Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Workshop – Kyberbezpečnost

15. června 2018

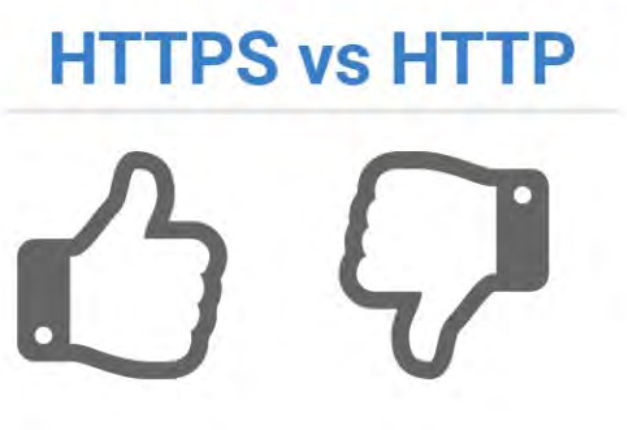
Mgr.Bc. Martin Vejvoda

Rozvoj systémové podpory digitální gramotnosti
DigiStrategie 2020
CZ.03.1.54/0.0/0.0/16_020/0005634

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

- **Jaký je rozdíl mezi http a https?**

- **A proč si na to dávat pozor?**



DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Proč vzniklo HTTP - HyperText Transfer Protocol ?

V internetových počátcích se administrátoři sítí museli dohodnout, jak budou sdílet informace na internetu.

Shodli se na postupu, který nazvali HTTP

Jde o komunikační protokol, který na internetové síti slouží k přenosu dat, dříve pouze hypertextových, dnes již však i fotografií a videí.

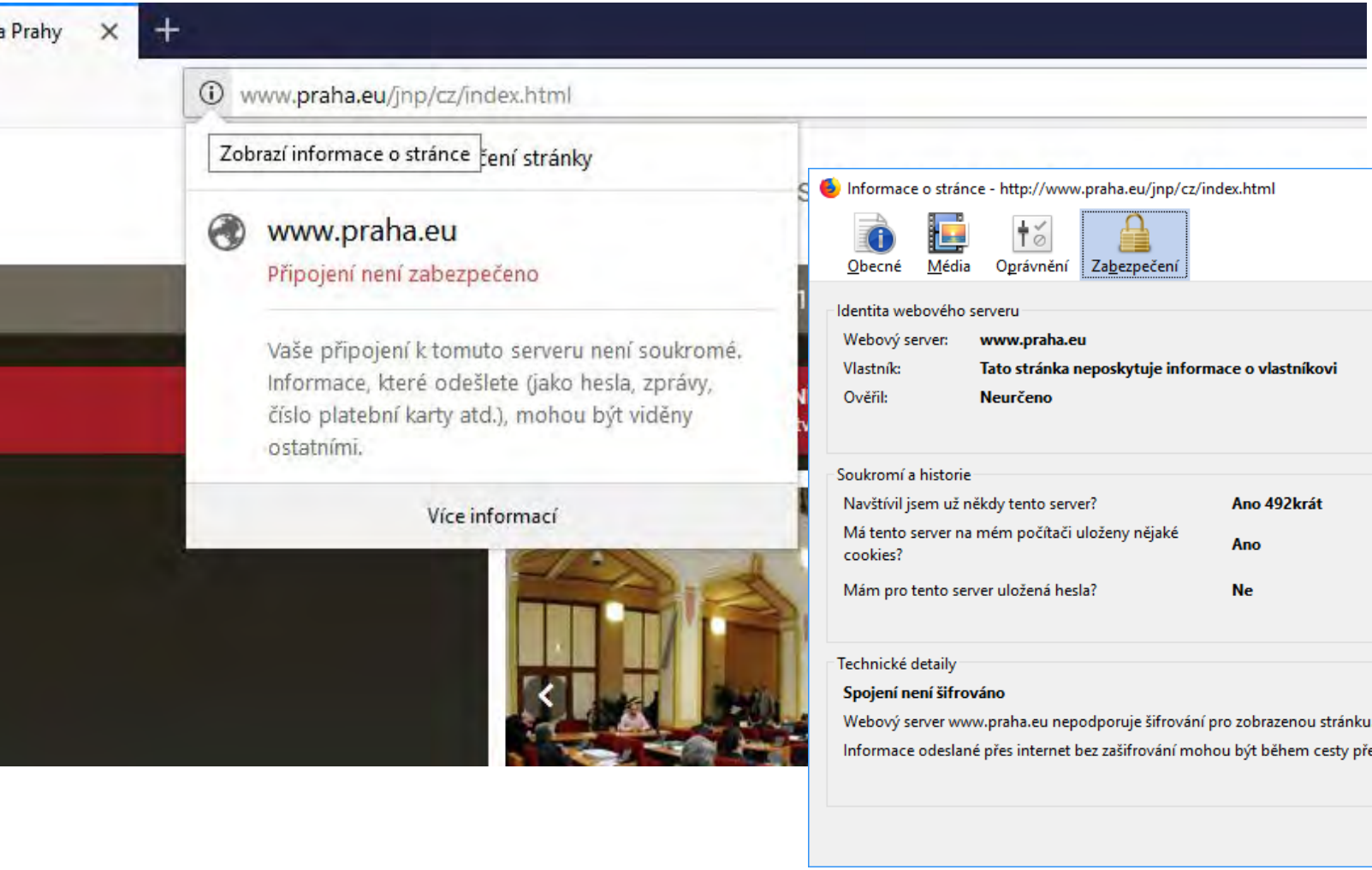
DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Co v adresní řádce znamená http

