ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ČESKÝ INSTITUT INFORMATIKY ROBOTIKY A KYBERNETIKY

ZÁKLADY KYBERNETICKÉ BEZPEČNOSTI (CZ)

Lze školit online? ANO

- *Cíle:* Seznámení s podstatou kybernetické bezpečnosti a souvisejících bezpečnostních opatření včetně využití efektivních přístupů k jejich využití. Školení je koncipováno jako úvod pro vstup a práci v prostředí ICT, zajištění bezpečnosti informací, slouží k pochopení řízení informační bezpečnosti a vysvětlení jednotlivých technických nástrojů.

Přínosy školení:

- Základní orientace v ICT prostředí (porozumění pojmům LAN, PC, notebook, tablet, mobil, tiskárna …).
- Primárně zvládnutí úlohy prevence v chování při práci v kyberprostoru
- Bezpečné zvládnutí těchto činností, v případě vzniku bezpečnostního incidentu jeho detekce a omezení dopadu na provoz systému s následným vyhodnocením

Zaměření školení:

- Kurz je vhodný pro širokou veřejnost se zájmem o moderní trendy v bezpečnosti informací a kohokoli kdo se v bezpečnosti informací neorientuje a měl by zájem o získání obecného přehledu

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ČESKÝ INSTITUT INFORMATIKY ROBOTIKY A KYBERNETIKY

Obsah školení:

- Co je to Kybernetická bezpečnost
- Hlavní bezpečnostní funkce
- Phishing
- Ransomware
- Malware
- Socialní inženýrství
- Ransomware
- Osobní data na Internetu
- Použití platebních karet
- Protokol http versus https a certifikáty
- 3D bezpečnost
- Hesla
- Práce na cizím PC
- PC, tablet a mobilní telefon (Smartphone)
- Použití veřejné sítě Wi-Fi
- VPN a vzdálené připojování (RDP)
- Zálohování a obnova dat
- Cloud
- Infrastructura jako služba (IaaS)
- Platforma jako služba (PaaS)
- Software jako služba (SaaS)

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ČESKÝ INSTITUT INFORMATIKY ROBOTIKY A KYBERNETIKY

Počet dní: 1 den s lektorem

Požadavky na předchozí znalosti: kurz je navržen tak, aby nevyžadoval žádní pokročilé IT znalosti a najdete v něm konkrétní scénáře, které vás seznámí se základními pravidly pohybu v ICT (kybernetickém) prostředí a upozorní na chyby, kterých je třeba se vyvarovat

Obsah LABů: Bez laboratorních cvičení

Technické vybavení: Bez nároků na laboratorní vybavení

Literatura: Všichni účastníci obdrží elektronickou verzi studijních materiálů.

Cena za účastníka: *4.890,- Kč (bez DPH 21%)*

Min. počet účastníků: *10*

Max. počet účastníků: *30*

Další skupiny po dohodě s pořádajícím

Obtížnost: základní

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ČESKÝ INSTITUT INFORMATIKY ROBOTIKY A KYBERNETIKY

Osobní údaje na internetu

Agenda

- Osobní údaje a jejich zneužití na internetu
- Podvodné e-maily – phishing - rybaření
- Hesla jejich tvorba a používání (silná hesla, stejné heslo k více službám)
- Surfujte bezpečně (http, https)
- Stahování programů a instalace doplňků (Malware)
- Bezpečný prohlížeč
- Zásady používání cizího počítače pro připojení k Internetu
- Zabezpečení chytrého telefonu
- Zabezpečení počítače & notebooku – antivirus, fw
- Zálohování a obnova
- Cloud

Dávejte velký pozor komu a údaje sdělujete

Pokud s někým uzavíráte smlouvu (například e-shop) má právo na vaše údaje

- **Souhlas se zpracováním údajů musíte dnes dát (zakliknout)**
- **Tento souhlas můžete později odvolat**
- **Co nesdělovat a na co si dát pozor:**
  - **kopie občanského průkazu, pasu – velký pozor (možnost zneužití například úvěr)**
- **Platební karta – nikdy neposílat fotku karty – velká možnost zneužití**

Platby na internetu

- Prostředník – PayPal, GoPay, Moneybookers/Skrill
- Převodem – bankou viz bankovnictví
- Platby na Internetu lze zakázat v bance (prevence) - e-commerce transakce
- Limit na kartě pro platby na internetu
- Lze mít speciální kartu jen na platy po internetu (limit/povolení)
- Virtuální na platební karta na Internetu
- Předplacená karta
- 3D Secure – bezpečný způsob placení kartou
- Premium SMS
- Virtuální měna – Bitcoin, …

