

Pavel Dvořák

Gymnázium Velké Meziříčí

**Bezpečnost služby WWW a E-mail**

Registrační číslo projektu: CZ.1.07/1.5.00/34.0948

Datum: 18. 1. 2014

Jazyk: čeština

Cílová skupina: studenti vyššího gymnázia, 15–16 let

Druh učebního materiálu: výklad + testové otázky

Očekávaný výstup: Student se seznámí s protokolem https, podvodnými webovými stránkami a dalšími možnými riziky a pravidly etikety spojenými nejen se službou www. Dále se student se seznámí s elektronickým podpisem a podvodnými e‑maily.

Anotace: výklad + testové otázky

# Bezpečnost služby www

* všechna data posílaná e-mailem či přes www rozhraní jsou standardně nešifrovaná – kdokoliv může data odposlechnout a dále s nimi manipulovat.
* je nutné zvážit
	+ zda zprávy (komunikaci) **šifrovat** – např. posílaný e-mail s databázi žáků školy s jejich rodnými čísly by bylo vhodné nějakým způsobem zabezpečit
	+ nebo nic **nešifrovat** – např. poslat e-mail kamarádovi o tom, jak jsme minulý víkend „zapařili“ asi nemá cenu kódovat …

## Protokol https (na portu 443)

* jeden ze zabezpečených protokolů pro přístup k citlivým datům
* jakmile použijeme tento protokol, musíme přijmout (popř. si nainstalovat) certifikát a pak budeme automaticky pracovat v „zabezpečené zóně“, kde každá informace ze serveru do našeho prohlížeče a naopak bude zašifrovaná
* při vstupu do „zabezpečené zóny“ jsme upozorněni (hláškou, změnou ikony v prohlížeči),
* certifikát můžeme přijmout, nainstalovat, popř. si prohlédnout další informace (kdo jej vystavil, jak dlouho platí atd.)
* instalace certifikátů – uložiště certifikátů v operačním systému Windows XP (Internet Explorer – Nástroje – Možnosti Internetu – Obsah – Certifikáty)
* certifikáty lze taktéž ukládat na USB klíčenku a další paměťová média

# Podvodné techniky

## Phishing

Phishing (někdy převáděno do češtiny jako rhybaření) je podvodná technika používaná na Internetu **k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci**.

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. Uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze.

## Pharming

Pharming (někdy překládáno do češtiny jako farmaření) je podvodná technika používaná na Internetu k získávání citlivých údajů od obětí útoku. Principem je **napadení DNS a přepsání IP adresy, což způsobí přesměrování klienta na falešné stránky** internetbankingu po napsání URL banky do prohlížeče. Tyto stránky jsou obvykle k nerozeznání od skutečných stránek banky. Ani zkušení uživatelé nemusejí poznat rozdíl (na rozdíl od příbuzné techniky phishingu).

## Podvodné loterie

Podvodné loterie jsou druhem podvodu, kdy jsou lidem rozeslány e-maily s **oznámením o výhře vysoké částky** v eurech, dolarech nebo v jiné zajímavě měně. V případě, že oslovený výherce kontaktuje provozovatele loterie, je mu sděleno, že výhra bude vyplacena, jakmile zaplatí manipulační poplatek ve výši v přepočtu až několika desítek tisíc korun, který samozřejmě není možné odečíst ze slíbené výhry. V případě, že uživatel poplatek zaplatí, je po něm obvykle požadován další, dokud je ochoten platit. Zaplacené peníze a slíbenou výhru už nikdy neuvidí.

## SCAM 419 (Nigerijské dopisy)

Scam 419 je označení pro druh podvodu u nás známého spíše jako Nigerijské dopisy. Tyto podvody nejsou žádnou novinkou, existovaly již dříve buď ve formě dopisu nebo jako faxy. Rozvojem e‑mailové komunikace se podvody masově rozšířily, ale princip zůstává stejný. **Osloví vás neznámý člověk, že zdědil, získal nebo dokonce spravuje něčí majetek ve výši několika desítek miliónů dolarů a potřebuje pomoc při jeho převodu ze země.** Za to je slíbená tučná odměna ve výši několika desítek procent z celkové částky. Princip podvodu spočívá v tom, že oběť musí neustále platit nečekané administrativní poplatky a převod majetku se stále oddaluje.

## Malware

MALWARE je všeobecné označení pro škodlivý kód. Nejčastěji to může být počítačový vir, červ nebo stále častěji Trojský kůň. Dříve se podobná havěť šířila přímo e-mailem, ale v dnešní době se stále více využívá sociální inženýrství, kdy v textu e-mailu nebo webové stránky je pouze odkaz na tento škodlivý kód pod záminkou, že odkaz směřuje na zajímavý obrázek, video nebo e-pohlednici. Pokud neopatrný uživatel na odkaz klikne, stáhne si namísto slibovaných obrázků škodlivý kód.

Obranou je kromě dobrého antispamového filtru, kvalitního antivirového programu a včas aktualizovaného systému hlavně rozum. Tvůrci malware jsou vždy o krok před výrobci antivirů, kteří reagují na nové hrozby.

## Hoax

**Hoax** (anglické slovo hoax označuje **podvod, mystifikaci či žert**) je nevyžádaná e-mailová zpráva, která uživatele varuje před nějakým virem, prosí o pomoc, informuje o nebezpečí, snaží se ho pobavit apod. Hoax většinou obsahuje i výzvu žádající další rozeslání hoaxu mezi přátele, příp. na co největší množství dalších adres, proto se někdy označuje také jako **řetězový** e-mail.

