Prevencia

(verzia 3.1)

Projekt je spolufinancovaný Európskou Úniou v rámci komunitárneho programu Safer Internet *plus*.

Obsah

Pedofília, pornografia (Pedofília, pornografia, sexturizmus, zverejňovanie erotiky)

Pedofília

Pedofília je sexuálne správanie odchyľujúce sa od spoločenských noriem. Sexuálna deviácia (úchylka) predstavuje pohlavný styk a ukájanie sa s deťmi. Vyskytuje sa u ľudí, ktorí nie sú z rôznych príčin schopní adekvátneho sexuálneho partnerstva a styku.

Pedofília podľa Medzinárodnej klasifikácie chorôb F65.4 - je porucha voľby sexuálneho objektu. Ako sexuálny objekt sú uprednostňované deti, chlapci alebo dievčatá, prípadne aj chlapci, aj dievčatá. Prevažne ide o deti v prepubertálnom alebo skorom pubertálnom veku.

Dôsledky pre dieťa

Negatívne dôsledky sú vždy, keď sa dieťa stane obeťou nežiaduceho jednorazového alebo opakovaného sexuálneho aktu. Takýto zážitok prevažne zasahuje do všetkých základných sfér života dieťaťa, teda biologickej, psychologickej a sociálnej.

Dieťa nie je vývinovo telesne, fyziologicky ani psychicky pripravené na sexuálnu aktivitu, jej poznanie a prežívanie. Sexualita sa v somatickej, psychickej, ale i v sociálnej rovine vyvíja postupne a jej zrelosť má hoci individuálne, ale jasné hranice. Následky nežiaducej predčasnej sexuálnej skúsenosti vážne ohrozujú ďalší vývin dieťaťa. Môžu sa začať prejavovať známky strachu, depresie, strata sebaúcty, zníženie dôvery v dospelých. U mnohých detí sa objavuje častá chorobnosť, obmedzenie oblasti záujmov, apatia, zhoršenie školských výkonov, narušenie rovesníckych vzťahov až úplný únik do izolácie. V adolescencii a ranej dospelosti býva poznačená odmietaním opačného pohlavia, strachom z partnerstva a odporom k intímnemu životu. Vážne je tak narušená kvalita života detstva, dospievania a žiaľ i dospelosti.

Pomoc, podpora a spolupráca s odborníkmi

Nežiaduci a neakceptovateľný zážitok si samotné dieťa nevie ošetriť a spracovať samo a väčšinou sa do budúcna nevie brániť. Nevyhnutne potrebuje pomoc odborníka a dôslednú ochranu dospelých. Je dôležité konať rýchlo, nestresujúco a veľmi citlivo. Poskytnúť dieťaťu pocit bezpečia a uistiť ho, že na tom čo sa stalo nenesie žiadnu vinu.

Dôležité je čo najskôr vyhľadať lekára (pediater, gynekológ) a ohlásiť udalosť na polícii. Poskytnúť dieťaťu psychologickú krízovú intervenciu a následne zabezpečiť ďalšiu odbornú starostlivosť (terapiu, poradenstvo...). Neošetrené a nespracované zážitky často sprevádzajú človeka po celý život.

Pornografia

Pornografia je prezentácia sexu a sexuálnych aktivít, ktorá sa odkláňa od spoločensky akceptovateľnej morálky. Najčastejšie sa prezentuje vo forme fotografií, pornografických filmov a v literárnom

prevedení. Z hľadiska etiky a estetiky sú spracovávané v škále od jemnej erotiky až po tvrdé, vulgárne až patologické sexuálne praktiky. Dnes sa možno najčastejšie stretnúť s časopiseckou pornografickou produkciou a s porno kinematografiou. Masívnym zdrojom ponuky sú elektronické média hlavne TV a internet. Dostupnosť oboch je aj pre deti bez náročnejších prekážok. V súčasnosti sa internet považuje za najsilnejšie médium v rámci pornografie.

Výrazne ohrozujúco pre deti a mládež môžu pôsobiť pornografické produkcie s absenciou emocionálnej výrazovosti, s prvkami agresivity, sadistickými a masochistickými technikami, pornografia homosexuálnych a lesbických párov a tiež mnohé patologické zvrátenosti (pedofília, zoofília...).

Za zvlášť nebezpečnú je považovaná detská pornografia ako jedna z najzávažnejších foriem pohlavného vykorisťovania.

Dôsledky pre dieťa

Súčasťou jednotlivých vývinových štádií človeka je aj proces sexuálneho dozrievania v postupnej biologickej a psychologickej rovine. Harmonický vývin vedie k prirodzenej sexualite ako súčasti života človeka.

Akcelerácia vývinu sexuality prostredníctvom rôznych stimulov ako je aj častý kontakt s pornografiou môže posunúť dieťa, pubescenta, ale i adolescenta do neprirodzeného postoja k sexualite, pretože neboli na toto poznanie ešte pripravení. Hlavne mladšie deti bez nedostatku informácií a prirodzeného neporozumenia môžu následne prežívať strach, hnus, a tak i odpor k sexu ale i naopak, takéto poznanie môže vyvolávať ďalšiu zvedavosť a zdraviu nebezpečné experimentovanie.

Časté využívanie pornografie (časopisy, internetové porno stránky) na sexuálne uspokojenie môže mať za následok znížený záujem o reálne partnerstvo. Dochádza k úniku do virtuálneho sveta a v ňom do ilúzií o svojej všemocnosti.

Pomoc, podpora a spolupráca s odborníkmi

Dieťa alebo mladý človek, ktorý sa stane obeťou pornografického pôsobenia, by mal vyhľadať odborného lekára sexuológa a tiež odborníka z oblasti klinickej alebo poradenskej psychológie. Svoj problém môže konzultovať aj na špecializovaných linkách pomoci.

Sexturizmus

Sexturizmus je známy najmä v afrických a ázijských krajinách. Vo východnej Európe nedosahuje takú organizovanosť ani rozmery. Napriek tomu sa s ním stretávame aj na Slovensku. Zo skúseností vieme, že s obeťou sa väčšinou staršia osoba kontaktuje cez internet. Obeť je v niektorých prípadoch využitá aj pri vyhľadaní hotela, v ktorom sa potom obaja stretnú. Ohrozenejšie sú najmä dievčatá.

Niektoré krajiny robia praktické kroky na odstrašenie tých, ktorí by sa chceli angažovať v sexturizme, ako napríklad premietanie filmov v lietadlách, rozdávanie letáčikov turistom pri odchode z lietadla alebo v hoteloch o sexuálnom zneužívaní detí.

Slovenská legislatíva:

- Každý, kto využije, získa, ponúkne alebo inak zneužije dieťa na výrobu detskej pornografie alebo umožní takéto jeho zneužitie, či inak sa podieľa na takejto výrobe, v najzávažnejších prípadoch sa potrestá odňatím slobody až na 20 rokov!
- Každý, kto rozmnožuje, prepravuje, zadovažuje, sprístupňuje alebo inak rozširuje detskú pornografiu, sa potrestá odňatím slobody až na 12 rokov!
- Každý, kto prechováva detskú pornografiu, sa potrestá odňatím slobody až na 2 roky!
- Sex s osobou mladšou ako 15 rokov je na Slovensku považovaný za trestný čin! V najzávažnejších prípadoch sa trestá odňatím slobody až na 20 rokov!
- Sex s osobou mladšou ako 18 rokov je považovaný za trestný čin vtedy, ak je takáto osoba zneužitá napríklad rodičom, či opatrovníkom, alebo je jej za to zaplatené, alebo k takémuto konaniu bola donútená z poslušnosti, nátlakom alebo hrozbou! Všetky tieto menované činy sa trestajú odňatím slobody až na 8 rokov!

Zverejňovanie erotiky

Zverejňovanie akýchkoľvek fotografií alebo videí na internete alebo cez mobil môže byť nebezpečné najmä v prípadoch, keď sa dostanú k nepravým ľuďom. Fotografie nemusia byť ani výslovne erotické stačí ak osoba je na nich v plavkách, v spodnej bielizni, má odhalené časti tela alebo pôsobí eroticky. Fotoalbumy, videoalbumy na internete alebo v mobiloch nie sú bezpečné, aj keď sa píše, že sú „súkromné“, „zamknuté“ a podobne. Obsah sa môže dostať na voľne dostupné miesta a vaše fotografie, videá uvidia všetci: rodičia, učitelia, spolužiaci ale aj osoby, ktoré vám môžu ublížiť. Fotografie z detstva môžu byť zneužité pedofilom, fotografie z rodinných osláv, dovoleniek prezradia rodinné, sociálne zázemie. Fotografie alebo videá, na ktorých je váš byt, dom, škola môžu identifikovať adresy vášho pobytu. Ostatné osobné fotografie zverejňujte v malom rozlíšení (max 200x200 pixlov/bodov), tak sťažíte ich zneužitie. Fotografie alebo videá môžu byť zneužité aj za účelom poníženia, zahanbenia, zastrašenia alebo vydierania.

Legislatíva

Zákon č. 300/2005 Z.z. – Trestný zákon v znení neskorších predpisov

- *§179* Obchodovanie s ľuďmi - Kto s použitím podvodného konania, ľsti, obmedzovania osobnej slobody, násilia, hrozby násilia, hrozby, inej ťažkej ujmy alebo iných foriem donucovania, prijatia alebo poskytnutia peňažného plnenia či iných výhod na dosiahnutie súhlasu osoby, na ktorú je iná osoba odkázaná alebo zneužitia svojho postavenia alebo zneužitia bezbrannosti alebo inak zraniteľného postavenia zláka, prepraví, prechováva, odovzdá alebo prevezme iného, hoci aj s jeho súhlasom, na účel jeho prostitúcie alebo inej formy sexuálneho vykorisťovania vrátane pornografie, nútenej práce či nútenej služby, otroctva alebo praktík podobných otroctvu, nevoľníctva, odoberania orgánov, tkanív či bunky alebo iných foriem vykorisťovania alebo kto zláka, prepraví, prechováva, odovzdá alebo prevezme osobu mladšiu ako osemnásť rokov, hoci aj s jej súhlasom, na účel jej prostitúcie alebo inej formy sexuálneho vykorisťovania vrátane pornografie, nútenej práce či nútenej

služby, otroctva alebo praktík podobných otroctvu, nevoľníctva, odoberania orgánov, tkanív či bunky alebo iných foriem vykorisťovania.

- *§180* Obchodovanie s deťmi - Kto v rozpore so všeobecne záväzným právnym predpisom zverí do moci iného dieťa na účel adopcie.
- *§181* Kto za odmenu zverí dieťa do moci iného na účel jeho využívania na detskú prácu alebo na iný účel,
- *§187* Zavlečenie do cudziny - Kto iného zavlečie do cudziny.
- *§199* Znásilnenie - Kto násilím alebo hrozbou bezprostredného násilia donúti ženu k súloži alebo kto na taký čin zneužije jej bezbrannosť.
- *§200* Sexuálne násilie - Kto násilím alebo hrozbou bezprostredného násilia donúti iného k orálnemu styku, análnemu styku alebo k iným sexuálnym praktikám alebo kto na taký čin zneužije jeho bezbrannosť.
- *§201* Sexuálne zneužívanie - Kto vykoná súlož s osobou mladšou ako pätnásť rokov alebo kto takú osobu iným spôsobom sexuálne zneužije.
- *§202* Kto osobu mladšiu ako osemnásť rokov pohne k mimomanželskej súloži alebo ju iným spôsobom sexuálne zneužije, ak takou osobou je osoba zverená do jeho starostlivosti alebo pod jeho dozor alebo odkázaná osoba.
- *§367* Kupliarstvo - Kto iného zjedná, pohne, zvedie, využije, získa alebo ponúkne na vykonávanie prostitúcie, alebo kto koristí z prostitúcie vykonávanej iným, alebo umožní jej vykonávanie.
- *§368* Výroba detskej pornografie - Kto využije, získa, ponúkne alebo inak zneužije dieťa na výrobu detskej pornografie alebo umožní také jeho zneužitie, alebo sa inak podieľa na takejto výrobe.
- *§369* Rozširovanie detskej pornografie- Kto rozmnožuje, prepravuje, zadovažuje, sprístupňuje alebo inak rozširuje detskú pornografiu.
- *§370* Prechovávanie detskej pornografie - Kto prechováva detskú pornografiu.
- *§371* Ohrozovanie mravnosti - Kto vyrába, kupuje, dováža alebo si inak zadovažuje a následne predáva, požičiava alebo inak uvádza do obehu, rozširuje, robí verejne prístupnými alebo zverejňuje pornografiu, nosiče zvuku alebo obrazu, zobrazenia alebo iné predmety ohrozujúce mravnosť, v ktorých sa prejavuje neúcta k človeku a násilie alebo ktoré zobrazujú sexuálny styk so zvieraťom alebo iné sexuálne patologické praktiky.
- *§372* Kto pornografiu ponúka, prenecháva alebo predáva osobe mladšej ako osemnásť rokov alebo
  na mieste, ktoré je osobám mladším ako osemnásť rokov prístupné, vystavuje alebo inak sprístupňuje.

Dohovor o právach dieťaťa

Článok 34 - Sexuálne zneužívanie

Štáty, ktoré sú zmluvnými stranami tohto Dohovoru, sa zaväzujú chrániť dieťa pred všetkými formami sexuálneho vykorisťovania a sexuálneho zneužívania. Za týmto účelom prijímajú predovšetkým nevyhnutné vnútroštátne, dvojstranné a mnohostranné opatrenia, aby zabránili:

- zvádzaniu alebo donucovaniu detí k akejkoľvek nezákonnej sexuálnej činnosti,
- vykorisťovaniu a zneužívaniu detí na prostitúciu alebo na iné nezákonné sexuálne praktiky,
- vykorisťovaniu a zneužívaniu detí pre pornografiu a pornografické materiály,
- štát musí chrániť dieťa pred sexuálnym vykorisťovaním a zneužívaním, vrátane prostitúcie a pornografie.

Informácie na internete

www.wikipedia.sk – Online encyklopédia

Prevencia

- **Pedofil sa často snaží, aby si dieťa zaplo webkameru (odfotilo sa), on sa mu ale cez webkameru neukáže.** Ak sa to deťom prihodí alebo majú inú nepríjemnú skúsenosť z používania webkamery, nech to oznámia rodičom. Pre najmenšie deti používanie webkamery bez prítomnosti rodiča zakážte. Vysvetlite, že keď už s niekým dieťa komunikuje cez webkameru, musia sa vidieť navzájom, aby si bolo isté, kto je v skutočnosti na druhej strane.
- **Všímajte si správanie, zvyky, pocity a prejavy dieťaťa.** Následky nežiaducej predčasnej sexuálnej skúsenosti sa môžu prejavovať známkami strachu, depresie, stratou sebaúcty, znížením dôvery v dospelých. U mnohých detí sa objavuje častá chorobnosť, obmedzenie oblasti záujmov, apatia, zhoršenie školských výkonov, narušenie rovesníckych vzťahov až úplný únik do izolácie. V adolescencii a rannej dospelosti býva sexualita poznačená odmietaním opačného pohlavia, strach z partnerstva a odpor k intímnemu životu.
- **Prezývku (nickname) si vytvorte takú, aby z nej nebolo na prvý pohľad jasné, že užívateľ je dieťa, alebo akého je pohlavia.** To isté platí o pomenovaní mobilného telefónu.
- **Nedávajte na internet alebo cez mobil žiadne fotografie, videá, na ktorých ste v plavkách, v spodnej bielizni, máte odhalené časti tela alebo pôsobíte eroticky.** Fotoalbumy, videoalbumy na internete alebo v mobiloch nie sú bezpečné, aj keď sa píše, že sú „súkromné“, „zamknuté“ a podobne. Obsah sa môže dostať na voľne dostupné miesta a vaše fotografie, videá uvidia všetci: rodičia, učitelia, spolužiaci ale aj osoby, ktoré vám môžu ublížiť. Fotografie z detstva môžu byť zneužité pedofilom, fotografie z rodinných osláv, dovoleniek prezradia rodinné, sociálne zázemie. Fotografie alebo videá, na ktorých je váš byt, dom, škola môžu identifikovať adresy vášho pobytu. Osobné fotografie zverejňujte v malom rozlíšení (max 200x200 pixlov/bodov), tak sťažíte ich zneužitie. Fotografie alebo videá môžu byť zneužité aj za účelom poníženie, zahanbenie, zastrašenie alebo vydierania.
- **Odtabuizujte témy sex a sexualita v rodinnom ako i školskom prostredí.** Rozprávajte sa o tom s dieťaťom a vysvetlite z rôznych hľadísk danú tému a všetky nebezpečenstvá. Zaujímajte sa o svoje dieťa a jeho vzťah k druhému pohlaviu a k sexualite. Informujte sa a kontrolujte aké stránky dieťa navštevuje na internete. Nementorujte, rozprávajte sa. V školách by sa mali podporovať diskusie o význame partnerstva a sexuality ako súčasti vzťahu.
- **Internet môže byť nebezpečný.** Oboznámte dieťa o tom, že tak ako v bežnom živote aj na internete alebo pri mobilnej komunikácii, číha nebezpečenstvo. Môžete použiť príklad s elektrinou. Je to rovnako ako internet potrebná a nenahraditeľná vec, ale je to rovnako ako internet pri nezodpovednom používaní nebezpečná vec pre vaše zdravie alebo dokonca pre život. Pri internete na rozdiel od elektriny stále chýba takáto skúsenosť, či skôr osveta.
- **Nikdy neviete, kto je v skutočnosti na druhej strane internetu alebo mobilu.** Na druhej strane môže byť človek, ktorý klame o svojom veku, pohlaví, záujmoch, vzhľade a podobne. Takýto ľudia chcú deťom veľmi ublížiť a sú to:
    - pedofili...
    - ľudia, ktorí chcú fotografie a videá detí...
    - navádzajú na užívanie drog...
    - navádzajú na šikanovanie, alebo šikanujú deti...
    - nenávidia určité skupiny ľudí...
    - správajú sa agresívne, násilne...
    - chcú sa s deťmi tajne stretnúť, ublížiť im, uniesť ich...
    - získať osobné údaje o dieťati, jeho rodine, kamarátoch...
    - chcú oklamať, podviesť dieťa...
    - návádzajú na sebapoškodzovanie...
- **Nie je bezpečné dávať na internet alebo cez mobil svoje osobné údaje.** Vysvetlite deťom, čo sú to osobné údaje a prečo je nebezpečné zverejňovať svoje pravé meno a priezvisko, svoju fotografiu, video, vek, emailovú adresu, telefónne číslo, adresu domov, adresu školy, majetkové pomery, prístupové mená a heslá alebo iné osobné údaje (záľuby, opis vzhľadu, povahy, znalosti, zručnosti, vzdelanie, obľúbené veci, túžby...).
- V prípade, že je nevyhnutné takéto údaje poskytnúť, musia o tom vedieť rodičia alebo učitelia.

- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- **S nikým, s kým sa dieťa zoznámilo iba cez internet alebo mobil, sa nesmie stretávať samé osobne.** Tak ako v reálnom živote nechodia deti na stretnutie s neznámou osobou bez sprievodu niekoho ďalšieho, najlepšie rodiča, alebo aspoň súrodenca, kamaráta, tak aj na stretnutie s neznámou osobou, s ktorou sa dieťa zoznámilo iba cez internet alebo mobil, je stretnutie veľmi nebezpečné. Ak už dieťa ide na stretnutie, tak vždy aspoň s kamarátom. Rodičom by malo oznámiť na aké stretnutie ide, za kým ide, kde a kedy sa plánuje vrátiť. Stretnutie by malo byť na verejnom mieste, kde je veľa ľudí. Znakom bezpečnejšieho stretnutia je, že tomu, čo pozýva, nevadí, že dieťa príde s rodičom alebo inou dospelou osobou. Ak mu to vadí, ten človek nemá čisté úmysly.
- **Buďte podozrievavý voči človeku, ktorý dieťa presviedča, aby zatajovalo svoje internetové kamarátstvo pred rodičmi, alebo vystupuje ako tínedžer, ale nevie väčšinu odpovedí na otázky, ktoré bežne rovesníci poznajú.** Takýto človek chce deťom ublížiť, a preto klame a navádza, aby zatajili pozvanie na stretnutie s ním, aby si zmazali históriu četu, jeho emaily, sms, mms správy, a podobne.
- **Použitie lokalizačných služieb mobilného telefónu dieťaťa neznámou osobou je nebezpečné**. Vďaka lokalizácii môže ktorákoľvek osoba vyhľadať miesto pobytu dieťaťa, ak mu to samo z nevedomosti umožní.
- **Bluetooth spojenie cez mobilný telefón dieťaťa s neznámou osobou je nebezpečné**. Pomenujte mobilný telefón dieťaťa tak, aby z neho nebolo hneď jasné, že sa jedná o dieťa.
- **Nie všetko, čo je na internete, je pravda.** Vysvetlite deťom, nech neveria všetkému čo nájdu na internete. Informácie si je potrebné porovnať z viacerých zdrojov a v prípade nejasností sa poradiť s rodičmi alebo učiteľmi v škole.
- **Ak dieťa na internete alebo cez mobil niečo vyľaká, našlo niečo škaredé, desivé, niečo z čoho sa cíti trápne, zraňuje ho to alebo ohrozuje, vysvetlite mu, že to nie je jeho chyba.**
- **Ak sa dieťa cíti nepohodlne alebo trápne pri online konverzácii, má právo ju okamžite prerušiť a odísť z četovej miestnosti**. Ak sa pritom snažil človek zaviesť tému do sexuálnej oblasti nech dieťa o tom povie rodičom, alebo v škole učiteľom.
- **Váš domáci počítač (alebo hraciu konzolu) postavte do obývacej izby alebo na iné spoločné prístupové miesto v byte.** Najlepšie tak, aby rodič mal vždy výhľad na monitor**.** Nedávajte počítač do detských izieb. Majte dobrý prehľad o všetkých ďalších počítačoch, ktoré sú deťom prístupné.
- **Stanovte medzi deťmi a rodičmi jasné pravidlá pre používanie internetu**. Urobte si rozvrh na dni a presný čas, kedy má dieťa povolenie stráviť čas na internete, najlepšie v čase vašej prítomnosti. Podpísanú zmluvu vystavte v blízkosti počítača na viditeľnom mieste. Nezabudnite, ak si s vaším dieťaťom vytvoríte pravidlá o používaní internetu, stanovte si práva a povinnosti pre obe strany. Pravidla, by sa mali pravidelne aktualizovať. Vzor takejto „rodinnej zmluvy" nájdete na stránkach Zodpovedne.sk.
- **Najmenšie deti by nemali používať četovacie miestnosti bez moderátora, v ktorých môže byť dieťa najviac ohrozené.**
- **Vytvorte medzi dieťaťom a rodičom vzťah vzájomnej dôvery.** Majte prehľad o prezývkach (nickname) vašich detí, ktoré používajú na internete. Buďte opatrný, nebuďte dotieravý pri kontrole dieťaťa, vzájomná dôvera je veľmi dôležitá. Prílišná kontrola by mohla dieťa dohnať ku skrývaniu a zatajovaniu činností. Netrestajte dieťa za to, čo nie je jeho chyba, môže vám prestať dôverovať a mať strach a neistotu pri zdôverovaní sa s nejakým problémom. Je potrebné sa s deťmi veľa rozprávať, upozorniť ich na rôzne nebezpečenstvá, zaujímať sa a vedieť kde a ako trávia voľný čas, s kým telefonujú, emailujú, četujú, s kým sa stretávajú. Menšie deti si vyžadujú pravidelnú kontrolu. Ponúknite deťom adekvátne, zmysluplné a zaujímavé mimoškolské aktivity. Všímajte si viac svoje okolie. Nebuďte ľahostajní ani k cudzím deťom.
- **Dôveruj, ale preveruj.** Nie vždy sa dieťa zdôveruje rodičom, preto nezabudnite sledovať jeho nálady, zvyky, zmeny nálad a správanie, ktoré môže byť kľúčom k objasneniu príčiny. Kontrolujte, ktoré stránky navštevuje, s kým si píše emaily, hovorte s ním s kým a o čom si píše. Ak dieťa chodí na stránky s nevhodným obsahom, je možné pomocou filtra zakázať prístup na tieto stránky. Ak nechcete aby dieťa bolo vystavené riziku pri otváraní emailov, nainštalujte si program, ktorý povolí otvorenie emailu iba od známych ľudí zo zoznamu,

adresáru. Pokiaľ to uznáte za vhodné, používajte monitorovacie nástroje, ktoré vám umožnia získať prehľad o chovaní vášho dieťaťa na internete.

- **Dbajte na to, aby dieťa hralo iba hry, ktoré sú určené správnej vekovej skupine a s vhodným obsahom.** Počítačové hry alebo hracie konzoly sú zatriedené podľa veku hráčov do skupín 3+, 4+, 6+, 7+, 12+, 16+, 18+. Obsahové ohrozenia hráčov sa delia na skupiny:
    - hra obsahuje vulgarizmy,
    - hra obsahuje diskriminačné prvky tj. obsahuje zobrazenia alebo materiály, ktoré môžu nabádať k diskriminácii,
    - hra znázorňuje užívanie drog,
    - hra môže pôsobiť na dieťa desivo až hrozivo,
    - hra znázorňuje nahotu alebo iné sexuálne správanie,
    - hra zobrazuje násilie,
    - hra, ktorá nabáda alebo vyučuje hazardné hry.
- **Pri výbere školy, mládežníckeho klubu, centra voľného času, letných táborov a podobne sa informujte, aké majú jednotlivé organizácie vypracované programy prevencie voči e-ohrozeniam.** Medzi e-ohrozenia patria:
    - Pedofília, pornografia (Pedofília, pornografia, sexturizmus, zverejňovanie erotiky...)
    - Závislosti (Drogy, anorexia, bulímia, sebapoškodzovanie, sekty, závislosť od internetu, mobilov, esemesiek, počítačových hier, návody na samovraždy, emo...),
    - Šikanovanie (Bullying, elektronické šikanovanie, zastrašovanie, ponižovanie, zosmiešňovanie, ohováranie, nadávanie, happy slapping...),
    - Diskriminácia (Xenofóbia, rasizmus, extréministické hnutia, totalitný režim...),
    - Násilie (Agresivita, klubové chuligánstvo, terorizmus, flaming, hate speech...),
    - Stretnutie s neznámou osobou (Internetové známosti, grooming, obchodovanie s ľuďmi...),
    - Poskytovanie osobných údajov (Poskytovanie kontaktných, osobných údajov, majetkové pomery, phishing...),
    - Internetové podvody (Počítačová kriminalita, falšovanie počítačových údajov, porušenia autorských a príbuzných práv...).
- **Neustále sa informujte, vzdelávajte, zlepšujte svoje zručnosti na internete, v mobilnej komunikácii a nových technológiách.** Súčasná generácia vyrastá s internetom a ich znalosti (aj jazykové), zručnosti sú vo väčšine prípadov lepšie ako u ich rodičov. Preto je potrebné snažiť sa s nimi aspoň držať krok a tak chrániť deti, seba a celú rodinu. Sledujte odbornú tlač, prípadne internetové stránky zaoberajúce sa danou problematikou.
- **Zvyšujte povedomie, šírte osvetu o zodpovednom používaní internetu, mobilu a nových technológií.**
- **Komunikujte s inými rodičmi, učiteľmi**, vymieňajte si informácie a poznatky.
- **Správajte sa Zodpovedne.sk!** Na internete alebo pri mobilnej komunikácii sa správajte tak ako v ozajstnom živote. Vysvetlite deťom, aby, neurobili niečo, čo by v skutočnom živote nespravili. Pravidlá slušného správania sa na internete nazývajú netiketa.

Závislosti (Drogy, anorexia, bulímia, sebapoškodzovanie, sekty, emo, závislosť od internetu, mobilov, esemesiek, počítačových hier, návody na samovraždy)

Drogy

Internet zasiahol do veľkej miery aj do takej oblasti akou sú drogy a ich výroba, predaj či užívanie. Množstvo webových stránok sa venuje problematike drog, popisovaniu ich účinkov, škodlivých dôsledkov, prevencie a pomoci v prípade závislosti.

Okrem toho je internet priestorom, kde funguje ilegálny obchod – na stránkach sa ponúkajú na predaj nezákonné drogy, lieky a ich zákonné alternatívy, zároveň sa propaguje ich užívanie. S využitím potenciálu internetu, jeho dosahu na množstvo ľudí majú obchodníci s drogami čoraz viac možností ako online šíriť nové informácie, postupy brania drog a tým zväčšovať sieť konzumentov.

Užívatelia majú prostredníctvom internetu ľahký prístup k:

- návodom na užívanie jednotlivých druhov drog,
- novým trendom, novinkám a „vychytávkam“,
- miestam alebo osobám predávajúcim marihuanu, kokaín, klubové drogy, alkohol, cigarety,
- návodom na prípravu niektorých syntetických drog,
- radám, ktoré legálne lieky alebo prostriedky sa dajú užiť ako drogy a ako ich kombinovať,
- k príslušenstvu, ktoré je nevyhnutné pre užívanie drog.

Okrem informácií, ktoré môžu nabádať alebo uľahčovať užívanie drog sú prístupné aj tie, ktoré sú užitočné pri hľadaní pomoci a liečenia:

- kontakty na liečebné centrá, psychológov,
- informácie v rámci prevencie,
- rady ako rozpoznať u rodinných príslušníkov užívanie drog a tým predísť závislosti,
- linky a kontakty na komunity, skupiny rodičov, abstinentov, ktoré môžu znamenať významnú pomoc v krízovej situácii,
- kontakty na voľnočasové centrá, športové a umelecké kluby, ktorých navštevovanie vypĺňa zmysluplne čas deťom a mladým ľuďom, čím predchádzajú pokušeniu.

Prostredníctvom internetu sa dajú tiež objednávať lieky, ide o rôzne upokojujúce prášky, tabletky na spanie, steroidy, viagru. Ľudia sa buď hanbia ísť si tieto lieky zakúpiť osobne, alebo im už lekár legálne lieky nepredpíše a objednávajú si preto rôzne náhrady, na ktoré nie je nutný predpis. Existuje tu však výrazné riziko poškodenia zdravia, keďže málokedy sa dá obsah takto zakúpených tabletiek overiť a často ide o zdraviu škodlivé prísady pridávané do napodobenín originálov. Zároveň je veľmi ťažké odhadnúť dávkovanie, keďže sa neudáva presné množstvo prísad, čím hrozí predávkovanie alebo otrava.

Aj mladí ľudia si môžu zakúpiť lieky či drogy ľahko s kreditnou kartou, podobne ako knihy či CD. Existuje množstvo stránok, ktoré ponúkajú predaj liekov na predpis aj bez toho, aby trvali na predpise od lekára. (sedatíva, lieky proti bolesti, na spanie...) Tieto sú potom doručené zákazníkovi v neoznačenom balíčku. Je preto na rodičoch, aby si všímali, či má ich dieťa prístup ku kreditným kartám alebo či navštevuje podobné stránky.

Príznaky, ktoré môžu značiť, že človek užíva drogy:

- nestará sa o svoj vzhľad,
- vytrvalo odmieta účasť na rodinnom živote,
- prestáva mať záujem o záľuby, šport, obľúbené aktivity,
- je podráždený, reaguje prehnane na kritiku, výkyvy nálad,
- mení stravovacie návyky a osobný režim,
- dochádza k zmene hodnôt, postojov, názorov, vyjadrovania,
- množia sa klamstvá o tom, kde bol, s kým a čo robil,
- objavujú sa problémy v škole, práci,
- miznú peniaze, osobné veci a predmety z domácnosti,
- môže mať červené oči, so skleneným výrazom,
- objavia sa cigaretové papieriky, fajky, fľaštičky z liekov, zapaľovače,
- navštevujú ho neznámi ľudia a má nejasné telefonáty.

Legislatíva

Zákon č. 300/2005 Z.z. – Trestný zákon v znení neskorších predpisov

- *§170* Ohrozovanie zdravia nepovolenými liečivami, zdravotníckymi pomôckami a potrebami - Kto, čo aj z nedbanlivosti, spôsobí alebo zvýši nebezpečenstvo ohrozenia zdravia ľudí tým, že pri poskytovaní zdravotnej starostlivosti predpíše, vydá, predá alebo podá liečivá, ktoré nie sú zaradené do liekopisu, lieky, ktoré nie sú registrované podľa osobitného predpisu alebo ktorých požívanie nepovolil príslušný orgán, alebo zdravotnícke pomôcky, ktoré boli uvedené na trh v rozpore so všeobecne záväzným právnym predpisom alebo vykonáva klinické skúšanie liečiv, liekov alebo zdravotníckych pomôcok v rozpore so všeobecne záväzným právnym predpisom, alebo bez povolenia zaobchádza s liekmi alebo so zdravotníckymi pomôckami.
- *§171, §172, §173* - Nedovolená výroba omamných a psychotropných látok, jedov alebo prekurzorov, ich držanie a obchodovanie s nimi - Kto neoprávnene prechováva pre vlastnú potrebu omamnú látku, psychotropnú látku, jed alebo prekurzor, kto neoprávnene vyrobí, dovezie, vyvezie, prevezie alebo dá prepraviť, kúpi, predá, vymení, zadováži, alebo prechováva po akúkoľvek dobu, omamnú látku, psychotropnú látku, jed alebo prekurzor alebo kto takú činnosť sprostredkuje, kto vyrobí, sebe alebo inému zadováži alebo prechováva predmet určený na nedovolenú výrobu omamnej látky, psychotropnej látky, jedu a prekurzora.
- *§174* Šírenie toxikománie - Kto zvádza iného na zneužívanie inej návykovej látky než alkoholu alebo ho v tom podporuje alebo kto zneužívanie takej látky inak podnecuje alebo šíri.

Informácie na internete

www.infodrogy.sk – Drogový informačný portál

http://www.antidoping.sk – Antidopingový výbor SR

http://www.drogy.sk/cpldz/ - Centrum pre liečbu drogových závislostí

Poruchy príjmu potravy (Anorexia, Bulímia)

Anorexia

Anorexia je strata chuti do jedla, strata pocitu hladu, nechutenstvo. Takýto stav signalizuje somatické alebo psychické problémy. Pre odbornú starostlivosť je preto dôležité hľadanie príčiny, od ktorej sa následná liečba odvíja.

Anorexia môže byť sprievodným znakom organického ochorenia (napr. žalúdka). Pri organickej príčine anorexia po vyliečení vymizne. Iný vznik ochorenia môže mať funkčný charakter (napr. reakcia na prostredie) a často vzniká ako dôsledok rôznych iných psychických príčin.

Psychicky podmienená dlhodobá strata chuti do jedla sa nazýva mentálna anorexia - Anorexia mentalis nervosa. Pri vzniku mentálnej anorexie participuje často viac faktorov, ktoré vzájomne pôsobia na psychiku človeka. V procese vývinu choroby sa často pridružujú ďalšie psychické, sociálne, ale už i zdravotné problémy a stav sa neustále zhoršuje. Psychicky podmienená anorexia si vždy vyžaduje medicínsku liečbu a psychoterapiu. Neliečená anorexia alebo neskoro vyhľadaná odborná pomoc môže viesť k úmrtiu.

Príčiny ochorenia

Anorexia nervosa sa vyskytuje predovšetkým u ženskej populácie (cca 2%). Štatistiky udávajú pomer žien a mužov 95:5. Najviac ochorení vzniká v období puberty a adolescencie, teda vo veku 12 až 18 rokov. Zárodky choroby však dieťa často získalo a ukladalo si už v predškolskom alebo rannom veku. Veľmi často ide o dievčatá vzdelané, úspešné a vzhľadné, z primerane dobre situovaných rodín.

Za najčastejšie príčiny vzniku sa považuje:

- nedostatočne saturovaná emocionalita,
- prekrývanie a neriešenie rodinných alebo individuálnych problémov,
- životný štýl predstierania rodinnej bezproblémovosti,
- tlak na dieťa dosahovať vysoké méty už od útleho veku,
- zo strany najbližších pretrvávajúca očakávaná úspešnosť vo všetkých rovinách,
- podvedomý strach z odmietnutia, zlyhania.

V dnešnej dobe významnú úlohu pri vzniku choroby zohráva silne vyzdvihovaný spoločenský status, kult tela a vzory byť „in“.

Signály a sprievodné prejavy choroby

Prvé príznaky sa len ťažko zachytávajú, často pôsobia ako prirodzená neškodná túžba dobre vyzerať a starať sa o seba. Sú však signály, ktoré sú opakovane vysielané a len veľmi ťažko ich človek maskuje:

- hyperaktivita, nadmerná športová činnosť,
- jedlo sa stáva dominantnou témou,
- časté diéty a skúmanie kalórii a energie v jednotlivej strave,

- neobjektívny pohľad na svoje telo a váhu,
- zdanlivo objektívne odmietanie spoločného stolovania s rodinou,
- postupne sa zvyšujúca frekvencia reakcií typu: „teraz nemám chuť“, „už som jedla“, „najem sa neskôr“ a podobne,
- objavuje sa sklon k izolácii od vrstovníkov,
- únik do depresie,
- zmena charakteru, postojov a hodnôt vnímania sveta.

Z telesného hľadiska sú významné zmeny:

- zmena telesného vzhľadu, výrazný úbytok váhy, kruhy pod očami, zhoršenie pleti,
- závrate, nízky tlak, nepravidelný tep srdca,
- časté infekcie, dehydratácia, ľadvinové problémy,
- znížená citlivosť na chlad, bolesť a únavu,
- poruchy menštruácie.

Asi 50% žien, u ktorých je diagnostikovaná anorexia, sa preorientuje po určitom čase na formu anorexie kompulzívnej – nutkavej. Tento stav sa nazýva bulímia – chorobná žravosť.

Bulímia

Bulímia je chorobná chuť do jedenia, žravosť až pažravosť. Je impulzívna, nutkavá, má charakter opakovaných záchvatov prejedania sa s následným vyvrátením obsahu žalúdka. Po záchvate nastupuje tvrdá diéta. Frekvencia záchvatov býva 1až 3 krát do týždňa. Objavuje sa prevažne u žien vo veku 15 až 24 rokov, ale i neskôr ako dôsledok súčasného sociálneho fenoménu - za každú cenu vyzerať dobre, atraktívne a príťažlivo, “byť dokonalá“. Preto bulimičky bývajú prevažne úspešné ženy. V poslednej dobe vzrastá aj počet prípadov porúch príjmu potravy u chlapcov a mladých mužov. Odborná literatúra uvádza, že počet tých, ktorí majú vážny problém so stravovaním sa pohybuje na hranici 1-3% u mladých dievčat a žien. Určité narušenie stravovacích návykov a správania sa objavuje až u 6-8% v tejto rizikovej skupine. Na desať až dvadsať chorých dievčat pripadá jeden chlapec alebo mladý muž.

Najčastejšie príznaky

- prejedanie sa, následné zvracanie, prísna diéta,
- užívanie rôznych liekov na prečisťovanie, laxatíva a lieky na odvodňovanie,
- depresia a odpor samej voči sebe,
- strach z odhalenia, strach z nezvládnutia situácie, neustály strach z nadváhy,
- nepravidelná menštruácia,
- podráždenie až poškodenie tráviaceho traktu.