Platba kartou - 3D Secure

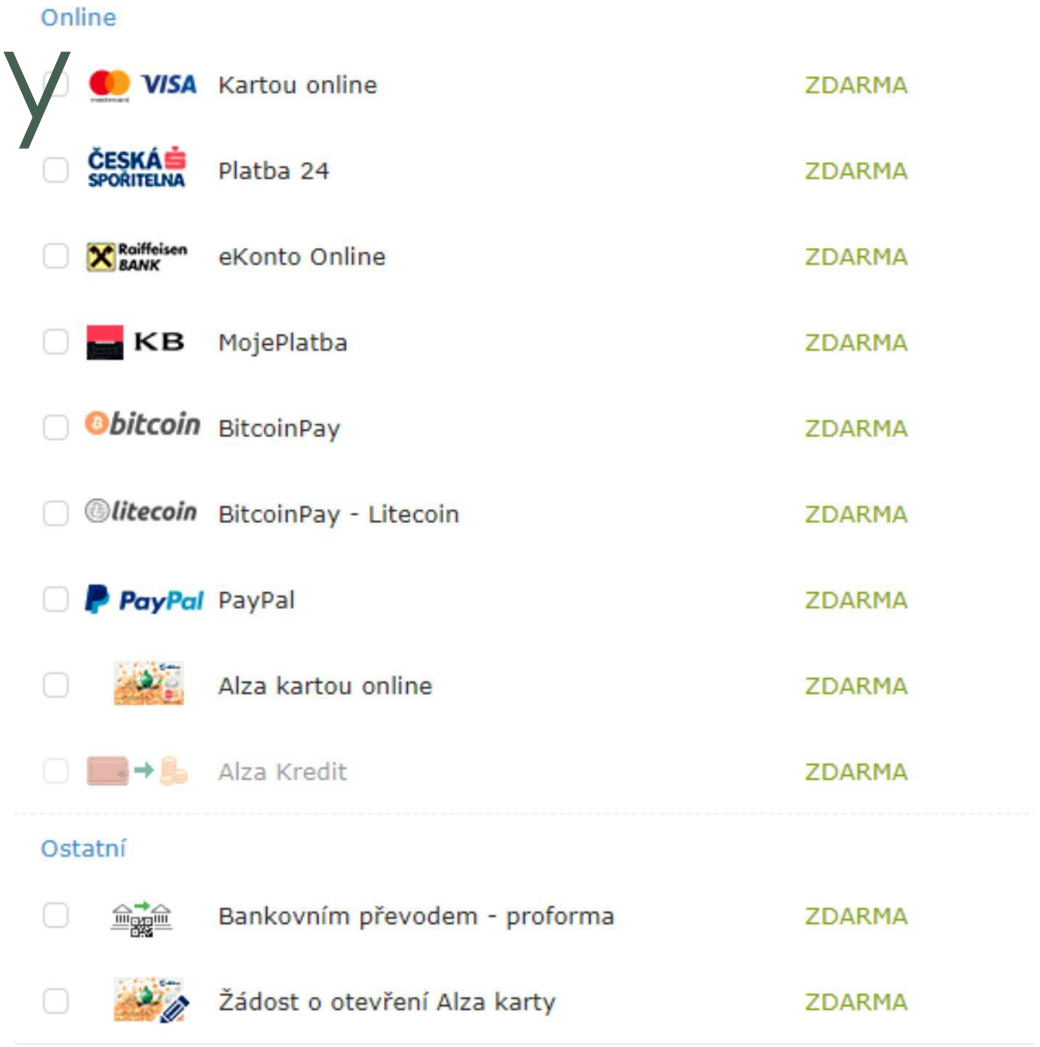
- **3D Secure technologie – dva neávislé kanály**
- **Posílá se jednorázový kód jiným kanálem – SMS**

Blokace karty – 3D Secure kód

- Zadáte-li špatně 3D Secure kód, je možné zadání opakovat, maximálně však 3x. Poté dojde k blokaci karty pro další 3D Secure transakce. Na ostatní platby kartou (nákupy v kamenných obchodech, výběry z bankomatu, nákupy na internetu, u obchodníků nepodporujících 3D Secure zabezpečení) nemá tato blokace vliv a kartu je možné běžně použít.

- Používejte 3D Secure kód (nechte si ho nastavit ve vaší bance) a obloukem se vyhněte tomu e-shopu co ho nemá.

