

Lekce 3.3:

Bezpečnost na webu



Ing. Pavel Roubal

Kapitola 3:

Web, prohlížeče, bezpečnost

K této prezentaci jsou k dispozici cvičení. Pracovní sešit pro žáky objednávejte na webu:

www.opocitacich.cz

Pro pohodlné promítnutí prezentace v prohlížeči webu klepněte vpravo nahoře na Spustit prezentaci a pak již pouze klepejte myší nebo mezerníkem...

Web – opakování

- ▶ **Webové stránky** jsou uloženy jako **soubory** ve **formátu HTML** na serverech připojených k Internetu.
- ▶ Jsou to **soubory** ve složkách uložených na discích serverů.
- ▶ **Prohlížeč** na našem počítači je umí přes Internet načíst a zobrazit.
- ▶ Samozřejmě s **podporou operačního systému**, který zajišťuje komunikaci zařízení pomocí paketů.



Nic neřeší vše, každá oblast má vlastní postupy

- **Jednoduché řešení bohužel neexistuje.** Ani nějakým postupem, ani „zázračným“ zařízením nejde vše vyřešit a zajistit.
- **Celkové řešení je skládkou (systémem)** mnoha dílčích řešení.

V této lekci si vysvětlíme **zabezpečení přenosu webových stránek** a **přístupu** k webovým serverům. Komplexní **bezpečnosti IT zařízení** je věnována celá kapitola **Bezpečný počítač**.

Bezpečnosti nás, naší (digitální) identity a stopy je věnována opět celá kapitola **Bezpečné digitální prostředí**.

Zásadní vliv na **naši bezpečnost** mají **naše znalosti** a jejich **využívání**.



Šifrovaný přenos dat

- **Bezpečný přenos dat** přes nebezpečné prostředí řeší jejich **šifrování**.
- Náš **webový prohlížeč data zašifruje** a pošle je zašifrovaná přes Internet serveru. Stejně **tak server data šifruje** a zašifrovaná je posílá prohlížeči v našem počítači.
- Útočník si tedy **může stáhnout pakety s daty**, protože však **nezná klíč k jejich dešifrování**, nepodaří se mu je dešifrovat a přečíst.

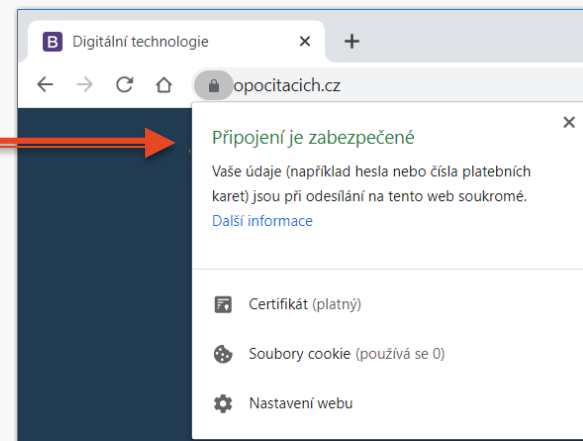
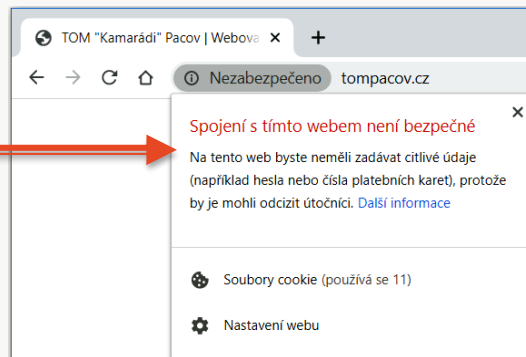
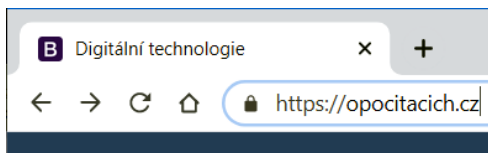
Jak to servery a prohlížeče dělají (symetrická a asymetrická šifra, soukromý a veřejný klíč...) se dozvíte v lekci **7-03B – Šifry jednoduché i složitější**.

Šifrování dat (kryptografie) je jedna z nejsložitějších informatických disciplín. Navenek, z našeho pohledu se naštěstí **využívá poměrně jednoduše**.



