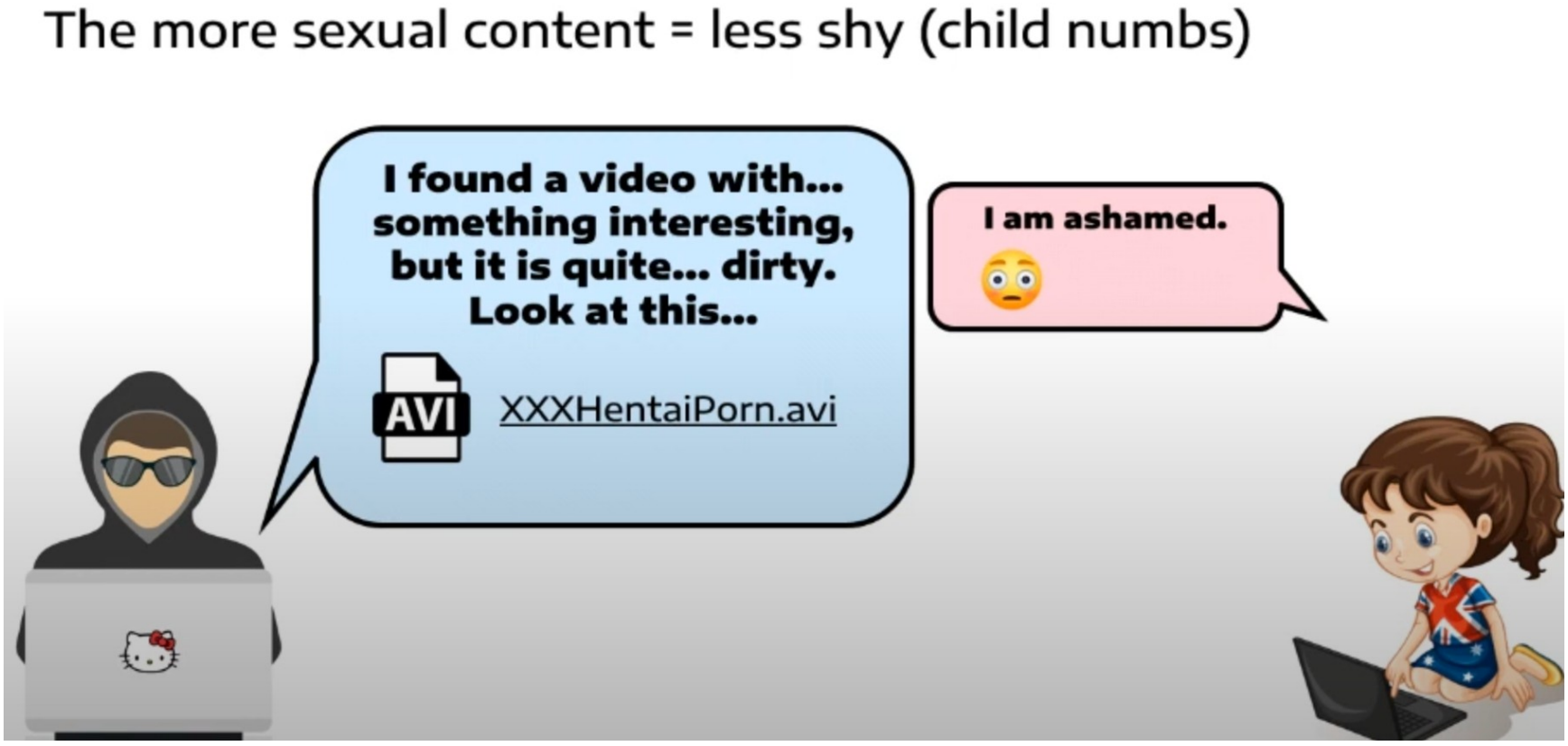
Příklady manipulace oběti - Uplácení

The attacker offers gifts in exchange for photos, videos, personal information...