Alza – příklad
Online platby

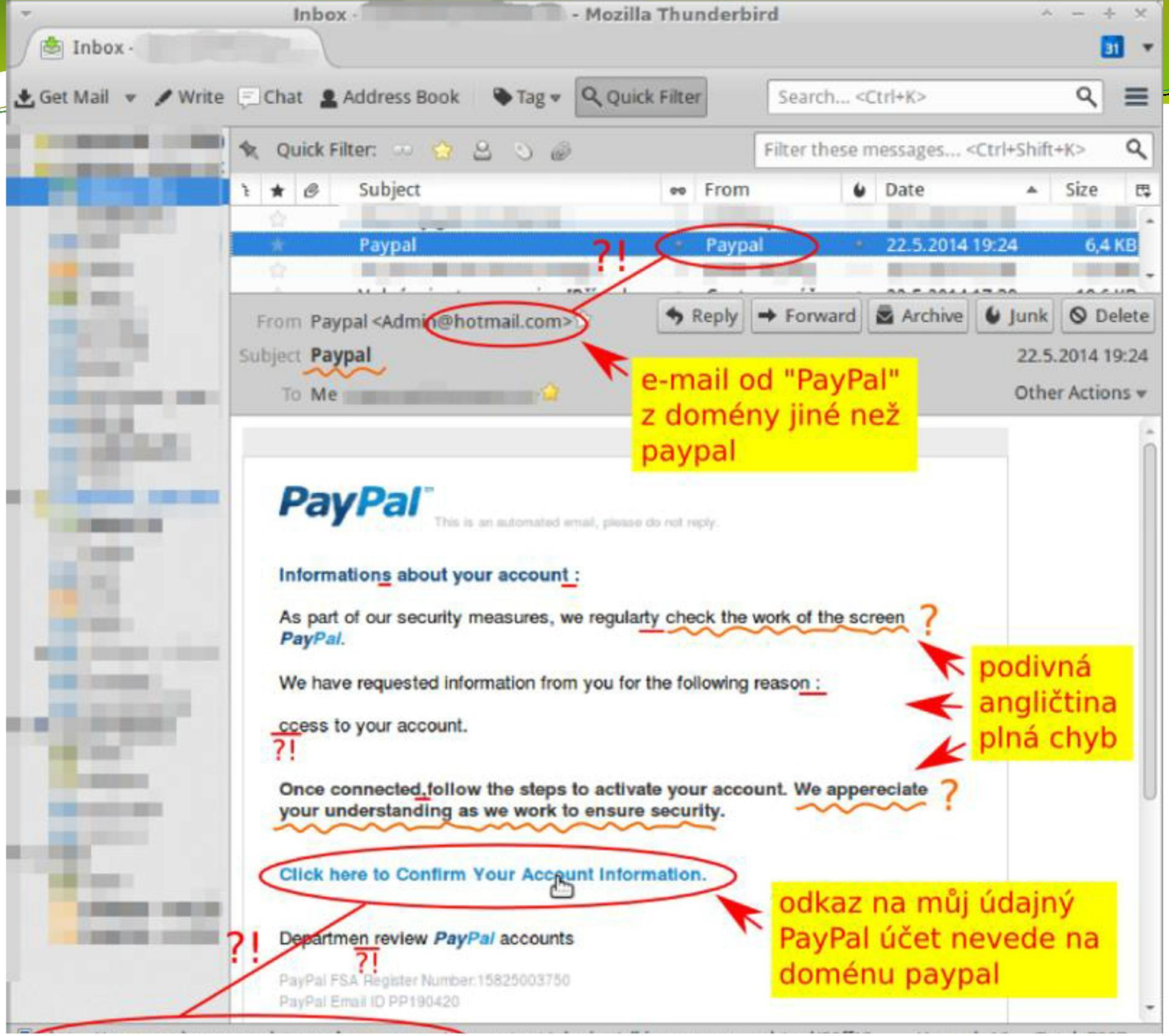


Jak poznám důvěryhodného obchodníka?

