Uživatel počítačových sítí

Intenzivní kurz IBA

Daniel Klimeš, Roman Šmíd, Milan Blaha

© Institute of Biostatistics and Analyses

Organizace kurzu

- Podmínky zápočtu
  - Registrace v is.muni.cz
  - Účast na teoretické části
  - Zvládnutí elektronického testu (po skončení přednášky)

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Osnova

- Pojmy, termíny
- Počítačová síť - základní hardware a topologie
- Připojení k síti
  - Možnosti připojení, co je zapotřebí, srovnání
- Bezpečnost na síti
  - Hesla a průzkumník vůbec, Firewall, email, spyware, phishing
- Šifrování a elektronický podpis
- Mobilní zařízení

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Data a jejich objem

- Jak vyjádřit informaci
- **1 bit (b) - základní informační jednotka 1/0**
- **1 Byte (B) – 8 bitů, celé číslo od 0 do 255,**
  - **1 textový znak (ASCII), např. "A" = 65**
- 1 Kb = 1024 bitů
- 1 KB = 1024 Bytů
- 1 MB = 1024 KB = 1 048 576 Bytů = 8 388 608 bitů
- 1 GB = 1024 MB
- 1 TB = 1024 GB

Pozn.

Někdy je K = 1000 x

KiB je vždy 1024 – norma (omezené využívání)

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

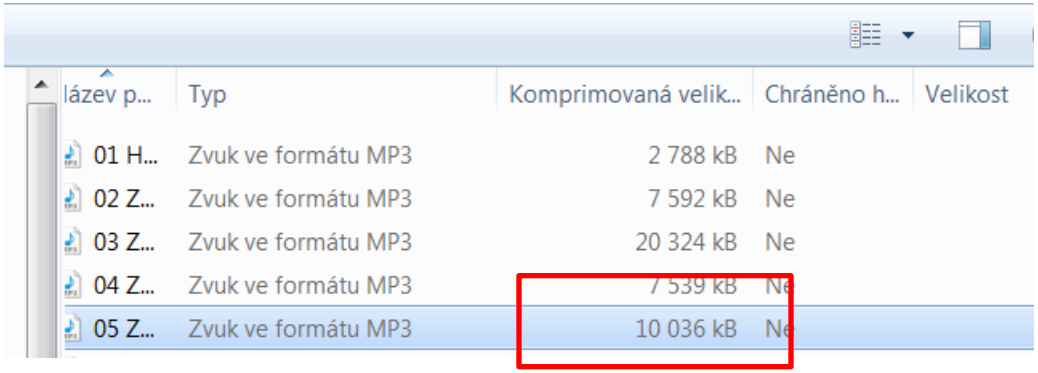
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Počítačová síť

- Propojení dvou a více počítačů
- Součástí sítě jsou síťové prvky
  - Počítač (zařízení) se síťovou kartou, modemem, wifi adaptér
  - Kabeláž (metalická, optická)
  - Rozbočovače, směrovače a přepínače, wifiroutery, antény
  - Zařízení poskytující síťové služby, síťové tiskárny…
- Kvalitu sítě, respektive konkrétní cesty v síti, lze hodnotit podle
  - **Propustnosti** (rychlosti) sítě - (K/M/G) bity za sekundu (**b/s**)
  - **Rychlosti odezvy** (milisekundy) – program **ping**

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Rychlost připojení



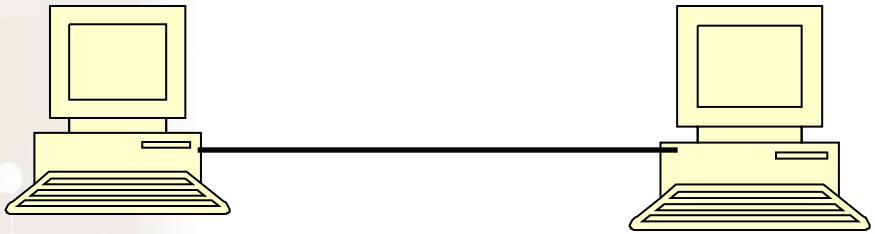
Soubor o velikosti
10 036 kB * 8 bitů = 80 288 kilobitů

Přeneseme přes síť s rychlostí 1 Mb/s (1024 Kb/s) za
80 288 Kb / 1024 Kb/s = 78 s

Film - 1,5 GB = 12 Gb = 12 288 Mb => 12 000 s ~ přes 3hodiny

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Propojení dvou počítačů



Potřebné vybavení

- 2 síťové karty
- kabel

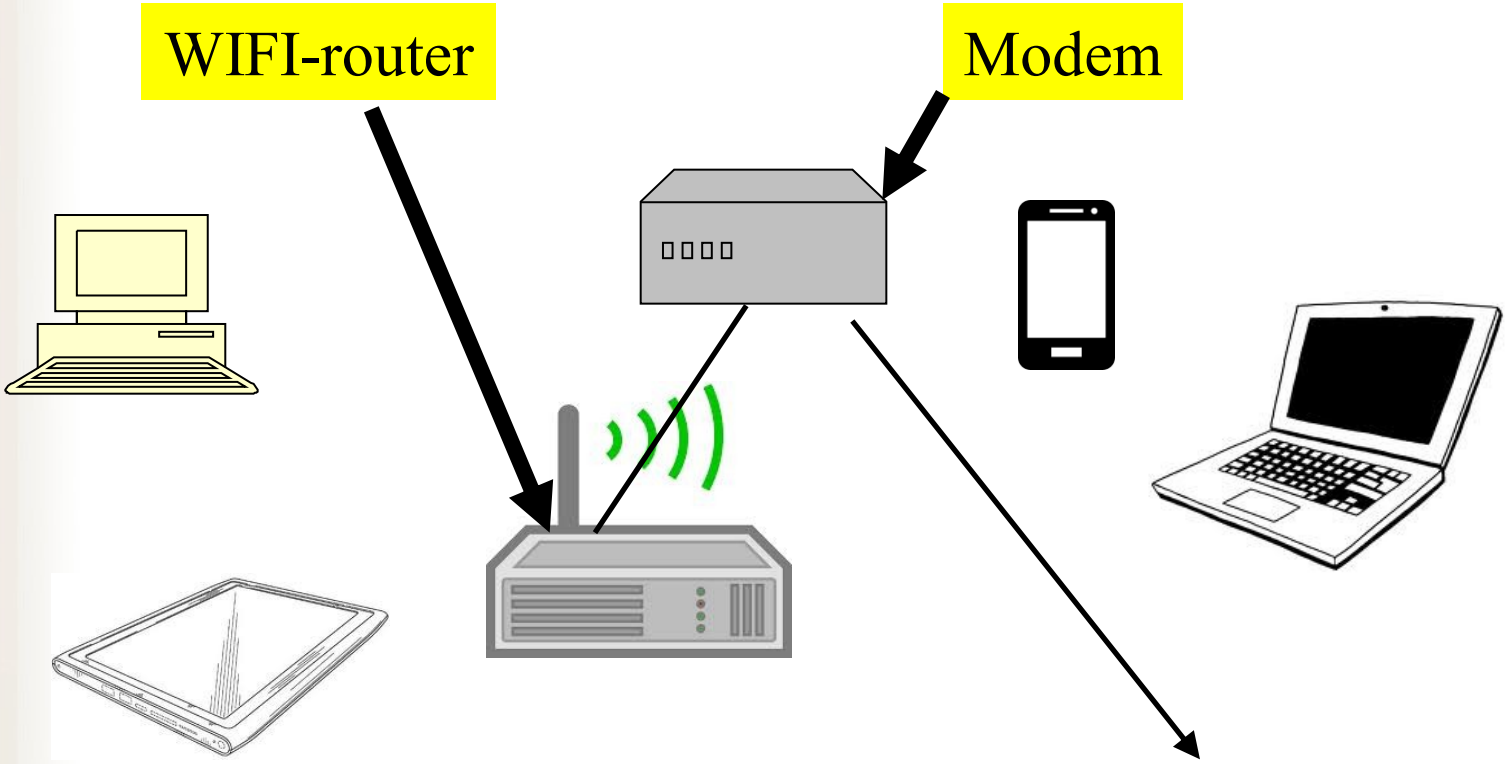
Alternativy:

- bezdrátové připojení - Bluetooth
- Wi-fi
- propojení kabelem přes USB
  - v. USB 1.1 = 1.5Mbit/s; v2.0 = 400Mbit/s; v3.0 = 5Gbit/s
  - **USB Easy Transfer Cable**

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Jde to i bez drátů



Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Identifikace PC v síti

- Identifikace síťové karty
  - Celosvětově „jedinečná“ MAC adresa (fyzická adresa)
  - 00-0A-E4-C0-36-81
- IP adresa (obdoba IČO nebo telefonu)
  - Celosvětově „jedinečné“
  - 147.251.147.76
- Internetové jméno (obdoba pošt. adresy) - URL
  - Celosvětově jedinečné
  - www.iba.muni.cz
- Windows jméno počítače (číslo kanceláře)
  - Lokální jméno pouze v rámci místní sítě
  - Např.: Server1, kancelar1, kancelar2

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

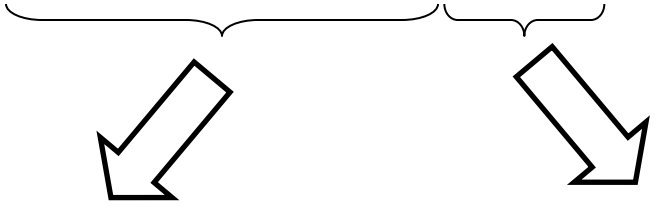
IP adresa

IPv4 x IPv6

- IPv4: 32b = 2^{32} IP adres => cca 4 * 10^{9} adres
- IPv6: postupně zaváděna 128b => 3,4 * 10^{38} adres

- Identifikace sítě
- Identifikace počítače

```
147.251.147.76
255.255.255.0
```



ID sítě

ID počítače

Stejný počítač přenesený do jiné sítě má zpravidla jinou IP adresu!

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

IP adresa

- Pevná x dynamická IP adresa
- Veřejná x neveřejná IP adresa
  - Neveřejná IP není celosvětově unikátní – pouze v rámci lokální podsítě
  - Neveřejné adresy nemívají přiřazené internetové jméno
  - Dynamická + neveřejná IP – typický konzument služeb
  - Pevná + veřejná IP – typický poskytovatel služeb

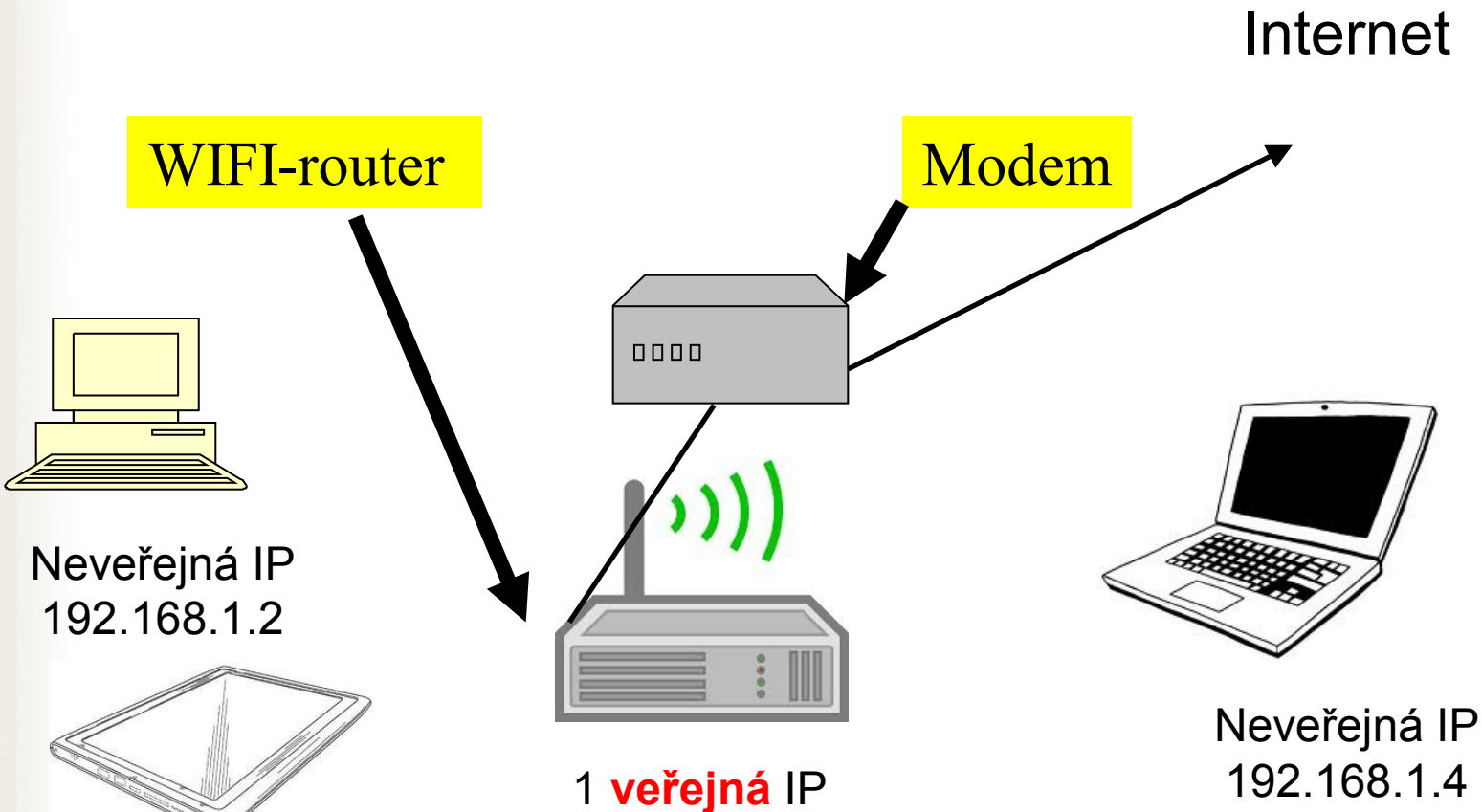
http://www.ip-adress.com/

cmd - ipconfig

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

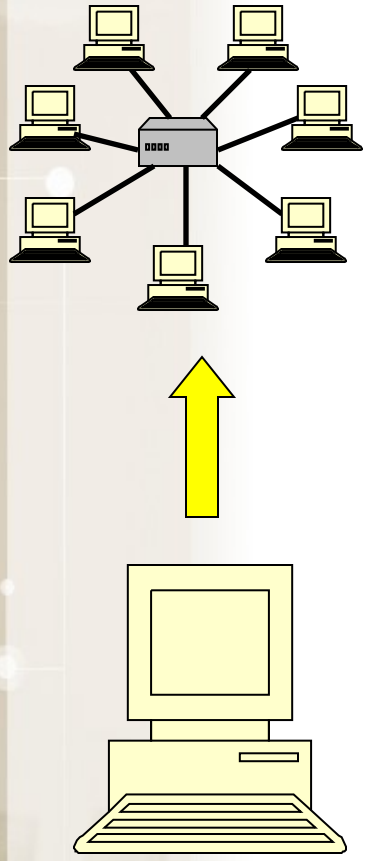
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Neveřejné IP adresy
192.168.*.*



Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

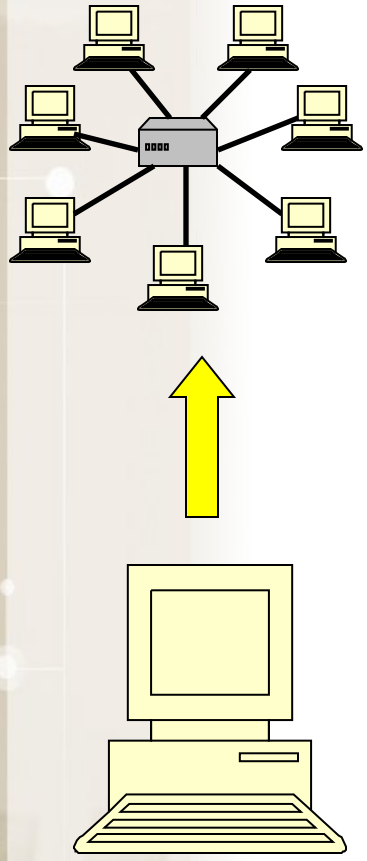
Fyzické připojení PC do sítě



- Pevné páteřní připojení
  - Síťová karta (až 1 Gb/s)
- Telefonní linka
  - ADSL modem
- Mobilní připojení
  - Modem nebo mobilní telefon
- Bezdrátové připojení – WIFI
  - Speciální zařízení/karta, anténa
- Kabelová televize
  - Modem