Bulimici prísne utajujú svoje záchvaty prejedania sa ako i následné aktivity, ktoré ich dehonestujú. Samotný proces prejedania sa je pre nich únik od svojich negatívnych pocitov, problémov a strachu.

Pôvod problému je prevažne v rodine a jej nárokoch na dieťa. Objavuje sa tiež u mladých žien, ktoré mali s nadváhou problém už od puberty. Ďalšiu skupinu tvoria vyliečené anorektičky. Nezanedbateľnú časť žien tvoria tie, ktoré podľahli tlaku a spoločenskému očakávaniu.

Kde hľadať poradenstvo a pomoc

Dôležité je, aby okolie neprehliadalo problém, čo najskôr ho pomenovalo a ponúklo možnosti riešenia:

- konzultácia u odborníka z oblasti klinickej psychológie,
- konzultácia u odborníka z oblasti psychiatrie,
- podľa zdravotného stavu vyšetrenie u gynekológa, internistu a iného špecialistu,
- poradiť sa na linkách pomoci.

Človeku by sme pri tom nemali siahať na jeho kompetencie a schopnosť postaviť sa reálne k chorobe. Samotnú tému neanalyzujme. Pozornosť venujme primárne človeku, nie chorobe. Počas celej choroby a liečby je dôležité poskytovať pocit istoty, bezpečia a podpory.

Všetky roviny vývinu človeka - biologickú, psychologickú i sociálnu - je potrebné kvalitne rozvíjať a v prípade problému hlavne v detstve a v období puberty ošetrovať.

Informácie na internete

www.wikipedia.sk – Online encyklopédia

Sebapoškodzovanie

Sebapoškodzovanie - automutilácia je akt fyzického násilia, ktoré jedinec úmyselne spôsobuje sám sebe. Ide o vyjadrenie psychickej bolesti pomocou fyzickej. Sebazraňovanie je vysielaný signál – je to „volanie o pomoc“.

Príčina je v prežívaní psychickej záťaže, ktorú človek nevie zvládať, spracovať a riešiť. Spôsobovanou fyzickou bolesťou sa snaží prekrývať psychickú bolesť. Pri fyzickej bolesti sa produkujú endorfíny, ktoré následne uvoľňujú prežívaný stav napätia, hlavne stres a úzkosť. Proces sebapoškodzovania má rituálny charakter - príprava, ubližovanie, ošetrenie. Medzi najčastejšie formy sebazraňovania patrí škrabanie, rezanie, pichanie a prepichovanie, pálenie a pod.

Sebapoškodzovateľ sa sám dobrovoľne nezdôveruje, následky starostlivo ukrýva. Postupne sa na tomto procese stáva závislým, rituál si starostlivo chráni. Včasné odhalenie býva preto len náhodné. Je to jeho osobné tajomstvo, o ktorom sa nerozpráva. Najčastejšie sa vyskytuje v období puberty vo veku 11 až 16 rokov, ale objavuje sa aj v neskoršom veku.

Medzi typické prejavy automutilácie patrí:

- škrabanie,
- extrémne obhrýzanie nechtov,
- vytrhávanie vlasov (trichotilomania),
- bodanie, rezanie, strihanie,
- udieranie,
- pálenie kože (cigaretami, zapaľovačom, horľavinami, žehličkou),
- zásahy do rán (zoškriabavanie si chrást, otváranie rán),
- lámanie kostí.

Spoločensky akceptovaným sebapoškodzovaním je tetovanie a piercing.

Príčiny sebapoškodzovania

- kríza rodiny, rozvod, strata blízkeho,
- rozchody, sklamanie v láske, neopätovaná láska,
- násilie, týranie, šikanovanie, zneužívanie,
- nedostatok akceptovaného sociálneho kontaktu,
- pocity osamelosti, izolácie, chaosu, zneistenia, sebaobviňovanie, pochybnosti o sebe,
- zanedbávanie, nezáujem, nedostatok lásky, podpory.

Pomoc a odborné poradenstvo

- najdôležitejšia pomoc je zo strany najbližších (rodičia, súrodenci…),
- sieť odborníkov: praktický lekár, psychiater, psychológ, psychoterapeut, kožný lekár…,
- dlhodobá psychoterapeutická starostlivosť.

Sebapoškodzovanie a internet – plusy a mínusy

V súčasnosti internet ponúka nielen informačné a pomáhajúce poradenské príspevky, ale tiež stránky poskytujúce podnety na sebapoškodzovanie, postupnosť krokov, spôsoby a formy sebapoškodzovania a návody na následné ošetrenie.

Ďalším ohrozením pre dieťa zo strany internetu môžu byť anonymné kontakty. Vyhľadávanie a udržiavanie virtuálneho vzťahu, ktorého predmetom záujmu je sebapoškodzovanie. Je to zdroj informácií a skúseností, rozširovanie, ale i utvrdzovanie sa v danom konaní.

Tieto stránky a kontakty sú preto veľmi nebezpečné. Ukazujú nové trendy deštrukčného procesu, ktoré môžu ohrozovať zdravie a život človeka. Tvorivosť sebapoškodzovania a rôzne súvislosti s daným aktom majú stále rastúci trend.

Informácie na internete

www.zdravotnictvo.sk

www.psychopomoc.cz

www.wikipedia.sk – Online encyklopédia

Sekty

Sekta je organizácia alebo spoločenstvo s odlišnou filozofiou ako uznáva väčšina spoločnosti. Ide o odtrhnutie, vyčlenenie alebo vytvorenie nového zoskupenia ľudí, ktoré zastáva ideologické alebo náboženské názory odlišujúce sa od spoločensky akceptovateľných hodnôt a noriem. Sekty majú stáročia dlhú históriu a preto existujú prevažne vo veľkých spoločenstvách. Pojem sekta pochádza z

latinského slova sequi, čo znamená nasledovať a slova secta - učenie. V súčasnosti sa pojem sekta nahrádza pojmami nové náboženstvo, netradičné náboženstvo alebo hnutie a pod.

Všetky tieto skupiny-spoločenstvá majú určité spoločné charakteristiky.

Najsilnejšími znakmi sú:

- rola vodcu, ktorý vystupuje ako charizmatická, no autoritatívna osobnosť,
- atmosféra neslobodného myslenia, čiže potláčanie osobnostnej identity,
- poslušnosť, oddanosť a podriaďovanie sa prísnym pravidlám sekty.

Nový člen je postupne vťahovaný do skupiny. Príjemnou starostlivosťou a akceptáciou sa zvyšuje jeho očakávanie, prežíva obdobie zvyšovania sebavedomia, a tak i zdanlivú sebarealizáciu. Prijíma svoje postavenie v rolovej hierarchii členov sekty a spoločenstvu venuje postupne viac času. Stráca väčšinový kontakt s reálnym svetom a pomalým, ale intenzívnym preprogramovaním sa postupne dostáva do závislosti na skupine a jej rituáloch. Príslušnosť k sekte sa volá sektárstvo.

Príčiny vstupu do sekty

Členom sekty sa stávajú poväčšine ľudia, ktorí prežívajú rôzne problémy a sami nie sú schopní ich riešiť. Sú to psychicky labilní ľudia, nezrelé osobnosti, ktoré sú ľahko manipulovateľné. Obeťami siekt sú často aj inteligentní, vzdelaní ľudia, ktorí sa z rôznych príčin ocitli v nežiadúcej situácii a prostredníctvom nejakého spoločenstva a jeho ideológie hľadajú vyriešenie svojho problému a stabilizáciu. Veľmi ľahko sa získavajú deti a dospievajúca mládež. Ich príčiny a motivácia sú rôzne napr. neakceptovateľná rola v rovesníckej skupine, nedostatok sociálneho kontaktu, únik z rodinného prostredia, ktoré ho nechápe, potreba niekam patriť, hľadanie cesty riešenia rôznych situácií alebo únik pred neschopnosťou riešiť problém. Mnohí mladí ľudia s nedostatkom informácií a skúseností podľahnú túžbe po zvedavosti a preto vstupujú do rôznych spoločenstiev.

Ako sa získavajú členovia - nábor

Pri získavaní nových členov je aktívne spoločenstvo – sekta a jej splnomocnení členovia. Oslovujú okruh svojich priateľov a členov bližšej i širšej rodiny. Oslovujú aj neznámych ľudí v rôznom prostredí. Miestom sa stáva ulica, kaviareň, obchodné centrum, tiež návštevy priamo v bytoch. V súčasnosti prezentujú a ponúkajú svoju existenciu, výhody spoločenstva a prínos pre záujemcu cez internet.

Oslovenia a ponuky pre zlepšenie života majú široký záber:

- náboženské a duchovné aktivity (biblické stretnutia, spoločné spevy, meditácie, magické rituály, proroctvá...),
- sociálne aktivity (dobročinné akcie, spoločenské kontakty pre osamelých, pomoc v životnej kríze, poskytovanie drobných darčekov...),
- ponuky pre telesné a psychické zdravie (zdravá výživa, ochrana proti AIDS, riešenie závislostí, zvládanie stresu, ako relaxovať...),
- liečiteľské ponuky netradičnou formou (zmena vedomia, práca s podvedomím...),
- zvyšovanie vzdelania a profesionálny rast (semináre, kurzy, tréningy, ponuka na kongresy, výstavy, školenia, testy, výbery...),
- ekonomické iniciatívy a poradenstvo (sponzoring, zakladanie firmy, sprostredkovanie práce...).

Možné následky

V mnohých prípadoch dochádza k úplnej zmene životného štýlu, ktorú člen bezvýhradne rešpektuje. Zdanlivo prežíva spokojnosť. Nepripúšťa resp. nie je schopný si uvedomiť, čo so svojím životom spravil. Mnohí členovia si však postupom času uvedomujú svoje premeny, ale nie vždy ich bezvýhradne akceptujú. Prežívaný vnútorný konflikt prináša ďalšiu krízu. Vzoprieť sa nevie. Má strach z autority a ani nechce určitým spôsobom opustiť komunitu a vytvorené vzťahy. Nemá tiež odvahu vstúpiť do reálneho sveta zo strachu z neprijatia a zaradenia sa v postupnom procese odprogramovania.

Najčastejšie zmeny v prejave stúpencov sekty:

- vznik psychickej závislosti na sekte, neschopnosť samostatne žiť,
- narušenie až zaniknutie prirodzených vzťahov v rodinnom, priateľskom a partnerskom živote,
- strata prirodzeného kontaktu s reálnym svetom,
- strata vlastnej identity, podriaďovanie sa skupinovej identite,
- zmena a preprogramovanie postojov a hodnôt,
- podriaďovanie sa, poslušnosť, strata samostatného rozhodovania sa a slobodného života,
- neopodstatnené pocity viny, strachu, depresie,
- nesamostatnosť a spoliehanie sa na autoritu, ktorá rozhoduje a preberá zodpovednosť,
- názorová uniformnosť a neschopnosť akceptovať iný názor ako má spoločenstvo,
- ohrozenie zdravia, odmietanie klasickej medicíny a nahradzovanie liečbou výlučne pomocou viery,
- strata majetku, dobrovoľné príspevky do spoločenstva,
- vystavenie sa trestu za opustenie alebo kritiku sekty.

EMO

Čo je vlastne emo?

V polovici 80-tych rokov minulého storočia to bol americký slangový výraz používaný pre hudobný žáner (emotion hardcore, emotional hardcore) V dnešnej dobe je slovo emo používané pre viacero hudobných žánrov, a je často považované za skratku slova „emotívny“.

Screamo je hudobný žáner, ktorý sa vyvinul z ema a hardcore punku na začiatku 90-tych rokov. Dnes by sa dalo povedať, že je to akýsi emocionálny punkrock. Charakteristickým pre tento žáner je niekedy až chaotické kolísanie zvuku hudby od hlučnej do tichej fázy, so šialene drsným krikom, až revom s rozhnevanými, abstraktnými, seba pozorujúcimi textami piesní.

Od hudby k móde

Dnes emo neznamená len štýl hudby, ale aj štýl života, ktorý vyznávajú hlavne mladí dospievajúci ľudia. Sú nápadní svojim oblečením, účesom, ale najmä správaním. Obliekajú sa prevažne do čierneho, ale prípustné sú aj ružová a červená farba, prúžky a bodky na pančuchách a kravatách, chlapci si zvyknú obliekať dievčenské nohavice. Typické je nosenie ofiny cez oči. Dievčatá, ale aj chlapci používajú čierne očné tiene, obľúbený je aj piercing a rôzne prívesky v tvare lebky, žiletiek a pod.

Od módy k správaniu

Niektorí emo predstavitelia sa označujú aj za homosexuálov alebo bisexuálov. Čo je však oveľa dôležitejšie je asociácia ema s depresívnym správaním a so sebapoškodzovaním. Emo ľudia majú zmysel pre prehnané melodramatické prejavy, radi plačú a robia „scény“. Niektorí si podrezávajú žily alebo sa dokonca pokúšajú aj o samovraždu. Treba byť preto obozretný a sledovať správanie vášho

dieťaťa, ktoré vyznáva tento štýl. Väčšina týchto mladých ľudí však nie je nijako psychicky narušená a ich správanie je viac-menej spojené s tým, že sa chcú niekam zaradiť.

Legislatíva

Zákon č. 300/2005 Z.z. – Trestný zákon v znení neskorších prepisov

- *§154* Účasť na samovražde - Kto iného pohne k samovražde alebo inému k samovražde pomáha, ak došlo aspoň k pokusu o samovraždu.
- *§155* Ublíženie na zdraví - Kto inému úmyselne spôsobí ťažkú ujmu na zdraví.
- *§156* Kto inému úmyselne ublíži na zdraví.
- *§157* Kto inému z nedbanlivosti spôsobí ťažkú ujmu na zdraví.
- *§182* Pozbavenie osobnej slobody – Kto iného neoprávnene pozbaví osobnej slobody.
- *§183* Obmedzovanie osobnej slobody – Kto inému bez oprávnenia bráni užívať osobnú slobodu.
- *§184* Obmedzovanie slobody pobytu – Kto ľsťou alebo násilím, hrozbou násilia alebo inej ujmy:
- iného neoprávnene núti k pobytu na určitom mieste,
- inému neoprávnene bráni v pobyte na určitom mieste.
- *§186* Vydieračský únos - Kto sa zmocní iného proti jeho vôli, a tým mu bráni užívať osobnú slobodu, alebo ho unesie a hrozbou jeho usmrtenia, ujmy na zdraví alebo inej ujmy si od neho alebo od tretej osoby vynucuje poskytnutie plnenia majetkovej povahy alebo nemajetkovej povahy.
- *§189* Vydieranie – Kto iného násilím, hrozbou násilia alebo hrozbou inej ťažkej ujmy núti, aby niečo konal, opomenul alebo trpel.
- *§190* Hrubý nátlak – Kto iného násilím, hrozbou násilia alebo hrozbou ťažkej ujmy núti poskytnúť plnenie majetkovej alebo nemajetkovej povahy pre seba alebo pre tretiu osobu za služby vlastné alebo služby tretej osoby, ktoré mu za takéto plnenie proti jeho vôli vnucuje, a to aj vtedy, keď takéto služby predstiera.

Informácie na internete

http://www.slovanet.sk/integra - Centrum prevencie v oblasti siekt

http://www.duch.sk/ - Ústav pre vzťahy štátu a cirkví

http://www.sekty.sk/ - Centrum pre štúdium siekt

www.sekty.cz

www.wikipedia.sk – Online encyklopédia

Závislosť od internetu, mobilov, esemesiek, počítačových hier

Odborníci ešte stále vedú diskusie o tom, či môže reálne existovať závislosť od internetu a mobilného telefónu alebo či ide skôr o závislosti od rôznych druhov služieb, ktoré ponúkajú (nakupovanie, hazard, čet, sms...).

Tak ako mnoho ľudí trávi priveľa času pri TV či knihách, existujú ľudia, ktorí trávia čas prevažne na internete alebo s mobilným telefónom. Do veľkej miery ide o nahradenie sociálneho kontaktu a

interakcie z bežného života, o vytváranie sociálnych sietí online. Ak surfujeme na internete alebo používame mobilný telefón, nemusíme riešiť veci každodenného života, sme v okruhu svojich známych a cítime sa bezpečne.

Na otestovanie internetovej závislosti môže slúžiť zodpovedanie nasledujúcich otázok:

- Často ostávate online dlhšie ako ste pôvodne zamýšľali?
- Zanedbávate svoje domáce povinnosti, lebo ste práve na internete?
- Uprednostňujete vzrušenie, ktoré vám prináša internet pred intímnymi chvíľami s vaším partnerom?
- Vytvárate si nové priateľstvá, vzťahy prostredníctvom internetu?
- Sťažujú sa vaši blízki, že trávite veľa času na internete?
- Zanedbávate školské alebo pracovné povinnosti kvôli internetu?
- Často sa vám stane, že skontrolujete prioritne vaše emaily aj keď máte inú prácu?
- Reagujete prehnane alebo útočne, ak sa vás niekto opýta, čo robíte na internete?
- Riešite nepríjemné udalosti vo vašom živote tým, že sa pripojíte na internet a ignorujete ich?
- Obávate sa, že život bez internetu by bol nudný, nezaujímavý?
- Reagujete agresívne, prehnane ak vás niekto ruší počas toho, keď ste online?
- Cítite sa nesvoj, stiesnene, ak nemáte možnosť sa pripojiť na internet?
- Snažíte sa tajiť reálny čas, ktorý strávite pripojený na internet?
- Stáva sa vám, že uprednostníte čas na internete pred časom stráveným s priateľmi?
- Myslíte na to, kedy sa budete môcť pripojiť aj počas iných aktivít?
- Cítite úľavu a pocit šťastia ak sa pripojíte na internet?
- Má väčšina vašich známych v mene @?

Z výskumu o závislosti od mobilných telefónov vo Veľkej Británii vyplýva, že 90% opýtaných ľudí sa cíti nervózne, keď im telefón aspoň raz za hodinu nezazvoní alebo nepípne esemeska, 80% sa necíti „vo svojej koži“ ak vypadne mobilná sieť a 84% z oslovených musí mať svoj mobilný telefón neustále na dohľad. Extrémny prípad závislosti sa objavil tiež vo Veľkej Británii, kde 19 ročný chlapec týždenne poslal 700 sms správ a za mesiac bol schopný odoslať až 8 000 emailov.

Závislosť od mobilného telefónu sa môže prejaviť ak:

- Mobil nevypínate ani v noci v strachu, že zmeškáte niečo dôležité.
- Ste v strese a máte pocit, že na vás svet zabudol, ak ste nedostali v poslednej pol hodine esemesku.
- Evidujete všetky novinky v oblasti mobilných telefónov a šetríte na nové modely.
- Po príchode na nové miesto ako prvé skontrolujete, či je dostatočný signál.
- Zvonenie vášho telefónu dokážete rozpoznať aj počas toho najhlučnejšieho rockového koncertu.

Na Slovensku sa od roku 2006 liečia aj nelátkové závislosti, medzi ktoré patria práve závislosť od internetu a mobilného telefónu. Ľudia liečiaci sa zo závislosti sa cítia osamelo, stratení, bez kontaktu so svetom a často pociťujú svoj život bez internetu ako neprekonateľný problém.

Rozvoj modernej techniky znamenal aj posun od závislosti na kartových hrách, hazarde a kockách k závislosti na počítačových hrách. Človek sa aj pri tejto závislosti správa impulzívne, pociťuje túžbu hrať sa na počítači a snaží sa ju uspokojiť.

Počítačové hry dokážu hráča strhnúť svojím verným stvárnením reality, možnosťou byť hrdinom a ovládať priebeh hry. Výrazným fenoménom dnešnej doby sú hromadné online hry, kedy hráč zdieľa priestor so stovkami, tisíckami ďalších hráčov a vytvára tak hru, ktorá je non-stop k dispozícii. Práve pri týchto hrách, kedy sa môžu viacerí hráči online zúčastňovať v tú istú dobu, dochádza najčastejšie k vytvoreniu závislosti.