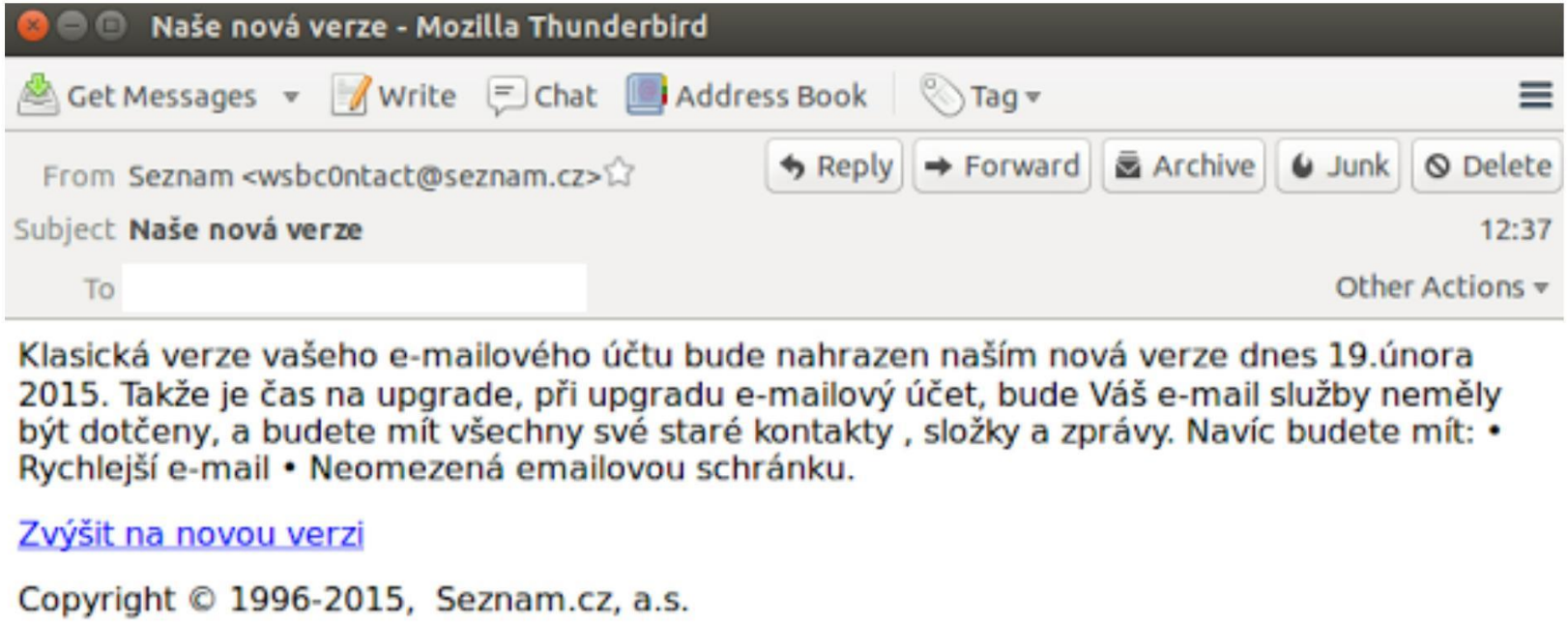
- Obchodník svůj e-shop provozuje na stránkách, které mají zabezpečený přenos dat (tzv. SSL protokol). To, že obchodník tento protokol na svých stránkách používá, poznáte podle toho, že v adresním řádku prohlížeče se zobrazuje **https://** a také ikonka visacího zámku.
- Nicméně stále je třeba BÝT OBEZŘETNÝ a dbát ZVÝŠENÉ OPATRNOSTI při výběru obchodníka a nakupovat pouze tam, kde nakupuje buď velké množství zákazníků nebo máte vlastní pozitivní zkušenost.

Phishing

- Phishing (rhybaření) je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.).
- Phishing je příkladem techniky sociálního inženýrství používané k oklamání uživatelů za využití slabých míst současných bezpečnostních technologií (jejich implementací).
- Principem phishingu je typicky rozesílání e-mailových zpráv nebo instant messaging, které často vyzývají adresáta k zadání osobních údajů na falešnou stránku, jejíž podoba je takřka identická s tou oficiální. Stránka může například napodobovat přihlašovací okno internetového bankovnictví.


Inbox - Mozilla Thunderbird
Get Mail
Write
Chat
Address Book
Tag
Quick Filter
Search... <Ctrl+K>
Filter these messages... <Ctrl+Shift+K>
Subject
From
Date
Size
Paypal
Paypal
22.5.2014 19:24
6,4 KB
?!
From Paypal <Admin@hotmail.com>
Reply
Forward
Archive
Junk
Delete
Subject Paypal
22.5.2014 19:24
To Me
Other Actions
e-mail od "PayPal" z domény jiné než paypal
PayPal
This is an automated email, please do not reply.
Informations about your account :
As part of our security measures, we regularty check the work of the screen ?
PayPal.
We have requested information from you for the following reason :
ccess to your account.
?!
podivná angličtina plná chyb
Once connected,follow the steps to activate your account. We appereciate ?
your understanding as we work to ensure security.
Click here to Confirm Your Account Information.
odkaz na můj údajný PayPal účet nevede na doménu paypal
?!
Departmen review PayPal accounts
?!
PayPal FSA Register Number:15825003750
PayPal Email ID PP190420