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Telefonní linka



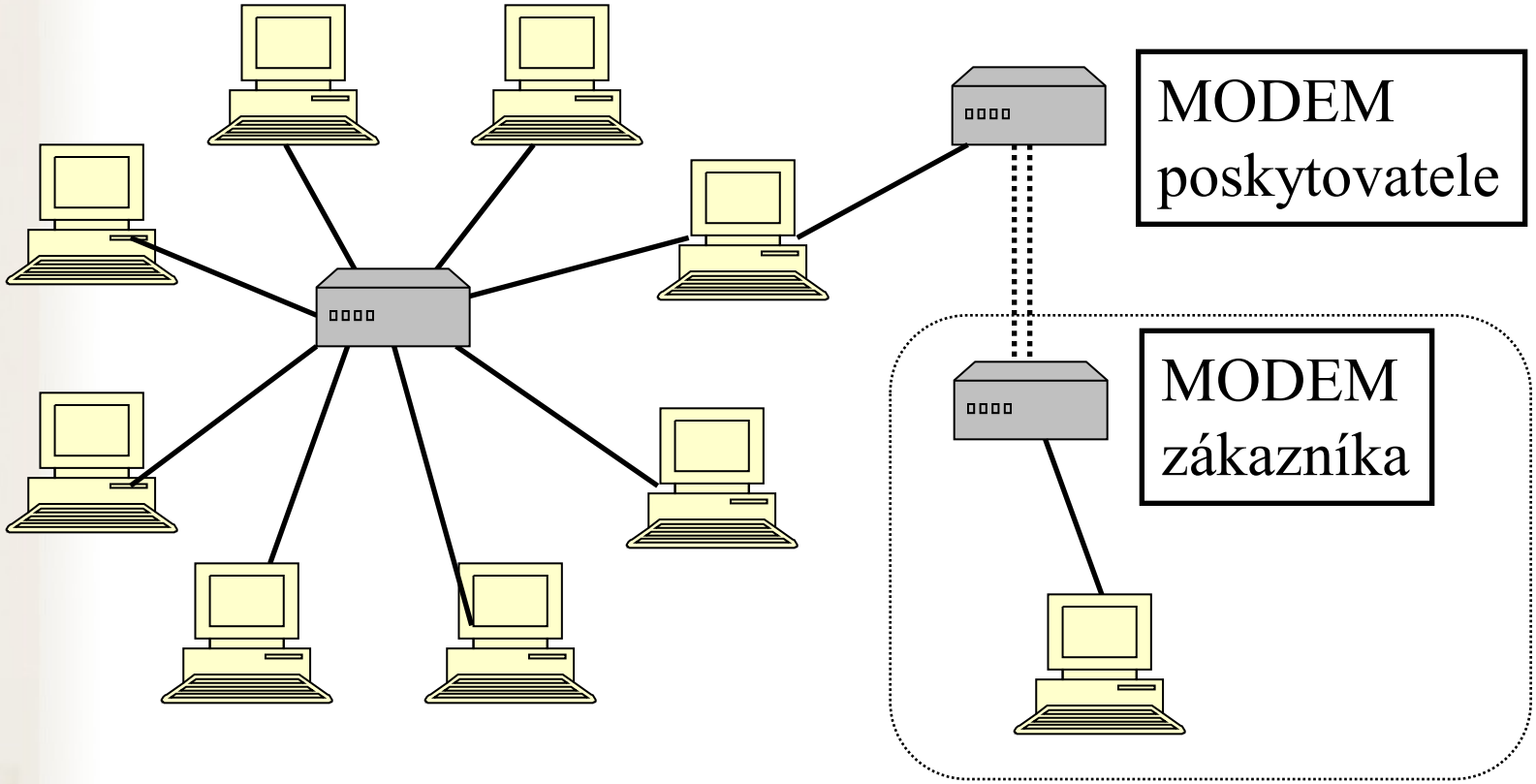
- ~~Vytáčené připojení (až 56 kb/s)~~
- ~~ISDN (až 128 kb/s)~~
- ADSL (až 16 Mb/s)
- VDSL (teroreticky až 100 Mb/s)
  - Nabízeno do 1,3 km od ústředny

- Každý typ vyžaduje specifický modem

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

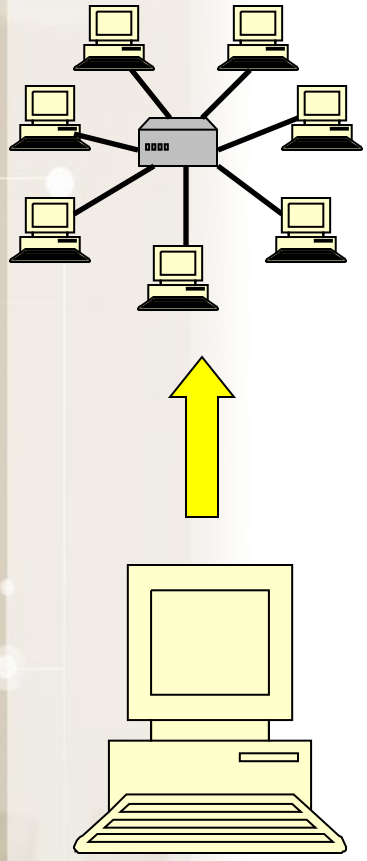
Telefonní linka 1



Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

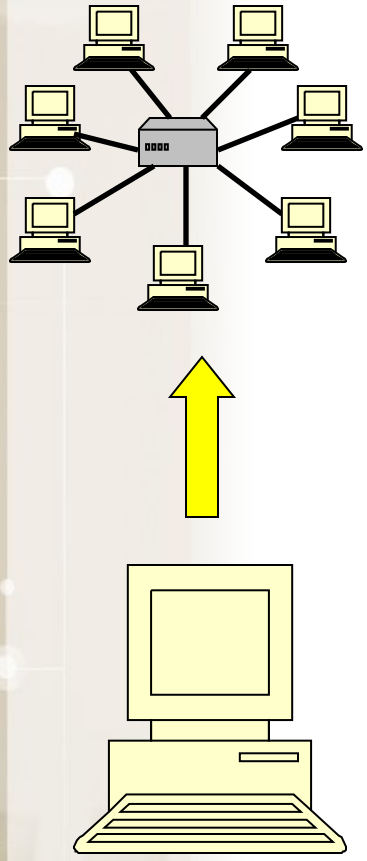
Kabelová televize



- V místech dostupnosti kabelové televize
- Rychlost až 240 Mb/s
- Metalické x optické připojení
- Speciální modem
- www.upc.cz
- www.netbox.cz
- http://www.selfnet.cz
- http://www.internetprovsechny.cz/catv.php
- http://rychlost.cz/pripojeni-internetu/kabelova-tv/

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

WiFi-připojení



- Komerční/komunitní sítě
- Lokální domácí síť
- Rychlost typicky až 11Mb/s (54 Mb/s)
- Speciální cenově dostupné vybavení
- Zabudované v notebooku - indoor
- Riziko rušení, odposlouchávání, neoprávněného připojení
- Přístupový bod /Access point/ hot spot
- www.internetprovsechny.cz
- http://www.muni.cz/ics/services/wifi
  - Eduroam

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Wi-Fi připojení - rychlost

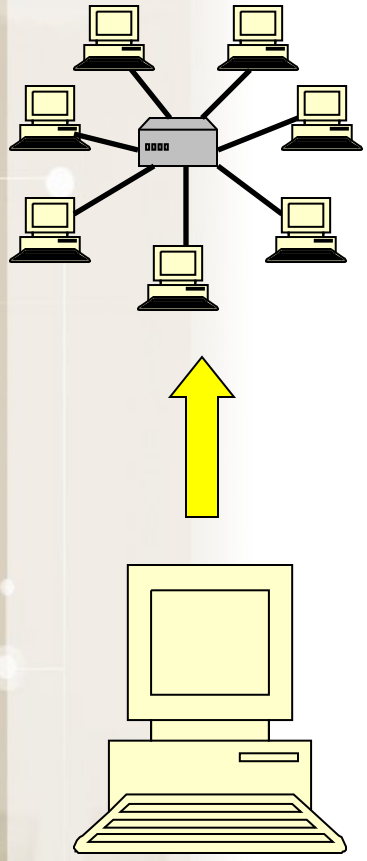
- **V rozmezí 5 – 21 Mb/s**
- **Průměr kolem 10 Mb/s**

