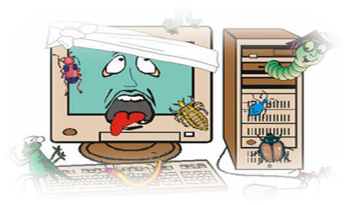
**Riziká IKT**

**Riziká sa delia do dvoch skupín:**

****  
**1. Sociálne riziká**  
a) strata súkromia na webe  
b) reklama na webových stránkach  
c) jednoduchý prístup k nevhodným informáciám  
d) dôveryhodnosť, pravdivosť informácií na webe, anonymita na webe  
e) kyberšikanovanie  
f) hry a gambling  
g) nevyžiadané e-maily – spamy, poplašné správy (hoax)  
  
**sociálne riziká informačných technológií** **=** nepriaznivé vplyvy, ktoré nepriaznivo vplývajú na sociálny vývoj jednotlivca  
  
**a. Strata súkromia na webe**  
- ide o zverejňovanie osobných údajov rozličným osobám na internete  
-tieto informácie sa dostavajú do veľkého informačného priestoru a hrozí riziko ich zneužitia a my postupne prichádzame o svoje súkromie, ktoré sa stáva pre iných ľahko dostupným  
  
**b. Reklama na webových stránkach**  
- môže byť rovnako pravdivá ako aj nepravdivá  
- môže spôsobiť narušenie sociálneho správania sa jednotlivcov  
  
**c. Jednoduchý prístup k nevhodným informáciám**  
- internet využívame hlavne na získavanie informácií, čo umožňuje pomerne ľahko získať aj informácie nevhodného charakteru, ktoré môžu negatívne vplývať na vývoj jedincov  
**- za nevhodný obsah pre deti sa považuje:**  
- nahota a sexualita, (pornografia)  
- násilie (násilné scény a videá, , sebapoškodzovanie, samovraždy, asistované samovraždy)  
- verbálna agresivita a vulgárne vyjadrovanie  
- prezentácia netolerancie, (rasizmus, nacionalizmus, xenofóbia, extrémizmus, náboženský fanatizmus, sekty,...)  
  
**d. Dôveryhodnosť, pravdivosť informácií na webe, anonymita na webe**  
  
**e. Kyberšikanovanie - formy kyberšikanovania:**  
- urážanie a nadávanie, obťažovanie, zastrašovanie, vyhrážanie a vydieranie, zverejnenie trápnych, intímnych alebo upravených fotografií alebo videí, šírenie osobných informácií alebo klebiet , vylúčenie zo skupiny, kybernetické prenasledovanie,...  
  
**f. Hry a gambling**  
**- riziká počítačových hier:**  
- jednostranné zameranie aktivít dieťaťa  
- riziko vzniku závislosti  
- nevhodné správanie a násilie v hrách  
- zdravotné riziká  
  
**g. Nevyžiadané e-maily – spamy, poplašné správy (hoax)**  
**- spam =**hromadne rozosielaná nevyžiadaná pošta  
**- ochrana:**ochrana osobných a kontaktných údajov, zamaskovanie emailovej adresy, ochrana počítača, nahlasovanie spamu, ochrana pred zasielaním reklamných správ  
  
**- hoax =**  pojmom hoax označujeme poplašné - podvodné správy



**2. Technologické riziká**

a) škodlivý softvér – malware (vírusy, trójske kone, počítačové červy, spyware, adware)  
b) počítačová kriminalita - prienik do počítačového systému, počítačové bankové krádeže (phishing, pharming, spoofing), dialery  
c) počítačová bezpečnosť (prevencia, detekcia, náprava) - zabezpečenie a spôsoby ochrany (heslá, šifrovanie, prístupové práva), elektronický podpis (súkromný a verejný kľúč), firewall

**a. Škodlivý softvér** – malware - všeobecné označenie škodlivého softvéru -  (vírusy, trójske kone, počítačové červy, spyware, adware)  
 **vírus** - je programový kód, ktorý sa bez vedomia užívateľa replikuje  
  