Phishing - seznam



Phising – reálný příklad

Vážení: Webmail, majiteľ e-mailového účtu

webmail <ryanwisty@gmail.com>

Vážení: Webmail, majiteľ e-mailového účtu

Týmto oznamujeme, že váš e-mailový účet prekročil limit úložiska. Nebudete môcť odosielať a prijímať e-maily a Váš e-mailový účet bude z nášho servera vymazaný. Ak sa chcete vyhnúť tomuto problému, odporúčame vám

Overte svoj e-mailový účet kliknutím na nižšie uvedený odkaz.

Overte svoj e-mailový účet. **(odkaz směřoval na : http://wbbs.000webhostapp.com/)**

Nedodržanie bude mať za následok trvalé ukončenie vášho e-mailového konta Ďakujeme.

Webmail, manažérsky tím.

Reálný Phishing – na firemní mail

From: Jana Nováková <budyi@post.cz>
Sent: Tuesday, January 8, 2019 8:52 AM
To: ucetni@realna-firma.cz
Subject: Platba

39750 EUR... můžeme zaplatit dnes?

Jana Nováková.

Odesláno z mého iPhone

Hesla

- Používejte silná hesla
- Nejhorší hesla: 123456, password, heslo, qwertz, jméno, příjmení
- Použijte malá velká písmena, zkomoleninu, zdrobnělinu, čísla
- Na silná hesla používejte divné znaky +, @, #, $, % ,^, &
- Nepoužívejte všude stejná hesla – mějte kategorie sociální sítě, email, banka, počítač v zaměstnání atd…
- Na banku například ani silné heslo nestačí použijte dvoufázové ověření
- Token, mobilní telefon, certifikát, otisk prstu, otisk oční duhovky

ČESKÝ INSTITUT INFORMATIKY
ROBOTIKY A KYBERNETIKY

Surfujte bezpečně

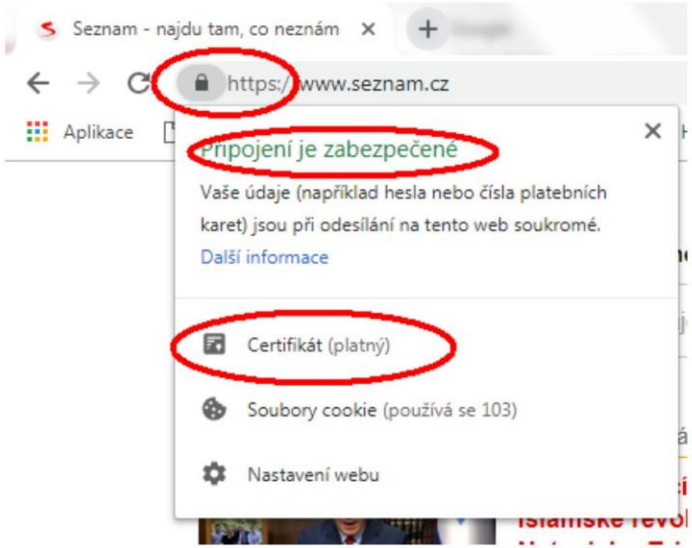
Stejně jako byste v reálném životě nedali přednost procházce nebezpečnou čtvrtí, vyhýbejte se pečlivě i na internetu podezřelému a potenciálně nebezpečnému obsahu. Nenechte se nalákat možností výhry nejnovějšího smartphonu ani údajnými fotografiemi nahých celebrit.