K prvej hre sa dieťa často dostane s pomocou rodiča. Pokiaľ bola kupovaná so zámerom vyplniť dieťaťu čas, kedy sa mu rodičia nemôžu venovať, existuje veľké riziko, že dieťa bude pri hrách tráviť enormné množstvo času. To neskôr vedie k sociálnej izolácii, neschopnosti komunikovať s okolím, k okliešteným schopnostiam interakcie s rovesníkmi tvárou v tvár a utiahnutosti.

Kedy môže byť človek závislý na počítačových hrách?

- Takmer nevychádza zo svojej izby, bytu
- Nestretáva sa osobne s kamarátmi, spolužiakmi, kolegami
- Ignoruje rodinu a rodinné povinnosti
- Nepravidelne sa stravuje a spí
- Nedbá o svoju hygienu a výzor
- Zhoršuje sa mu pracovný alebo školský výkon

Návody na samovraždy

Samovražda (suicídium) je negatívny jav, ktorý sa vyskytuje vo všetkých historických obdobiach a je súčasťou aj dnešnej doby. Svetová zdravotnícka organizácia WHO uvádza alarmujúce štatistiky. Zvyšuje sa hlavne počet pokusov, ale i dokonaných samovrážd, u mladých ľudí v období dospievania (adolescencie). Z uvádzaných svetových štatistík samovraždou ukončí svoj život denne okolo 2000 ľudí, niekoľko násobne viac sa o ňu pokúša a vyhráža sa ňou.

Príčiny:

- **zdravotné** - primárny pôvod je v chorobe, napr. ťažké depresie a iné duševné ochorenia, závislosti, nevyliečiteľné somatické choroby (onkologické ochorenia, telesné hendikepy...),
- **sociálno-psychologické** - zapríčinené existenčnými problémami, pocitmi osamotenia, neúspešnosťou, konfliktami,
- **skratové konanie** - náhla reakcia na určitú situáciu,
- **ideológiou motivované** - napr. pri sektách a iných manipuláciách,
- **imitačné** - napodobňovanie riešenia problémov deštruktívnou formou,
- zapletenie sa do problémov, ktoré majú trestnoprávny charakter.

Samovražda je vedomé rozhodnutie ukončiť svoj život sebadeštrukciou vopred pripraveným prostriedkom alebo spôsobom.

Sebausmrtenie nemá vedomý úmysel, aktér nie je schopný dôsledne odhadnúť svoje konanie. Do tejto skupiny zaraďujeme aj skratové a demonštratívne konanie. Príkladom môže byť náhla kríza,

potreba upozorniť na seba, ale aj predvádzanie svojich schopností pred rovesníkmi, napr. vylezením na komín, vypitím veľkého množstva alkoholu a pod.

Sebapoškodzovanie s následkom sebausmrtenia. Sebausmrtenie je náhodné ako dôsledok neodhadnutej intenzity, či formy sebapoškodzovania. Nie je realizované s úmyslom smrti.

Sebaobeť je dobrovoľné usmrtenie najčastejšie v mene určitej ideológie alebo vlastného presvedčenia.

Vývoj procesu ukončenia svojho života samovraždou:

- zaoberanie sa myšlienkou o ukončení života,
- pokus o samovraždu (často po pokuse dochádza k uvedomeniu si svojho konania, čo môže proces zastaviť),
- premyslený a pripravený akt, vykonanie samotnej dokonanej samovraždy.

Forma realizácie:

- individuálna, v izolácii,
- rozšírená samovražda, napr. milenecká, samovražda členov rodiny alebo inej skupiny ľudí vyplývajúca zo spoločných problémov,
- rituálne samovraždy, ide buď o dobrovoľný akt alebo z donútenia vodcom, či tlakom skupiny, môže ísť o jednotlivca alebo o početnejšiu skupinu.

Varovné signály:

- nezáujem o svoje veci, vzhľad, vzdelanie,
- psychické napätie, smútok, poruchy spánku,
- vyhýbanie sa spoločným rodinným aktivitám,
- nezáujem o kamarátske vzťahy, uzatváranie sa do vlastného sveta,
- neadekvátne reakcie, prehnané alebo naopak ľahostajné,
- zvýšená chorobnosť,
- bilancovanie svojho života, prehodnocovanie dosiahnutých úspechov/neúspechov.

Varovné signály môžeme označiť aj ako „volanie o pomoc“. Osoba, ktorá ich vysiela si vyžaduje od okolia empatický prístup, pochopenie, poskytnutie podpory, sprevádzanie pri hľadaní riešenia a alternatív pre budúcnosť. Efektivita sa dostaví, ak sa podarí ohrozenú osobu pozitívne naladiť, ponúknuť jej aktivity, pri ktorých sa navodí uspokojenie a príjemné pocity.

Prevencia

- **Akékoľvek navádzanie na závislosti (drogy, sebapoškodzovanie...) je potrebné oznámiť rodičom, učiteľom, polícii.**
- **Dieťa môže byť aj nezdvorilé a odmietnuť ponuku, ktorá je ohrozením jeho zdravia a života.** Vysvetlíte dieťaťu, že za niektorých okolností, ako je ponuka drog, alkoholu, fajčenia, navádzania na sebapoškodzovanie a podobne, má právo byť nezdvorilé a odmietnuť ponuku.
- **Dieťa má právo na svoj vlastný názor, aj keď ho kamaráti nebudú akceptovať.** Má právo povedať nie a stáť si za svojím názorom. Presvedčenie, tón hlasu i mimika dieťaťu pomôžu presadiť svoj názor. Dieťa je jedinečná a originálna osobnosť, preto sa nemusí prispôsobovať všetkému čo práve robia ostatní. Podporte zdravé sebavedomie a asertivitu dieťaťa, čo mu umožní byť sám sebou v skupine rovesníkov a odolať tak prvému skúšobnému kontaktu s drogou.

- **Dieťa si má vybrať skutočných kamarátov, ktorí sú k nemu tolerantní, akceptujú jeho názor, pohľad na vec a nenútia ho k ničomu čo sám nechce.** Ak dieťa niekto nahovára a neustále presviedča na zlé veci, nech používa metódu obohranej platne, to znamená, že má dookola trvať na svojej odpovedi. A najlepšie je odísť, lebo kamaráti, ktorí neakceptujú iný názor, nie sú skutoční kamaráti. Snažte sa spoznať priateľov vašich detí, umožnite im sa stretávať u vás doma. Ak je to možné, udržiavajte kontakt aj s ich rodičmi.
- **Všímajte si správanie, zvyky, pocity a prejavy dieťaťa.** Prvé príznaky poruchy príjmu potravy (anorexia, bulímia) sa len ťažko zachytávajú, často pôsobia ako prirodzená neškodná túžba dobre vyzerať a starať sa o seba. Sú však signály, ktoré sú opakovane vysielané a len veľmi ťažko ich človek maskuje:
    - hyperaktivita, nadmerná športová činnosť
    - jedlo sa stáva dominantnou témou
    - časté diéty a skúmanie kalórii a energie v jednotlivej strave
    - neobjektívny pohľad na svoje telo a váhu
    - zdanlivo objektívne odmietanie spoločného stolovania s rodinou
    - postupne sa zvyšujúca frekvencia reakcií typu: „teraz nemám chuť“, „už som jedla“, „najem sa neskôr“ a podobne
    - objavuje sa sklon k izolácii od vrstovníkov
    - únik do depresie
    - zmena charakteru, postojov a hodnôt vnímania sveta
    - zmena telesného vzhľadu, výrazný úbytok váhy, kruhy pod očami, zhoršenie pleti
    - závrate, nízky tlak, nepravidelný tep srdca
    - časté infekcie, dehydratácia, ľadvinové problémy
    - znížená citlivosť na chlad, bolesť a únavu
    - poruchy menštruácie
- **Hovorte so svojimi deťmi o rizikách a následkoch používania drog a iných návykových látok.** Vzdelávajte sa v oblasti rizík a dôsledkov užívania drog. Nepodceňujte svoje deti, často vedia o drogách viac ako vy, nesnažte sa ich poučovať. Diskutujte a prezentujte jasne váš postoj. Staňte sa a zostaňte súčasťou života vašich detí. Aj v puberte.
- **Sledujte, či vaše dieťa nehrá hry, ktoré znázorňujú užívanie drog.**

  Hry sa označujú: 
- **Sledujte, či vaše dieťa nehrá hry, ktoré nabádajú alebo vyučujú hazardné hry.**

  Hry sa označujú: 
- **V prípade podozrenia na akúkoľvek závislosť nezľahčujte to. Čo najskôr situáciu riešte pomocou blízkych dôveryhodných osôb alebo neváhajte požiadať o odbornú pomoc.** Je dobré nájsť aspoň jednu dobre stabilizovanú vzťahovú väzbu (dieťa-rodič, dieťa-súrodenec, dieťa-rodinný priateľ, dieťa-odborník).
- **S dieťaťom komunikujte na témy náboženstvo a sekty.** U detí je potrebné prevenciu realizovať od času, keď sa začínajú pohybovať vo svojom okolí samostatne. Vysvetlite deťom ako komunikovať s cudzou osobou, ktorá ho s danou témou osloví. Veďte deti k názorovej slobode, k zdravému sebavedomiu a sebarealizácii.
- **Internet môže byť nebezpečný.** Oboznámte dieťa o tom, že tak ako v bežnom živote aj na internete alebo pri mobilnej komunikácii, číha nebezpečenstvo. Môžete použiť príklad s elektrinou. Je to rovnako ako internet potrebná a nenahraditeľná vec, ale je to rovnako ako internet pri nezodpovednom používaní nebezpečná vec pre vaše zdravie alebo dokonca pre život. Pri internete na rozdiel od elektriny stále chýba takáto skúsenosť, či skôr osveta.
- **Nikdy neviete, kto je v skutočnosti na druhej strane internetu alebo mobilu.** Na druhej strane môže byť človek, ktorý klame o svojom veku, pohlaví, záujmoch, vzhľade a podobne. Takýto ľudia chcú deťom veľmi ublížiť a sú to:
    - pedofili...
    - ľudia, ktorí chcú fotografie a videá detí...

- navádzajú na užívanie drog...
- navádzajú na šikanovanie, alebo šikanujú deti...
- nenávidia určité skupiny ľudí...
- správajú sa agresívne, násilne...
- chcú sa s deťmi tajne stretnúť, ublížiť im, uniesť ich...
- získať osobné údaje o dieťati, jeho rodine, kamarátoch...
- chcú oklamať, podviesť dieťa...
- návádzajú na sebapoškodzovanie...

- **Buďte vnímavý** k členom najbližšej rodiny a k členom sociálnej skupiny, v ktorej sa človek pohybuje, zaujímajte sa o aktivity a záujmy dieťaťa.
- **Overujte prostredie** a sociálne vzťahy, v ktorých sa dieťa pohybuje.
- **Vytvárajte priestor pre komunikáciu**, pre ventilovanie rovnako pozitívneho ako i negatívneho prežívania a následne poskytujte spätnú väzbu. Deťom, hlavne v puberte a adolescencii, venujte veľa času, rozprávajte sa s nimi o ich životnej filozofii, postojoch a hodnotách.
- **Všímajte si a nepodceňujte ani drobné signály.** Problémy je dobré riešiť hneď v začiatkoch, aby neprerástli do ťažko riešiteľnej situácie.
- **Dávajte pocit istoty a bezpečia**, dostatok lásky, starostlivosti a porozumenia ľuďom v problémoch, v zdanlivo neriešiteľných situáciách, vo vážnej kríze, ale hlavne deťom v rodine a v širších rodinných vzťahoch. Ubezpečte deti, že vždy stojíte pri nich, a že všetky problémy majú riešenie.
- **Ponúknite pomoc** a spoločne hľadajte riešenia, ak je potrebné oslovte odborníkov (psychológ, psychiater...), poraďte sa o konkrétnych krokoch a možnostiach riešenia.
- **Nepodporujte výroky** typu: „už ma nič nebaví, nemá to zmysel, nikomu na mne nezáleží, ja už nevládzem“ **a zvláštne správanie** (izolácia, zmena správania, nezáujem o bežné veci a aktivity, ktoré boli predtým predmetom záujmu...), ale prijmite ich ako signál a podnet k hľadaniu riešenia.
- **Všímajte si, kde sa dieťa pohybuje vo virtuálnom svete** (internet, počítačové hry, mobilná komunikácia...).
- **Nie je bezpečné dávať na internet alebo cez mobil svoje osobné údaje.** Vysvetlite deťom, čo sú to osobné údaje a prečo je nebezpečné zverejňovať svoje pravé meno a priezvisko, svoju fotografiu, video, vek, emailovú adresu, telefónne číslo, adresu domov, adresu školy, majetkové pomery, prístupové mená a heslá alebo iné osobné údaje (záľuby, opis vzhľadu, povahy, znalosti, zručnosti, vzdelanie, obľúbené veci, túžby...).
  V prípade, že je nevyhnutné takéto údaje poskytnúť, musia o tom vedieť rodičia alebo učitelia.

- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- **S nikým, s kým sa dieťa zoznámilo iba cez internet alebo mobil, sa nesmie stretávať samé osobne.** Tak ako v reálnom živote nechodia deti na stretnutie s neznámou osobou bez sprievodu niekoho ďalšieho, najlepšie rodiča, alebo aspoň súrodenca, kamaráta, tak aj na stretnutie s neznámou osobou, s ktorou sa dieťa zoznámilo iba cez internet alebo mobil, je stretnutie veľmi nebezpečné. Ak už dieťa ide na stretnutie, tak vždy aspoň s kamarátom. Rodičom by malo oznámiť na aké stretnutie ide, za kým ide, kde a kedy sa plánuje vrátiť. Stretnutie by malo byť na verejnom mieste, kde je veľa ľudí. Znakom bezpečnejšieho stretnutia je, že tomu, čo pozýva, nevadí, že dieťa príde s rodičom alebo inou dospelou osobou. Ak mu to vadí, ten človek nemá čisté úmysly.
- **Buďte podozrievavý voči človeku, ktorý dieťa presviedča, aby zatajovalo svoje internetové kamarátstvo pred rodičmi, alebo vystupuje ako tínedžer, ale nevie väčšinu odpovedí na otázky, ktoré bežne rovesníci poznajú.** Takýto človek chce deťom ublížiť, a preto klame a navádza, aby zatajili pozvanie na stretnutie s ním, aby si zmazali históriu četu, jeho emaily, sms, mms správy, a podobne.
- **Použitie lokalizačných služieb mobilného telefónu dieťaťa neznámou osobou je nebezpečné**. Vďaka lokalizácii môže ktorákoľvek osoba vyhľadať miesto pobytu dieťaťa, ak mu to samo z nevedomosti umožní.
- **Bluetooth spojenie cez mobilný telefón dieťaťa s neznámou osobou je nebezpečné.** Pomenujte mobilný telefón dieťaťa tak, aby z neho nebolo hneď jasné, že sa jedná o dieťa.

- **Nie všetko, čo je na internete, je pravda.** Vysvetlite deťom, nech neveria všetkému čo nájdu na internete. Informácie si je potrebné porovnať z viacerých zdrojov a v prípade nejasností sa poradiť s rodičmi alebo učiteľmi v škole.
- **Ak dieťa na internete alebo cez mobil niečo vyľaká, našlo niečo škaredé, desivé, niečo z čoho sa cíti trápne, zraňuje ho to alebo ohrozuje, vysvetlite mu, že to nie je jeho chyba.**
- **Ak sa dieťa cíti nepohodlne alebo trápne pri online konverzácii, má právo ju okamžite prerušiť a odísť z četovej miestnosti**. Ak sa pritom snažil človek zaviesť tému do sexuálnej oblasti nech dieťa o tom povie rodičom, alebo v škole učiteľom.
- **Váš domáci počítač (alebo hraciu konzolu) postavte do obývacej izby alebo na iné spoločné prístupové miesto v byte.** Najlepšie tak, aby rodič mal vždy výhľad na monitor**.** Nedávajte počítač do detských izieb. Majte dobrý prehľad o všetkých ďalších počítačoch, ktoré sú deťom prístupné.
- **Stanovte medzi deťmi a rodičmi jasné pravidlá pre používanie internetu.** Urobte si rozvrh na dni a presný čas, kedy má dieťa povolenie stráviť čas na internete, najlepšie v čase vašej prítomnosti. Podpísanú zmluvu vystavte v blízkosti počítača na viditeľnom mieste. Nezabudnite, ak si s vaším dieťaťom vytvoríte pravidlá o používaní internetu, stanovte si práva a povinnosti pre obe strany. Pravidla, by sa mali pravidelne aktualizovať. Vzor takejto „rodinnej zmluvy" nájdete na stránkach Zodpovedne.sk.
- **Najmenšie deti by nemali používať četovacie miestnosti bez moderátora, v ktorých môže byť dieťa najviac ohrozené.**
- **Vytvorte medzi dieťaťom a rodičom vzťah vzájomnej dôvery.** Majte prehľad o prezývkach (nickname) vašich detí, ktoré používajú na internete. Buďte opatrný, nebuďte dotieravý pri kontrole dieťaťa, vzájomná dôvera je veľmi dôležitá. Prílišná kontrola by mohla dieťa dohnať ku skrývaniu a zatajovaniu činností. Netrestajte dieťa za to, čo nie je jeho chyba, môže vám prestať dôverovať a mať strach a neistotu pri zdôverovaní sa s nejakým problémom. Je potrebné sa s deťmi veľa rozprávať, upozorniť ich na rôzne nebezpečenstvá, zaujímať sa a vedieť kde a ako trávia voľný čas, s kým telefonujú, emailujú, četujú, s kým sa stretávajú. Menšie deti si vyžadujú pravidelnú kontrolu. Ponúknite deťom adekvátne, zmysluplné a zaujímavé mimoškolské aktivity. Všímajte si viac svoje okolie. Nebuďte ľahostajní ani k cudzím deťom.
- **Dôveruj, ale preveruj.** Nie vždy sa dieťa zdôveruje rodičom, preto nezabudnite sledovať jeho nálady, zvyky, zmeny nálad a správanie, ktoré môže byť kľúčom k objasneniu príčiny. Kontrolujte, ktoré stránky navštevuje, s kým si píše emaily, hovorte s ním s kým a o čom si píše. Ak dieťa chodí na stránky s nevhodným obsahom, je možné pomocou filtra zakázať prístup na tieto stránky. Ak nechcete aby dieťa bolo vystavené riziku pri otváraní emailov, nainštalujte si program, ktorý povolí otvorenie emailu iba od známych ľudí zo zoznamu, adresáru. Pokiaľ to uznáte za vhodné, používajte monitorovacie nástroje, ktoré vám umožnia získať prehľad o chovaní vášho dieťaťa na internete.
- **Dbajte, aby dieťa hralo iba hry, ktoré sú určené správnej vekovej skupine a s vhodným obsahom.** Počítačové hry alebo hracie konzoly sú zatriedené podľa veku hráčov do skupín 3+, 4+, 6+, 7+, 12+, 16+, 18+. Obsahové ohrozenia hráčov sa delia na skupiny:
    - hra obsahuje vulgarizmy,
    - hra obsahuje diskriminačné prvky tj. obsahuje zobrazenia alebo materiály, ktoré môžu nabádať k diskriminácii,
    - hra znázorňuje užívanie drog,
    - hra môže pôsobiť na dieťa desivo až hrozivo,
    - hra znázorňuje nahotu alebo iné sexuálne správanie,
    - hra zobrazuje násilie,
    - hra, ktorá nabáda alebo vyučuje hazardné hry.
- **Pri výbere školy, mládežníckeho klubu, centra voľného času, letných táborov a podobne sa informujte, aké majú jednotlivé organizácie vypracované programy prevencie voči e-ohrozeniam.** Medzi e-ohrozenia patria:
    - Pedofília, pornografia (Pedofília, pornografia, sexturizmus, zverejňovanie erotiky...)
    - Závislosti (Drogy, anorexia, bulímia, sebapoškodzovanie, sekty, závislosť od internetu, mobilov, esemesiek, počítačových hier, návody na samovraždy, emo...),

- Šikanovanie (Bullying, elektronické šikanovanie, zastrašovanie, ponižovanie, zosmiešňovanie, ohováranie, nadávanie, happy slapping...),
- Diskriminácia (Xenofóbia, rasizmus, extréministické hnutia, totalitný režim...),
- Násilie (Agresivita, klubové chuligánstvo, terorizmus, flaming, hate speech...),
- Stretnutie s neznámou osobou (Internetové známosti, grooming, obchodovanie s ľuďmi...),
- Poskytovanie osobných údajov (Poskytovanie kontaktných, osobných údajov, majetkové pomery, phishing...),
- Internetové podvody (Počítačová kriminalita, falšovanie počítačových údajov, porušenia autorských a príbuzných práv...).

