**Prevence – bezpečný internet**

**ZÁSADY**

* používat zabezpečený počítač, notebook, mobil (aktualizovat)
* instalovat pouze ověřené a známé programy (neotvírat programy, které neznám, podezřelé mailové adresy)
* nesdělovat žádné osobní informace  (jméno, příjmení, bydliště, škola, datum narození, rodné číslo, tel. číslo, heslo, PIN…)
* používat silné heslo (8 znaků – velká a malá písmena, číslo a nespecifický znak, nikomu ho nesdělovat)
* informace nepřeceňovat, nešířit dál (možná nepravdivost informací, neověřené inf., např. trestný čin šíření poplašné zprávy, pomluva…)
* komunikovat ve virtuálním světě  efektivně (netrávit všechen volný čas) a cíleně (jen s tím, s kým chci já a koho bezpečně znám)
* nevhodnou komunikaci vždy včas ukončit
* neposílat intimní fotografie, videa (trestný čin – do 18 let nemohu zaslat erotické foto)
* nepoužívat webovou kameru s neznámou osobou (možnost nahrávání)
* informace jsou ve virtuální komunikaci přístupné všem, šíří se, nejdou jednoduše smazat (žijí vlastním životem od chvíle jejich zveřejnění)
* chovat se vždy tak, abych svými činy neubližoval jinému a zároveň chránil sám sebe

**ŠIKANA**

* **kyberšikana**         odehrává se prostřednictvím virtuální komunikace
* **kyberstalking**       opakované obtěžování adresáta
* **kybergrooming**   vzbudit důvěru a přinutit k osobnímu setkání
* **flaming**                 urážlivé a zesměšňující napadání oběti
* **sexting**               zasílání textů a obrázků, videí se sexuální tematikou
* **phishing**               podvodné vylákání hesel a dalších přihlašovacích informací od adresáta, např. otevřením

nastraženého mailu od fiktivní banky, apod.

* **sniffing**                odposlech komunikace (hrozí i zcizení virtuální identity, vaším jménem může být páchána

trestná činnost)

* **hoax**                     přátel, adresy využívány k spamu…
* **hacking**               nabourávání se do cizího zabezpečeného systému
* **cracking**             odstranění technologické ochrany programu (porušování autorských práv)
* **skiming**               rizika spojená s platební kartou (kartu nedávat z ruky, chránit si pin)

**ZDRAVOTNÍ  RIZIKA**

* tělesný vývoj
* zdravotní obtíže
* psychické problémy
* netolismus  (závislost na virtuální realitě a ztráta reálného vnímání světa)
* omezenost smyslového vnímání
* nižší schopnost „čtení“ neverbální komunikace
* vyšší agresivita v on-line komunikaci
* snižování prahu bolesti
* zažívací a spánkové obtíže
* pokles fyzické kondice

**SOCIÁLNÍ RIZIKA**

* ztráta přátel a sociálních vazeb
* zkreslené vnímání reality
* využívání herních schémat při řešení běžných situací
* necitlivost a neochota

**DOPORUČENÍ - RODIČE**

* vzdělávat se a být informován v oblasti IT
* kontrola vyplnění profilu
* brát ohled na věk dítěte
* zabezpečit počítač – např. erotické stránky
* sledovat čas, který dítě tráví u počítače
* sledovat varovné signály a vnímat změny v chování (náladovost, výměna přátel, stravovací návyky, osamocenost…)
* vštěpovat dítěti zásady bezpečného internetu
* nácvik jednoduchých dovedností (jak reagovat, když…)
* komunikovat s dítětem
* informovat dítě o možnostech páchání trestných činů při virtuální komunikaci (dítě může být pachatel i oběť)

**TRESTNÉ ČINY**

* poškození a zneužití záznamu na nosiči informací
* mravnostní
* porušování autorských práv
* šikana (viz výše)

**hledat pomoc v případě potřeby (nezlehčovat situaci, nestydět se …)**

**POMOC**

rodičovská linka     606 021 021

linka bezpečí        116 111

 policie ČR 158

PPC Arkáda Písek

<http://sikana.pb.cz>

<http://www.linkabezpeci.cz>

<http://www.rodicovskalinka.cz>

[http://www.ditevohrozeni.cz](http://www.ditevohrozeni.cz/)

[http://www.horkalinka.cz](http://www.horkalinka.cz/)    hlášení nevhodného či nezákonného obsahu na internetu

**Naše škola je registrována v systému Nenech to být. Více informací na**[**https://nntb.cz**](https://www.nntb.cz/)

Mgr. Jan Adámek, ředitel školy