Komunikace je otevřená a přenášené informace může po cestě mezi prohlížečem a serverem kdokoliv:

- číst, včetně hesel a dalších citlivých údajů, například z kontaktního formuláře
- případně **změnitelná**

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti



- někdo může vědět co posíláte a přijímáte, ale také může do komunikace zasahovat.

- může podvrhnout zcela jiné informace v okamžiku, kdy jste připojení, např. online bankovnictví.

- místo neškodných inzerátů posílat útočný kód, co do vašeho počítače dostane malware.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Malware - **škodlivý software**, **zákeřný software -** program určený k poškození nebo vniknutí do počítačového systému.

Pod souhrnné označení malware se zahrnují:

- počítačové viry,
- počítačové červy,
- trojské koně,
- crimeware,
- špehovací software (spyware),
- vyděračský software (ransomware)
- reklamní software (adware)

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

nešifrovaně přistupovat kamkoliv znamená,

případný útočník získá data zahrnující všechny informace,
nejen to, co na stránce vidíme, ale také to, co tam děláme,
což přináší velká rizika.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Aby se takovému odposlechu zabránilo,
byl vyvinut HTTPS (anglicky Secured, zabezpečený) protokol,
který veškeré informace mezi serverem a Vaším počítačem
přenáší v zašifrované podobě.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