- **Čím blíže anténě, tím lépe**
- **Se vzdáleností klesá rychlost**

zdroj: www.dsl.cz

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Mobilní připojení



- GPRS (až 128 kb/s)
  - Mobilní telefon s podporou GPRS - **G**
- EDGE (až 512 kb/s)
  - Mobilní telefon s podporou EDGE - **E**
- CDMA (až 800 kb/s)
  - www.cdma.cz
  - CDMA modem
- 3G-UMTS/HSDPA (1024 kb/s a více) - **H**
  - Speciální modem
  - Novější mobilní telefon nebo notebook
  - Omezené pokrytí ČR
- **LTE (80 Mb/s a více) - L**
  - **Větší pokrytí než 3G**
  - Novější smartphony a modemy

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Mobilní připojení - rychlost

Prosinec 2015

Technologie	Poskytovatel	Rychlost v Mb/s	Meziměsíční změna	Meziroční změna
LTE	O2	26,56	-8 %	8 %
LTE	T-Mobile	27,76	8 %	13 %
LTE	Vodafone	27,63	1 %	13 %
3G	O2	8,37	-10 %	28 %
3G	T-Mobile	7,50	-7 %	-7 %
3G	Vodafone	6,76	-11 %	-15 %
2G	O2	0,11	0 %	-6 %
2G	T-Mobile	0,11	10 %	-4 %
2G	Vodafone	0,08	-11 %	-14 %
CDMA	U:fon	1,65	0 %	-34 %

zdroj: www.dsl.cz

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

LTE pokrytí

- Velká dynamika
- Stránky poskytovatelů nebo
- http://lte.ctu.cz/pokryti/
- Pro všechny operátory

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Typy připojení – srovnání

	Výhody	Nevýhody
Kabel/ optika	rychlost, spolehlivost	dostupnost
Telefonní linka	dostupnost (ADSL)	cena
WI-FI	cena, dostupnost	spolehlivost
Mobilní připojení	dostupnost, mobilita	spolehlivost cena, FUP

Aktuální rychlost mezi dvěma počítači lze orientačně změřit pomocí speedmetrů
Např.: http://nastroje.lupa.cz/mereni-rychlosti/, www.dsl.cz

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Výběr připojení k internetu

- Způsob použití – pevné PC x notebook
- Dostupnost v daných lokalitách, pokrytí
- Rychlost, většinou v Mb/s
  - symetrické x **asymetrické** (download, upload)
  - (např.: 2048/128)
  - Skutečnou rychlost ověřit v praxi
- Fair user policy (FUP) – omezení rychlosti po přenesení určitého množství dat
- Agregace (např.: 1:32) – (ADSL, bezdrátové připojení)

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Konfigurace připojení

- Automatické x manuální

- IP adresa — např.: 147.251.147.250
- maska sítě — např.: 255.255.255.0
- IP adresa brány (gateway) — např.: 147.251.147.1
- IP adresy DNS serverů — např.: 147.251.26.1

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

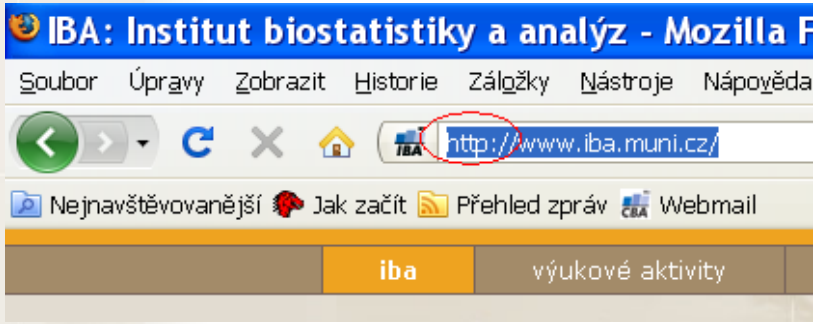
DNS služba

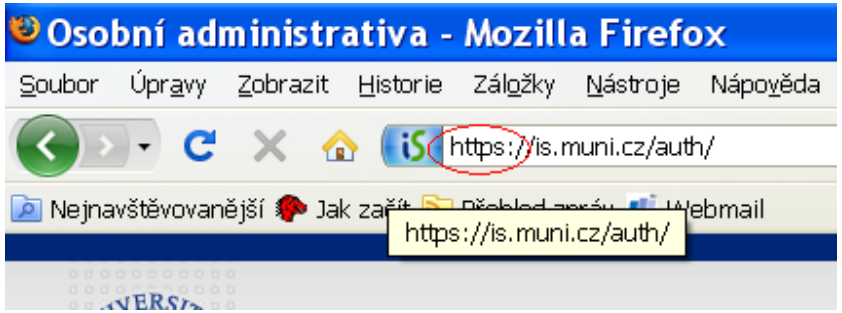
- Překlad internetových jmen na IP adresy
- Ne každá IP adresa má definováno internetové jméno
- Překlad realizují DNS servery, které udržují seznam známých internetových jmen a případně se dotazují dalších DNS serverů na neznámá jména
- Bez dostupnosti této služby nelze využívat internetová jména, pouze IP adresy

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

HTTP x HTTPS

- Veškerá komunikace klienta se serverem je šifrována – data jsou během přenosu nečitelná
- HTTPS má vlastní port 443
- Server musí podporovat službu HTTPS





Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

COOKIES

- Malé soubory ukládané na vašem počítači
- Svázané s konkrétním serverem
- Prohlížeč je zasílá s požadavkem na server
- Server je tvoří/upravuje, posílá prohlížeči
- Kampaň k ochraně soukromí

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Bezpečnostní zásady při práci s PC

Rizika při práci v počítačové síti

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE
esf
UNIVERZITA KARLOVA V PRAZE
MU
IBA
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Úvod – co nám hrozí?

- Útok hackera
  - **Automatizovaný a plošný** (e-mail, www, IM, sociální sítě)
    - Cílem hackera je ovládnout váš PC, získat z něj citlivé údaje (čísla kreditních karet, hesla…), odcizit hotovost z účtu nebo jej použít k dalším útokům
  - Cílený přímo na Vás
    - Cílem může být získání citlivých firemních dat (konkurenční boj, diskreditace)

Možné následky útoku:

  - Přímá finanční ztráta (odcizení peněz z účtu přes kreditní kartu)
    - Správné nastavení limitů na kartě
  - Policejní stíhání (obvinění z použití PC k nelegálním aktivitám)
  - Problémy v zaměstnání
  - Vydírání a diskreditace (zveřejnění citlivých informací, fotografií, e-mailů…)
  - Odcizení výpočetního výkonu (zpomalení PC) za účelem výdělku (Bitcoin)

- Ztráta dat
  - V případě selhání hardware, ztráty nebo odcizení PC, zavirování

Následky ztráty dat jsou individuální, záleží na povaze dat.

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Úvod – jak se bránit?