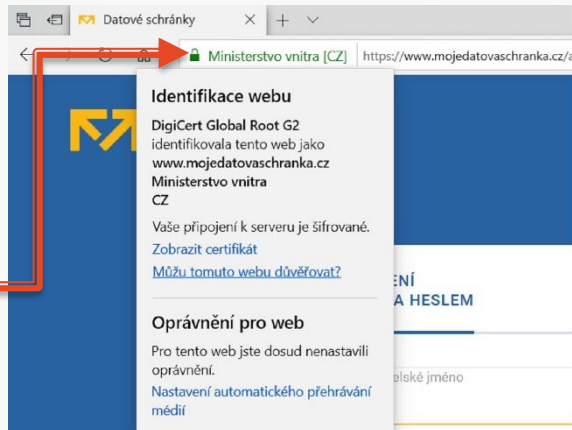
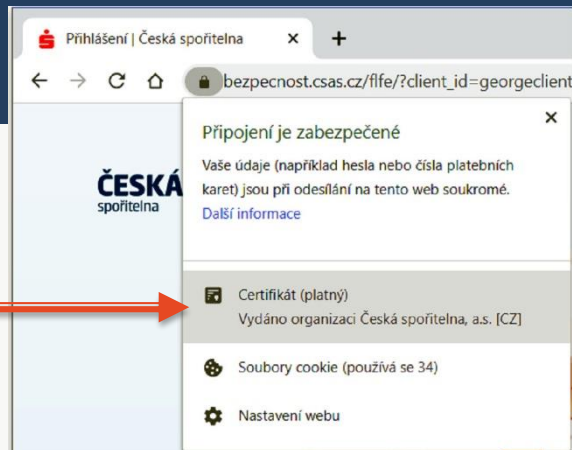
Jak poznáme šifrovaný přenos dat – HTTPS

- ▶ Již víme, že prohlížeč používá k přenosu dat nějaký způsob, přesněji protokol.
- ▶ **HTTP** je „obyčejný“, desítky let starý protokol. **Nezabezpečuje nijak přenášená data.** Dnes se proto přestává používat.
- ▶ **HTTPS** (**s**=secured, bezpečný) **je šifrovaný protokol**, který **spojuje** zastaralý protokol HTTP se **šifrováním metodou SSL**.
- ▶ Dnes většina stránek (webových serverů) používá šifrovaný přenos dat protokolem **HTTPS** a časem nejspíše bude tento protokol **povinný** pro všechny přenosy dat.



Ověření webu – certifikáty serverů

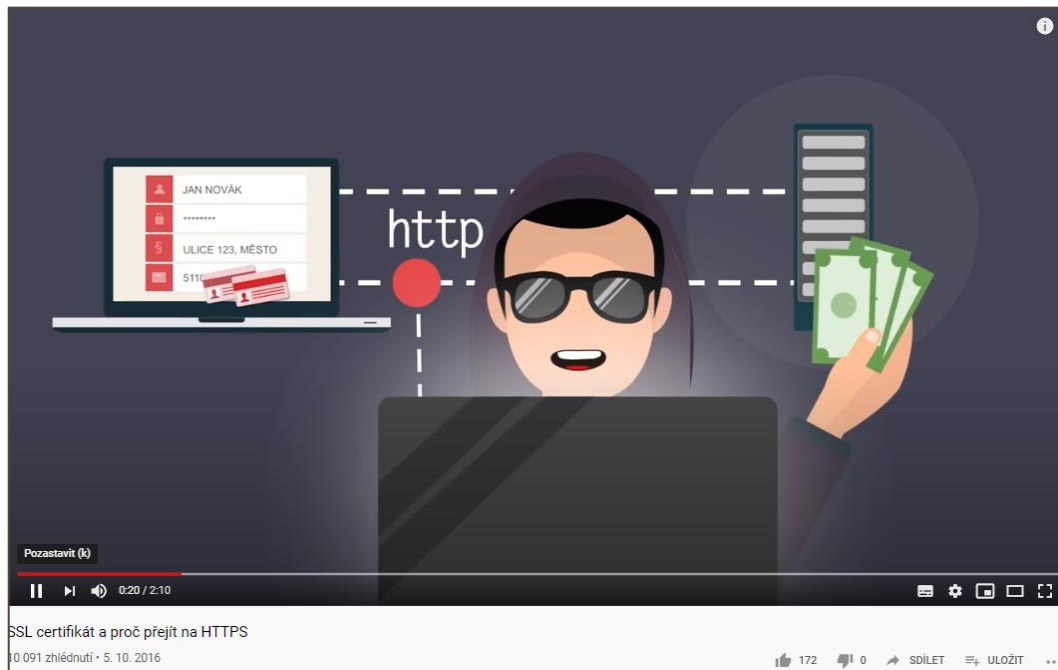
- ▶ Vidíme-li v adresním řádku URL webu např. www.nejakabanka.cz **není ještě jisté**, že jde opravdu o stránky Nějaké banky a.s.
- ▶ Pozor, také **protokol HTTPS nedává jistotu**, komu **patří web**, na kterém jsme. (HTTPS znamená šifrovaný přenos dat, můžeme však **šifrovaně komunikovat s útočníkem**.)
- ▶ **Jistotu**, na jakém webu jsme a komu tedy sdělujeme své číslo účtu, heslo k e-mailu apod., dávají tzv. **certifikáty serverů**.
- ▶ **Prohlížeče webu** po klepnutí na ikonu zámečku ukazují, zda **má web ověřený certifikát a komu patří**.
- ▶ U **rozšířeného ověření** např. prohlížeč MS Edge ukazuje zeleným pruhem, komu web patří. (Rozšířené ověření nejčastěji využívají banky a státní orgány.)