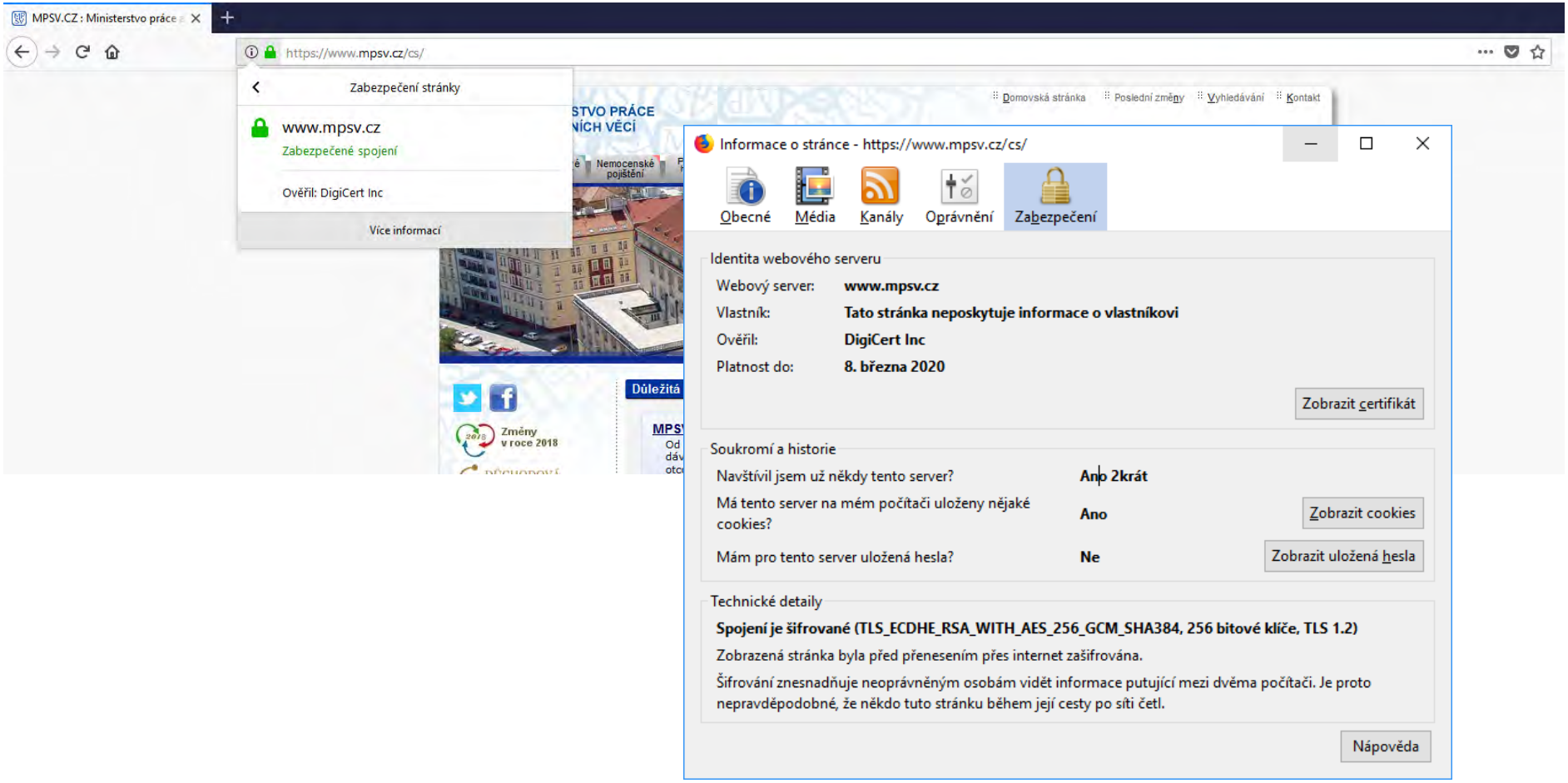
https v adresní řádce

(zpravidla vizuálně indikované i nějakým zámečkem či jinou formou)

znamená, že komunikace mezi vámi a webem

probíhá šifrovaně a (teoreticky) nikdo nemůže tuto komunikaci odposlouchávat.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti



DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Proto je důležité aby **https** bylo vždy aktivní tam kde:

- odesíláte přihlašovací údaje,
- řešíte emaily,
- online bankovnictví,
- nakupujete,
- přenášíte jakékoliv osobní či citlivé informace
- ...

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Pozor

To že v prohlížeči máte ikonku šifrovaného připojení, ale **neznamená,** že web na který jste právě přišli je bezpečný.

Není to nic jiného, než příznak toho, že komunikace mezi vámi a webem **probíhá šifrovaně a (teoreticky) nikdo nemůže tuto komunikaci odposlouchávat**.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Podezřelé odkazy