- PC jako pracovní nástroj: je nutné dodržovat bezpečnostní pravidla jako s každým jiným nástrojem, zejména v těchto oblastech:
  - Práce s emailem a přílohami
  - Instant messaging (Skype, ICQ, Jabber…)
  - Sociální sítě (Facebook, Google+, LinkedIn, Twitter…)
- Je třeba **rozumět hlášením operačního systému** a dalších programů, které vyžadují uživatelskou akci a adekvátně reagovat
- Je třeba udržovat OS, antivir a všechny používané aplikace aktualizované
- Data jsou často důležitější než samotný hardware – je důležité **zálohovat**:
  - Vím, co se z mého PC zálohuje, kam a v jakých intervalech?
  - Umím si zkontrolovat, zda zálohování funguje?
  - Umím si zálohovaná data v případě potřeby obnovit?
- Přístupové údaje k různým službám – jaká mám kde hesla? Kam je ukládám?
- Správně zabezpečená WiFi síť

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Bezpečnost E-mailu

- Hrozby:
  - SPAM – nevyžádané zprávy posílané za účelem:
    - Rozesílání reklamy
    - Sběru aktivních emailových adres
    - Distribuce škodlivého kódu
    - Vylákání peněz
  - Phishing – nevyžádaná zpráva, hromadně rozesílaná za účelem:
    - Vylákání přístupových údajů k různým službám
    - Vylákání soukromých informací
  - Spear Phishing – nevyžádaná zpráva cílená a upravená pro konkrétního uživatele
    - Převážně na objednávku
    - Cílem bývá zavlečení škodlivého kódu do vnitřní sítě organizace za účelem získání přístupu k citlivým firemním datům
    - Jde o velmi zákeřný útok, na který se mohou nachytat i zkušení uživatelé
  - RansomWare – vydírání (ve vašem PC jsme nalezli kradený software, pokud nezaplatíte, vystavíte se trestnímu stíhání)

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Bezpečnost E-mailu

- Pravidla:
  - Neklikat na odkazy v neznámých zprávách (nebezpečí podvržení adresy, nasměrování na stránku se škodlivým kódem)
  - Neotvírat přílohy v neznámých a podezřelých zprávách
  - Nikam neposílat loginy a hesla, čísla kreditních karet
  - Všímat si podezřelých rysů ve zprávách (strojově přeložený text, odkazy vedou jinam než jejich popis, zprávy předstírající že pocházejí od masově používaných služeb (Facebook, banky atd…), podezřelá adresa odesílatele
  - Neignorovat případná varování antivirových programů
  - Nenechat se zastrašit (Pokud nenainstalujete software X.Y., váš počítač bude ohrožen…)

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Instant Messaging (Skype, Jabber, ICQ)

- Hrozby ve zprávách: jsou podobné hrozbám E-mailovým
  - IM SPAM – nevyžádané zprávy posílané za účelem:
    - Rozesílání reklamy
    - Sběru aktivních emailových adres
    - Distribuce škodlivého kódu
    - Vylákání peněz
  - Phishing – nevyžádaná zpráva, hromadně rozesílaná za účelem:
    - Vylákání přístupových údajů k různým službám
    - Vylákání soukromých informací
  - Spear Phishing – nevyžádaná zpráva cílená na konkrétního uživatele
    - Převážně na objednávku
    - Cílem bývá zavlečení škodlivého kódu do vnitřní sítě organizace za účelem získání přístupu k citlivým firemním datům
- Hrozby pramenící z neaktualizovaného IM klienta
  - Neaktualizovaný IM klient může být zneužit k instalaci škodlivého kódu do PC bez vědomí uživatele
- Pravidla:
  - Neklikat na odkazy ve zprávách od neznámých osob (nebezpečí nasměrování na stránku se škodlivým kódem
  - Neotvírat soubory od neznámých osob
  - Nikam nezadávat ani neposílat loginy a hesla, čísla kreditních karet
  - Všímat si podezřelých zpráv od známých osob v kontaktech – mohou mít zavirovaný počítač a zprávu odesílá virus
  - Neignorovat případná varování antivirových programů
  - Nenechat se zastrašit (Pokud nenainstalujete software X.Y., váš počítač bude ohrožen…)
  - **Zabezpečit pravidelnou aktualizaci používaného klienta na poslední verzi**

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Příklad phisingu

- Vážená paní, vážený pane,
- děkujeme za projevenou důvěru v internetové obchody obchody24.cz.
- Tímto emailem potvrzujeme, že jsme v pořádku přijali vaši objednávku.
-
- Číslo objednávky (variabilní symbol): JCBDF729B439057 Datum a čas objednávky: 11.01.15 00:45 Kontaktní údaje:
- Barbora Záňová
- +420 604 920 148
-
- Vaše objednávka:
- ----------
- SONY DSC-F828 Cyber-Shot 8 mil. obraz.bodu, bílá: 1 x 23 549,00 Kč =23 549,00 Kč
- Doúprava PPL: 113 Kč
- ----------
- Celková cena nákupu vč. DPH: 23 662,00 Kč Způsob platby: Platba předem – platební karta
- Poznámka: Potvrzení platby a fakturu najdete v přiloženém souboru (ucet111D535.zip)
- -
- Nyní prosím vyčkejte na našeho operátora, který se s vámi spojí maximálně do 1 pracovního dne a dohodne podrobnosti ohledně Vaší objednávky.

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Sociální sítě

- **Facebook** – zneužíván pro šíření spamu, hoaxů, škodlivého kódu
  - Nebezpečná je důvěra v přátele: kliknu na cokoli, co postne někdo z mých přátel
  - Obtížná orientace v prostředí, které se často mění – pasti na neznalé uživatele
  - Clickjacking – kombinace sociálního inženýrství a tlačítek To se mi líbí
    - Příklad: Klikněte postupně na všechna tlačítka To se mi líbí pro zobrazení videa apod.
    - Na konci často pouze webová stránka se škodlivým kódem, stránka tahající z lidí peníze nebo zvyšující si uměle návštěvnost
- **Google+** - platí obdobná pravidla jako pro Facebook, zatím méně rozšířené
- **Twitter** – šíření adres stránek obsahujících škodlivý kód

Základní pravidlo – neklikat na cokoli, přemýšlet. I počítače vašich přátel mohou být napadeny škodlivým kódem, který na jejich FB profilu posílá příspěvky…

Na sociální sítě přistupujeme většinou přes internetový prohlížeč – tedy platí zásady zabezpečení prohlížeče (viz. dále)

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Antivirus a antispyware

Pokud nepoužíváme nějaký **placený antivirový program**, je vhodné použít **zdarma dostupné antivirové produkty.**

Pro domácí nekomerční použití jsou to například

- **Microsoft Security Essentials** – produkt Microsoftu, distribuovaný přes Microsoft Update. Nenáročný, dostačující, v češtině
- **Avast Free Antivirus** – produkt české firmy AVAST Software, velmi oblíbený, automatické aktualizace, mírně náročnější na systémové zdroje, nutná obnova bezplatné registrace po 1 roce
- **AVG Antivirus FREE** – další český produkt, také vhodný pro běžné použití
- **Panda Cloud Antivirus FREE** – antivir pracující na cloudové bázi, menší zátěž PC
- **Comodo Antivirus** – základní ochrana od firmy Comodo

Antiviry si většinou automaticky aktualizují své virové databáze, je třeba nechat tuto funkci povolenou!

Antispyware – software na odstranění a blokování spyware (programy, které odesílají data o uživateli třetí straně bez jeho vědomí)

- **Spybot Search & Destroy** – zdarma pro nekomerční účely, český překlad
- **Spyware Terminator** – zdarma i pro komerční účely, český překlad
- **Ad Aware SE Personal Edition** – zdarma pro nekomerční účely
- **Windows Defender** – standardní součást Windows Vista a vyšších verzí

Antispyware není většinou nutné používat stále, ale je vhodné občas nějaký nainstalovat a nechat proskenovat počítač.

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Přístupová hesla

Běžně využíváme mnoho různých internetových služeb – máme mnoho přístupových údajů

- Nebezpečné tendence – všude používat stejné a jednoduché heslo
- Známé služby čelí častým útokům hackerů s cílem ukrást přístupové údaje uživatelů (často úspěšně)
- Pokud mám všude stejný login a heslo, hacker najednou získá přístup do všech mých účtů!
- Zásady:
  - do důležitých služeb (přístupy do banky atd.) používat **unikátní přístupové údaje**
  - Jako přístupové údaje jsou často vyžadovány e-mail a heslo. **Nikdy nezadávat stejné heslo, jako máme do emailu!!** Při vyzrazení těchto údajů hackeři začnou využívat váš e-mail k šíření spamu a virů, hrozí zablokování účtu.
  - Pokud máme hesel mnoho, zvážit použití **softwarového správce hesel**

Správce hesel – užitečný pomocník pro bezpečnou práci s hesly

Je třeba si pamatovat pouze jedno hlavní heslo, ostatní hesla jsou bezpečně a přehledně uloženy v programu.

Mezi nejznámější software této kategorie patří:

- **KeePass Password Safe** – přehledný správce hesel, zdarma i pro komerční použití, existuje i verze pro mobilní telefony
- **LastPass** – doplněk pro internetové prohlížeče, předvyplní internetové formuláře, generuje hesla
- **Password Agent** – umí uchovat hesla a další informace, možnost instalace na USB klíčenku

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Zabezpečení domácí sítě

Vstupní branou do domácí sítě je často **domácí router**. Jeho kvalita a adekvátní zabezpečení zásadně ovlivňuje bezpečnost celé domácí sítě.