**Klasické počítačové vírusy:**  
- súborové vírusy  
- boot vírusy  
- multipartitné vírusy  
- stealth  
- polymorfné  
  
**adware =** softvér, ktorý automaticky zobrazuje, prehráva alebo sťahuje reklamný materiál do počítača po svojej inštalácii alebo pri používaní tohto softvéru, často ho používajú firmy  
  
**spyware =** softvér skrývajúci sa v počítači bez vedomia majiteľa, zbiera informácie o počítači, o surfovacích návykoch, heslách, emailových adresách a ďalšie osobné údaje  
  
**Detekovanie vírusov (škodlivých programov):**  
- antivírusový softvér je program, ktorého cieľom je identifikovať a eliminovať počítačové vírusy  
  
**Typy antivírusových programov:**  
****- jednoúčelové antivírusy  
- balík jednoúčelových antivírusov  
- komplexné antivírusové systémy  
  
**Príklady antivírusových systémov:**   
- ESET Smart Security  
- Avast  
- AVG  
- Norton AntiVirus  
- Kaspersky AntiVirus  
  
**b. Počítačová kriminalita**

**Druhy kriminality:**  
- útok na počítač, program, údaje, komunikačné zariadenie, neoprávnené užívanie počítača alebo komunikačného zariadenia,..  
  
Prienik do počítačového systému je druh počítačovej kriminality a znamená útok na počítačový systém. Človek zaoberajúci sa touto činnosťou sa v počítačovom slangu nazýva hacker.  
  
Hacker - počítačový expert, dobrý programátor, hľadajúci ezpečnostné diery v systémoch, za účelom zlepšenia ich bezpečnosti.   
  
Cracker - má technické schopnosti ako hacker, ktoré ale používa vo svoj prospech, väčšinou ilegálne. Patria sem aj takzvaní softvéroví, filmoví a hudobní piráti, lovci čísiel kreditných kariet a iní.   
   
Počítačové bankové krádeže:  
Phishing - falšovaná správa, ktorá vás pod určitou zámienkou nabáda ku zmene osobných údajov.  
  
Pharming  
Pharming (farmárčenie) má rovnaký efekt ako phishing, ale pracuje na inej báze. V tomto prípade je napadnutý buď internetový poskytovateľ, alebo užívateľský počítač, kde sú zmenené tzv. DNS záznamy.  
  
Dialery sú programy, ktoré menia telefonické pripojenie počítača, programy používajú za účelom prístupu na platené služby v Internete bez použitia kreditnej karty.

**3. Počítačová bezpečnosť**

**Cieľom počítačovej bezpečnosti je zabezpečiť:**  
ochranu pred neoprávneným manipulovaním so zariadeniami počítačového systému  
 bezpečnú komunikáciu a prenos dát  
bezpečné uloženie dát  
**prevencia** - hovorí o predchádzaní bezpečnostných rizík,  
**detekcia** - hovorí o spôsobe odhaľovania narušenej bezpečnosti,  
**náprava** - hovorí o odstraňovaní škôd a zamedzení opakovania v prípade zistenia narušenia bezpečnosti.

**﻿Základné pravidlá prevencie:**﻿  
- Zálohujte všetky svoje údaje  
- Kontrolujte, aké číslo pri pripájaní počítač vytáča, v prípade, že máte pochybnosti o vytočenom čísle, odpojte sa od internetu  
- Zabezpečte svoje bezdrôtové WiFi siete  
  
​  
**Firewall =** softvér alebo hardvér, ktorý blokuje vstup hackerov alebo škodlivého softvéru z internetu do počítača. Tiež umožňuje zastaviť odosielanie škodlivého softvéru z počítača do ďalších počítačov.  
  
**Elektronický podpis =**  súčasnosti je možné písomnosti posielať elektronickou formou. Aby bolo možné odoslaným dokumentom dôverovať, je potrebné zaručiť nepopierateľnosť a nepozmeniteľnosť dokumentov. Na tento účel slúži elektronický podpis,