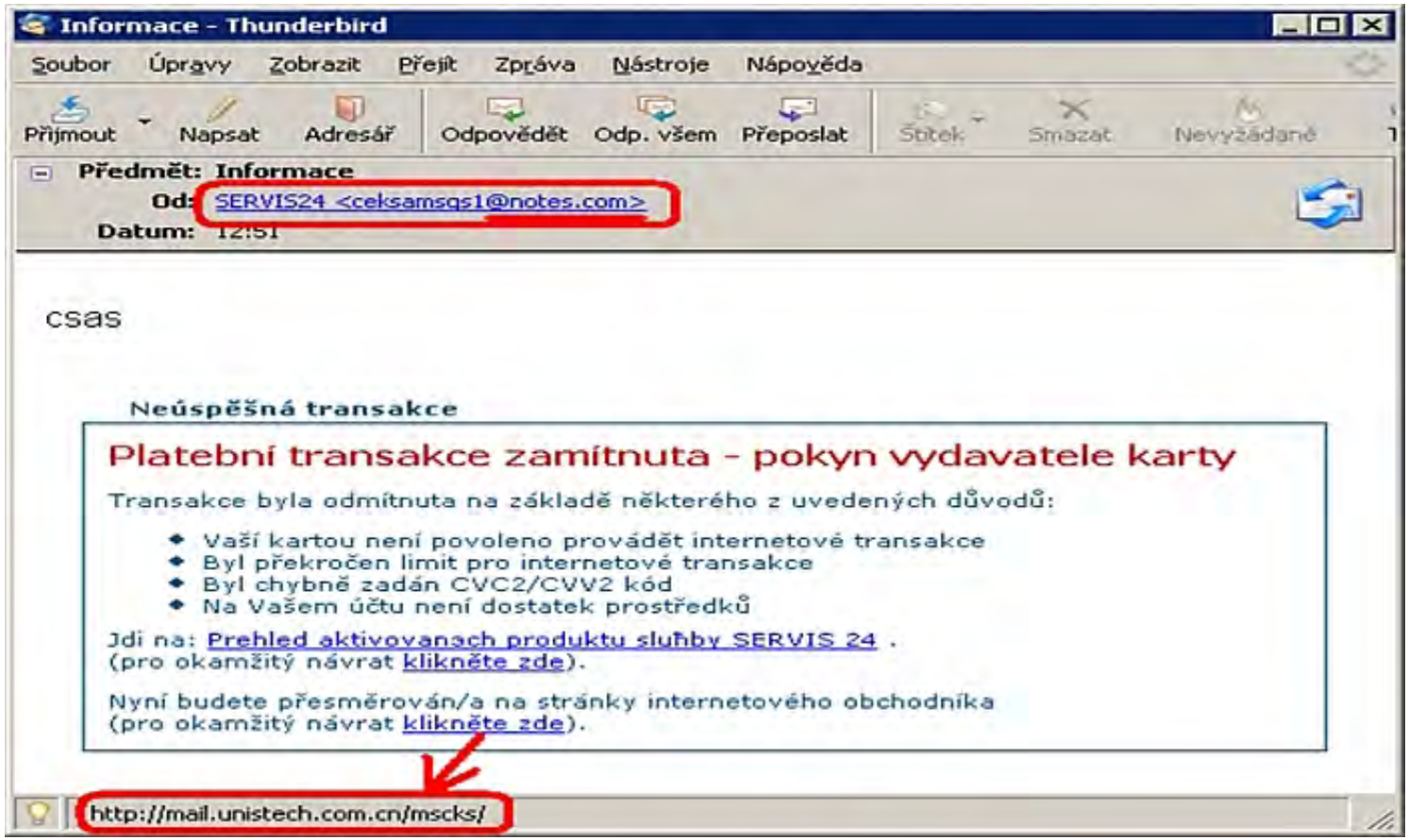
Podvodné přesměrování bohužel odhalíte velmi obtížně, pokud vůbec.

Nepoznáte žádný rozdíl v adresní řádce prohlížeče a vizuální obsah webu bude buď totožný, nebo velmi podobný stránce, kterou jste chtěli navštívit.

Na možné zneužití může upozorňovat také adresní řádek (tam, kde zadáváte webovou adresu).

Pokud neobsahuje obvyklou webovou adresu vaší banky, je to známka, že může jít o podvodnou webovou stránku.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti



odkaz směruje na špatnou adresu, doménové jméno v adrese e-mailu se neshoduje s oficiálním názvem domény společnosti.

podezřelé odkazy

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

V adresním řádku je uvedena podezřelá webová adresa, která nesouhlasí s oficiální adresou společnosti. Chybí bezpečnostní certifikát.

podezřelé odkazy

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Přihlašování a hesla

- pravidla pro tvorbu hesel
- jednofaktorové x dvoufaktorové ověření
- správci hesel

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Heslo představuju klíč pro přístup k různým typům účtů:

- v počítači,
- firemní síti
- službám
- obchodům
- portálům na internetu
- …

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Co se může stát pokud dojde k odcizení hesla:

- ke ztrátě kontroly nad počítačem,
- převedení peněz z vašeho bankovního účtu
- uskutečnění on-line plateb vaším jménem,
- ukradení identity a její zneužití pro různé typy trestné činnosti.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Jaké heslo?

Při tvorbě hesla by neměla být hlavním kritériem pouze snadnost zapamatování, ale také jeho bezpečnost.

Heslo by mělo odolat útokům od odhadování

až po prolomení hesla hrubou silou.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Bezpečné heslo by mělo splňovat následující kritéria:

- mělo být dostatečně **dlouhé** (min. 8 znaků), složité a přitom snadno zapamatovatelné
- každý další znak v heslu mnohonásobně zvyšuje ochranu, kterou heslo poskytuje.
- Heslo by mělo obsahovat minimálně 8 znaků, ideální je 14 a více znaků.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

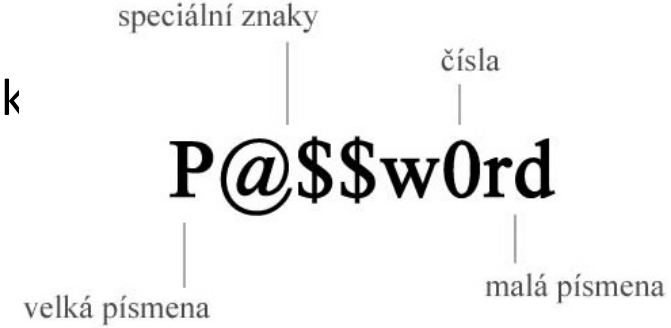
Bezpečné heslo by mělo splňovat následující kritéria:

Mělo by obsahovat **velká a malá písmena, čísla** a **speciální znaky**

Kombinujte písmena, číslice a symboly. Čím rozmanitější znaky heslo obsahuje, tím obtížnější je ho uhodnout.