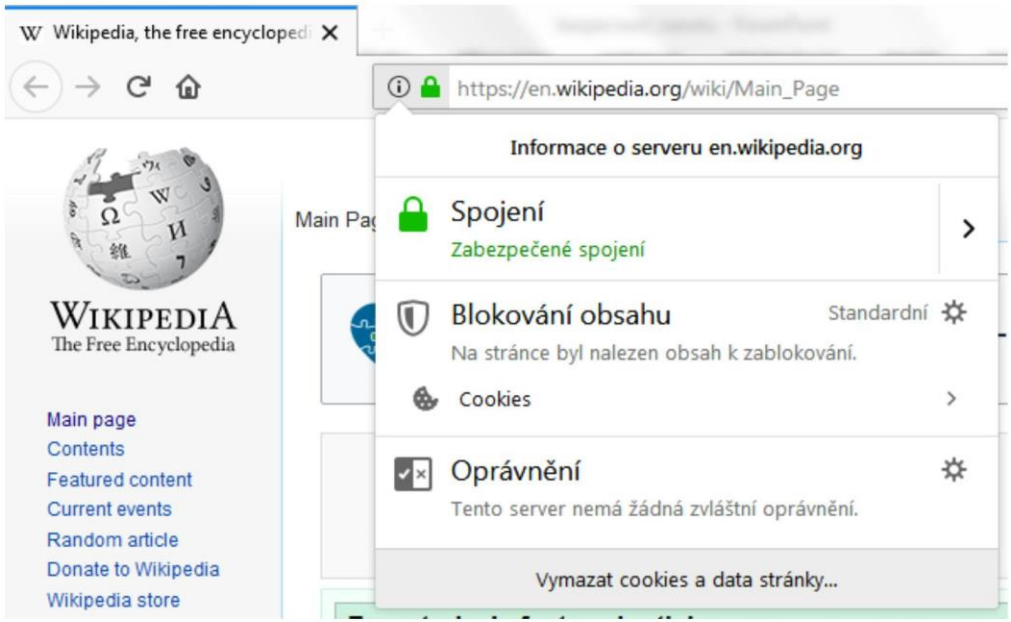
ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ČESKÝ INSTITUT INFORMATIKY ROBOTIKY A KYBERNETIKY

