Služby Internetu - www, e-pošta

25. Ukážte možnosti vzdelávania sa cez Internet.

Internet ponúka nové spôsoby vzdelávania. Začnem webovým portálom ministerstva školstva **www.minedu.sk**, ktorý ponúka informácie pre učiteľov, žiakov a rodičov o aktualitách v oblasti školstva, predpisoch a základných pedagogických dokumentoch. Na stránkach **školských organizácií** (napr. www.iuventa.sk) nájdeme informácie o projektoch, súťažiach, školeniach, publikáciách atď. Okrem organizácií majú svoje weby rôzne **projekty zamerané na vzdelávanie** (napr. www.infovek.sk), ktoré obsahujú webové stránky s učebnými textami, aktivitami pre žiakov, metodickými odporúčaniami, diskusnými fórami, videami atď.

Knižnice (napr. zlatyfond.sme.sk) a ďalšie inštitúcie začínajú v súčasnosti digitalizovať niektoré diela klasikov a sprístupňovať ich verejnosti. Samozrejmosťou je elektronické publikovanie rôznych typov informačných zdrojov, napr. e-kníh, e-časopisov, encyklopédií, slovníkov atď.

Blogy (napr. www.birdz.sk/blogy) zamerané na oblasť vzdelávania označujeme edublogy. Učitelia na nich zverejňujú pre žiakov zadania úloh, odkazy na informačné zdroje, videá, komentujú žiacke riešenia, komunikujú s ďalšími učiteľmi atď. Edublogy sa môžu využiť aj na kolaboratívne riešenie projektových skupinových úloh.

V modernej škole sa žiaci zapájajú do tvorby **projektov**, pomocou ktorých riešia problémy zo života. Na úspešnú realizáciu projektu je dôležité stanoviť ciele, navrhnúť plán projektu, uskutočniť projekt a napokon ho vyhodnotiť a prezentovať jeho výsledky. Projekty, pri ktorých sa využívajú rôzne internetové služby a informačné zdroje označujeme ako **teleprojekty** (napr. www.etwinning.net). Pri teleprojektoch spolupracujú dva alebo viacero tímov žiakov, ktoré môžu pochádzať z rôznych krajín, s inou kultúrou, iným vierovyznaním. Spoločným sú však ciele projektu, dohodnutý postup a spôsob komunikácie, záujem objavovať a spoznávať sa.

Ďalším príkladom využívania Internetu vo vzdelávaní je tzv. **WebQuest** (WQ, napr. www.webquest.cz). Ide o učiteľom pripravenú lekciu podporujúcu samostatnú prácu žiakov, ktorí využívanú hlavne internetové zdroje. Prostredníctvom WQ sa dajú riešiť konkrétne problémy praxe, žiak sa vžije do rôznych profesií, zdokonalí sa v oblasti spracovania a prezentácie, prehĺbi si skúsenosti z tímovej práce, vďaka zverejnenej tabuľke sám zhodnotí výsledky svojej práce.

Nadaní žiaci môžu rozvíjať svoj talent aj mimo školy, napr. zapojením sa do rôznych súťaží, olympiád, korešpondenčných seminárov. Súťaže, pri ktorých sa Internet používa počas celého ich priebehu označujeme ako **on-line súťaže**, napr. ibobor.sk.

Pre názorné pochopenie podstaty fyzikálnych javov, matematických vzťahov, fungovania algoritmov sa využívajú **simulácie**. Na weboch vzdelávacích inštitúcií sa nachádzajú simulácie vo forme appletov, napr. phet.colorado.edu/simulation. Na iných webových stránkach môžeme na diaľku pracovať s reálnym experimentálnym zariadením – nastavovať vybrané parametre a pozorovať výsledné správanie, napr. kdt-12.karlov.mff.cuni.cz. Ide o vzdialený experiment – **teleexpetiment**.