Další důležité aspekty:

- Čím méně typů znaků heslo obsahuje, tím delší musí být. Heslo skládající se z 15 náhodných písmen a číslic je přibližně 33 tisíckrát bezpečnější než heslo tvořené 8 znaky z celé klávesnice.
- Nemůžete-li vytvořit heslo obsahující symboly, je třeba udělat iei mnohem delší, abyste dosáhli stejné úrovně ochrany.
- Ideální heslo je dlouhé a obsahuje různé typy znak



DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Bezpečné heslo by mělo splňovat následující kritéria:

- Nemělo by obsahovat slovo, které lze nalézt ve slovníku
- Nemělo by být stejné jako Vaše uživatelské jméno
- Nemělo by mít logický vztah k uživateli (přezdívka, jméno manželky, rodné číslo apod.)
- Nemělo by obsahovat opakující se znaky a posloupnosti.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Nejpoužívanějšího hesla

	Heslo		Heslo
1	123456	14	abc123
2	password	15	111111
3	12345	16	mustang
4	12345678	17	access
5	qwerty	18	shadow
6	123456789	19	master
7	1234	20	michael
8	baseball	21	superman
9	dragon	22	696969
10	football	23	123123
11	1234567	24	batman
12	monkey	25	trustno1
13	letmein		

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

- **Neprozrazujte je dalším osobám.** Schovejte hesla před známými a členy rodiny (hlavně před dětmi), kteří by je mohli sdělit dalším, méně důvěryhodným osobám.

- **Chraňte zaznamenaná hesla.**

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

- **Neposkytujte hesla v e-mailu nebo v odpovědi na e-mailovou žádost.** Jakýkoli e-mail s žádostí o heslo nebo ověření hesla na webu je s nejvyšší pravděpodobností podvodný.

- **Hesla pravidelně měňte.** Složitější heslo může být bezpečné delší dobu.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

- **Nezadávejte hesla v počítačích, nad kterými nemáte kontrolu.**

Například počítače v internetových kavárnách, počítačových laboratořích, sdílených systémech, kioskových systémech, na konferenčních místech a na letištích nelze považovat za bezpečné pro jakékoli osobní použití kromě anonymního prohlížení internetu.

Nepoužívejte tyto počítače k on-line kontrole elektronické pošty, pracovní pošty, bankovních účtů, k návštěvám konverzačních skupin a přístupu k dalším účtům, které vyžadují uživatelské jméno a heslo.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

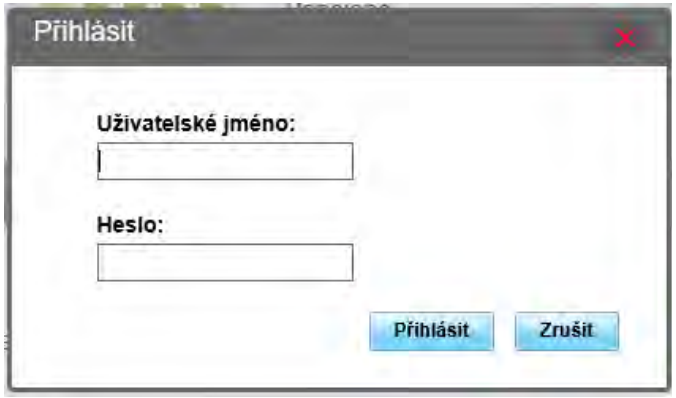
Ověření identity

jednofaktorové x dvoufaktorové ověření

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Jednofázové ověření identity pomocí uživatelského jména a hesla.

- Využívá většina služeb na internetu.
- Tento způsob je nejméně spolehlivý, protože spoléhá jen na „faktor znalostí“. To znamená, že pokud dojde k úniku hesla, tak ověření přestává být bezpečné.



DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Dvoufázové ověření identity je proces, který zahrnuje dva nezávislé způsoby, jak ověřit totožnost uživatele při přihlašování počítačům v síti, nebo k přihlašování k různým službám na internetu.