- **Neustále sa informujte, vzdelávajte, zlepšujte svoje zručnosti na internete, v mobilnej komunikácii a nových technológiách.** Súčasná generácia vyrastá s internetom a ich znalosti (aj jazykové), zručnosti sú vo väčšine prípadov lepšie ako u ich rodičov. Preto je potrebné snažiť sa s nimi aspoň držať krok a tak chrániť deti, seba a celú rodinu. Sledujte odbornú tlač, prípadne internetové stránky zaoberajúce sa danou problematikou.
- **Zvyšujte povedomie, šírte osvetu o zodpovednom používaní internetu, mobilu a nových technológií.**
- **Komunikujte s inými rodičmi, učiteľmi**, vymieňajte si informácie a poznatky.
- **Správajte sa Zodpovedne.sk!** Na internete alebo pri mobilnej komunikácii sa správajte tak ako v ozajstnom živote. Vysvetlite deťom, aby, neurobili niečo, čo by v skutočnom živote nespravili. Pravidlá slušného správania sa na internete nazývajú netiketa.

Šikanovanie (Bullying, elektronické šikanovanie, zastrašovanie, ponižovanie, zosmiešňovanie, ohováranie, nadávanie, happy slapping)

Bullying

Existuje množstvo definícií a opisov šikanovania (anglický výraz bullying). Mierne sa odlišujú, ale z veľkej časti hovoria o tom istom:

- šikanovanie je zákerné, opakované zneužívanie sily alebo postavenia na trápenie, zámerné prenasledovanie, robenie príkoria,
- šikanovanie pokrýva veľkú škálu vedomých, pretrvávajúcich a nevítaných činov medzi jednotlivcami a skupinami, ktoré sú charakterizované fyzickým, psychickým, sexuálnym násilím a iným utrpením,
- šikanovanie je dané rozdielnou mocou medzi osobou, ktorá šikanuje a osobou, ktorá je šikanovaná. Táto rozdielna moc je rozpoznaná, a preto využívaná tým, kto šikanuje.

Šikanovanie je extrémne rozšírené najmä medzi mladými ľuďmi. V poslednej dobe sa realizujú rozsiahle štúdie v celej Európe, ktoré majú pomôcť zmapovať tento fenomén a napomôcť jeho riešeniu.

Tejto činnosti prepadajú osoby, ktoré sa snažia dosiahnuť uznanie prostredníctvom utrpenia a provokovania ostatných. Šikanujúci – agresor sa takto snaží zakryť svoju neschopnosť, zredukovať strach zo seba samého a nájsť stratené sebavedomie.

Šikanovanie sa môže prejavovať ako priama aktivita (vyhrážky, fyzické alebo psychické násilie) alebo ako nepriama aktivita (izolácia z blízkeho sociálneho prostredia). Medzi ďalšie činnosti, ktoré sa využívajú ako forma šikanovania sú zahrnuté:

- sexuálna diskriminácia,
- sexuálne narážky, zneužívanie,
- šikanovanie na základe odlišnosti (rasy, jazyka, kultúry),
- urážanie pre zjavnú odlišnosť od rovnorodého davu,
- poškodzovanie rodiny, znevažovanie rodinnej situácie (využívajú najmä deti),
- diskriminácia na základe veku (napr. staršie deti sa vŕšia na mladších),
- odcudzovanie peňazí, majetku (vreckové, mobilný telefón, odovzdávanie desiaty).

Kde sa šikanovanie odohráva?

Vo väčšine prípadov sa šikanovanie berie ako záležitosť, ktorá sa odohráva v školskom prostredí. Môžeme sa s ním však stretnúť aj na miestach ako napr. nočné kluby, mládežnícke kluby, ihriská, športoviská, pracoviská, cez mobilné telefóny a internet, četové miestnosti či email.

Elektronické šikanovanie (cyberbullying)

Ide o zneužívanie mobilných telefónov a internetu na posielanie agresívnych a nenávistných správ a zastrašovanie osôb. Internetové prostredie poskytuje jedinečné možnosti pre podobné aktivity. Anonymita, ktorú poskytuje uľahčuje túto činnosť a kryje ľudí, ktorí majú za cieľ útočiť na ostatných užívateľov internetu. Elektronický násilník si užíva pocit zadosťučinenia, ktorý mu poskytuje odosielanie textových správ, mailov. Chce tak človeka rozrušiť, zneistiť a vystrašiť. Pri elektronickom šikanovaní väčšia fyzická sila agresora, jeho popularita a sociálna sieť ustupujú do úzadia a dôležitou sa stáva schopnosť a spôsobilosť používať počítač, mobil a internet.

Zákernosť tohto druhu šikanovania spočíva aj v tom, že je nepretržité – 365 dní v roku 24 hodín denne a k inkriminujúcim informáciám má prístup veľké množstvo užívateľov internetu a mobilných telefónov. Nie je už viazané na bezprostredné stretnutia obete a agresora a tak môže mať oveľa hlbší dosah ako šikanovanie fyzické.

Príklady

- vytvorenie web stránky, ktorá má ponížiť, vystrašiť a znevážiť,
- šírenie obrázkov, upravených fotiek, alebo fotiek z inkriminujúcich situácií, ktoré ponižujú a urážajú,
- zasielanie výstražných, obscénnych, nenávistných mailov, okamžitých správ, sms,
- obťažovanie, vyhrážanie alebo zasielanie obscénnych obrázkov prostredníctvom mobilného telefónu,
- vyhrážanie, zastrašovanie alebo obťažovanie v internetových četových miestnostiach,
- uverejnenie ponižujúcich, urážajúcich videí na internete,
- šírenie nepravdivých alebo skreslených informácií prostredníctvom mailu, mobilného telefónu a internetu,
- zneužitie identity užívateľa internetu,
- zneužitie dôverných online rozhovorov a získaných informácií na poníženie a urážanie.

Ako sa brániť?

Človek, ktorý šikanuje, si týmto spôsobom reflektuje svoj vnútorný hnev a nenávisť k iným ľuďom. Jeho nenávisť sa stupňuje, ale zároveň sa stáva menej účinnou v prípade, ak narazí na človeka, ktorý pochopí, že ide o slabého, osobnostne nevyzretého jednotlivca, neschopného sa zaradiť do spoločnosti a presadiť si svoju vôľu konformným spôsobom.

Nástrojmi násilníka sú sila, kontrola, dominancia a podmanenie. Ich cieľom je vyvolať vo vás reakciu, nech je už akákoľvek. Už to, že zareagujete, odpoviete na ich provokáciu, im poskytuje pocit sily a kontroly, ktorú týmto spôsobom nad vami získali. Čím viac sa snažíte vyjednávať, vysvetľovať, uvádzať veci na pravú mieru, tým viac ich provokujete k ďalším výpadom.

Dieťa môže byť elektronicky šikanované ak:

- nečakane prestane používať počítač,
- sa zdá nervózne alebo neisté pri čítaní emailov alebo okamžitých správ, správ v mobile,
- nechce chodiť do školy alebo medzi ľudí všeobecne,
- sa zdá nahnevané, depresívne alebo frustrované po odchode od počítača,
- vyhýba sa rozhovoru o tom, čo robí na počítači,
- sa stane abnormálne uzavreté voči priateľom alebo rodine.

Dieťa môže elektronicky šikanovať ak:

- rýchlo vypína obrazovku alebo zatvára programy v počítači, keď sa priblížite,
- trávi pri počítači dlhé hodiny v noci,
- je rozčúlené, ak nemôže nečakane použiť počítač,
- prehnane sa smeje pri používaní počítača,
- vyhýba sa rozhovoru o jeho práci na počítači,
- používa niekoľko online účtov alebo adries, ktoré ani nie sú jeho.

Legislatíva

Zákon č. 300/2005 Z.z. – Trestný zákon v znení neskorších predpisov

- *§155* Ublíženie na zdraví - Kto inému úmyselne spôsobí ťažkú ujmu na zdraví.
- *§183* Obmedzovanie osobnej slobody – Kto inému bez oprávnenia bráni užívať osobnú slobodu.
- *§189* Vydieranie – Kto iného násilím, hrozbou násilia alebo hrozbou inej ťažkej ujmy núti, aby niečo konal, opomenul alebo trpel.
- *§192* Nátlak - Kto iného núti, aby niečo konal, opomenul alebo trpel, zneužívajúc jeho hmotnú núdzu alebo naliehavú nemajetkovú potrebu, alebo tieseň vyvolanú jeho nepriaznivými osobnými pomermi.
- *§345* Krivé obvinenie - Kto iného lživo obviní z trestného činu v úmysle privodiť jeho trestné stíhanie.
- *§373* Ohováranie – Kto o inom oznámi nepravdivý údaj, ktorý je spôsobilý značnou mierou ohroziť jeho vážnosť u spoluobčanov, poškodiť ho v zamestnaní, v podnikaní, narušiť jeho rodinné vzťahy alebo spôsobiť mu inú vážnu ujmu.
- *§360* Nebezpečné vyhrážanie – Kto sa inému vyhráža smrťou, ťažkou ujmou na zdraví alebo inou ťažkou ujmou takým spôsobom, že to môže vzbudiť dôvodnú obavu.

Informácie na internete

http://www.prevenciasikanovania.sk

www.wikipedia.sk – Online encyklopédia

Prevencia

- **Akékoľvek šikanovanie je potrebné oznámiť rodičom, učiteľom, polícii.** Pomoc potrebujú najmä deti a mládež, ale ani dospelí nemusia byť dostatočne silní zvládnuť takéto zastrašovanie, vyhrážanie. Niekedy totiž môžete mať do činenia s nebezpečnou a prípadne aj chorou osobou, kedy je pomoc odborníkov nevyhnutná. Páchateľ sa po čase alebo trvalej ignorácii väčšinou unaví. Nájde si ale inú obeť, a preto je potrebné zastaviť jeho správanie, a tak pomôcť ďalšej obeti a aj samému útočníkovi.
- **Šikanovanie riešte okamžite.** Šikanovanie môže začať na internete alebo cez mobil, čo je veľmi traumatizujúce. Často však prerastie aj do fyzickej podoby, preto je potrebné riešiť situáciu už v počiatočnom štádiu.
- **Pri šikanovaní nech v žiadnom prípade dieťa neodpovedá, nereaguje a nijakým iným spôsobom nevytvára vzťah, spätnú väzbu, interakciu.** Nie je to však také ľahké ako to znie. Je prirodzenou reakciou sa brániť, snaha očistiť svoje meno a vysvetliť reálnu situáciu. Nikdy sa však nedohadujte s násilníkom. Nie je možné sa s ním rozumne dohovoriť, väčšinou to skončí ako diskusia s rozmaznaným dieťaťom alebo spurným tínedžerom.
- **Pri šikanovaní prostredníctvom internetu alebo cez mobil blokujte príjem správ, emailov od daného užívateľa (emailovým klientom, v četovej miestnosti...), a tak obmedzíte možnosti páchateľa.**
- **Uschovávajte si dôkazový materiál (emaily, sms, mms, históriu četu, www stránky).** V prípade emailov si vytvorte napríklad nový adresár, v ktorom si tieto emaily budete uchovávať. Nemusíte ich čítať, ale použijete ich v prípade dokazovania. Násilníci menia emailové adresy, identity, ale prostredníctvom uložených emailov sa bude dať identifikovať, či ide o tú istú osobu. V prípade sms, mms správ si ich odfoťte aj s číslom odosielateľa,

dátumom a časom. Uchovajte si výpis prijatých správ. V prípade www stránok si urobte kópiu stránky napríklad funkciou „printscreen“.

- **Buďte ostražitý voči provokácii, pokusom o šikanovanie.** Niektoré emaily, správy na čete môžu byť návnadami ako obeť nájsť a vtiahnuť do diskusie. Udeje sa to skôr, ako si to stihne uvedomiť. Ak odpoviete rozčúlený a necháte sa vyprovokovať k reakcii, dávate tým provokatérovi pocit zadosťučinenia. Už sa len môže prizerať, ako sa dohadujete buď s ním alebo s ďalšími osobami, ktoré tiež zatiahol do svojej hry.
- **Internet môže byť nebezpečný.** Oboznámte dieťa o tom, že tak ako v bežnom živote aj na internete alebo pri mobilnej komunikácii, číha nebezpečenstvo. Môžete použiť príklad s elektrinou. Je to rovnako ako internet potrebná a nenahraditeľná vec, ale je to rovnako ako internet pri nezodpovednom používaní nebezpečná vec pre vaše zdravie alebo dokonca pre život. Pri internete na rozdiel od elektriny stále chýba takáto skúsenosť, či skôr osveta.
- **Nikdy neviete, kto je v skutočnosti na druhej strane internetu alebo mobilu.** Na druhej strane môže byť človek, ktorý klame o svojom veku, pohlaví, záujmoch, vzhľade a podobne. Takýto ľudia chcú deťom veľmi ublížiť a sú to:
    - pedofili...
    - ľudia, ktorí chcú fotografie a videá detí...
    - navádzajú na užívanie drog...
    - navádzajú na šikanovanie, alebo šikanujú deti...
    - nenávidia určité skupiny ľudí...
    - správajú sa agresívne, násilne...
    - chcú sa s deťmi tajne stretnúť, ublížiť im, uniesť ich...
    - získať osobné údaje o dieťati, jeho rodine, kamarátoch...
    - chcú oklamať, podviesť dieťa...
    - návádzajú na sebapoškodzovanie...
- **Nie je bezpečné dávať na internet alebo cez mobil svoje osobné údaje.** Vysvetlite deťom, čo sú to osobné údaje a prečo je nebezpečné zverejňovať svoje pravé meno a priezvisko, svoju fotografiu, video, vek, emailovú adresu, telefónne číslo, adresu domov, adresu školy, majetkové pomery, prístupové mená a heslá alebo iné osobné údaje (záľuby, opis vzhľadu, povahy, znalosti, zručnosti, vzdelanie, obľúbené veci, túžby...).
  V prípade, že je nevyhnutné takéto údaje poskytnúť, musia o tom vedieť rodičia alebo učitelia.

- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- **S nikým, s kým sa dieťa zoznámilo iba cez internet alebo mobil, sa nesmie stretávať samé osobne.** Tak ako v reálnom živote nechodia deti na stretnutie s neznámou osobou bez sprievodu niekoho ďalšieho, najlepšie rodiča, alebo aspoň súrodenca, kamaráta, tak aj na stretnutie s neznámou osobou, s ktorou sa dieťa zoznámilo iba cez internet alebo mobil, je stretnutie veľmi nebezpečné. Ak už dieťa ide na stretnutie, tak vždy aspoň s kamarátom. Rodičom by malo oznámiť na aké stretnutie ide, za kým ide, kde a kedy sa plánuje vrátiť. Stretnutie by malo byť na verejnom mieste, kde je veľa ľudí. Znakom bezpečnejšieho stretnutia je, že tomu, čo pozýva, nevadí, že dieťa príde s rodičom alebo inou dospelou osobou. Ak mu to vadí, ten človek nemá čisté úmysly.
- **Buďte podozrievavý voči človeku, ktorý dieťa presviedča, aby zatajovalo svoje internetové kamarátstvo pred rodičmi, alebo vystupuje ako tínedžer, ale nevie väčšinu odpovedí na otázky, ktoré bežne rovesníci poznajú.** Takýto človek chce deťom ublížiť, a preto klame a navádza, aby zatajili pozvanie na stretnutie s ním, aby si zmazali históriu četu, jeho emaily, sms, mms správy, a podobne.
- **Použitie lokalizačných služieb mobilného telefónu dieťaťa neznámou osobou je nebezpečné**. Vďaka lokalizácii môže ktorákoľvek osoba vyhľadať miesto pobytu dieťaťa, ak mu to samo z nevedomosti umožní.
- **Bluetooth spojenie cez mobilný telefón dieťaťa s neznámou osobou je nebezpečné**. Pomenujte mobilný telefón dieťaťa tak, aby z neho nebolo hneď jasné, že sa jedná o dieťa.
- **Nie všetko, čo je na internete, je pravda.** Vysvetlite deťom, nech neveria všetkému čo nájdu na internete. Informácie si je potrebné porovnať z viacerých zdrojov a v prípade nejasností sa poradiť s rodičmi alebo učiteľmi v škole.