Formu vzdelávania, pri ktorej sa využívajú rôzne multimediálne technológie a Internet označujeme pojmom **e-Learning**. Internet je hlavným prostriedkom na doručovanie obsahu výučby a komunikáciu pri **on-line vzdelávaní**. Vzdelávacie **on-line kurzy** sú umiestnené na webe so systémom pre správu výučby – LMS (Learning Management System). Tento systém umožňuje doručiť študijný materiál žiakom, komunikáciu medzi učiteľmi a žiakmi, uskutočniť rôzne aktivity žiakov, zaznamenať a vyhodnotiť výsledky práce žiakov. On-line kurzy sa úspešne využívajú pri tzv. **dištančnom vzdelávaní**, pri ktorom sú väčšinu času učiteľ a žiak od seba oddelení. Úspešnosť takejto výučby závisí od kvalitných učebných materiálov, rôznych komunikačných nástrojov, sebadisciplíny a záujmu žiaka o štúdium.

26. Vysvetlite rozdiel medzi intranetom a extranetom.

Intranet predstavuje počítačovú sieť používajúcu služby a technológie typické pre Internet na vnútorné potreby organizácie, ktorá nie je na Internete závislá – môže byť od neho úplne izolovaná, oddelená prostredníctvom firewallu alebo v niektorých prípadoch môže byť i jeho súčasťou.

Používaním Intranetu získava organizácia hotové technické riešenia a nepotrebuje investovať do špeciálnych a zvyčajne i drahších technológií, vďaka čomu nie je závislá na jedinom dodávateľovi. Zamestnanci schopní pracovať s Internetom nemajú problém používať služby Intranetu. Najpoužívanejšie služby Intranetu sú:

- **www** na zverejňovanie informácií a prístup do informačných systémov. Organizácií postačí použiť vlastný webový server a sprístupniť ho len pre vnútornú časť siete.
- **e-mail** určený na vnútornú komunikáciu, ale prakticky bez problémov fungujúci i navonok. Organizácia použije niektorý z mailových serverov, ktorý okrem okamžitej výmeny správ vo vnútri organizácie zabezpečí i komunikáciu navonok a prijímanie došlých správ.
- **ftp** zabezpečí zdieľanie dokumentov a prístup k ním na základe oprávnení.

Intranet v klasickom ponímaní reprezentuje lokálna sieť, no často sa možno stretnúť aj s prepojením počítačov na rôznych miestach sveta prostredníctvom virtuálnej siete – VPN (Virtual Private Network). Počítač kryptovane pripojený cez VPN sa stáva súčasťou lokálnej siete, pričom nie je dôležité, kde sa klient nachádza.

V súčasnosti sa dostáva do povedomia používateľov aj pojem **Extranet**, ktorý obvykle na základe autorizácie menom a prístupovým heslom umožňuje prístup používateľov z počítačov mimo Intranetu (napr. zákazníkom, dodávateľom, zamestnancom v teréne a pod.) a poskytuje im určité informácie z neho. Inak povedané do Extranetu majú prístup zo siete Internet aj počítače, ktoré nie sú pripojené na VPN organizácie, v Intranete takáto možnosť neexistuje.

27. Objasnite niektoré riziká komunikácie prostredníctvom počítačovej siete a možnosti jej ochrany.

Informácie sa cez počítačovú sieť prenášajú v čistej, čitateľnej podobe. To znamená, že ktokoľvek, kto sa k týmto informáciám dostane, ich vie prečítať a zmeniť. A to bez toho, aby si to odosielateľ alebo prijímateľ všimol. Takýto spôsob komunikácie je však v istých prípadoch neprijateľný. Mali by sme teda zabezpečiť, aby sa citlivé informácie nedostali do nepovolaných rúk.

O bežnej e-mailovej správe, doručenej do našej poštovej schránky, nevieme s istotou tvrdiť takmer nič. Nemôžeme si byť istý tým, kto je jej odosielateľom alebo autorom. Nevieme zistiť, či správu čítal niekto iný, alebo či správa bola cestou zmenená. Jedným z riešení, ako vniesť viac istoty do takejto komunikácie, je správy šifrovať a elektronicky podpisovať. Šifrovať správy znamená zmeniť ich obsah pomocou šifrovacieho algoritmu podľa nejakého kľúča. Výsledkom šifrovania je nečitateľný súbor - šifra. Prístup k nemu má každý, ale prečítať ho vie iba ten, kto má na to prístupové právo, teda dešifrovací algoritmus a pozná kľúč. Elektronický podpis sa realizuje buď elektronickými identifikačnými údajmi autora (odosielateľa) elektronického dokumentu, pripojené k nemu alebo šifrovaním.