Například internetové bankovnictví, email a sociální sítě.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Příklad

Bankomaty vyžadují dvoufázové ověření.

Aby klient dokázal, že je tím, co tvrdí, systém vyžaduje dvě položky.

Platební kartu – faktor vlastnictví a dále osobní identifikační číslo (PIN) – faktor znalostí.

V případě ztráty karty je účet v bezpečí, protože zloděj nezná PIN. Totéž platí v opačném případě.

Zloději je PIN bez karty k ničemu.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Správce hesel velmi jednoduchý program.

Jedná se o databázi, která uchovává název služby, uživatelské jméno, heslo a případně nějaké další související údaje.

Tato databáze je potom chráněna jedním "super heslem", které ji dokáže odemknout.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

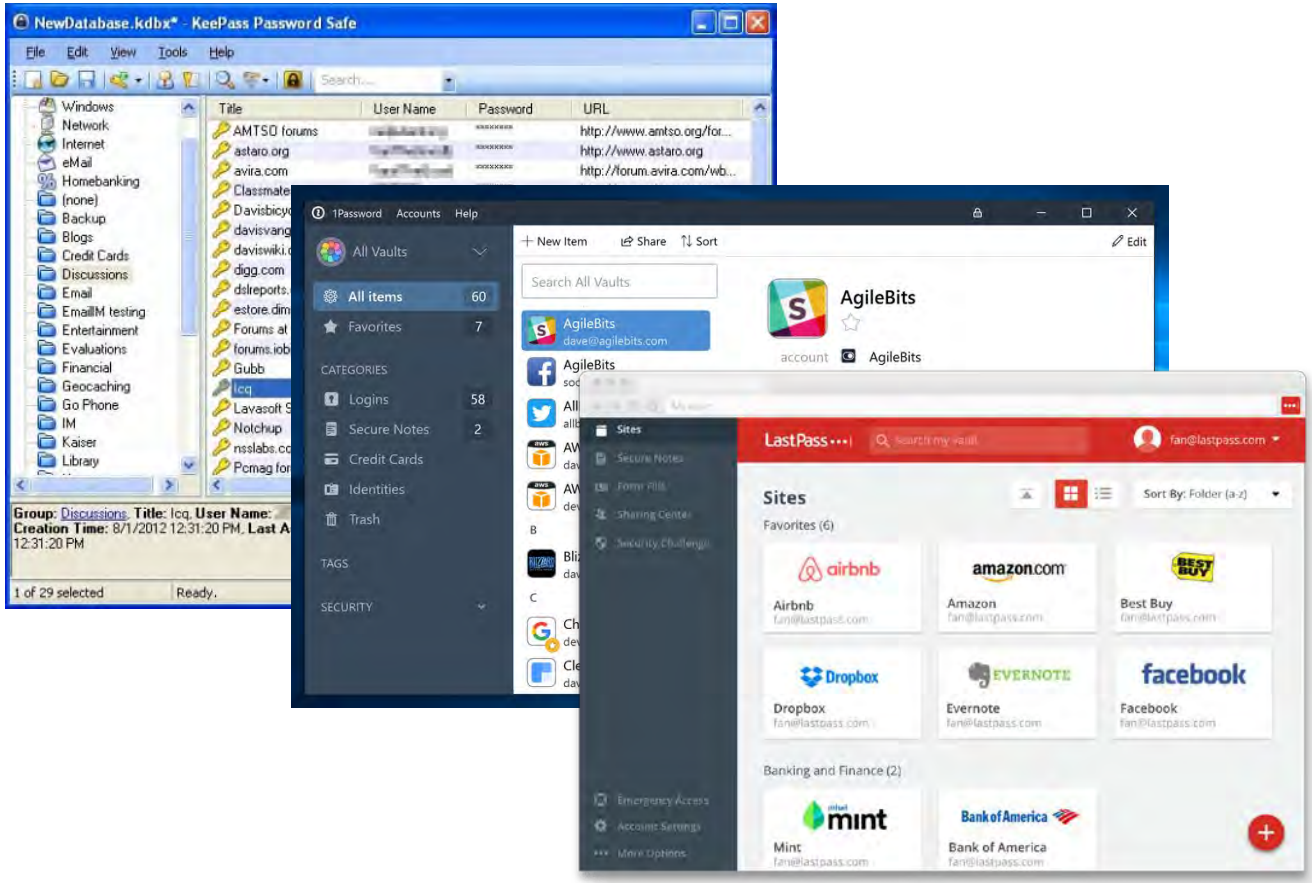
Jakého správce hesel zvolit?