### Škodlivost hoaxů:

* Obtěžování příjemců
* Nebezpečné rady např. jak se zbavit domnělého viru smazáním nějakého souboru.
* Zbytečné zatěžování linek a serverů
* Ztráta důvěryhodnosti – může utrpět i pověst příslušné firmy či úřadu.
* Prozrazení důvěrných informací – e-mailové adresy přátel, spolupracovníků, v některých případech dokonce hoax žádá o vyplnění dalších údajů jako adresy či rodného čísla a odeslání takové zprávy na jakousi adresu.

## E-mailoví červi

E-mailové červy a viry používají elektronickou poštu k tomu, aby se mohly šířit do ostatních zranitelných počítačů. Poté, co infikují nový počítač, se začnou rozesílat na e-mailové adresy, které získají buď z e-mailového adresáře oběti počítače, nebo prohledáváním obsahu uložených souborů a extrahováním řetězců, které vyhovují tvaru e-mailové adresy. Zvláštním případem jsou sítě **botnet**, složené z počítačů infikovaných k tomu uzpůsobeným červem, kdy infikované počítače na příkaz autora infekce zasílají hromadně SPAM (nevyžádanou poštu), nebo uskutečňují útoky typu **DDoS** (technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele) na jiné počítače.



Licence Creative Commons, BY, [cit. 2014/01/18],: Tom-b, [http://cs.wikipedia.org/wiki/Soubor:Botnet.svg](http://cs.wikipedia.org/wiki/Soubor%3ABotnet.svg)

## Elektronický podpis

**Elektronický podpis** jsou **elektronické identifikační údaje autora** (odesílatele) elektronického dokumentu, připojené k němu.

Za elektronický podpis se v širším významu považuje i prosté nešifrované uvedení identifikačních údajů (například jména a adresy, názvu a sídla, rodného nebo jiného identifikačního čísla atd.) na konci textu v elektronické (digitální) podobě, které zaručuje identifikaci (tedy jednoznačné určení) označené osoby, avšak nikoliv integritu podepsaného dokumentu ani autentizaci podepsaného.

**Zaručený elektronický podpis** je elektronický podpis v takové formě, která, zpravidla kryptografickými metodami (šifrováním), zaručuje i integritu dokumentu a autentizaci podepsaného. Pro některé účely je navíc vyžadován zaručený elektronický podpis pouze s předepsanými typy certifikace, tedy „založený na kvalifikovaném certifikátu“. Zaručený elektronický podpis zajišťuje:

* **autentizaci (nepopiratelnost)** – lze prokázat, že autorem je skutečně ten, kdo je pod dokumentem podepsán, autor nemůže popřít, že dokument podepsal.
* **integritu dokumentu** – lze prokázat, že po podepsání nedošlo k žádné změně, soubor není poškozen (ani záměrně, ani omylem),
* někdy má i **funkci časového razítka**, tedy prokazuje datum a čas podepsání dokumentu

Rozdíl mezi **prostým** a **zaručeným** *elektronickým podpisem* je obdobný rozdílu mezi úředně neověřeným a ověřeným vlastnoručním podpisem, přičemž možnost, obtížnost a spolehlivost grafologického rozboru neověřeného vlastnoručního podpisu lze přirovnat k možnosti, obtížnosti a spolehlivosti ověření autenticity nezaručeného elektronického podpisu.

Jak získat elektronický podpis? Třeba u České pošty, s. p.

Bez osobních bezpečnostních opatření e-mail nezaručuje soukromí, protože

* e-mailové zprávy všeobecně nejsou šifrované
* e-mailové zprávy musí projít cizími počítači v síti předtím, než dosáhnou cílový počítač, což znamená, že je relativně jednoduché je cestou zachytit a přečíst si cizí zprávu
* většina poskytovatelů internetového připojení (Internet service provider) ukládá na své servery kopie vašich e-mailových zpráv předtím, než je doručí. Tyto zálohy můžou zůstat na serveru až několik měsíců, a to i v případě, že si je ve své schránce vymažete.

# RFC 1855 -  PRAVIDLA CHOVÁNÍ V SÍTI – NETIKETA

Dokument uvádí základní pravidla chování v síti "Network Etiquette - Netiquette", tedy jakousi etiketu sítě Internet, kterou organizace může používat a upravovat pro vlastní potřebu. Jako takový je uspořádán do oddílů tak, aby jeho adaptace byla co nejsnazší. Slouží také jako přehled základních pravidel pro jednotlivce, ať už se jedná o uživatele nebo administrátory. Autorem je "Responsible Use of the Network - RUN - Working Group" z [IETF](http://www.ietf.org/). Odkaz na dokument – [Netiketa](file:///%5C%5Cfile%5Cusers%5Czamestnanci%5Cdvorakpavel%5Cprace%5Cgrant_sablony_SS%5CDUMy-dvorak-GVM%5CPocitacove_site%5Cnetiketa.doc).

# Kontrolní otázky

* 1. Co je to phishing?
	2. Co je to pharming?
	3. Jaký protokol se používá pro zabezpečenou komunikaci mezi serverem a klientem? Popiš podrobněji.
	4. Popis fungování Nigerijských dopisů v elektronické komunikaci.
	5. Jak se vydělává na podvodných loteriích v elektronické komunikaci?
	6. Co je to malware? Jak jej nejčastěji „chytneme“?
	7. Co je to Netiketa?
	8. Co je to hoax?
	9. Co je to e-mailový červ?
	10. Jak funguje útok typu DDoS?
	11. Projdi webové stránky České pošty, s. p. a najdi informace k získání elektronického podpisu – podmínky, ceny, … Porovnej vše s dalšími poskytovateli této služby.