Převzato od Kamil Kopecký, e-bezpečí

Příklady manipulace oběti - snižování hranic vkládáním sexuálního obsahu do konverzace



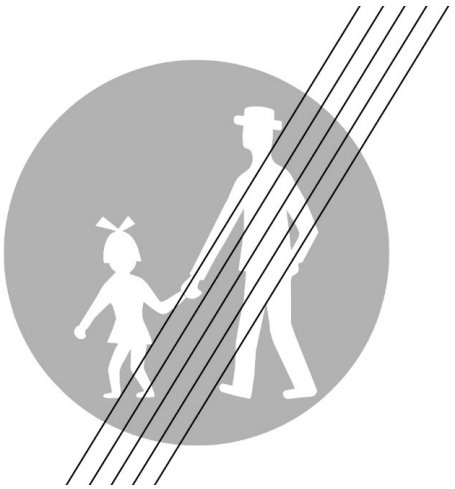
Převzato od Kamil Kopecký, e-bezpečí

- … a mnoho dalších jako:

  - Nátlak
  - Phishing
  - Izolace dítěte od okolí (tajemství,…)
  - Přímé vydíráni
  - Vytěžování osobních informací
  - Využívání "fake webcam loopů"
  - ….

K čemu kybergrooming směřuje?

- Primárně:
  1) Osobní setkání s obětí/sexuální zneužití dítěte
  2) Vytěžení dítěte stran autentického pornografického materiálu buď pro osobní potřebu nebo pro obchod

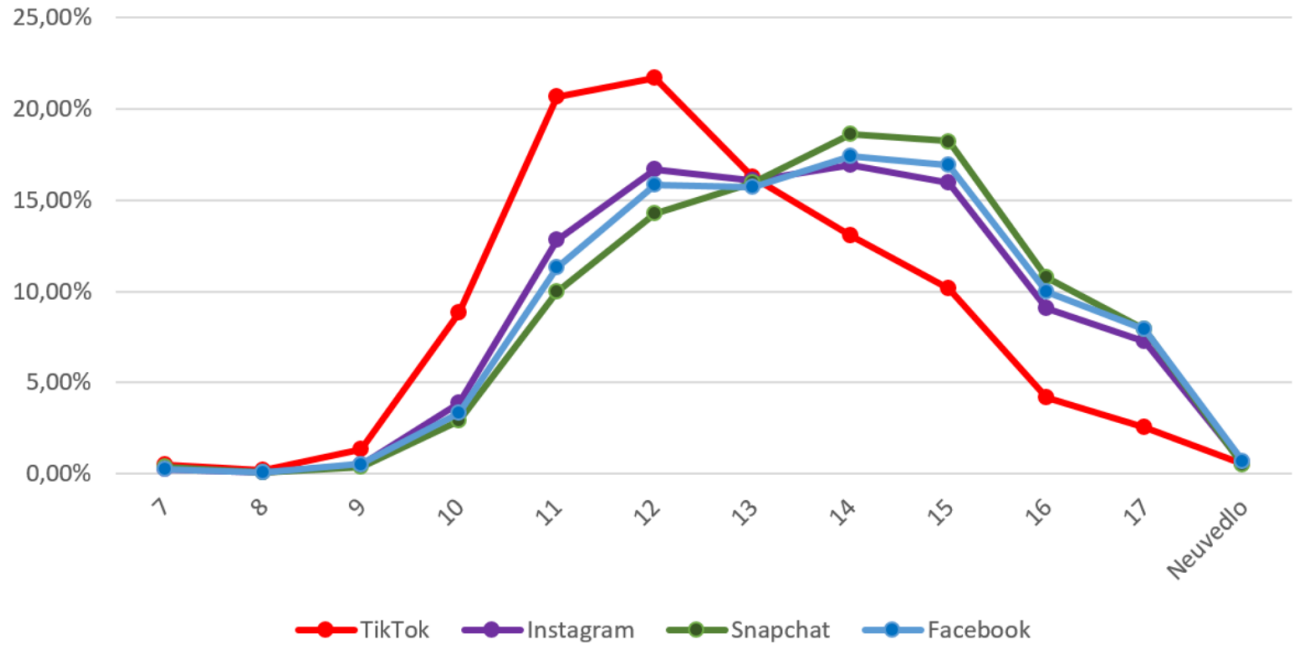


Další nebezpečné fenomény

- Sexting
- Cyberstalking
- Pranky a challange (**vzpomenete si na nějaké virální?**)
- A mnoho dalších…