Problémem levných routerů bývá nedostupnost sw. aktualizací od výrobce a nekvalitní software – tyto routery bývají nebezpečné.

Základní pravidlo je **neponechávat** AP ve výchozím nastavení od výrobce!! Nastavit administrátorské heslo a zvolit vhodné zabezpečení Wi-Fi:

Existující formy zabezpečení domácích AP (Access point, bezdrátový router):
- Otevřená síť (bez zabezpečení) (nepoužívat ani omylem, kom. není šifrována)
- Šifrování WEP (zastaralé, dávno prolomeno)
- **Šifrování WPA-PSK nebo WPA2-PSK**
- Šifrování WPA(2) – Enterprise (Eduroam, podnikové)

Nekvalitně zabezpečený AP vystavuje nebezpečí vás!!

zdroj: www.dsl.cz

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Zabezpečení domácí sítě

V domácích podmínkách preferujeme zabezpečení **WPA2-PSK** v kombinaci se šifrováním **AES** (někdy označováno jako CCMP)

- nabízí rozumnou míru bezpečnosti
- je nutné zvolit **kvalitní PSK** (rozumně dlouhé a složité heslo)
  - doporučuje se **alespoň 13 znaků**
  - kombinace písmen a číslic
  - nepoužívat známá hesla (existují seznamy nejpoužívanějších hesel)
- **vypnout WPS (QSS)** (WiFi Protected Setup) na AP (prolomeno v prosinci 2011)
- Pokud má router přednastavené jméno sítě a náhodné heslo od dodavatele, je nutné jej změnit na vlastní, bezpečné (časté například u UPC)

Vhodné je nelitovat vyšší investice a koupit kvalitní router, který kromě vyšší rychlosti nabídne i kvalitní software a bezpečnostní aktualizace. Těchto routerů však není na trhu mnoho (Turris Omnia od CZ NIC).

Nekvalitně zabezpečený router vystavuje nebezpečí vás!!

zdroj: www.dsl.cz

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

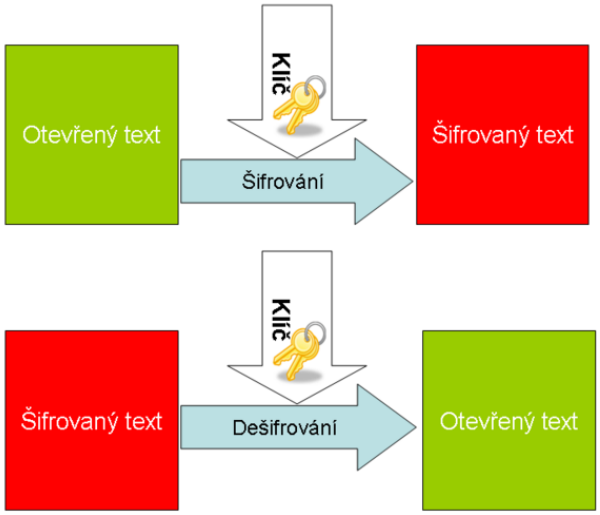
Nové nástrahy

Virus, který se při přihlášení „zaktivuje“, je v počítači. Jen čeká na to, až se uživatel přihlásí.

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Šifrování

- Změna podoby (zakódování) textu a dat do formy, která je bez znalosti dešifrovacího klíče (hesla) nečitelná



- Lze šifrovat např.
  - Dokumenty (7zip, winrar - symetricky)
  - Emaily (podpora emailových klientů, veřejný klíč adresáta)
  - Síťovou komunikaci (https, sftp, imaps, ssh)
  - Disky (truecrypt, realcrypt)
- Utajení obsahu komunikace a dokumentů

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Typy šifrování

- Symetrické šifrování
  - Jednodušší podoba, pro šifrování i dešifrování je použit jediný klíč - heslo
- Asymetrické šifrování
  - Klíč má dvě části, **soukromou** a **veřejnou**
    - Pokud mi chce někdo zaslat **šifrované** informace, zašifruje je pomocí **veřejné části klíče příjemce**.
    - Jediný, kdo dokáže tato data dešifrovat je vlastník privátní části klíče, tedy já

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Elektronický podpis

- **Využívá prvky asymetrického šifrování**
- Pokud chci nějaký text digitálně **podepsat**, stačí pro podepsání použít **soukromou** část klíče (provede emailový klient)
- Každý, kdo zná veřejnou část mého klíče (je odesílána automaticky s podepsaným emailem) pak může mnou digitálně podepsaný text
  - Přečíst
  - **Ověřit, zda jsem autorem/odesílatelem**
  - **Ověřit, zda nebyl text někým neoprávněně pozměněn**
- Podepsaný email/dokument **není šifrovaný!!**
  - Nemusíte nic „počítat“ nebo si pamatovat, provede emailový klient nebo jiná aplikace (pdf reader)
- **Není určen k podepisování archivních dokumentů s dlouhodobou platností**

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Digitální certifikát

- **Kvalifikovaný** x komerční certifikát
- Fyzicky = počítačový soubor od certifikační autority
- Vydává certifikační autorita
- Omezená platnost certifikátu (obvykle 1 rok)
- Obsahuje
  - Hlavička
  - **Údaje o subjektu** (uživatel, server)
    - Jméno
    - E-mailová adresa
    - Další identifikační údaje
  - Veřejný klíč certifikační autority
  - Podpis certifikační autority (hash veřejného klíče subjektu)
  - **Veřejný klíč subjektu**

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Komunikace se státní správou

- Ustanovení § 11 ZoEP výslovně stanoví, že k podepisování nebo označování dokumentu v podobě datové zprávy, jehož prostřednictvím se činí úkon vůči státu, územnímu samosprávnému celku, právnické osobě zřízené zákonem, zřízené nebo založené státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem, lze použít pouze uznávaný elektronický podpis, který je založen na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb..

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Komerční certifikát

Na rozdíl od kvalifikovaného certifikátu nepodléhá vydávání tzv. komerčních certifikátů komplexnější právní regulaci. Důvěryhodnost komerčního certifikátu neplyne ze zákona, nýbrž ze vzájemné dohody stran používajících daný komerční certifikát na tom, že příslušný komerční certifikát považují za důvěryhodný. S ohledem na povahu komerčních certifikátů se tyto používají při vzájemné komunikaci soukromoprávních subjektů.

Např. Komunikace zdravotnického zařízení se zdravotní pojišťovnou

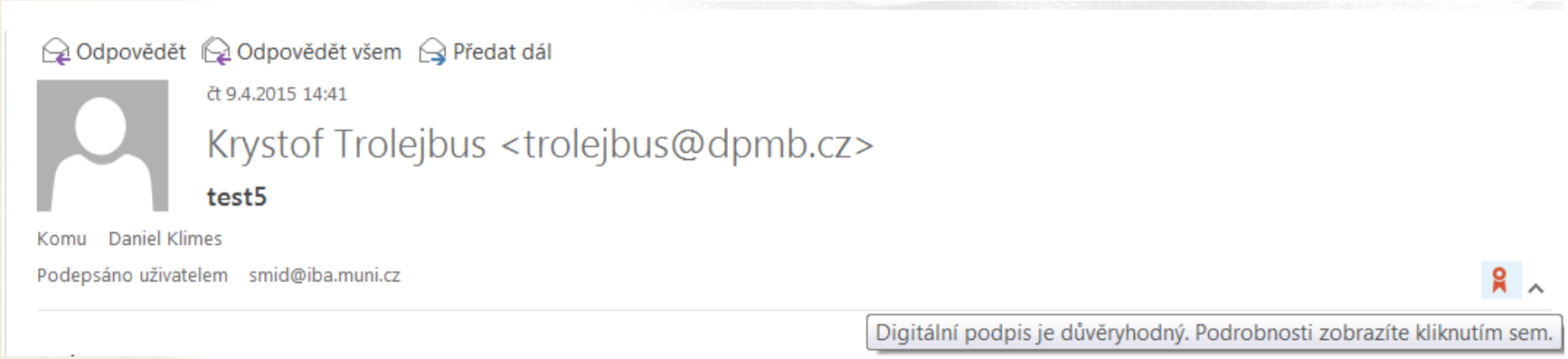
Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Elektronické podpisy v praxi

- **Chování aplikací**
  - **Když nám programy řeknou, že konkrétní podpis je platný, musíme si sami zjistit, zda jde o uznávaný podpis, či jde o podpis komerčním certifikátem.**
  - **A když nám naopak řeknou, že platnost podpisu nedokáží ověřit (tj. že platnost podpisu je neznámá), může to být způsobeno jen tím, že příslušný certifikát není umíst*ěn na správném místě v úložišti důvěryhodných certifikátů.***
  - ***Aplikace často neověřují revokaci certifikátů***
  - ***U emailu není součástí podpisu Předmět emailu ani zobrazená adresa odesílatele***
  - ***Neověřuje se shoda emailu odesílatele s emailem v certifikátu***
- http://TSL.gov.cz/certiq/
  - Tato aplikace hodnotí pouze to, zda jí předložený certifikát je či není kvalifikovaný.