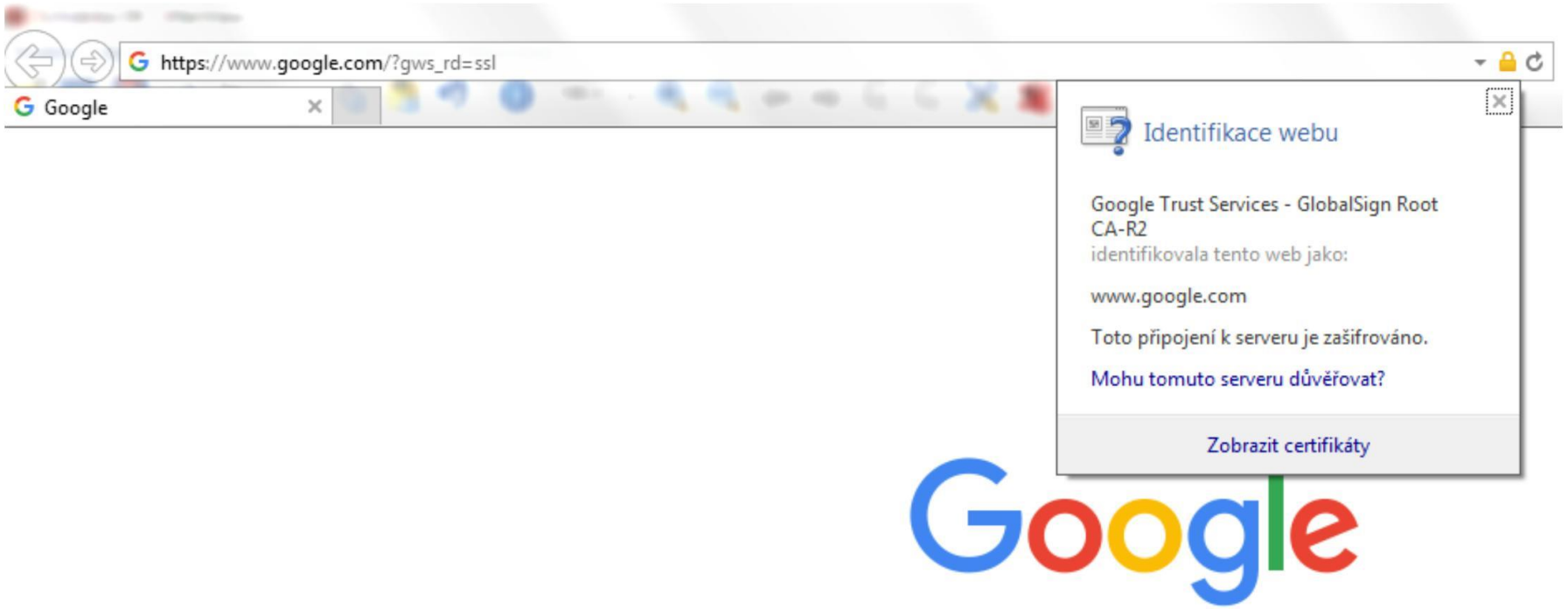
http v https

Banky, web mail, e-shop jedině s **https** a důvěryhodný certifikát



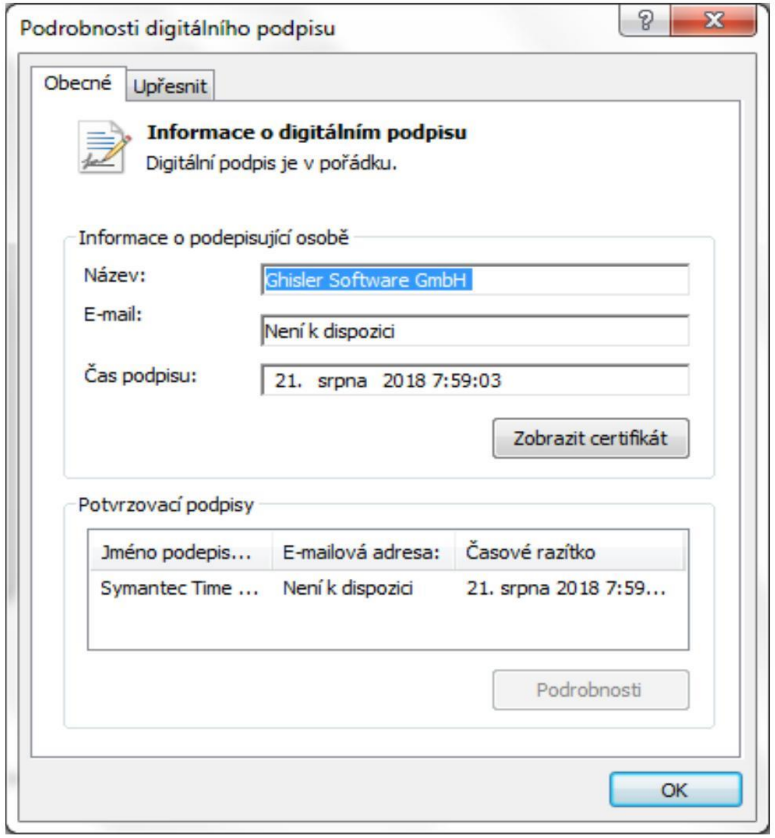


http v https


https://www.google.com/?gws_rd=ssl
Google
Identifikace webu
Google Trust Services - GlobalSign Root CA-R2
identifikovala tento web jako:
www.google.com
Toto připojení k serveru je zašifrováno.
Mohu tomuto serveru důvěřovat?
Zobrazit certifikáty
Google

Stahování programů

- Stahujte z důvěry hodných zdrojů!!!!
- Nestahujte nelegální SW!!!
- Velké firmy OK:
  - Dell
  - HP
  - Microsoft
  - Google
  - Lenovo
  - Velcí výrobci HW, SW … OK



Stahování SW, her - Malware

Stahování neověřeného obsahu je nejjednodušší cestou, jak svůj počítač infikovat malwarem.

V lepším případě zaznamenáte „pouze“ zpomalení a zhoršené fungování, v horším případě budou vaše data ukradena a zneužita. Malware může mít podobu populární hry i užitečné aplikace.

Software vždy stahujte z ověřených stránek výrobce, pro stahování her využívejte důvěryhodné platformy, jako je například Steam. Snaha ušetřit se vám nemusí vyplatit.

Malware (složení anglických slov malicious software, škodlivý software, zákeřný software) je program určený k poškození nebo vniknutí do počítačového systému.

Ransomware

- Ransomware (jiné názvy: vyděračský software, vyděračský program; angl. ransomware - složení anglických slov ransom "výkupné" software "software")
- Program vám postupně zašifruje disk – ale i síťové disky jsou-li dostupné a požaduje pak zaplatit výkupné za zaslání hesla…
- **Android ransomware** i na telefonech a tabletech Android
  - ransomware přes zamykací obrazovku
  - zamykací obrazovka s PIN
  - krypto ransomware

Internetový - Webový prohlížeč

Používejte moderní, bezpečné a aktualizované prohlížeče!!! (Windows)

MS říká že IE není Internetový prohlížeč ale „řešení pro kompabilitu “

chrome

Mozilla Firefox
Webový prohlížeč

Opera

Internet Explorer
Webový prohlížeč

Použití cizího PC

- Po ukončení práce se odhlaste!!! (webmail, Facebook, firemní stránky, e-shop, banka, intranet, …)
- Pokud nechcete by se vědělo co jste dělal/a smažte historii.
- Pokud jste paranoidní použijte anonymní mód.
- Zavřete všechna okna prohlížeče a tím i celý prohlížeč.
- Smažte po sobě stažené soubory (i z koše).
- Můžete udělat restart počítače po ukončení všeho.