HTTPS – video

- ▶ Prohlédněte si **krátký film**, vysvětlující potřebu **SSL šifrování**:
https://www.youtube.com/watch?v=Lm_cOGsFwnM

Česky, jde o reklamní video, vysvětluje však také stručně a jednoduše potřebu HTTPS.



- ▶ Data přes internet jdou **nezabezpečeně**.
- ▶ Protokol **https** šifruje naši komunikaci s webovým serverem.
- ▶ **Ne** však naše e-maily, obrázky, zprávy...
- ▶ To zajišťuje tzv. **end-to-end šifrování**, **koncové šifrování**.
- ▶ Funguje tak, že
 1. na **našem počítači** se zpráva (obecně soubor) **zašifruje silnou šifrou**,
 2. přenese se přes nebezpečné prostředí (Internet)
 3. a na **počítači příjemce** se stejnou šifrou **dešifruje**.

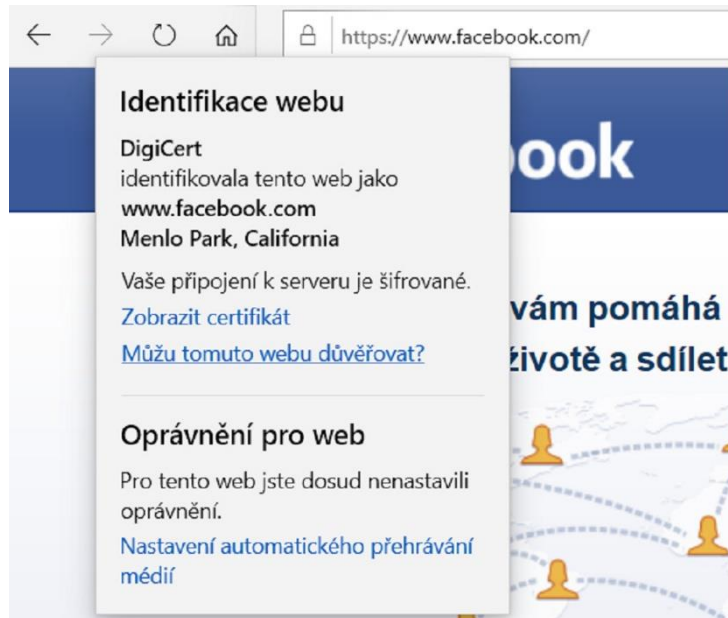
Šifra vždy vyžaduje:

- ▶ Šifrovací **algoritmus**.
- ▶ Aktuální **klíč** použitý pro toto šifrování.

Pro **šifrování** se používají nesmírně složité matematické metody, tzv. **symetrická** nebo **asymetrická kryptografie**.

