Číslo projektu	CZ.1.07/1.5.00/34.0394
Škola	SOŠ a SOU Hustopeče, Masarykovo nám. 1
Autor	Ing. Miriam Sedláčková
Číslo	VY_32_INOVACE_ICT.3.05
Název	Teorie internetu- e-mail
Téma hodiny	Teorie internetu
Předmět	Informační a komunikační technologie
Ročník/y/	3, 1
Anotace	Žák má k dispozici vlastní PC s Internetem. Učitel využívá projektor a PC s Internetem.
Datum vytvoření:	Vytvořeno 22. října 2012
Očekávaný výstup	Žák je schopen rozpoznat práci on a off line, zná způsoby práce v mailu, netiketu a zásady psaní e-mailů. Vypracováno 21. října 2012, navazuje VY_32_INOVACE_ICT.3.05 a VY_32_INOVACE_ICT.3.08 – pracovní list
Druh učebního materiálu	Prezentace

Jakou schránku můžeme mít?

- Pokud elektronickou schránku chceme, musíme si ji zřídit – na straně poskytovatele služby musí být funkční poštovní server, na straně naší si ale můžeme vybrat .
- buď budeme **přímo na serveru s klientským rozhraním** (email.seznam.cz, mail.atlas.cz, post.cz a další),
- nebo využijeme **služeb poštovního klienta**, který je nainstalován v našem počítači (např. Outlook Exchange).

Internetové rozhraní

Výhody:

- nemusíme se starat o konfiguraci připojení
- k poště máme přístup vždy, když se dostaneme k Internetu
- do počítače se nic neinstaluje „navíc“
- ke standardním službám patří i přesměrování pošty nebo upozornění formou SMS vždy, když nám přijde mail. Stejně tak bývá součástí i volný prostor pro webové stránky a další výhody.

Nevýhody:

- dokud pracujeme s poštou, musíme být on-line
- pokud máme více schránek, ztrácíme přehled – nelze zřídit k jedné schránce více účtů (přesněji lze, ale je to nedoporučený postup)

Poštovní klient

Výhody:

- můžeme pracovat off-line
- klient může být propojen s dalšími programy a pak lze posílat maily přímo z nich
- můžeme soustředit poštu z více schránek

Nevýhody:

- klienta je nutné nakonfigurovat
- na jiném počítači nemusí být klient vůbec nainstalován
- pošta není přenositelná – vidíte ji jen z toho počítače, kde je klient a je správně nastaven

Mailová adresa

- Skládá se ze jména adresáta a z názvu domény, na které je umístěna mailová schránka. Obě části adresy jsou od sebe odděleny symbolem @.
- Například chceme-li napsat panu Josefu Novákovi, zjistíme, že existují adresy:

pepa.novak@seznam.cz; pepanovak@seznam.cz; josefnovak@seznam.cz; josef.novak@seznam.cz, novakjosef@seznam.cz ; novak.josef@seznam.cz

Každá z uvedených adres ovšem patří úplně jinému člověku.

Malá a velká písmena

- V dnešní době by se dalo předpokládat, že všechny maily mají libovolný tvar písmenek – a je tedy jedno, jestli zadám malá nebo velká písmena.
- **Nemusí to tak být vždy** – některé servery to rozlišují, někdy (třeba ve firmě) je to i úmysl, aby nepsali cizí lidé.
- Pokud byste chtěli napsat mě na moji soukromou adresu, pak musíte dodržet velká počáteční písmena: Miriam.Sedlackova@seznam.cz
- Schránka miriam.sedlackova@seznam.cz totiž ještě před rokem existovala, ale nebyla nedostupná. Proč, to nedokázal nikdo říct – jde o starou chybu v systému. Pokud napíšete s malými písmeny, je vždycky sporné, kam mail opravdu dorazí…

Hlavička mailu

- **Komu** je jasné – adresát, který má zprávu obdržet.
- **Kopie** – také jasné: všichni, kdo mají obdržet tutéž zprávu. V obchodní korespondenci bychom řekli „rozdělovník“. Volíme ji v případě, že adresáti mají navzájem vědět, kdo všechno zprávu obdržel.

- **Skrytá** –Pokud umístíte adresy do řádku Kopie, tak všichni oslovení dostanou seznam všech adresátů. Nic jim nebrání, aby si jej okopírovali a příště jej použili místo vás. Adresy, umístěné v položce „Skrytá kopie“ jsou ovšem ostatním adresátům skryté - neviditelné

Předmět

- **Předmět** – měl by stručně vyjadřovat, o co se ve zprávě jedná. Je to ekvivalent kolonky „Věc“ v obchodním dopise. **Pokud jej nevyplníte, bude váš mail nejspíš označen za nedůvěryhodný a jako takový vymazán – většinou už antispamovým filtrem.** Stejně tak se s ním naloží v případě, že předmět bude nesmyslný – „Ahoj“ nebo „Nabídka Viagry“ určitě nevzbudí důvěru adresáta.
- Stejně tak působí zkratky v hlavičce předmětu. Obvykle se mail „ztratí“ cestou a adresáti se pak velice diví.