- Správců hesel jsou stovky.
- Liší se počtem podporovaných platforem, funkcemi a celkovou architekturou.
- Volte tedy podle toho, jak vám který program vyhovuje.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Tři nejpoužívanější password managery jsou:

- **KeePass**
- **1Password**
- **LastPass**



DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Email

- SPAM
- PHISHING
- Podezřelé přílohy

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

SPAM - nevyžádaná pošta.

- Spočívá v hromadném rozesílání emailů uživatelům, kteří o ně nestojí.
- Zpravidla obsahují reklamu či hoaxové zprávy.
- Mohou také obsahovat viry a nebo podvodné nabídky.

Hoax - poplašná zpráva, která varuje před vymyšleným neexistujícím nebezpečím. Je to falešná poplašná zpráva, která se nezakládá na pravdě, ale uživatelé ji uvěří a sami jí šíří dál emailem nebo přes instant messangery.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Jak se proti spamu bránit?

- **Zbytečně nezveřejňovat svou e-mailovou adresu na internetu**, tj. neregistrovat se v podezřelých, neznámých formulářích nebo soutěžích. (Na internetu jsou roboti, kteří sbírají e-mailové adresy za účelem rozesílání spamu.)
- **Na konci zprávy bývá tlačítko Odhlásit** (Unsubscribe). Správně by vás po kliknutí na odhlášení měla tato funkce skutečně odhlásit, ale pokud se jedná o podvodný e-mail, často se přihlásíte jen k odebírání dalších spamových zprav. **Pokud si tedy nejste stoprocentně jisti, že jde o newsletter či obchodní sdělení, k jehož zasílání jste dali dříve souhlas, neklikejte.**
- **Přemýšlejte, buďte ostražití a neotevírejte jakoukoli příchozí spamovou zprávu.**
- **Většina spamů je odesílána z uživatelova počítače bez jeho vědomí**, protože je jeho počítač napaden virem. Doporučuje se tedy používat aktualizovaný operační systém + firewall + aktualizovaný antivir, jinak může rozesílat spam i váš počítač.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Výraz PHISHING pochází ze slova fishing, tj. rybaření. Přeneseně můžeme říct, že útočník hodí návnadu a čeká, než se uživatel (oběť) „chytí“.

- Jedná se o speciální techniku (sociálního inženýrství) používanou na internetu se snahou získat citlivé údaje (přihlašovací údaje, hesla, čísla kreditních karet).
- Principem těchto zpráv je věrohodné napodobení oficiální žádosti banky nebo podobné instituce a vynutit si od adresáta jeho přihlašovací údaje na odkazované stránce.
- Po zadání údajů oběti útočník získává přihlašovací údaje.
- Velkým problémem phishingu je to, že podvržené stránky jsou velmi věrohodné a těžko rozeznatelné. Proto musíte vědět, jak phishing rozeznat a jak se mu bránit.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Jak se proti phishingu bránit?

- Doručené e-maily ignorujte, „neklikejte“ na žádné odkazy v e-mailu, pro přihlášení používejte oficiální stránky.
- Buďte opatrní. Mějte na paměti, že phishing nemusí být spojen jen s tématem elektronického bankovnictví, ale je to např. i snaha o získání hesla do e-mailu nebo jiných služeb.
- Buďte opatrní, než se někde přihlásíte či zaregistrujete.
- Myslete na to, že žádná instituce, a už vůbec ne bankovní instituce, po vás nikdy nebude žádat přihlašovací údaje e-mailem. Toto se řeší oficiální formou, nikoli e-mailem.
- Používejte zabezpečené spojení.
- Když phishing pochází ze zahraničí, většinou ho rozeznáte díky špatné češtině, jako je skloňování slov atd.
- Aktualizovaný internetový prohlížeč a e-mailový klient informují uživatele, že se jedná o phishing.
- V neposlední řadě mějte za každých okolností aktualizovaný operační systém, firewall a aktualizovaný antivirus.

- obezřetní při otevírání souborů zaslaných od někoho, koho neznáte, nebo jste od něj žádný soubor nečekali.
- Škodlivá příloha ale může přijít i od důvěryhodného zdroje, jehož e-mailový účet napadli hackeři a byl zneužit k šíření malware.
- Proto je třeba dávat opravdu velký pozor na typy souborů, které zpráva obsahuje.
- Některé mohou svými názvy nebo ikonami vzbuzovat dojem, že se jedná o legitimní dokument nebo mediální soubor.
- Jde třeba o ikony Word, PDF, MP3 nebo JPEG. Samotný název dokumentu má ale odlišnou příponu. Název wordovského dokumentu například nekončí „.doc“ nebo „.docx“, ale jinými písmeny, které nekorespondují s ikonou Wordu.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Digitální stopa je informace zanechaná uživatelem v prostředí internetu

- Informace, které po sobě uživatelé internetu zanechávají, se dělí na **aktivní** a **pasivní**.