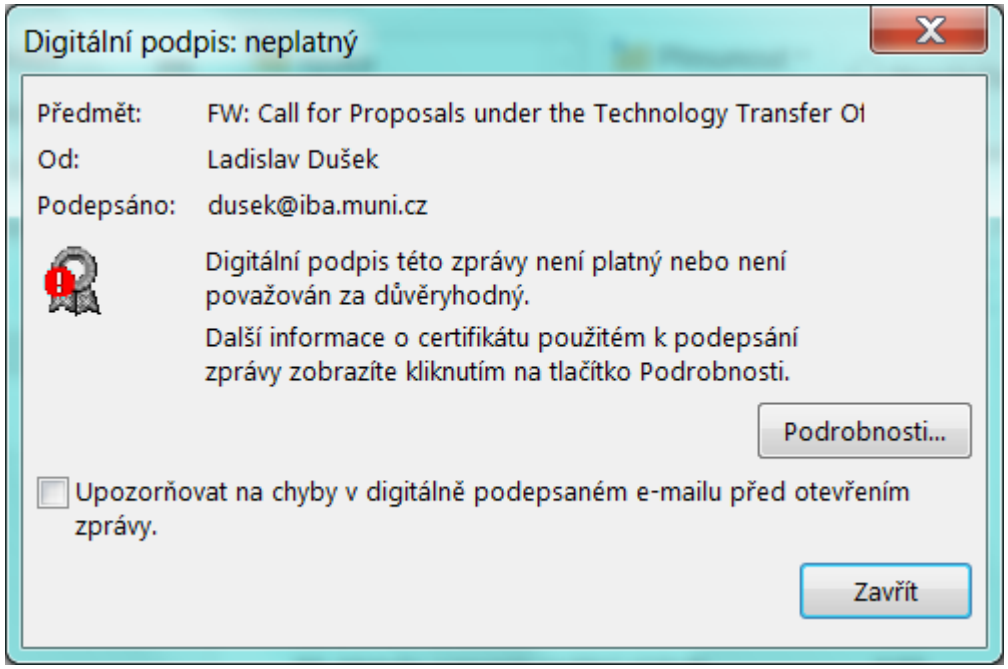
Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Problémy v aplikacích



Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Falešný poplach



MS Outlook 2010
Diakritika v názvech přiložených souborů v emailu

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

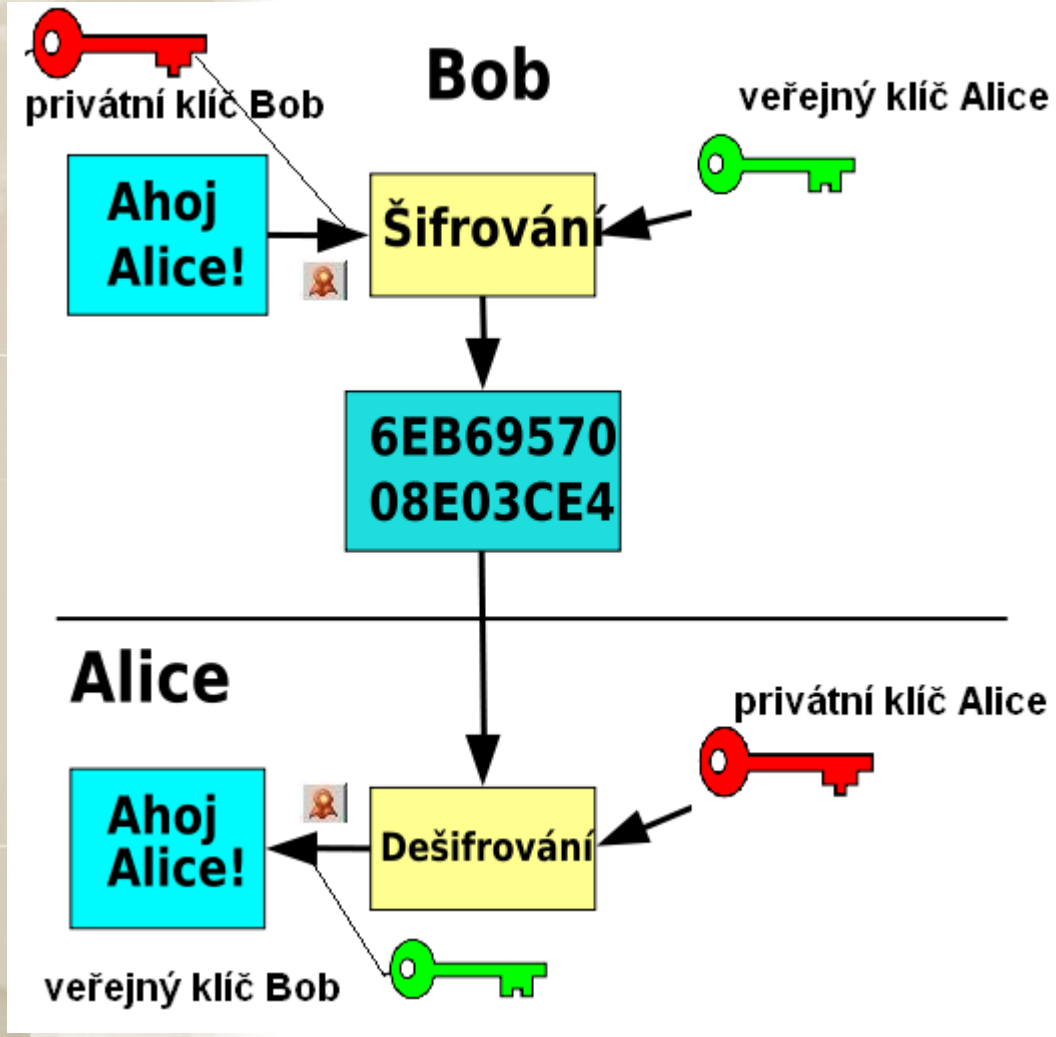
Digitální certifikát – jak získat prakticky

- Vydávají tzv. certifikační autority (např. Česká pošta)
  - Přihlášení do webové (případně stažení off-line) aplikace
  - Vlastnoruční vygenerování a uložení páru klíčů s heslem
  - Vyplnění žádosti
  - Návštěva pobočky s žádostí, ověření údajů
  - Zařazení veřejné části klíče certifikační autoritou do seznamu ověřených klíčů
  - Obdržení podepsaného certifikátu s veřejným klíčem a identifikací
  - http://www.linuxexpres.cz/praxe/elektronicky-podpis-za-par-minut
- Lze snadno integrovat do používaných emailových aplikací ve formě certifikátu = zaručený digitální (elektronický) podpis

- Na MU lze získat osobní digitální certifikát pro uživatele zdarma na adrese http://pki.cesnet.cz/cs/tcs-personal.html

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Šifrovaný email



- Bob **podepíše** zprávu Alici svým soukromým klíčem
- E-mail **zašifruje** veřejným klíčem Alice
- Alice **dešifruje** zprávu svým privátním klíčem
- **Ověří** Bobův podpis pomocí jeho veřejného klíče

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Další odkazy

- Kniha **Báječný svět elektronického podpisu (zdarma)** http://knihy.nic.cz/ (pdf)
- http://www.businessinfo.cz/cz/clanek/it-telekomunikace/elektronicky-podpis-a-jeho-vyuziti/1000473/2984/
- http://www.linuxexpres.cz/praxe/elektronicky-podpis-za-par-minut