Kontext

Věkové rozložení dětských uživatelů (7-12 let) u dominantních sociálních sítí

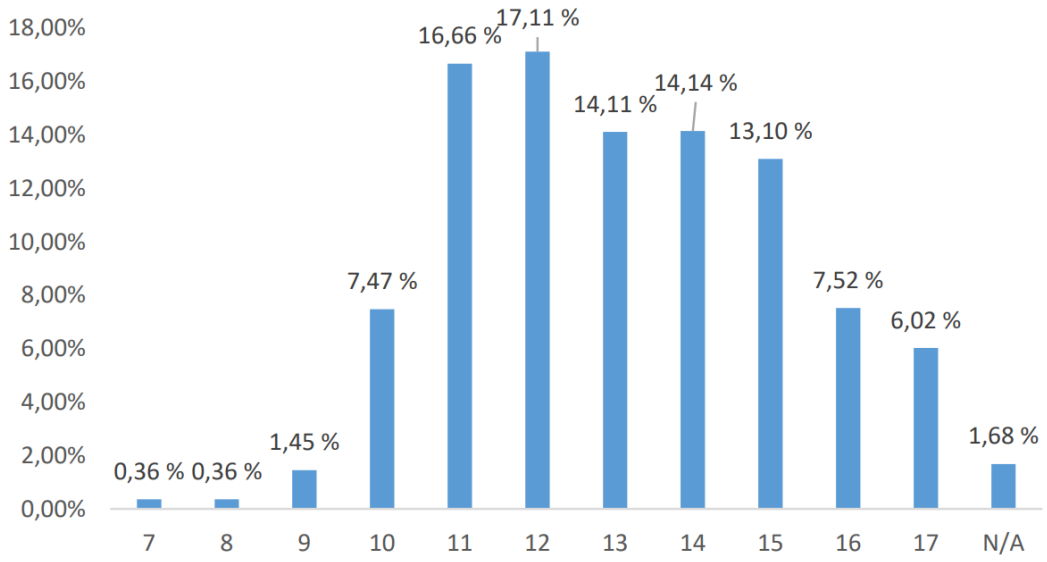


Zdroj: Výzkum České děti v kybersvětě 2019

- Tyto data jsou z roku 2019, tedy 4 roky stará….
- A jsou z doby před COVIDEM…
- A ještě jeden problém (další strana)

Kontext

Tabulka 1. Věková struktura výzkumného souboru



(n=27177)

- Výzkum má sice relativně velký vzorek (n=27177 dětí) , ale extrémně nízký počet účastníků ve věku 7-9 let….
- Tudíž nám výzkumná data o soc. Sítích do jisté míry kopírují věk účastníků
- Proto je potřeba data zkoumat komplexně ;)

Zpátky k výuce a školnímu prostředí...

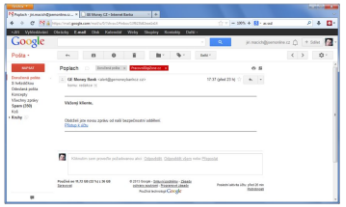
- Kde děláme jako učitelé chyby?
- Co je potřeba naučit?
- Na co cílit?
- Jak motivovat k využívání?
- ....

Časté chyby v předávání znalostí

- Zastaralé informace (principy virů, chování útočníků, motivace útočníků)
- Opakované chyby odvětví (metodika hesel)
- Menší akcent na bezpečnost mobilních zařízení
- **Malá návaznost na žákovskou realitu**

Kde je nebezpečí?