Tělo mailu

- **Prostý text**
- Nemá možnost text formátovat, to znamená, že celá zpráva bude psána jedním písmem.
- **Formát HTML** umožňuje upravit dopis, jako byste ho napsali např. v textovém editoru. Problémy, který s sebou tento formát nese, jsou dva: jednak není jistota, že se vámi pečlivě upravený text zobrazí příjemci v téže podobě, jakou vidíte vy, jednak se v takovém souboru může skrývat počítačový virus, přesněji prográmek, který jej spouští.
- Další problém, který je spojen s posíláním mailů, je **čeština**. Ta totiž používá speciální znaky – písmena s diakritikou. Pokud si nejsme jistí, zda příjemce, resp. jeho mailová schránka umí tyto znaky zobrazit, píšeme pro jistotu bez nich – tedy „cesky“. Podrobné informace si můžete najít na serveru http://www.cestina.cz

Přílohy a soubory

- Příloha je „přilepena“ sponkou ke zprávě a příjemce si ji může otevřít a uložit nebo s ní naložit jinak. Není rozumné posílat velké přílohy. Pošleme-li například obrázek o velikosti několika megabajtů, může se snadno stát, že se během své cesty změní nebo že adresát má omezenou schránku a příloha se do ní prostě nevejde nebo se dokonce nepodaří zprávu ani odeslat.
- V takovém případě můžeme využít služeb úschovny: http://www.uschovna.cz nebo jiného podobného serveru. Jsou to specializované servery, které umožňují uložit velké soubory na určitou dobu a příjemce si je odtud stáhne na svůj počítač. Mailem se pak posílá jen zpráva o souboru.

Základní bezpečnost

Většinu běžných uživatelů šokují především dvě zjištění:

- že **k obsahu jejich zpráv se může dostat každý, kdo má potřebné znalosti a možnosti** (například odposlechem síťové komunikace nebo přímým přístupem k souborům na poštovním serveru).
- Jedinou skutečně spolehlivou cestou jak ochránit data posílaná elektronickou poštou, je jejich *šifrování*.
- Optimální ochranu poskytují metody založené na *asymetrické kryptografii*, například *PGP klíče a X.509 certifikáty*.

Bezpečnost II.

- kdokoliv na světě může poslat e-mail, který bude mít jako odesilatelskou adresu uvedenu adresu vaši.
- To, že do položky *Odesilatel* může každý vložit cokoliv, se uživatel většinou dozví až v okamžiku, kdy jim od nich samých přijde nesmyslný e-mail, o kterém ví, že si jej určitě neposlali.
- Stejně jako v případě ochrany obsahu zprávy, i tento problém má řešení - tím je ***elektronický podpis***.
- Elektronický podpis je navíc řešením i při ochraně integrity zprávy. Umožňuje totiž zjistit, jestli zpráva nebyla cestou změněna.

Šifrování – několik pojmů

- Šifrovací algoritmus je funkce sestavená na matematickém základě a provádí samotné šifrování a dešifrování dat.
- Šifrovací klíč říká šifrovacímu algoritmu jak má data (de)šifrovat, podobá se počítačovým heslům, avšak neporovnává se zadaná hodnota s očekávanou, nýbrž se přímo používá a vždy tedy dostaneme nějaký výsledek, jehož správnost závisí právě na zadaném klíči.
- Délka klíče ovlivňuje, kromě jiného, časovou náročnost při útoku hrubou silou – což je kryptoanalytická metoda, kdy postupně zkoušíme všechny možné hodnoty, kterých klíč může nabývat

Symetrické a asymetrické šifrování

- **šifrování s privátním klíčem** (zvaném též symetrické či se symetrickým klíčem), kdy existuje jen jediný klíč pro zašifrování i odšifrování
- na **šifrování s veřejným klíčem** (zvaném též asymetrické či s asymetrickým klíčem) – jednu část klíče má odesilatel, druhou příjemce
- a ještě uvažujeme šifrování hybridní.

Elektronický podpis

Vychází z asymetrického šifrování. Zašifrujeme zprávu svým soukromým klíčem a připojíme šifrovanou zprávu k původní.

Pokud dokáže adresát zprávu dešifrovat, nemohl ji zašifrovat nikdo jiný, než vlastník soukromého klíče.

Protože je prakticky nemožné z jednoho klíče odvodit druhý párový klíč, není možné takovýto podpis zfalšovat.

Zároveň máme důkaz, že dokument nebyl nijak pozměněn, v opačném případě by totiž původní zpráva nebyla shodná s dešifrovanou.

Prémiové otázky

Určete, která mailová adresa je napsána správně:

- Lojza@dvorak.www
- Lojza @ dvorak. sk
- lojza.dvorak@seznam.cz
- cz.www@lojza.sk

Předmět e-mailu

- Musíme vždy vyplnit – jinak naši poštu může vyřadit protivirový filtr příjemce
- Nevyplňujeme, je to zbytečné
- Můžeme, ale nemusíme vyplnit – stejně ho nikdo nečte
- Nepíšeme - v hlavičce nic takového není

Zdroje

- http://cs.wikipedia.org/wiki/E-mail
- http://cs.wikipedia.org/wiki/E-mailov%C3%A1_adresa
- http://www.ics.muni.cz/bulletin/articles/353.html
- http://www.root.cz/clanky/sifrovani-uvod-do-problematiky/
- http://interval.cz/clanky/jak-funguje-digitalni-podpis/

- A vlastní archiv autorky