Protokol http žiadnym spôsobom nezaručuje, že údaje prenášané v počítačovej siete nemôže byť zmenené alebo, že ich niekto neprečíta. Na bezpečnú komunikácia sa používa protokol HTTPS (Hypertext Transfer Protokol Secure). Ide o kombináciu protokolov http a SSH (Secure Socket Layer) alebo TLS (Transport Layer Security), ktoré umožňujú bezpečné, šifrované pripojenie lokálneho počítača k vzdialenej stanici. Vytvorenie spojenia prebieha prostredníctvom asymetrického šifrovania, kde používateľ v prvom kroku požiada server, s ktorým chce komunikovať, o doručenie kľúča pre komunikáciu a určenie kryptovacieho algoritmu, prostredníctvom ktorého bude prebiehať ďalšia komunikácia. Server kľúč odošle spolu s bezpečnostným certifikátom, ktorý slúži na overenie jeho totožnosti a hodnovernosti. Bezpečnostný certifikát je elektronický dokument, ktorým sa preukazuje totožnosť jeho držiteľa Obsahuje údaje o tom, pre koho a kedy bol vyhotovený, dokedy je platný, ktorá certifikačná autorita ho vydala a na aký účel. Aby bola zaručená dôveryhodnosť takéhoto certifikátu, obsahuje navyše elektronický podpis certifikačnej autority. Certifikačná autorita je úrad alebo inštitúcia, ktorá overuje skutočnú identitu vlastníka certifikátu. Jej úloha v digitálnom svete je ekvivalentom notára, ktorý overuje podpisy na papierových listinách.

Nemôžeme si byť istý ani tým, či údaje zverejnené na Internete niekto nezmenil a nezakomponoval do nich časť škodlivého kódu. V tejto situácii môžu pomôcť hashovacie funkcie. Hashovacia funkcia vytvorí pre vstup ľubovoľnej dĺžky, napr. aj celý súbor, jeho kontrolný súčet, tzv. odtlačok. Po stiahnutí údajov z Internetu stačí overiť, či odtlačok týchto údajov je rovnaký ako odtlačok, ktorý zverejnil pôvodný autor.

28. Uveďte spôsoby ochrany proti prieniku do systému a zneužitiu údajov.

Aj keď sme vlastníkmi najnovšieho operačného systému, ktorý sa chváli prívlastkom bezpečný, nemôžeme sa na to spoliehať. Je len otázkou krátkeho času, kedy sa niekomu podarí nájsť jeho slabé miesto. V tej chvíli sa náš počítač stáva otvorenou bránou pre prieniky z Internetu. Toho sú si vedomí aj samotní autori operačných systémov. Snažia sa čo najskôr problém vyriešiť. Riešením sú bezpečnostné **záplaty** (security patch) alebo bezpečnostné **aktualizácie** (security update).

Pri práci používajme len **legálny softvér**. Pirátske kópie z pochybných zdrojov môžu obsahovať škodlivé časti softvéru, pomocou ktorých môže byť náš počítač ovládnutý.

Ak keď je náš systém aktualizovaný, stále mu hrozí riziko. Nielen z Internetu alebo lokálnej siete, ale paradoxne aj zo samotného počítača. Prípadný útočník sa môže pokúsiť do počítača preniknúť cez málo zaistený vstup. Ak sa mu to podarí, môže nekontrolovane prenášať údaje jedným aj druhým smerom. Nič mu už nebráni v tom, aby na náš počítač nainštaloval akýkoľvek program, prípadne ho pomocou tohto programu aj ovládol. **Firewall** je špeciálny program, ktorého úlohou je zabezpečiť počítač pred prípadným útokom a zároveň filtrovať sieťovú komunikáciu. Firewall vyhodnocuje, či údaje z Internetu sú bezpečné a povolené. Len v tom prípade ich prepustí ďalej. Rovnako pri prenose údajov do Internetu skontroluje, či daná aplikácia má právo posielať údaje smerom von z počítača. Firewall teda kontroluje, či sieťová prevádzka dodržiava vopred definované pravidlá. Komunikácia, ktorá tieto pravidlá porušuje, je zablokovaná.