Chytrý telefon

- Aktualizujte!!!
- Zálohujte!!! (kontakty, fotky, dokumenty) – Cloud, PC, karta, …
- Používejte poslední dostupné verze OS a všech aplikací (ano stojí to nějaký čas ale vyplatí se to!).
- Instalujte aplikace z důvěryhodných zdrojů:
  - Android – Google Play
  - Apple – App Store
  - Nestahujte aplikace jinak!!!

PC, notebook

- Zálohujte!!! (jiné médium – externí disk, flash, cloud, cokoliv)
- Zálohujte, zálohujte, zálohujte!!! Geograficky oddělená záloha je vho
- Používejte legální a aktuální OS a SW (zejména prohlížeč, Javu, Flah, prohlížeč PDF, MS Office)
- Používejte Antivirový program (jeden!!!):
  - ESET NOD32
  - AVG
  - Kaspersky
  - McAfee Antivirus
  - Microsoft Defender

Starý Antivir = žádný Antivir

Další bezpečnostní tipy

Používejte Firewall – součástí OS nebo součástí antivirového prog

Šifrovaný disk – v případě ztráty NTB se nikdo nedostane k datů

Používejte biometrické snímače

K vzdálenému připojení používejte bezpečná – šifrovaný kanál, V tokeny, wihelisty, …

Citlivé věci posílejte mailem šifrovaně nebo jiným kanálem (SCP,

Neposílejte mailem hesla, bezpečnostní certifikáty atd …

Citlivá data šifrujte – PGP (Pretty Good Privacy)

Chovejete se obezřetně!!!!

Zálohování - zálohujte

- Zálohujte, zálohujte a zálohujte!!!!
- Zálohujte a zálohujte pravidelně nejlépe automatizovaně.
- Zálohu mějte 3 x
  1. rychlou klidně na stejném disku (kvůli vašemu nechtěnému smazání přepsání, poškození souboru…)
  2. Na jiném meédiu ale ve stejné budově – kanceláři
  3. Někde jinde – geograficky oddělená záloha (požár, živelná katastrofa, krádež – médium muže být v trezoru jiné serverovně atd… tato záloha by neměla být on-line a ne tak snadno přístupná (ransonware).
- Použijete cloud a zálohujte do cloudu

Obnova, disaster recovery

- Testujte obnovitelnost záloh!!! Není nic horšího když si myslíte že máte zálohu a ona přitom nefunguje nebo neobsahuje to co chcete …
- Udělejte si plán co je pro vás nebytné co je důležité co můžete nějaký čas oželet – stanovte si priority pro chod vašeho podniku, firmy, školy…
- Prověřujte čas od času postupy kontrolujte zálohu zkuste ze zálohy obnovit (dá se to dělat automaticky.
- V případě disaster recovery je plán naprosto nutný!!!

Cloud

- Privátní – váš cloud - ve vaší správě (a nebo víte kde je kdo se o něj stará a kde přesně jsou uložena vaše data…)
- Veřejný cloud – public cloud – Google, Amazanon
- Hybrdní cloud – kombinace obojího

Distribuční model

- IaaS – infrastruktura jako služba (Infrastructure as a Service) – poskytovatel služeb se zavazuje poskytnout infrastrukturu. Typicky se jedná o virtualizaci. O veškeré problémy s hardwarem se stará poskytovatel. IaaS je vhodné pro ty, kteří vlastní software (či jejich licence) a nechtějí se starat o hardware
- PaaS – platforma jako služba (Platform as a Service) – poskytovatel garantuje kompletní prostředky pro podporu celého životního cyklu tvorby a poskytování webových aplikací a služeb; to plně na internetu, bez možnosti stažení softwaru. Koncepce zahrnuje různé prostředky pro vývoj aplikací, jako jsou IDE nebo API, ale rovněž např. pro údržbu.
- SaaS – software jako služba (Software as a Service) – aplikace je licencována jako služba pronajímaná uživateli. Uživatelé si tedy kupují přístup k aplikaci, ne aplikaci samotnou. SaaS je ideální pro ty, kteří potřebují jen běžný aplikační software a požadují přístup odkudkoliv a kdykoliv.

Nevýhody cloudu

- Závislost na internetovém připojení
- Závislost na poskytovateli cloudu
- Migrační náklady
- Odezvy a dostupnost služby jsou závislé na kvalitě internetového připojení - latence.
- Odlišný právní řád poskytovatele a klienta – poskytovatel cloud computingu může být podřízen jiné jurisdikci než jeho klient. (data v jiné zemi – co právník to názor …)