- Sociální sítě
- Herní platformy
- „Náhodné klikání“
- Pornografie
- Phising



- ~~Bankovnictví~~
- ~~Pracovní maily~~
- ~~Datová uložiště~~

Co chceme žáky naučit (příklady)

- **Obecné povědomí**

- Často se učí
- Co je to malware
- Jak pracuje
- Jak pracují antiviry, firewall
- Co je to ransomware
- …a mnoho dalších

- **Dobrou praxi**

- Ovládat a používat prvky zabezpečení
- Two-step verification
- Zabezpečení domácí wi-fi
- Zásady dobrého hesla
- Rozpoznání závadných stránek (phising, hoax, …)
- Rozpoznání soc. inženýrství
- Fake news
- … mnoho dalších

Dobrá praxe je velice užitečná, ale jak docílíme toho, aby ji žáci integrovali do svých životů?

Jak motivovat k využívání naučeného?

- Provázat svoji výuku se službami a technologiemi, které žáci sami využívají
- Hledat a ukázat reálné dopady a případy
- Otevřeně s žáky diskutovat o tom jak využívají sociální sítě a další služby a o jejich zkušenosti výuku opírat

Mobile News News

PlayStation Network Hacked. Again.

August 23, 2017

VAROVÁNÍ KRADOU IDENTITU I PENÍZE

POZOR: Na Facebook ve velkém útočí hackeři! Tyto triky používají

Ilustrační foto

174 To se mi líbí

Tweet

G+

Témata: facebook, hacker, varování, policie, vir, podvod, domácí

Policie varuje před masivním útokem hackerů, kteří v posledních dnech napadají uživatelské účty na Facebooku. Snaží se podvodnými triky dostat až k přístupu do bankovních účtů. Rychle se šíří ale i zprávy, které jednoduše zavirují počítač.

77,000 Steam users are hacked every month. Here's how Valve is fixing it

by LAUREN HOCKENSON — Dec 10, 2015 in INSIDER

0 266 SHARES http://tnw.to/j4x7p

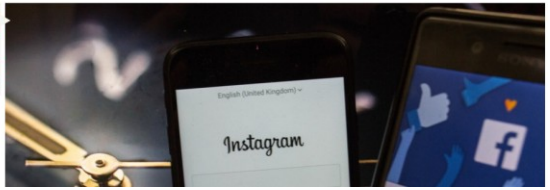
One of the crucial parts of Steam — the computer gaming platform developed by Valve Software — is th
items and collectibles
net users a tidy sum o