Skupinu všetkých škodlivých alebo nechcených aplikácií označujeme pojmom **malware**. Patria sem vírusy (škodlivé programy, ktoré sú schopné vytvárať svoje kópie a zabezpečiť ich aktiváciu), spyware (programy využívajúce Internet na odosielanie údajov z počítača bez vedomia používateľa) a rookit (programy, ktorý sa dokáže schovať nielen pred zrakom používateľa, ale aj pred antivírusovým alebo iným bezpečnostným programom). Antivírusové programy už dnes integrujú ochranu nielen pred vírusmi, ale aj pred spyware a rookitmi. Pri ich používaní je ale nevyhnutná pravidelná aktualizácia a správne nastavenie, kontrola nielen údajov v počítači, ale aj komunikácie.

Riziko prieniku do nášho počítača hrozí aj z **e-mailu**, z poplašných správ (Hoax), ktoré nás varujú pred neexistujúcim rizikom a odporúčajú nám inštaláciu „vhodného bezpečnostného softvéru“. Podvodné e-maily informujúce o výhre v lotérii alebo možnosti získať veľké množstvo financií sa označujú SCAM. Často žiadajú zaslanie osobných údajov alebo uhradenie poplatkov súvisiacich s prevodom peňazí. Správy budiace dojem, že ich autorom je naša banka a zvyčajne informujúce o nejakom probléme s naším účtom, sa označujú ako **Phishing**. Často žiadajú vyplniť formulár alebo prihlásiť sa do služby Internetbanking prostredníctvom podstrčenej webovej stránky. Táto stránka je veľmi podobná oficiálnej stránke banky.

29. Uveďte spôsoby ochrany proti neoprávnenému prístupu k osobným údajom a spôsoby ochrany dôvernosti dát.

Aktualizovaný operačný systém vrátane aplikácií na ňom bežiacich, dobre nastavený kvalitný firewall a aktualizovaný antivírusový systém predstavujú pomerne slušnú úroveň ochrany počítača. Napriek tomu, naše počítače sú často obeťou internetového útoku alebo zákerného vírusu. Ako je to možné? Zlyhal najslabší článok v ochrannej reťazi – používateľ počítača. Človek nie je stroj. Často sa rozhodujeme v časovom strese a nezvažujeme všetky dôsledky svojich rozhodnutí. Ochrane osobných údajov sa v poslednej dobe venuje veľa pozornosti. Mali by sme mať stále na pamäti tieto pravidlá:

- Nezverejňujeme svoje osobné údaje, nešifrované informácie o sebe neposkytujeme nikomu cez Internet, ani keď nás o to požiadajú.
- Neposkytujeme žiadne informácie o svojich blízkych a známych.
- Vždy sa uistíme, že vieme, komu poskytujeme informácie a načo a ako ich použije.
- Ak použitie nejakej služby vyžaduje našu e-mailovú adresu, vytvorme si na tento účel nový e-mailový účet.
- Z prihlasovacieho mena alebo prezývky, ktorú používame vo verejných diskusiách, by sa nemalo dať určiť naše pohlavie, adresa, vek a pod.

Medzi údaje, ktoré by sme nemali zverejňovať, patria: osobné údaje (meno, adresa, telefónne číslo, vek, pohlavie, rodné číslo), bankové údaje (čísla účtov a platobných kariet, heslá), fotografie (z dovolenky v plavkách), sociálne a ekonomické pomery (s kým a kde žijeme, vybavenie našej domácnosti a pod.).