Aktivní - veškeré informace, které o sobě uživatel **dobrovolně a vědomně** zveřejní prostřednictvím různých služeb. Například se jedná o:

- profily a následné příspěvky zanechané na sociálních sítích
- emaily, sms, historie chatu…
- různé úřední údaje

Pasivní - jedná se o soubor informací, který bez našeho přímého záměru vznikající při interakci v prostředí internetu:

- IP adresa
- vyhledávané výrazy na internetu
- údaje o času stráveném na určité webové stránce (cookies)
- poskytovatel připojení, lokace

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Možnosti zneužití digitální stopy

- krádež osobních informací (údaje z kreditních karet, rodné číslo, e-mailová adresa)
- Kyberšikana jedná se o specifický druh šikany, který k útokům využívá informační komunikační technologie.
- Kyberstalking zneužívání informačních a komunikačních technologií ke stallkingu.
- Zdroj informací pro personalisty - z volně dostupných informací na sociálních sítích mohou zaměstnavatelé získat velké množství informacích o stávajících i o budoucích zaměstnancích.
- Sledování návyků uživatelů - ve většině případů je realizováno navštívenou webovou stránkou, nebo tzv. třetími stranami reprezentovanými sběrateli dat a reklamními společnostmi.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Odstranění digitálních stop

- **Smazání digitálních stop v dnešní době je prakticky nemožné.**
- Závisí proto na samotném uživateli, jak své *aktivní stopy* bude kontrolovat. Následky aktivních digitálních stop se dají minimalizovat například tím, že budeme používat více přihlašovacích jmen a e-mailových adres.
- *Pasivní stopy* mají určitou dobu platnosti uchování dat. Uživatelé mohou jen zabránit dodatečnému sběru dat, například pomocí softwarových řešení nebo správou cookies. Poté zbývá jen vyčkat, než uplyne stanovená doba uložení a již získaná data budou smazána.
- Ovšem na rozdíl od aktivní digitální stopy nemáme nad vznikem a následnou správou pasivní stopy prakticky žádnou kontrolu.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Rizika sociálních sítí

- **Uvědomte si, že to, co na internetu zveřejníte, už většinou nemůžete vzít zpět. Pečlivě si proto rozmyslete, co o sobě chcete sdělovat.**
- Denně je prostřednictvím sociálních sítí ukradeno několik desítek identit. Mnohdy to uživatelé ani netuší. Pokud to zjistí, jen málokdo ví, jak se může bránit.
- Nejčastěji jsou vystaveny rizikům na internetu děti. Informace o školácích denně vyhledává několik set slídilů a mohou cíleně sbírat osobní údaje, fotografie nebo intimní materiály.

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Jak se bránit v případě zneužití údajů

- Kontaktujte technickou podporu služby s žádostí o smazání údajů.
- V závažných případech neváhejte kontaktovat policii.

Mýtus: Internet je anonymní.

Skutečnost: *Nikdo není na internetu anonymní. Většina provozovatelů udržuje logy k jednotlivým uživatelským účtům a ty pak na základě žádostí předává policii. Informace získané z připojení, mohou významně přispět k dopadení pachatele.*

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Pokud se vám stane na internetu nějaké příkoří nebo se stanete svědky nějaké nestandardní situace, nenechte si ji pro sebe

- Neuvádějte na veřejném profilu telefonní číslo nebo adresu.
- Neposílejte nikomu svoji intimní fotografii, nikdy nevíte, kde se může objevit.
- Udržujte hesla (k e-mailu i jiná) v tajnosti, nesdělujte je ani osobě blízké či kolegovi v práci.
- Nikdy neodpovídejte na neslušné, hrubé nebo vulgární maily a vzkazy.
- Nedomlouvejte si schůzku přes internet, aniž byste o tom neřekli někomu jinému
- Nevěřte každé informaci, kterou na internetu získáte
- Když s někým nechcete komunikovat, nekomunikujte
- Nesdělujte informace typu, kdy jedete na dovolenou, po návratu by vás mohlo čekat překvapení
- Při používání webové kamery buďte obezřetní, kdokoli může na druhé straně hovor nahrávat
- Než cokoli potvrdíte, přečtěte si podmínky užívání

Děkuji za pozornost