Shrnutí: na jakém webu jsme a je přenos dat bezpečný?

Jakmile jdeme na web, kde **zadáваме** svá hesla, adresu, osobní údaje nebo jakákoliv **citlivá data**, vždy se podíváme do adresního řádku a zkontrolujeme, zda je použit **šifrovaný protokol HTTPS** a zda se web **prokazuje platným certifikátem**.





username

password

☐ remember me



Většina našich dat je chráněna kombinací
uživatelského jména (username)
a hesla (password).

Heslo by mělo být tzv. **silné**, neuhodnutelné, **neprolomitelné**.

Asi tušíte, že heslo **123456** moc silné není...

Silné heslo – tvorba

- ▶ Jak si **zapamatujeme** takto složité heslo?
- ▶ Řekneme si frázi (pár slov za sebou), kterou si dobře zapamatujeme. Například:
- ▶ Z prvních písmen vytvoříme heslo, vložíme navíc nějaké číslo, které s námi souvisí. A přidáme třeba jeden speciální znak.
- ▶ Možnou alternativou je také několik slov bez mezer, která sice sama něco znamenají, ale jako celek tvoří silné heslo. Takové heslo musí být mnohem delší než 10 znaků.

Silné heslo:

- ▶ Je dlouhé minimálně 10 znaků.
- ▶ Nic neznamená.
- ▶ Obsahuje malá i velká písmena, číslice a nejlépe i další speciální znaky (*?! apod.).

Narodil jsem se v **B**rně a **b**ydším v **P**raze
Nejraději mám **F**otbal a **z**eleninu

NaBrby19?Pr
NejFot75+zel

Tato vzorová hesla samozřejmě
určitě nikde nepoužívejte!

HoryStrom1079Hradec

Silná hesla – různá hesla

- Pro **různé weby** je nutné mít **různá hesla**. Řeší to tzv. správci hesel.
- Pokud správce hesel zatím nepoužíváte, vytvořte si minimálně:
- **Speciální různá hesla** pro nejdůležitější služby (e-mail, Facebook, Instagram, internetové bankovníctví apod.)
- **Jiné heslo** pro e-shopy.
- **Jiné heslo** pro další méně důležité služby.

Důležitost (silných a různých) hesel nepodceňujte. Chrání vaše osobní údaje, vaše soukromí a vaše peníze.

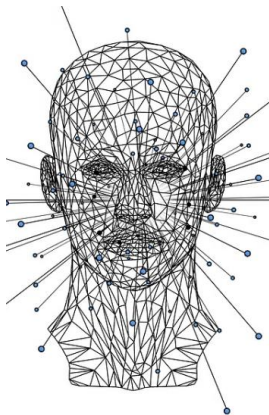
Desítka nejpoužívanějších (a **nejhorších**) hesel v roce 2021:

- | | |
|-----------|----------------|
| 1. 123456 | 2. 123456789 |
| 3. Qwerty | 4. password |
| 5. 12345 | 6. qwerty123 |
| 7. 1q2w3e | 8. 12345678 |
| 9. 111111 | 10. 1234567890 |

Nevypadá podobně také nějaké **vaše heslo**?

Biometrická autentizaci

- **Heslo se dá zapomenout.** Stále častěji se proto používá **biometrická autentizaci**.
- **Biometrická autentizace = určení totožnosti člověka podle jeho jedinečných biologických (fyzických) vlastností**, rysů.
- Nejčastěji se dnes používá:
 - ▶ **Otisk prstu.**
 - ▶ **3D obraz obličeje (Face ID).**
- Existují další, méně běžné metody identifikace.

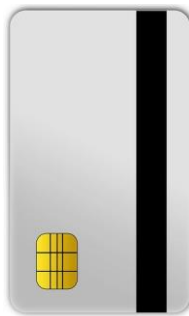


Biometrika se využívá stále více a více a nejspíše se v blízké budoucnosti stane **dominantní metodou** ověření člověka.

Přijdete do školy, kamera vás zaznamená, dveře se (samy) otevřou, pozdraví vás (a systém zapíše přesnou dobu vašeho příchodu i odchodu...)