Mashable VIDEO ENTERTAINMENT CULTURE TECH SCIENCE SOCIAL GOOD SHOP MORE

Tech

Instagram users are reporting the same bizarre hack

Share on Facebook Share on Twitter



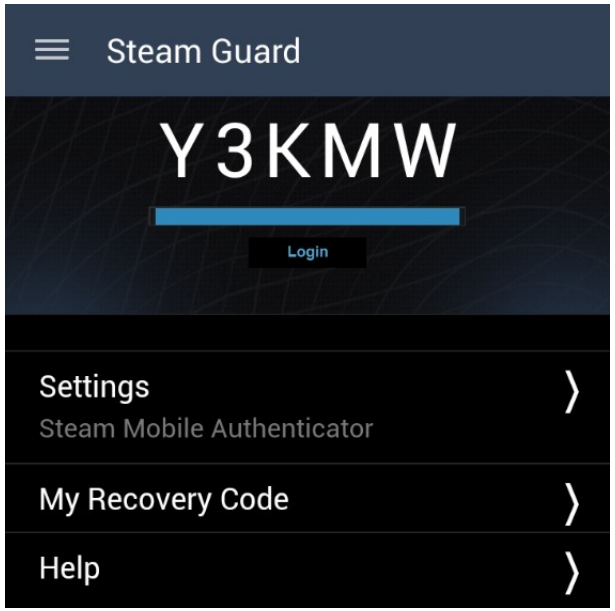
Mos

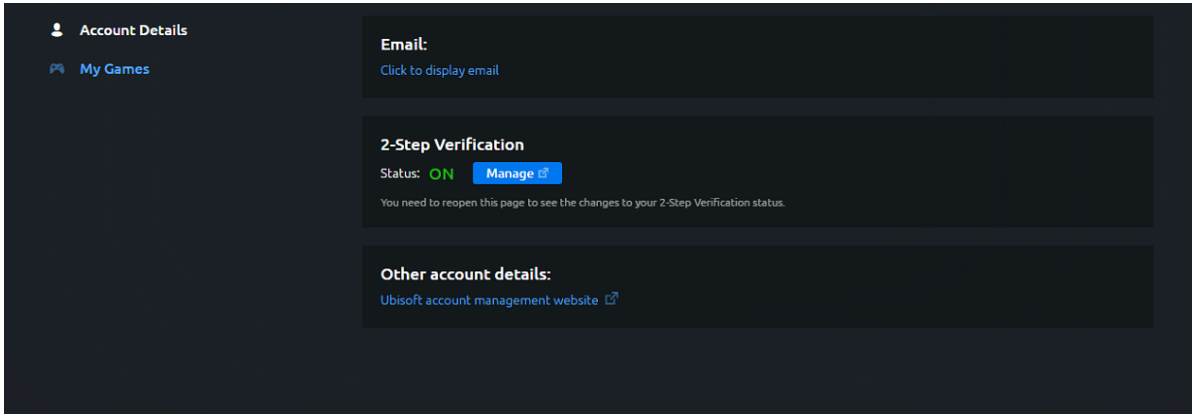
Neve

Co tedy žáci využívají?

- **Herní platformy** – Steam, Uplay, Origin, GoG, Google play, Playstation Network, Xbox Live Marketplace….
- **Sociální sítě** – Facebook, Instagram, Youtube, Snapchat, Musical.ly…
- **Další služby** – maily, různé aplikace, diskuzní fóra, el. žákovské knížky,…

Two-step verification





„If it's free, you are the product."

If it’s free, you are the product

- Na příkladu sociálních sítí, které žáci používají se dá tento koncept dobře demonstrovat
- Slouží k lepšímu pochopení principu ochrany našich osobních údajů a identity online

If it's free, you are the product

- Pochopení, že vše co sdílíme a na síti děláme má nějakou cenu
- Žáci většinou nevidí jako problém, že se jim zobrazují cílené reklamy
- Potřebujeme žákům vysvětlit jak je možné s nimi manipulovat zobrazováním cíleného obsahu na soc. sítích
- Jak z hlediska konzumerismu, tak třeba politicky nebo názorově (viz skandál Cambridge Analytica)
- Uvědomit si propojení komplexních informací o nás

LOL

If it’s free, you are the product

- 1) Cílení reklamy
- 2) Cílená manipulace
- 3) Testování pro budoucí vývoj
- 4) Testování pro placenou formu produktu
- 5) Obchod s osobními údaji
- 6) Obchod s vašimi preferencemi a čímkoliv co jde měřit
- 7) Vyložené podvody

Rady na závěr

- Buďte paranoidní ! Pomáhá to ☺
- Nepodceňujte svoji významnost !
- Když nevíte nechte si poradit od vašeho správce sítě!
- Vždycky někdo někde poslouchá !

Zdroje

- http://prf-czv.osu.cz/nabidka/seminar/data/Kryptografie.pdf
- http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c05.pdf
- http://mi21.vsb.cz/sites/mi21.vsb.cz/files/unit/mzka.png
- http://frakira.fi.muni.cz/~izaak/PBIT/Kryptografie_a_bezpe%C4%8Dnost.html
- http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c02.pdf
- http://www.flops.cz/zaklady-sifrovani-symetricka-a-asymetricka-kryptografie
- http://cs.wikipedia.org/wiki/Autentizace
- http://www.guardmyip.com/images/wireless_security1.jpg

- DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2., aktualiz. vyd. Brno: Computer Press, 2009, 542 s. ISBN 978-80-251-2619-6.