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Datové schránky

- V komunikaci se státní správou lze použít ke stejnému účelu jako elektronický podpis
- Zřízení a komunikace se státní správou zdarma
- Není omezena platnost jako u certifikátů
- Uchovává dokumenty pouze 90 dnů
- Funguje jako „webový email“, místo emailové adresy je kód datové schránky
- Komunikace mimo orgány státní moci je zpoplatněna
- Zřízení na poště, jednoduchý formulář a OP

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Mobilní zařízení

- Obyčejné x chytré telefony
- OS telefonů a kompatibilita
- Internet v telefonu, tabletu
- Bezpečnost a rizika plynoucí z mobility

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Obyčejné x chytré telefony

- Chytrý telefon (smartphone) – obsahuje pokročilý operační systém, umožňuje instalaci a úpravy dalších programů, které dále rozšiřují možnosti telefonu.
- Příklady OS pro smartphony: Android, iOS, Windows Phone, Firefox OS, Tizen, Symbian, MeeGo
- Výhody: velké množství aplikací a tím i možností, co lze s telefonem dělat (kancelář, hry, čtení knih, internetové aplikace, navigace atd.)
- Nevýhody: typicky kratší výdrž baterie, často větší rozměry, různá bezpečnostní rizika (viry, vyzrazení soukromých informací), cena
- V roce 2013 se poprvé prodalo celosvětově více smartphonů než obyčejných telefonů.

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Tablety

- Dotyková zařízení, OS často stejný jako na smartphonech, mohou mít i telefonní funkce.
- Tvoří mezičlánek mezi smartphony a klasickými osobními počítači. Některé novější tablety jsou plnohodnotnými počítači se standardním OS
- Používané OS: Android, iOS, Linux, Windows
- Prodeje klesají, nastupují menší „phablety“

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

EVROPSKÁ UNIE

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Kompatibilita

- Různé OS mobilních zařízení NEJSOU mezi sebou kompatibilní (nelze spouštět programy pro Android např. na iPhonech)
- Nejvíce používané programy však bývají napsány pro nejpoužívanější OS (např. Skype existuje pro Android, iOS i Symbian nebo Windows)
- Z pohledu uživatele tedy absence kompatibility nepředstavuje většinou problém, je však třeba na to myslet při koupi nového zařízení – programy koupené pro iOS nelze instalovat na Android – nutné zakoupit znovu.

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

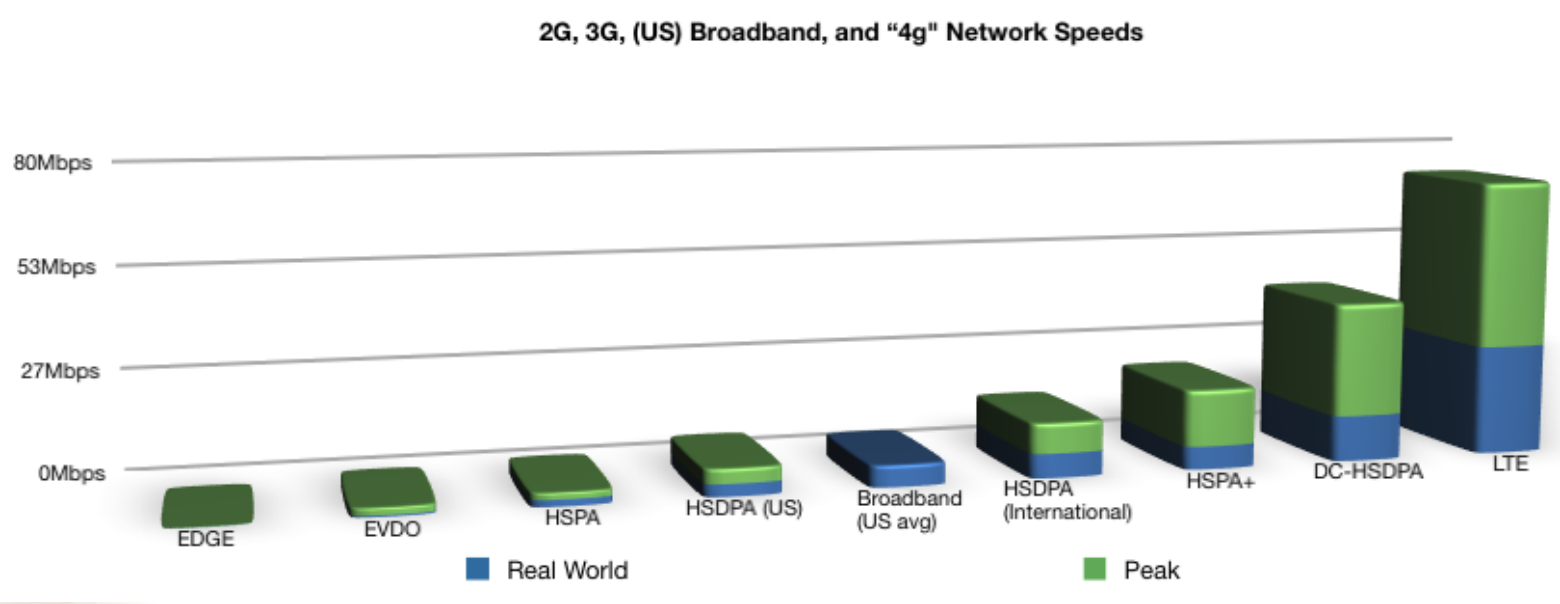
Internet v mobilních zařízeních

- Mobilní zařízení (smartphony a tablety) byla navržena pro práci s internetem. Přípojení je bezdrátové (WiFi, GSM). Obsahují zpravidla plnohodnotný internetový prohlížeč, emailový klient, lze doinstalovat řadu dalších programů (komunikátory, VoIP klienty, VPN, terminálové klienty, vzdálenou plochu atd.).
- Při připojení přes GSM může být limitujícím faktorem datový tarif. Po vyčerpání datového limitu se připojení zpomalí a práce s internetem se stává nepohodlná nebo nefunguje prakticky vůbec. Důležitý je správný výběr datového tarifu.

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Rychlost připojení přes GSM

- Mnoho termínů a zkratek – GPRS, EDGE, UMTS, HSPA, HSPA+, HSDPA, HSUPA, WCDMA, 3G, 4G, LTE….



Zdroj: tasel.wordpress.com

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Bezpečnost mobilních zařízení

- Hlavní problémy:
  - Operační systémy a jejich aktualizace

    Ze strany výrobců zařízení je aktualizace OS v reakci na nové bezpečnostní zranitelnosti často pomalá nebo žádná. Hlavně starší modely telefonů bývají často výrobcem ponechány bez aktualizací a tedy zranitelné vůči dávno známým chybám.
  - Nepozornost uživatele

    Při instalaci nových aplikací se OS vždy ptá uživatele, zda smí aplikaci udělit oprávnění k určitým činnostem v rámci systému (např. čtení/posílání SMS, přístup na internet atd.). Uživatelé by měli dávat pozor, jaká oprávnění aplikaci udělí a jaké aplikace instalují.

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Bezpečnost mobilních zařízení

– Data a přístupy v mobilních zařízeních

Zařízení často obsahují důvěrná data uživatelů nebo přístupy k různým službám (email, bankovnictví apod.). Často však nebývají adekvátně zabezpečena pro případ ztráty zařízení. **PIN ani odemčení gestem nestačí!!** Dostačující ochranou je **šifrování** celého zařízení včetně SD karty. Tuto možnost dnes nabízí většina současných modelů. Vhodná je i aktivace možnosti **vzdáleného vymazání** zařízení v případě ztráty.

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Test

- V ISu:
- Student – vybrat předmět UPS – Odpovědníky
- Vybrat odpovědník Test UPS –
  - Chci sestavit první sadu otázek
  - Na konci „Uložit a vyhodnotit“

- 20 otázek
- 90 minut – Nelze přerušit
- 5 pokusů provedení hodnocení
- U některých je více správných odpovědí (každá za bod)
- Odečítání bodů za chybnou odpověď
- Minimum pro splnění je 15 bodů

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
EVROPSKÁ UNIE
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