Dvoustupňová identifikace (dvoustupňové ověřování)

- **Heslo se dá odcizit.** Stále častěji se proto používá **dvoustupňová identifikace** (také **autorizace**).
- **Dvoustupňová identifikace = určení totožnosti** člověka podle **dvou zadaných údajů**. (Něco **vím** + něco **mám** u sebe.)
- Nejčastěji se dnes používá kombinace **hesla a čísla (PIN)** zaslaného na zadaný mobilní telefon.
- Další možností jsou **bezpečnostní aplikace** (v mobilu).
- Nejvyšší stupeň zabezpečení nabízí speciální **čipové karty** nebo **tokeny** (flash disky) s elektronickými **certifikáty**.



Po zapnutí dvoustupňové identifikace budete **vždy potřebovat dva údaje**, jinak se například ke svému účtu nedostanete.

Doporučuje se proto raději **zadat údaje minimálně tři**, k heslu a telefonu přidat ještě **e-mail**, případně kontakt na blízkou osobu (rodiče).

Dvoustupňová identifikace výrazně zvyšuje zabezpečení přístupu (k účtu), např. banky ji dnes vyžadují povinně.

Shrnutí: ověření přístupu

Při používání webových a cloudových služeb je zcela zásadní používání silných různých hesel, případně využívání biometrické identifikace a dvoustupňového ověřování.

Jen tak máme velkou šanci, že o svá osobní data a o své peníze nepřijdeme.



Silná hesla – video

- Prohlédněte si **krátký film**, **vysvětlující potřebu silného šifrování**:

<https://www.youtube.com/watch?v=tTFEbY6S58g>

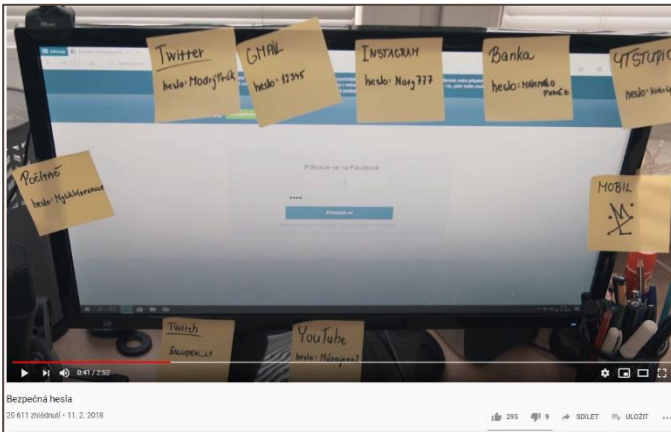
Česky. 4:24 min.



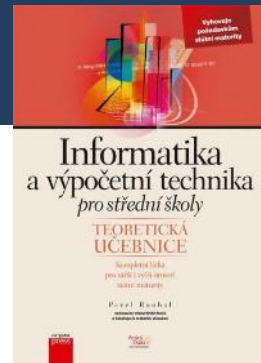
- A třeba ještě tento film:

https://www.youtube.com/watch?v=sUpGHM_Adxo

Česky. 2:52 min.



1. ROUBAL, Pavel. *Informatika a výpočetní technika pro střední školy: [kompletní látka pro nižší a vyšší úroveň státní maturity]*. 2. vydání. Brno: Computer Press, 2019. Česká škola (Computer Press). ISBN 978-80-251-4951-5.
2. ROUBAL, Pavel. *Počítač pro učitele*. Brno: Computer Press, 2009. ISBN 978-80-251-2226-6.
3. Pixabay.com. [online]. [cit. 2020-04-05]. Dostupný z URL: < <https://pixabay.com/>>. Fotky od OpenClipart-Vectors z Pixabay. <https://pixabay.com/cs/users/openclipart-vectors-30363/>
4. OpenPhoto Gallery. [online]. [cit. 2009-04-05]. Dostupný z URL: < <http://openphoto.net/gallery/index.html> >.
5. Wikimedia Commons[online]. [cit. 2020-01-09]. Dostupný z https://commons.wikimedia.org/wiki/Main_Page



© Ing. Pavel Roubal 2020.

Tento dokument podléhá autorskému zákonu.

Proto prosím, abyste ho nešířili a používali ho pouze pro účely výuky ve spojení s pracovním sešitem.

www.opocitacich.cz