- Na podozrivú alebo nevyžiadanú e-mailovú správu nikdy nereagujme, neotvárajme prílohu v nej, neklikajme na žiadne odkazy v tejto správe, neposielajme ju ďalej.
- Ak partnera v diskusii poznáme len z Internetu, nemôžeme si byť istí, s kým v skutočnosti komunikujeme, preto ak sa nám zdá komunikácia nepríjemná alebo sa cítime nepohodlne alebo trápne, ukončime ju. Zvýšme opatrnosť, ak náš partner na Internete nechce, aby sme o našom vzťahu informovali niekoho ďalšieho alebo ak sa nám zdá, že náš partner má veľa rovnakých záľub a názorov ako my.
- Buďme opatrní pri zverejňovaní informácií. Informácia, ktorá bola raz zverejnená na Internete, sa stáva verejnou, je prakticky nemožné ju z Internetu vymazať.
- Nenechajme sa zatiahnuť do urážlivých diskusií, tzv. flaming.
- Všetko, čo sa k nám dostalo z internetu, považujme za nedôveryhodné a podozrivé, a podľa toho sa aj správajme.
- Buďme opatrní pri sťahovaní údajov z Internetu, používajme len overené zdroje. Čím sú údaje pre nás atraktívnejšie, tým väčšie riziko infiltrácie škodlivého softvéru nám hrozí.
- Voľme dlhé a bezpečné heslá. Nikomu ho neprezrádzajme. Niektoré aplikácie ponúkajú možnosť zapamätať si heslo, využívajme to veľmi opatrne, na inom ako súkromnom počítači by sme túto možnosť nemali využívať vôbec.
- Správajme sa zodpovedne. O svojich Internetových kontaktoch hovorme so svojimi najbližšími.

30. Vysvetlite pojem netiketa a uveďte dôvody prečo je potrebné dodržiavať jej pravidlá pri používaní Internetu.

Tak ako v bežnom sociálnom kontakte existujú pravidlá spoločenskej etikety, tak aj v komunikácii v elektronickom svete existujú isté pravidlá. Hovorí sa im **netiketa** (netiquette). Slovo netiketa vzniklo spojením slov net (sieť) a etiketa (súhrn pravidiel spoločenského správania a zvykov). Predstavuje teda pravidlá správania sa na sieti. Aj keď sa považuje len za nepísaný súbor pravidiel, jej nedodržanie sa chápe ako prejav neúcty.

Elektronická komunikácia môže mať rôzne podoby a formy. Prezeranie webových stránok, diskusné skupiny a fóra, chat, e-mail alebo publikovanie informácií na Internete. To všetko sú formy komunikácie odohrávajúce sa prostredníctvom elektronických prostriedkov. Každá z nich má svoje špecifiká, zásady a pravidlá.

Vo všeobecnosti platí, že v prostredí Internetu sa treba správať rovnako ako v reálnom živote. Treba myslieť na to, že naše správy sa môžu dostať k tisícom ľudí po celom svete a závisí len od tónu a obsahu správy, aký obraz si o nás títo ľudia vytvoria.

Dodržiavaním pravidiel netikety teda prezentujeme seba v príjemnom svetle, neoberáme ľudí zbytočne o čas a priestor na disku, vyhýbame sa nepríjemnostiam, ktoré by mohli neskôr vzniknúť.

Okrem netikety platí v elektronickom svete i počítačová etika, čo je sústava mravných noriem, ktoré určujú, čo je dobré a čo zlé. Etický kódex používateľa počítača znie:

1. Nepožiješ počítač ku škode iného.
2. Nebudeš ničiť prácu iných.
3. Nebudeš prezerať údaje iných ľudí.
4. Nepoužiješ počítač ku krádeži.
5. Nepoužiješ počítač na krivé svedectvo.
6. Nepoužiješ alebo nevytvoríš kópiu softvéru, ktorý si nezaplatil.
7. Nepoužiješ neoprávnené počítačové zdroje iných ľudí.
8. Neprivlastníš si intelektuálne dielo iného.
9. Budeš premýšľať o spoločenských následkoch programu, ktorý si stvoril.
10. Budeš používať počítač ohľaduplne a s úctou.