- **Ak dieťa na internete alebo cez mobil niečo vyľaká, našlo niečo škaredé, desivé, niečo z čoho sa cíti trápne, zraňuje ho to alebo ohrozuje, vysvetlite mu, že to nie je jeho chyba.**
- **Ak sa dieťa cíti nepohodlne alebo trápne pri online konverzácii, má právo ju okamžite prerušiť a odísť z četovej miestnosti**. Ak sa pritom snažil človek zaviesť tému do sexuálnej oblasti nech dieťa o tom povie rodičom, alebo v škole učiteľom.
- **Váš domáci počítač (alebo hraciu konzolu) postavte do obývacej izby alebo na iné spoločné prístupové miesto v byte.** Najlepšie tak, aby rodič mal vždy výhľad na monitor**.** Nedávajte počítač do detských izieb. Majte dobrý prehľad o všetkých ďalších počítačoch, ktoré sú deťom prístupné.
- **Stanovte medzi deťmi a rodičmi jasné pravidlá pre používanie internetu**. Urobte si rozvrh na dni a presný čas, kedy má dieťa povolenie stráviť čas na internete, najlepšie v čase vašej prítomnosti. Podpísanú zmluvu vystavte v blízkosti počítača na viditeľnom mieste. Nezabudnite, ak si s vaším dieťaťom vytvoríte pravidlá o používaní internetu, stanovte si práva a povinnosti pre obe strany. Pravidla, by sa mali pravidelne aktualizovať. Vzor takejto „rodinnej zmluvy" nájdete na stránkach Zodpovedne.sk.
- **Najmenšie deti by nemali používať četovacie miestnosti bez moderátora, v ktorých môže byť dieťa najviac ohrozené.**
- **Vytvorte medzi dieťaťom a rodičom vzťah vzájomnej dôvery.** Majte prehľad o prezývkach (nickname) vašich detí, ktoré používajú na internete. Buďte opatrný, nebuďte dotieravý pri kontrole dieťaťa, vzájomná dôvera je veľmi dôležitá. Prílišná kontrola by mohla dieťa dohnať ku skrývaniu a zatajovaniu činností. Netrestajte dieťa za to, čo nie je jeho chyba, môže vám prestať dôverovať a mať strach a neistotu pri zdôverovaní sa s nejakým problémom. Je potrebné sa s deťmi veľa rozprávať, upozorniť ich na rôzne nebezpečenstvá, zaujímať sa a vedieť kde a ako trávia voľný čas, s kým telefonujú, emailujú, četujú, s kým sa stretávajú. Menšie deti si vyžadujú pravidelnú kontrolu. Ponúknite deťom adekvátne, zmysluplné a zaujímavé mimoškolské aktivity. Všímajte si viac svoje okolie. Nebuďte ľahostajní ani k cudzím deťom.
- **Dôveruj, ale preveruj.** Nie vždy sa dieťa zdôveruje rodičom, preto nezabudnite sledovať jeho nálady, zvyky, zmeny nálad a správanie, ktoré môže byť kľúčom k objasneniu príčiny. Kontrolujte, ktoré stránky navštevuje, s kým si píše emaily, hovorte s ním s kým a o čom si píše. Ak dieťa chodí na stránky s nevhodným obsahom, je možné pomocou filtra zakázať prístup na tieto stránky. Ak nechcete aby dieťa bolo vystavené riziku pri otváraní emailov, nainštalujte si program, ktorý povolí otvorenie emailu iba od známych ľudí zo zoznamu, adresáru. Pokiaľ to uznáte za vhodné, používajte monitorovacie nástroje, ktoré vám umožnia získať prehľad o chovaní vášho dieťaťa na internete.
- **Dbajte, aby dieťa hralo iba hry, ktoré sú určené správnej vekovej skupine a s vhodným obsahom.** Počítačové hry alebo hracie konzoly sú zatriedené podľa veku hráčov do skupín 3+, 4+, 6+, 7+, 12+, 16+, 18+. Obsahové ohrozenia hráčov sa delia na skupiny:
    - hra obsahuje vulgarizmy,
    - hra obsahuje diskriminačné prvky tj. obsahuje zobrazenia alebo materiály, ktoré môžu nabádať k diskriminácii,
    - hra znázorňuje užívanie drog,
    - hra môže pôsobiť na dieťa desivo až hrozivo,
    - hra znázorňuje nahotu alebo iné sexuálne správanie,
    - hra zobrazuje násilie,
    - hra, ktorá nabáda alebo vyučuje hazardné hry.
- **Pri výbere školy, mládežníckeho klubu, centra voľného času, letných táborov a podobne sa informujte, aké majú jednotlivé organizácie vypracované programy prevencie voči e-ohrozeniam.** Medzi e-ohrozenia patria:
    - Pedofília, pornografia (Pedofília, pornografia, sexturizmus, zverejňovanie erotiky...)
    - Závislosti (Drogy, anorexia, bulímia, sebapoškodzovanie, sekty, závislosť od internetu, mobilov, esemesiek, počítačových hier, návody na samovraždy, emo...),
    - Šikanovanie (Bullying, elektronické šikanovanie, zastrašovanie, ponižovanie, zosmiešňovanie, ohováranie, nadávanie, happy slapping...),
    - Diskriminácia (Xenofóbia, rasizmus, extréministické hnutia, totalitný režim...),

- Násilie (Agresivita, klubové chuligánstvo, terorizmus, flaming, hate speech...),
- Stretnutie s neznámou osobou (Internetové známosti, grooming, obchodovanie s ľuďmi...),
- Poskytovanie osobných údajov (Poskytovanie kontaktných, osobných údajov, majetkové pomery, phishing...),
- Internetové podvody (Počítačová kriminalita, falšovanie počítačových údajov, porušenia autorských a príbuzných práv...).

- **Neustále sa informujte, vzdelávajte, zlepšujte svoje zručnosti na internete, v mobilnej komunikácii a nových technológiách.** Súčasná generácia vyrastá s internetom a ich znalosti (aj jazykové), zručnosti sú vo väčšine prípadov lepšie ako u ich rodičov. Preto je potrebné snažiť sa s nimi aspoň držať krok a tak chrániť deti, seba a celú rodinu. Sledujte odbornú tlač, prípadne internetové stránky zaoberajúce sa danou problematikou.
- **Zvyšujte povedomie, šírte osvetu o zodpovednom používaní internetu, mobilu a nových technológií.**
- **Komunikujte s inými rodičmi, učiteľmi**, vymieňajte si informácie a poznatky.
- **Správajte sa Zodpovedne.sk!** Na internete alebo pri mobilnej komunikácii sa správajte tak ako v ozajstnom živote. Vysvetlite deťom, aby, neurobili niečo, čo by v skutočnom živote nespravili. Pravidlá slušného správania sa na internete nazývajú netiketa.

Diskriminácia (Diskriminácia, Xenofóbia, rasizmus, extréministické hnutia, totalitný režim)

Diskriminácia

Pojem diskriminácia pochádza z latinského slova discriminare, ktoré znamená rozlišovanie, rozdeľovanie. Diskriminácia je nežiaduce a nespravodlivé konanie, kedy sa zaobchádza s človekom či skupinou inak, ako s iným človekom na základe jeho odlišnosti, napr. rasového alebo etnického pôvodu, zdravotného či mentálneho stavu, veku, pohlavia, sexuálnej orientácie alebo vierovyznania. Diskriminujúco sa môže správať jednotlivec, skupina, firma aj štát.

Diskriminácia na základe:

Rasového pôvodu

Znamená, že sa s človekom zaobchádza odlišne pre jeho rasovú odlišnosť. Takýto prístup bol oficiálnym v niektorých štátoch, napr. Južnej Afriky počas apartheidu (oddelené spolužitie príslušníkov rôznych rás). Niektoré rasové skupiny môžu byť diskriminované aj geograficky a sociálne, čím sa znižuje ich šanca na rovnocenný prístup aj k takým veciam ako je internet, mobilný telefón.

Zdravotného, mentálneho stavu

Telesne či mentálne postihnutí ľudia sa stretávajú s diskrimináciou v každodennom živote neustále. Môže ísť o nerovný prístup pri hľadaní zamestnania, poskytovaní zdravotnej starostlivosti, fyzické bariéry pri pohybe, ktoré je možné odstrániť, ale nedeje sa tak a podobne. Medzi hlavné problémy pri zamestnávaní ľudí so zdravotným postihnutím patrí aj postoj zamestnávateľov a postoj verejnosti, ktorý pomáha udržiavať nepriaznivé konanie voči osobám s telesným alebo mentálnym znevýhodnením.

Nevýhody existujú napr. aj pri kurzoch internetu, počítačov. Nie vždy sú školitelia dodatočne vzdelávaní tak, aby mohli efektívne pomôcť jednotlivcom s osobitnými potrebami zvládať informačné technológie. Diskriminácia je aj to, keď internetová stránka nie je upravená pre nevidiace alebo slabozraké osoby (http://blindfriendly.sk).

Veku (ageizmus)

Môže sa zdať, že diskriminácia založená na veku je rovnaká pri všetkých vekových skupinách. Dá sa však povedať, že ide prevažne o tri vekové skupiny: diskriminácia mladých ľudí, ľudí nad 40 rokov a diskriminácia starých ľudí vo vysokom veku.

Pohlavia

Ide o nerovný prístup, ktorý vychádza z odlišnosti pohlaví. V spoločnosti sa často argumentuje touto odlišnosťou ako s príčinou slabosti a podriadenosti jedného pohlavia druhému, z čoho vychádzajú rodové nerovnosti a sexizmus prítomný v mnohých sférach spoločenského života. Často sa vo firmách napríklad stáva, že ak existuje možnosť výberu, automaticky sú na kurzy informačných technológií alebo výpočtovej techniky posielaní muži.

Sexuálnej orientácie

S nerovným zaobchádzaním sa stretávajú ľudia, ktorí majú odlišnú sexuálnu orientáciu ako väčšina spoločnosti. Môžu to byť gejovia a lesbičky, bisexuáli a bisexuálky, transsexuáli a transexuálky (GLBT). Medzi prejavy patria narážky, urážky, hanlivé kresby, oslovenia, slovné útoky a neskôr až otvorené násilie a fyzické útoky.

Vierovyznania

Diskriminácia na základe vierovyznania sa môže prejavovať u ľudí, ktorí majú odlišné vierovyznanie ako väčšina spoločnosti, prípadne sú bez vyznania. Priamo môžu byť títo ľudia diskriminovaní pri prijímaní do zamestnania, kedy sa preferuje určité (alebo naopak žiadne) vyznanie. Nepriamo ide o pravidlá a predpisy, ktoré znevýhodňujú niektoré skupiny ľudí a upierajú im práva a možnosti, ktoré majú ostatní príslušníci spoločnosti.

Pozitívna diskriminácia

Vyjadruje súbor politických či sociálnych opatrení alebo pravidiel, ktoré sú zamerané na podporu skupín menej zastúpených v spoločnosti na úkor dominantných. Ide napríklad o zámerné zvýhodňovanie a upravovanie pravidiel zamestnávania mladých ľudí, žien či príslušníkov iných rás ako je tá najrozšírenejšia. Odborníci vedú rozsiahle diskusie o tom, či je pozitívna diskriminácia naozaj riešením problémov alebo ich iba odsúva a prináša ďalšie.

Proces, ktorý zahŕňa aj diskrimináciu a vychádza prvotne z odlišnosti, môže viesť v konečnom dôsledku až ku genocíde. Má niekoľko stupňov:

- **Osočovanie** - ohováranie a slovné útoky na jednotlivcov a skupiny, šírenie fám.
- **Exklúzia** - vylúčenie z väčšinovej spoločnosti, vynechávanie so skupinových aktivít.
- **Diskriminácia** - nerovné zaobchádzanie s človekom na základe jeho odlišnosti.
- **Fyzické násilie** - agresivita a fyzické útoky na človeka či skupinu motivované jeho inakosťou.
- **Vyhladenie** - odstránenie skupiny ľudí, genocída (národa, rasy, etnickej alebo náboženskej skupiny).

Podľa zákona sa za diskrimináciu nepovažuje také odlišné zaobchádzanie z niektorého so spomínaných dôvodov, ktoré je odôvodnené povahou činností vykonávaných v zamestnaní alebo okolnosťami, za akých sa tieto činnosti vykonávajú. Tento dôvod musí byť opodstanený a tvoriť rozhodujúcu požiadavku na zamestnanie.

Xenofóbia

Pojem xenofóbia pochádza z gréckych slov xenos - cudzinec, neznámy a phobos – strach, obava. Ide o neopodstatnený strach a nenávisť voči neznámemu a odlišnému. Xenofóbny človek je ten, kto sa správa nenávistne, alebo pohŕdavo k odlišným ľuďom ako je on sám, predovšetkým k cudzincom, bez zjavného dôvodu alebo racionálneho vysvetlenia.

Xenofóbia môže mať dva rôzne smery. Prvým je nenávisť zameraná voči skupine populácie, ktorá sa vyskytuje v spoločnosti, ale nepovažuje sa za jej súčasť, napríklad imigranti. Môže ísť tiež o nenávisť voči skupine, ktorá sa v danej spoločnosti vyskytuje dlhodobo a táto môže vyústiť do agresívnych a násilných reakcií vedúcich k vylúčeniu tejto skupiny zo spoločnosti, v horšom prípade ku genocíde. Druhým smerom je xenofóbia kultúrna, ktorá je zameraná na nenávisť voči kultúrnym prvkom spoločnosti, ktoré sú považované za cudzorodé.

Xenofóbia je odlišná od rasizmu, aj keď sa na prvý pohľad zdajú veľmi podobné. Ak napríklad nemáme radi černocha z Francúzska preto, lebo je z Francúzska ide o xenofóbiu. Ak voči nemu máme nenávistné prejavy kvôli tomu, že je černoch, ide o rasizmus.

Rasizmus

Je konanie a praktiky, ktoré znevýhodňuje človeka alebo skupinu ľudí na základe jeho rasy.

Príklady zjavného rasizmu sú napríklad zastrašovanie, rasistické kresby, fyzické násilie, šikanovanie, rasistické poznámky a vtipy. Medzi ďalšie formy rasizmu, ktoré nie sú tak zjavné patrí napríklad diskriminácia pri prijímaní do zamestnania alebo diskriminačná politika, ktorá znevýhodňuje príslušníkov niektorých rás či už úmyselne alebo nie.

Rasizmus existuje v troch rovinách: individuálny, inštitucionálny a kultúrny.
Individuálnu rovinu pokrýva správanie jednotlivca, jeho prístupy, viera a hodnoty. Rasistické predsudky, stereotypy, fanatizmus, ponižovanie, násilie, vyhrážky alebo žiarlivosť patria medzi príklady rasistického postoja.

Inštitucionálna rovina sa prejavuje v praktikách, zvykoch, pravidlách a štandardoch organizácie, ktoré znevýhodňujú ľudí pre ich rasu alebo etnickú príslušnosť. Nemusí ísť vždy o zjavné odlišné správanie.

Napríklad pri prijímaní do zamestnania sa môže rasizmus prejaviť pri požadovaní vzdelania, ktoré nie je potrebné pre dané pracovné miesto.

Rasizmus sa môže prejavovať aj v kultúrnych hodnotách a viere. Ide napríklad o predstavu ako má vyzerať krásny človek, kto by mal zastávať post riaditeľa alebo naopak, kto by mohol byť zločinec.

Extrémistické hnutia

Nárast používania internetu je vhodným zázemím pre rôzne extrémistické skupiny (fašistické, xenofóbne, nacistické...). Prostredníctvom neho môžu propagovať svoje myšlienky, posolstvá a idey, vzájomne komunikovať, získavať nových členov a rozširovať sieť. Zároveň im poskytuje možnosť celosvetovo veľmi efektívne organizovať svoje aktivity – pochody, demonštrácie, stretnutia.

Vzniká množstvo internetových stránok, ktoré propagujú hnutia, a na ktorých ich členovia umiestňujú dokumenty, fotografie, videá zo svojich podujatí, organizujú výmenu predmetov a literatúry.

Prostredníctvom internetu je možné vyhľadávať celosvetovo hudobné CD, filmy s hľadanou témou, plagáty, letáky a iné materiály, ktoré sa používajú pri pochodoch a aktivitách hnutí. Je možné si stiahnuť životopisy diktátorov, ich knihy, posolstvá, preklady kníh ako je napr. Mein Kampf. Takto sa jednoducho môžu materiály reprodukovať, dopĺňať a globálne šíriť bez akejkoľvek cenzúry. Na internete sa môžeme stretnúť aj so súkromnými blogmi (internetové denníky) členov hnutí a prostredníctvom mobilných telefónov s nechcenými sms alebo mms správami.

Extrémistické hnutia používajú informačné technológie a internet na štyri základné aktivity:

- propagovanie ideológie,
- propagovanie nenávisti a násilia,
- ovládanie a kontrola,
- vyhľadávanie a atakovanie odporcov.

Obsah stránok vytvorených prívržencami extrémistických hnutí propaguje fašizmus, násilné hnutia, potlačuje práva ľudí. Nevyhnutne preto vyvstala potreba kontrolovať obsah internetu a vytvoriť zákony, ktoré by riešili tieto nenávistné prejavy vedúce k násiliu, diskriminácii a izolácii niektorých skupín.

Snahy mimovládnych organizácií a zákonodarcov tu však narážajú na slobodu slova a vyjadrovania, anonymitu páchateľov a ťažkú identifikáciu obete, preto je vytvorenie zákonov o počítačovej kriminalite výzvou pre mnoho odborníkov.

Je dôležité si uvedomiť, že často legálne aktivity majú dôsledky na formovanie verejnej mienky alebo názorov detí a mladých ľudí. Podobne aj celosvetový dosah týchto informácií spôsobuje, že aktivity uskutočnené na Slovensku môžu mať dosah takmer bez obmedzení kdekoľvek (protesty, násilnosti, štrajky...).

Legislatíva

Zákon č. 300/2005 Z. z. – Trestný zákon v znení neskorších predpisov

§421, §422 Podpora a propagácia skupín smerujúcich k potláčaniu základných práv a slobôd.

§423 Hanobenie národa, rasy a presvedčenia - Kto verejne hanobí

a) niektorý národ, jeho jazyk, niektorú rasu alebo etnickú skupinu, alebo
b) skupinu osôb pre jeho vyznanie alebo preto, že sú bez vyznania.

§424 Podnecovanie k národnostnej, rasovej a etnickej nenávisti – Kto verejne

a) sa vyhráža jednotlivcovi alebo skupine osôb pre ich príslušnosť k niektorému národu, národnosti, rase alebo etnickej skupine alebo pre ich farbu pleti, obmedzovaním ich práv a slobôd alebo kto takéto obmedzenie vykonal alebo
b) podnecuje k obmedzovaniu práv a slobôd niektorého národa, národnosti, rasy alebo etnickej skupiny.

Informácie na internete

www.diskriminacia.sk

www.stop-discrimination.info

www.futbal.rasizmus.sk

www.rasizmus.sk – Ľudia proti rasizmu

www.wikipedia.sk – Online encyklopédia

Prevencia

- **Akékoľvek prvky diskriminácie (xenofóbia, rasizmus, nacizmus, neofašizmus...) je potrebné oznámiť rodičom, učiteľom, polícii.**
- **Učte dieťa, aby si vážilo vlastnú osobnosť, jedinečnosť a originalitu.** Nemusí sa prispôsobovať rovesníkom za každú cenu pokiaľ bude mať dostatok vlastného sebavedomia.
- **Pomôžte dieťaťu v rozlišovaní skutočných priateľov, ktorí prejavujú úctu a porozumenie a bezohľadnými, ktorí skôr využívajú svoje známosti.**
- **Sledujte, či vaše dieťa nehrá hry, ktoré obsahujú diskriminačné prvky.** Také hry obsahujú zobrazenia alebo materiály, ktoré môžu nabádať k diskriminácii.

  Hry sa označujú: 
- **Naučte sa rozpoznávať znaky nenávistných prejavov**: hákové kríže, znaky, kresby, ponižovanie ľudí, násilné videá, snahu manipulovať a kontrolovať.
- **Uschovávajte si dôkazový materiál (emaily, sms, mms, históriu četu, internetové stránky).**

- **Vzdelávajte sa v histórii**. Získavajte informácie o fašizme, o dôsledkoch holokaustu, rasizme, totalitných režimoch, diskriminácii, ľudských právach. Budete si vedieť vytvoriť vlastný názor a brániť sa proti manipulujúcim argumentom.
- **Zabráňte diskriminačným (xenofóbnym, rasistickým, nacistickým) poznámkam a vtipom vo svojom okolí už v ich počiatkoch**. Môžete tak zastaviť vlnu ďalších skutkov a primäť ľudí sa zamyslieť.
- **Informujte sa o kritériách, na základe ktorých má byť vybraný uchádzač o zamestnanie, štúdium a podobne.** Budete tak mať možnosť sa ohradiť, ak budete mať pocit, že sa s vami jedná nespravodlivo.
- **Buďte aktívny a zistite si svoje občianske a ľudské práva**. Budete vedieť aké máte práva, kedy sú porušované a kam sa môžete obrátiť v prípade ich porušovania.
- **Internet môže byť nebezpečný.** Oboznámte dieťa o tom, že tak ako v bežnom živote aj na internete alebo pri mobilnej komunikácii, číha nebezpečenstvo. Môžete použiť príklad s elektrinou. Je to rovnako ako internet potrebná a nenahraditeľná vec, ale je to rovnako ako internet pri nezodpovednom používaní nebezpečná vec pre vaše zdravie alebo dokonca pre život. Pri internete na rozdiel od elektriny stále chýba takáto skúsenosť, či skôr osveta.
- **Nikdy neviete, kto je v skutočnosti na druhej strane internetu alebo mobilu.** Na druhej strane môže byť človek, ktorý klame o svojom veku, pohlaví, záujmoch, vzhľade a podobne. Takýto ľudia chcú deťom veľmi ublížiť a sú to:
    - pedofili...
    - ľudia, ktorí chcú fotografie a videá detí...
    - navádzajú na užívanie drog...
    - navádzajú na šikanovanie, alebo šikanujú deti...
    - nenávidia určité skupiny ľudí...
    - správajú sa agresívne, násilne...
    - chcú sa s deťmi tajne stretnúť, ublížiť im, uniesť ich...
    - získať osobné údaje o dieťati, jeho rodine, kamarátoch...
    - chcú oklamať, podviesť dieťa...
    - návádzajú na sebapoškodzovanie...
- **Nie je bezpečné dávať na internet alebo cez mobil svoje osobné údaje.** Vysvetlite deťom, čo sú to osobné údaje a prečo je nebezpečné zverejňovať svoje pravé meno a priezvisko, svoju fotografiu, video, vek, emailovú adresu, telefónne číslo, adresu domov, adresu školy, majetkové pomery, prístupové mená a heslá alebo iné osobné údaje (záľuby, opis vzhľadu, povahy, znalosti, zručnosti, vzdelanie, obľúbené veci, túžby...).
  V prípade, že je nevyhnutné takéto údaje poskytnúť, musia o tom vedieť rodičia alebo učitelia.

- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- **S nikým, s kým sa dieťa zoznámilo iba cez internet alebo mobil, sa nesmie stretávať samé osobne.** Tak ako v reálnom živote nechodia deti na stretnutie s neznámou osobou bez sprievodu niekoho ďalšieho, najlepšie rodiča, alebo aspoň súrodenca, kamaráta, tak aj na stretnutie s neznámou osobou, s ktorou sa dieťa zoznámilo iba cez internet alebo mobil, je stretnutie veľmi nebezpečné. Ak už dieťa ide na stretnutie, tak vždy aspoň s kamarátom. Rodičom by malo oznámiť na aké stretnutie ide, za kým ide, kde a kedy sa plánuje vrátiť. Stretnutie by malo byť na verejnom mieste, kde je veľa ľudí. Znakom bezpečnejšieho stretnutia je, že tomu, čo pozýva, nevadí, že dieťa príde s rodičom alebo inou dospelou osobou. Ak mu to vadí, ten človek nemá čisté úmysly.
- **Buďte podozrievavý voči človeku, ktorý dieťa presviedča, aby zatajovalo svoje internetové kamarátstvo pred rodičmi, alebo vystupuje ako tínedžer, ale nevie väčšinu odpovedí na otázky, ktoré bežne rovesníci poznajú.** Takýto človek chce deťom ublížiť, a preto klame a navádza, aby zatajili pozvanie na stretnutie s ním, aby si zmazali históriu četu, jeho emaily, sms, mms správy, a podobne.
- **Použitie lokalizačných služieb mobilného telefónu dieťaťa neznámou osobou je nebezpečné**. Vďaka lokalizácii môže ktorákoľvek osoba vyhľadať miesto pobytu dieťaťa, ak mu to samo z nevedomosti umožní.
- **Bluetooth spojenie cez mobilný telefón dieťaťa s neznámou osobou je nebezpečné**. Pomenujte mobilný telefón dieťaťa tak, aby z neho nebolo hneď jasné, že sa jedná o dieťa.

- **Nie všetko, čo je na internete, je pravda.** Vysvetlite deťom, nech neveria všetkému čo nájdu na internete. Informácie si je potrebné porovnať z viacerých zdrojov a v prípade nejasností sa poradiť s rodičmi alebo učiteľmi v škole.
- **Ak dieťa na internete alebo cez mobil niečo vyľaká, našlo niečo škaredé, desivé, niečo z čoho sa cíti trápne, zraňuje ho to alebo ohrozuje, vysvetlite mu, že to nie je jeho chyba.**
- **Ak sa dieťa cíti nepohodlne alebo trápne pri online konverzácii, má právo ju okamžite prerušiť a odísť z četovej miestnosti.** Ak sa pritom snažil človek zaviesť tému do sexuálnej oblasti nech dieťa o tom povie rodičom, alebo v škole učiteľom.
- **Váš domáci počítač (alebo hraciu konzolu) postavte do obývacej izby alebo na iné spoločné prístupové miesto v byte.** Najlepšie tak, aby rodič mal vždy výhľad na monitor**.** Nedávajte počítač do detských izieb. Majte dobrý prehľad o všetkých ďalších počítačoch, ktoré sú deťom prístupné.
- **Stanovte medzi deťmi a rodičmi jasné pravidlá pre používanie internetu.** Urobte si rozvrh na dni a presný čas, kedy má dieťa povolenie stráviť čas na internete, najlepšie v čase vašej prítomnosti. Podpísanú zmluvu vystavte v blízkosti počítača na viditeľnom mieste. Nezabudnite, ak si s vaším dieťaťom vytvoríte pravidlá o používaní internetu, stanovte si práva a povinnosti pre obe strany. Pravidla, by sa mali pravidelne aktualizovať. Vzor takejto „rodinnej zmluvy" nájdete na stránkach Zodpovedne.sk.
- **Najmenšie deti by nemali používať četovacie miestnosti bez moderátora, v ktorých môže byť dieťa najviac ohrozené.**
- **Vytvorte medzi dieťaťom a rodičom vzťah vzájomnej dôvery.** Majte prehľad o prezývkach (nickname) vašich detí, ktoré používajú na internete. Buďte opatrný, nebuďte dotieravý pri kontrole dieťaťa, vzájomná dôvera je veľmi dôležitá. Prílišná kontrola by mohla dieťa dohnať ku skrývaniu a zatajovaniu činností. Netrestajte dieťa za to, čo nie je jeho chyba, môže vám prestať dôverovať a mať strach a neistotu pri zdôverovaní sa s nejakým problémom. Je potrebné sa s deťmi veľa rozprávať, upozorniť ich na rôzne nebezpečenstvá, zaujímať sa a vedieť kde a ako trávia voľný čas, s kým telefonujú, mailujú, četujú, s kým sa stretávajú. Menšie deti si vyžadujú pravidelnú kontrolu. Ponúknite deťom adekvátne, zmysluplné a zaujímavé mimoškolské aktivity. Všímajte si viac svoje okolie. Nebuďte ľahostajní ani k cudzím deťom.
- **Dôveruj, ale preveruj.** Nie vždy sa dieťa zdôveruje rodičom, preto nezabudnite sledovať jeho nálady, zvyky, zmeny nálad a správanie, ktoré môže byť kľúčom k objasneniu príčiny. Kontrolujte, ktoré stránky navštevuje, s kým si píše emaily, hovorte s ním s kým a o čom si píše. Ak dieťa chodí na stránky s nevhodným obsahom, je možné pomocou filtra zakázať prístup na tieto stránky. Ak nechcete aby dieťa bolo vystavené riziku pri otváraní emailov, nainštalujte si program, ktorý povolí otvorenie emailu iba od známych ľudí zo zoznamu, adresáru. Pokiaľ to uznáte za vhodné, používajte monitorovacie nástroje, ktoré vám umožnia získať prehľad o chovaní vášho dieťaťa na internete.
- **Dbajte, aby dieťa hralo iba hry, ktoré sú určené správnej vekovej skupine a s vhodným obsahom.** Počítačové hry alebo hracie konzoly sú zatriedené podľa veku hráčov do skupín 3+, 4+, 6+, 7+, 12+, 16+, 18+. Obsahové ohrozenia hráčov sa delia na skupiny:
    - hra obsahuje vulgarizmy,
    - hra obsahuje diskriminačné prvky tj. obsahuje zobrazenia alebo materiály, ktoré môžu nabádať k diskriminácii,
    - hra znázorňuje užívanie drog,
    - hra môže pôsobiť na dieťa desivo až hrozivo,
    - hra znázorňuje nahotu alebo iné sexuálne správanie,
    - hra zobrazuje násilie,
    - hra, ktorá nabáda alebo vyučuje hazardné hry.
- **Pri výbere školy, mládežníckeho klubu, centra voľného času, letných táborov a podobne sa informujte, aké majú jednotlivé organizácie vypracované programy prevencie voči e-ohrozeniam.** Medzi e-ohrozenia patria:
    - Pedofília, pornografia (Pedofília, pornografia, sexturizmus, zverejňovanie erotiky...)
    - Závislosti (Drogy, anorexia, bulímia, sebapoškodzovanie, sekty, závislosť od internetu, mobilov, esemesiek, počítačových hier, návody na samovraždy, emo...),

- Šikanovanie (Bullying, elektronické šikanovanie, zastrašovanie, ponižovanie, zosmiešňovanie, ohováranie, nadávanie, happy slapping...),
- Diskriminácia (Xenofóbia, rasizmus, extréministické hnutia, totalitný režim...),
- Násilie (Agresivita, klubové chuligánstvo, terorizmus, flaming, hate speech...),
- Stretnutie s neznámou osobou (Internetové známosti, grooming, obchodovanie s ľuďmi...),
- Poskytovanie osobných údajov (Poskytovanie kontaktných, osobných údajov, majetkové pomery, phishing...),
- Internetové podvody (Počítačová kriminalita, falšovanie počítačových údajov, porušenia autorských a príbuzných práv...).

- **Neustále sa informujte, vzdelávajte, zlepšujte svoje zručnosti na internete, v mobilnej komunikácii a nových technológiách.** Súčasná generácia vyrastá s internetom a ich znalosti (aj jazykové), zručnosti sú vo väčšine prípadov lepšie ako u ich rodičov. Preto je potrebné snažiť sa s nimi aspoň držať krok a tak chrániť deti, seba a celú rodinu. Sledujte odbornú tlač, prípadne internetové stránky zaoberajúce sa danou problematikou.
- **Zvyšujte povedomie, šírte osvetu o zodpovednom používaní internetu, mobilu a nových technológií.**
- **Komunikujte s inými rodičmi, učiteľmi**, vymieňajte si informácie a poznatky.
- **Správajte sa Zodpovedne.sk!** Na internete alebo pri mobilnej komunikácii sa správajte tak ako v ozajstnom živote. Vysvetlite deťom, aby, neurobili niečo, čo by v skutočnom živote nespravili. Pravidlá slušného správania sa na internete nazývajú netiketa.

Násilie (Agresivita, klubové chuligánstvo, terorizmus, flaming, hate speech)

Agresivita

Agresivita (útočnosť, výbojnosť, dobyvačnosť) je energia vytvárajúca určitú dispozíciu reagovať resp. správať sa agresívne. Je úmyselná a pomáha dosiahnuť určený cieľ. Agresivita je prirodzenou súčasťou nášho života. Môže mať charakter pozitívneho ale i nežiaduceho negatívneho správania. Obe tieto formy prejavu pozorujeme rovnako v detstve ako i v dospelosti.

Pozitívna rovina

Efektívne využívanie agresivity v medziach normy pod vlastnou kontrolou, pomáha človeku zvládať mnohé situácie a dosahovať stanovené ciele. Najčastejšie ide o športové výkony, súťaženie, dosahovanie dobrých vzdelávacích výkonov, efektívne sebapresadzovanie, úspešná kariéra a pod. Teda zdravé využívanie agresívnej energie môže viesť k dosahovaniu mnohých cieľov a k sebarealizáciie v sociálnom prostredí.

Negatívna rovina

Ak agresivita má charakter útočného správania sa voči niečomu alebo niekomu s cieľom deštrukcie alebo ublíženia, ide o nežiaduce správanie. Niekedy prejav agresie u ľudí môže byť len situáciou vyvolané správanie, čiže nemá trvalý charakter. Ak však ide o zaužívaný spôsob reagovania na vonkajšie podnety, hovoríme o trvalej dispozícii agresívneho správania.

Človek, ktorý využíva agresívne správanie v negatívnej rovine je agresor

Charakteristika agresora: Túži po moci, je neschopný ovládať svoje správanie, napodobňuje negatívne vzory, má potrebu zviditeľniť sa, upozorniť na seba. Prevažne ide o človeka, ktorý má v niektorej oblasti života problémy. Niektorí agresori majú pocit sily len za podpory skupiny – partie, čo im dodáva odvahu, ale i pocit ochrany a tiež šancu ukázať sa a získavať rešpekt.

Kde všade sa s agresívnym správaním môžeme stretnúť?

V školskom prostredí, na ulici, v rodinnom prostredí, v kluboch, na športoviskách a pod. Súčasná doba priniesla nový priestor na prejavy agresivity a agresívneho správania – internet.

Ponúkané možnosti majú viac úrovní. Email, čet, instant Messenger - IM (ICQ, MSN, skype, yahoo a pod.), môžu byť využívané na vysielanie alebo prijímanie agresívnych správ vedúcich k obťažovaniu až manipulácii. Hry z hľadiska agresivity môžu mať na jednej strane charakter uvoľňovací na druhej podporujúci agresivitu. Mnohé stránky s charakterom informácie pre určité záujmové skupiny popisujú alebo zobrazujú rôzne agresívne aktivity a akcie, vyzdvihujú agresívne správanie, propagujú symboly smerujúce k agresívnemu vynucovaniu moci a nadvlády.

Útočník si svoje teritórium ako i obeť vždy vyhľadáva. Ohrozujúce je reagovanie na vysielané podnety vrátane náhodného zdanlivo pasívneho surfovania na týchto stránkach. Je to skrytá prevažne anonymná manipulácia.

Vývoj agresívneho správania

Najdôležitejší faktor pri formovaní správania človeka je rodinné prostredie, vzťahy v rámci rodiny, kultúra jej členov, akým vzorom sú pre svoje deti, aká je ich starostlivosť o deti a vzájomná úcta, ako sa stavajú k riešeniu problémov, aký majú hodnotový rebríček, ako sa správajú k iným ľuďom, k majetku svojmu a k cudziemu, aký je ich postoj k svojmu okoliu a pod.

Hneď po rodine zohráva najdôležitejšiu úlohu škola, v nej hlavne pedagógovia a spolužiaci. Učiteľ v živote žiaka zohráva mimoriadnu rolu nielen pre aktuálnu prítomnosť, ale i pre jeho budúcnosť. Je to človek ponúkajúci vedomosti, vzťah, dôveru, priateľstvo, autoritu a akceptáciu.

Významnú úlohu a vzor správania ďalej zohráva rovesnícka skupina hlavne v puberte. V dospelosti je to spoločenstvo združujúce ľudí podľa záujmov, životného štýlu, filozofie a hierarchie hodnôt , ktorá ich spája.

Agresor sa sám nezastaví. Obete a objekty stále rozširuje. Je schopný poškodzovať veci súkromné ale i spoločné. Útočí na mladších i starších, nezastaví sa ani pred autoritou. Na svoju realizáciu zdanlivej moci využíva všetky dostupné prostriedky. To znamená nielen priamy osobný kontakt, ale i anonymný, ktorý mu umožňuje manipulovať s neobmedzeným množstvom ľudí. Najľahšie sa získavajú deti, mladí dospelí a psychicky slabšie osobnosti.

Dôsledky pre obeť

Agresor vyvoláva pocity neistoty, strachu, časté zdravotné problémy ako sú bolesti hlavy, ranné nevoľnosti, búšenie srdca, vznik rôznych neurotických prejavov. U mladších detí sa môžu dostaviť nočné mory, pomočovanie, zajakávanie. Strata záujmu o školu, zhoršenie prospechu, záškoláctvo, únik od priateľov, únik do izolácie. Výrazne sa znižuje sebaúcta, zvyšuje sa pocit bezmocnosti, stráca sa sebadôvera. Objavuje sa depresia, sebadeštrukčné pokusy až túžba uniknúť – nežiť.

Všetci by mali poznať zákon, ktorý chráni každého človeka ako i majetok pred agresívnym správaním. Každý musí byť informovaný nielen o svojich právach ale i o povinnostiach. Každý človek je povinný udalosť agresívneho správania, ubližovania a poškodzovania oznámiť na príslušných orgánoch (polícia, sociálny odbor, prípadne na linku pomoci).

Pomoc, podpora a spolupráca s odborníkmi

Každý má právo na kvalitné prežitie svojho života. Obeť na ochranu a pokojný život, agresor na zmenu. Dôležité je hneď na začiatku zastaviť prvé známky negatívneho správania. Agresor musí dostať hranice, za ktoré nemôže ísť. Hranice musí dostať od rodičov, pedagógov, rovesníkov, od svojej partie od spoločnosti. V prípade, že to nepomôže, treba do situácie zapojiť zákonodarcov. Riešenie situácie neodkladajte, ak je potrebné vyhľadajte a využite sieť odborníkov, sociálnych pracovníkov, psychológov a pod.

Agresivita nie je izolovaný problém, preto je potrebný spoločný prístup hľadania pomoci, odhaľovania motivácie a nachádzania vhodných foriem riešenia v súčinnosti úzkej spolupráce

odborníkov a inštitúcií. Cieľom týchto krokov je presmerovanie negatívnej energie na pozitívnu, čo následne ponúka optimálnu kvalitu života.

Klubové chuligánstvo

Označuje neférové a deštruktívne správanie, ktoré je väčšinou spojené so športom, prevažne futbalom, hokejom. Ide o agresívne a násilné prejavy, vulgárne a slovné útoky často končiace fyzickým zranením.

Vznik futbalového chuligánstva sa spája s anglickými rowdies (preto sa často nazýva aj „anglická choroba“) na prelome 60. a 70. rokov 20. storočia. Následne sa začali skupiny organizovať, vytvárať kluby, plánovať svoju činnosť, výjazdy a rozvíjali sa aj medzinárodné kontakty s podobnými klubmi.

Futbalové chuligánstvo tvorí rizikovú kontrakultúru prevažne mladých ľudí, ktorí si týmto spôsobom hľadajú spriaznenú sociálnu skupinu. Môže ísť o ľudí, ktorí majú problém sa vyrovnať sami so sebou, majú nízke sebavedomie, sebahodnotenie a ťažko sa presadzujú v bežnom živote. Medzi chuligánov však patria aj vzdelaní a úspešní ľudia, pre ktorých je táto činnosť športom a relaxom vymykajúca sa bežným spoločenským normám.

Je ťažké jednoznačne stanoviť, kto tvorí chuligánov. Niektorí odborníci hovoria o tom, že ide hlavne o mladých, nevzdelaných ľudí, zo sociálne znevýhodnených vrstiev, prípadne z rozvráteného rodinného prostredia. Na druhej strane ich kritici tvrdia, že nie je možné takto striktne určiť skupinu chuligánov. Podľa nich ide o rôznorodé zoskupenia s rozličnými charakteristikami jednotlivcov, ktorých spája fenomén športového chuligánstva a jeho pravidlá.

Chuligánstvo rozhodne nepatrí k lacnému spôsobu trávenia voľného času – ceny vstupeniek a cestovného stúpajú hlavne pri zájazdoch do zahraničia. Tie si zároveň vyžadujú aj najviac času, čo sa prejavuje čerpaním dovoleniek, neplateného voľna alebo absenciou zo školy.

Chuligánstvo je založené na skupinových aktivitách – organizujú sa kluby, skupiny, partie, ktoré združujú jednotlivcov a spoločne realizujú svoje aktivity. Medzi hlavné činnosti, ktorými sa prejavujú chuligáni patrí:

- Vniknutie na hraciu plochu.
- Hádzanie predmetov na hráčov, rozhodcov, iných fanúšikov.
- Agresívne hádky s políciou, organizátormi.
- Vyhrážanie sa fyzickým útokom.
- Poškodzovanie majetku (sedačiek, vlakov, áut).
- Fyzické útoky voči ostatným fanúšikom, organizátorom, polícii, rozhodcom.
- Agresivita pri presunoch v dopravných prostriedkoch (demolovanie vlakov, autobusov, staníc, vyhrážky cestujúcim, fyzické ataky na okoloidúcich).

Športoví chuligáni sa v súčasnosti organizujú a koordinujú svoju činnosť aj prostredníctvom internetu, čím sa stávajú prístupní a videní širokému okruhu ľudí. Od polovice 90. rokov vznikajú internetové časopisy, web stránky, portály, na ktorých sa delia so svojimi zážitkami.

Skupiny chuligánov na svojich web stránkach uverejňujú:

- Fotografie a videá zo vzájomných bitiek, výtržností na štadiónoch.
- Presné popisy výjazdov (koľko ľudí a kde vycestovalo, aké boli pravidlá bitiek, na koho útočili...).
- Štatistiky výtržností (koľko chuligánov bolo zranených, zatknutých, aké boli najvážnejšie zranenia, koľko policajtov bolo zranených, aké boli škody na majetku, kto bol najvýraznejším výtržníkom...).
- Správy o svojej činnosti, plánované akcie.
- Propagáciu tohto životného štýlu, násilia.

Prostredníctvom internetu sa dajú jednotlivé skupiny veľmi jednoducho koordinovať, môžu si vymieňať skúsenosti, rady a podobne. Ide hlavne o:

- Prípravu a koordináciu stretnutí a násilností (bitkárska liga, tretí polčas).
- Výmenu zberateľských predmetov.
- Zdieľanie videí, fotografií.
- Predaj tričiek, šálov, zbraní.
- Tipy na miesta, kde je možné usporiadať stret dvoch klubov a vyhnúť sa polícii.
- Vytváranie medzinárodných „družieb“ klubov.
- Diskusie o pravidlách nastávajúcich bitiek, výsledkoch minulých.
- Odporúčania na bary, krčmy, v ktorých sa stretávajú.

Správanie športových chuligánov sa často dostáva do rozporu so zákonom, najmä ak ide o násilie voči skupine a jednotlivcovi, útok na verejného činiteľa, poškodenie veci a majetku, výtržníctvo, podnecovanie k národnostnej a rasovej neznášanlivosti, ubližovanie na zdraví...

Vzhľadom na to, že tento druh násilia nejavil od svojho vzniku tendenciu ustupovať vstúpili do platnosti dohovory a nariadenia, ktoré majú za cieľ eliminovať dôsledky a vyhnúť sa tomuto druhu násilností.

Legislatíva

Zákon č. 300/2005 Z.z. – Trestný zákon v znení neskorších prepisov

- *§144* Úkladná vražda – Kto iného úmyselne usmrtí s vopred uváženou pohnútkou.
- *§145* Vražda – Kto iného úmyselne usmrtí.
- *§147* Zabitie – Kto v úmysle spôsobiť ťažkú ujmu na zdraví inému z nedbanlivosti spôsobí smrť.
- *§155* Ublíženie na zdraví – Kto inému spôsobí ťažkú ujmu na zdraví.
- *§156* Kto inému úmyselne ublíži na zdraví.
- *§157* Kto inému z nedbanlivosti spôsobí ťažkú ujmu na zdraví, potrestá sa.
- *§245* Poškodzovanie cudzej veci - Kto zničí, poškodí alebo urobí neupotrebiteľnou cudziu vec a spôsobí tak na cudzom majetku malú škodu.
- *§359* Násilie proti skupine obyvateľov a proti jednotlivcovi – Kto sa skupine obyvateľov vyhráža smrťou, ťažkou ujmou na zdraví alebo inou ťažkou ujmou, alebo spôsobením škody veľkého rozsahu, alebo kto použije násilie proti skupine obyvateľov.

- *§360* Nebezpečné vyhrážanie – Kto sa inému vyhráža smrťou, ťažkou ujmou na zdraví alebo inou ťažkou ujmou takým spôsobom, že to môže vzbudiť dôvodnú obavu.
- *§364* Výtržníctvo – Kto sa dopustí verbálne alebo fyzicky, verejne alebo na mieste verejne prístupnom
- hrubej neslušnosti alebo výtržnosti najmä tým, že napadne iného, hanobí historickú alebo kultúrnu pamiatku,
- hrubým spôsobom ruší zhromaždenie občanov, alebo vyvoláva verejné pohoršenie vykonávaním pohlavného styku, vykonávaním sexuálneho exhibicionizmu alebo iných patologických sexuálnych praktík na takom mieste.

Európsky dohovor o násilí a neviazanosti divákov počas športových podujatí.

Zákon č. 300/2005 Z.z. – Trestný zákon

- *§364* – Výtržníctvo – Kto sa dopustí verbálne alebo fyzicky, verejne alebo na mieste verejne prístupnom
  a) hrubej neslušnosti alebo výtržnosti najmä tým, že napadne iného, hanobí historickú alebo kultúrnu pamiatku,
  b) hrubým spôsobom ruší zhromaždenie občanov, alebo
  c) vyvoláva verejné pohoršenie vykonávaním pohlavného styku, vykonávaním sexuálneho exhibicionizmu alebo iných patologických sexuálnych praktík na takom mieste
- *§155* - Kto inému spôsobí ťažkú ujmu na zdraví
- *§156* – Kto inému úmyselne ublíži na zdraví

Informácie na internete

www.futbal.rasizmus.sk/

www.radaeuropy.sk/?1413 - Európsky dohovor o násilí a neviazanosti divákov počas športových podujatí.

www.minv.sk/extremizmus

www.wikipedia.sk – Online encyklopédia

Prevencia

- **O agresivite a násilí sa otvorene rozprávajte.** Poznajte svoje práva a práva ostatných. Upozorňujte najmä deti na rôzne nebezpečenstvá, zaujímajte sa kde, ako a s kým trávia voľný čas, s kým telefonujú, mailujú, četujú, s kým sa stretávajú. Menšie deti pravidelne kontrolujte, rozprávajte sa o spolužiakoch a zážitkoch zo školy. Nájdite deťom vhodné voľno-časové aktivity, ktoré im vyplnia čas po škole. Veľa výtržníkov sa k tejto činnosti dostalo hlavne kvôli nude.
- **Zaregistrovanú agresivitu treba hneď v začiatkoch riešiť!**
- **Sledujte, či vaše dieťa nehrá hry, ktoré obsahujú vulgarizmy.**

  Hry sa označujú: 
- **Sledujte, či vaše dieťa nehrá hry, ktoré môžu pôsobiť na dieťa desivo až hrozivo.**

  Hry sa označujú: 

- **Sledujte, či vaše dieťa nehrá hry,** ktoré zobrazujú násilie.

  Hry sa označujú: 
- **V prípade, že sa vaše dieťa dostalo do skupiny chuligánov, vyhľadajte sociálne poradenstvo**. V zahraničí ale aj u nás sa začína odborná pomoc špecializovať na sociálnu a terénnu prácu s fanúšikmi, na prevenciu diváckeho násilia.
- **V zahraničí vyhľadajte „Fan Ambassy" počas veľkých súťaží (ME, MS) – koordinačné centrá pre fanúšikov.** Tieto centrá poskytujú informácie o ubytovaní, vstupenkách, organizácii podujatia a bezpečnostných opatrení. Pokiaľ sa chystáte vycestovať ako fanúšik, je to ideálny spôsob ako sa dostať k potrebným informáciám, a tak sa chrániť pred klubovým chuligánstvom.
- **Internet môže byť nebezpečný.** Oboznámte dieťa o tom, že tak ako v bežnom živote aj na internete alebo pri mobilnej komunikácii, číha nebezpečenstvo. Môžete použiť príklad s elektrinou. Je to rovnako ako internet potrebná a nenahraditeľná vec, ale je to rovnako ako internet pri nezodpovednom používaní nebezpečná vec pre vaše zdravie alebo dokonca pre život. Pri internete na rozdiel od elektriny stále chýba takáto skúsenosť, či skôr osveta.
- **Nikdy neviete, kto je v skutočnosti na druhej strane internetu alebo mobilu.** Na druhej strane môže byť človek, ktorý klame o svojom veku, pohlaví, záujmoch, vzhľade a podobne. Takýto ľudia chcú deťom veľmi ublížiť a sú to:
  - pedofili...
  - ľudia, ktorí chcú fotografie a videá detí...
  - navádzajú na užívanie drog...
  - navádzajú na šikanovanie, alebo šikanujú deti...
  - nenávidia určité skupiny ľudí...
  - správajú sa agresívne, násilne...
  - chcú sa s deťmi tajne stretnúť, ublížiť im, uniesť ich...
  - získať osobné údaje o dieťati, jeho rodine, kamarátoch...
  - chcú oklamať, podviesť dieťa...
  - návádzajú na sebapoškodzovanie...
- **Nie je bezpečné dávať na internet alebo cez mobil svoje osobné údaje.** Vysvetlite deťom, čo sú to osobné údaje a prečo je nebezpečné zverejňovať svoje pravé meno a priezvisko, svoju fotografiu, video, vek, emailovú adresu, telefónne číslo, adresu domov, adresu školy, majetkové pomery, prístupové mená a heslá alebo iné osobné údaje (záľuby, opis vzhľadu, povahy, znalosti, zručnosti, vzdelanie, obľúbené veci, túžby...). V prípade, že je nevyhnutné takéto údaje poskytnúť, musia o tom vedieť rodičia alebo učitelia.
- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- **S nikým, s kým sa dieťa zoznámilo iba cez internet alebo mobil, sa nesmie stretávať samé osobne.** Tak ako v reálnom živote nechodia deti na stretnutie s neznámou osobou bez sprievodu niekoho ďalšieho, najlepšie rodiča, alebo aspoň súrodenca, kamaráta, tak aj na stretnutie s neznámou osobou, s ktorou sa dieťa zoznámilo iba cez internet alebo mobil, je stretnutie veľmi nebezpečné. Ak už dieťa ide na stretnutie, tak vždy aspoň s kamarátom. Rodičom by malo oznámiť na aké stretnutie ide, za kým ide, kde a kedy sa plánuje vrátiť. Stretnutie by malo byť na verejnom mieste, kde je veľa ľudí. Znakom bezpečnejšieho stretnutia je, že tomu, čo pozýva, nevadí, že dieťa príde s rodičom alebo inou dospelou osobou. Ak mu to vadí, ten človek nemá čisté úmysly.
- **Buďte podozrievavý voči človeku, ktorý dieťa presviedča, aby zatajovalo svoje internetové kamarátstvo pred rodičmi, alebo vystupuje ako tínedžer, ale nevie väčšinu odpovedí na otázky, ktoré bežne rovesníci poznajú.** Takýto človek chce deťom ublížiť, a preto klame a navádza, aby zatajili pozvanie na stretnutie s ním, aby si zmazali históriu četu, jeho emaily, sms, mms správy, a podobne.
- **Použitie lokalizačných služieb mobilného telefónu dieťaťa neznámou osobou je nebezpečné**. Vďaka lokalizácii môže ktorákoľvek osoba vyhľadať miesto pobytu dieťaťa, ak mu to samo z nevedomosti umožní.
- **Bluetooth spojenie cez mobilný telefón dieťaťa s neznámou osobou je nebezpečné**. Pomenujte mobilný telefón dieťaťa tak, aby z neho nebolo hneď jasné, že sa jedná o dieťa.

- **Nie všetko, čo je na internete, je pravda.** Vysvetlite deťom, nech neveria všetkému čo nájdu na internete. Informácie si je potrebné porovnať z viacerých zdrojov a v prípade nejasností sa poradiť s rodičmi alebo učiteľmi v škole.
- **Ak dieťa na internete alebo cez mobil niečo vyľaká, našlo niečo škaredé, desivé, niečo z čoho sa cíti trápne, zraňuje ho to alebo ohrozuje, vysvetlite mu, že to nie je jeho chyba.**
- **Ak sa dieťa cíti nepohodlne alebo trápne pri online konverzácii, má právo ju okamžite prerušiť a odísť z četovej miestnosti**. Ak sa pritom snažil človek zaviesť tému do sexuálnej oblasti nech dieťa o tom povie rodičom, alebo v škole učiteľom.
- **Váš domáci počítač (alebo hraciu konzolu) postavte do obývacej izby alebo na iné spoločné prístupové miesto v byte.** Najlepšie tak, aby rodič mal vždy výhľad na monitor**.** Nedávajte počítač do detských izieb. Majte dobrý prehľad o všetkých ďalších počítačoch, ktoré sú deťom prístupné.
- **Stanovte medzi deťmi a rodičmi jasné pravidlá pre používanie internetu.** Urobte si rozvrh na dni a presný čas, kedy má dieťa povolenie stráviť čas na internete, najlepšie v čase vašej prítomnosti. Podpísanú zmluvu vystavte v blízkosti počítača na viditeľnom mieste. Nezabudnite, ak si s vaším dieťaťom vytvoríte pravidlá o používaní internetu, stanovte si práva a povinnosti pre obe strany. Pravidla, by sa mali pravidelne aktualizovať. Vzor takejto „rodinnej zmluvy" nájdete na stránkach Zodpovedne.sk.
- **Najmenšie deti by nemali používať četovacie miestnosti bez moderátora, v ktorých môže byť dieťa najviac ohrozené.**
- **Vytvorte medzi dieťaťom a rodičom vzťah vzájomnej dôvery.** Majte prehľad o prezývkach (nickname) vašich detí, ktoré používajú na internete. Buďte opatrný, nebuďte dotieravý pri kontrole dieťaťa, vzájomná dôvera je veľmi dôležitá. Prílišná kontrola by mohla dieťa dohnať ku skrývaniu a zatajovaniu činností. Netrestajte dieťa za to, čo nie je jeho chyba, môže vám prestať dôverovať a mať strach a neistotu pri zdôverovaní sa s nejakým problémom. Je potrebné sa s deťmi veľa rozprávať, upozorniť ich na rôzne nebezpečenstvá, zaujímať sa a vedieť kde a ako trávia voľný čas, s kým telefonujú, emailujú, četujú, s kým sa stretávajú. Menšie deti si vyžadujú pravidelnú kontrolu. Ponúknite deťom adekvátne, zmysluplné a zaujímavé mimoškolské aktivity. Všímajte si viac svoje okolie. Nebuďte ľahostajní ani k cudzím deťom.
- **Dôveruj, ale preveruj.** Nie vždy sa dieťa zdôveruje rodičom, preto nezabudnite sledovať jeho nálady, zvyky, zmeny nálad a správanie, ktoré môže byť kľúčom k objasneniu príčiny. Kontrolujte, ktoré stránky navštevuje, s kým si píše emaily, hovorte s ním s kým a o čom si píše. Ak dieťa chodí na stránky s nevhodným obsahom, je možné pomocou filtra zakázať prístup na tieto stránky. Ak nechcete aby dieťa bolo vystavené riziku pri otváraní emailov, nainštalujte si program, ktorý povolí otvorenie emailu iba od známych ľudí zo zoznamu, adresáru. Pokiaľ to uznáte za vhodné, používajte monitorovacie nástroje, ktoré vám umožnia získať prehľad o chovaní vášho dieťaťa na internete.
- **Dbajte, aby dieťa hralo iba hry, ktoré sú určené správnej vekovej skupine a s vhodným obsahom.** Počítačové hry alebo hracie konzoly sú zatriedené podľa veku hráčov do skupín 3+, 4+, 6+, 7+, 12+, 16+, 18+. Obsahové ohrozenia hráčov sa delia na skupiny:
    - hra obsahuje vulgarizmy,
    - hra obsahuje diskriminačné prvky tj. obsahuje zobrazenia alebo materiály, ktoré môžu nabádať k diskriminácii,
    - hra znázorňuje užívanie drog,
    - hra môže pôsobiť na dieťa desivo až hrozivo,
    - hra znázorňuje nahotu alebo iné sexuálne správanie,
    - hra zobrazuje násilie,
    - hra, ktorá nabáda alebo vyučuje hazardné hry.
- **Pri výbere školy, mládežníckeho klubu, centra voľného času, letných táborov a podobne sa informujte, aké majú jednotlivé organizácie vypracované programy prevencie voči e-ohrozeniam.** Medzi e-ohrozenia patria:
    - Pedofília, pornografia (Pedofília, pornografia, sexturizmus, zverejňovanie erotiky...)
    - Závislosti (Drogy, anorexia, bulímia, sebapoškodzovanie, sekty, závislosť od internetu, mobilov, esemesiek, počítačových hier, návody na samovraždy, emo...),

- Šikanovanie (Bullying, elektronické šikanovanie, zastrašovanie, ponižovanie, zosmiešňovanie, ohováranie, nadávanie, happy slapping...),
- Diskriminácia (Xenofóbia, rasizmus, extréministické hnutia, totalitný režim...),
- Násilie (Agresivita, klubové chuligánstvo, terorizmus, flaming, hate speech...),
- Stretnutie s neznámou osobou (Internetové známosti, grooming, obchodovanie s ľuďmi...),
- Poskytovanie osobných údajov (Poskytovanie kontaktných, osobných údajov, majetkové pomery, phishing...),
- Internetové podvody (Počítačová kriminalita, falšovanie počítačových údajov, porušenia autorských a príbuzných práv...).

- **Neustále sa informujte, vzdelávajte, zlepšujte svoje zručnosti na internete, v mobilnej komunikácii a nových technológiách.** Súčasná generácia vyrastá s internetom a ich znalosti (aj jazykové), zručnosti sú vo väčšine prípadov lepšie ako u ich rodičov. Preto je potrebné snažiť sa s nimi aspoň držať krok a tak chrániť deti, seba a celú rodinu. Sledujte odbornú tlač, prípadne internetové stránky zaoberajúce sa danou problematikou.
- **Zvyšujte povedomie, šírte osvetu o zodpovednom používaní internetu, mobilu a nových technológií.**
- **Komunikujte s inými rodičmi, učiteľmi**, vymieňajte si informácie a poznatky.
- **Správajte sa Zodpovedne.sk!** Na internete alebo pri mobilnej komunikácii sa správajte tak ako v ozajstnom živote. Vysvetlite deťom, aby, neurobili niečo, čo by v skutočnom živote nespravili. Pravidlá slušného správania sa na internete nazývajú netiketa.

Stretnutie s neznámou osobou (Internetové známosti, grooming, obchodovanie s ľuďmi)

Internetové známosti

Vyhľadávanie priateľov cez internet sa stáva v dnešnej dobe čoraz častejším spôsobom zoznamovania. Z rôznych dôvodov sa takto ľudia snažia nájsť spriaznené osoby, s ktorými by mohli stráviť niekoľko chvíľ, či už online alebo neskôr aj osobne. Zoznamovacie agentúry alebo web stránky si iba málokedy robia prieskum klientov a overovanie údajov, ktoré poskytli. Opatrnosť je preto v každom prípade tou najnutnejšou obranou pred nebezpečenstvami, ktoré takéto stretnutia môžu priniesť.

Treba si pamätať, že:

- internet je nevhodné miesto na udávanie detailov o svojej osobe, súkromných plánoch. Sú tu totiž dostupné komukoľvek a kedykoľvek,
- potenciálne nebezpečné osoby číhajú na zraniteľné a ľahko dostupné obete. Neustále kontrolujú údaje o osobách a vyberajú si objekt svojho záujmu,
- ak zverejníte svoje osobné údaje, detaily a ste ochotní sa stretnúť s osobou, ktorú ste spoznali cez internet, stávate sa aj nevedomky možnou obeťou,
- miesta, kde môžete stretnúť nebezpečných ľudí sú četové miestnosti, otvorené fóra, diskusie. Vždy si pamätajte, že kohokoľvek stretnete, nikdy neviete, ktoré informácie sú skutočne pravdivé.

Stretávanie sa s ľuďmi cez internet nesie so sebou v porovnaní s bežným fyzickým kontaktom väčšie riziká z niekoľkých dôvodov:

- Väčšina našich obranných mechanizmov vychádza z fyzickej blízkosti s osobou. Vidíme ako osoba vyzerá, ako sa oblieka, ako hovorí, gestikuluje, vieme lepšie odhadnúť či osoba klame podľa reakcie, očného kontaktu. Takto môžeme odpozorovať signály, ktoré nás vnútorne varujú. Žiadna z týchto vecí nám nie je dostupná pokiaľ komunikujeme s človekom cez internet a tak sa výrazne oslabujú naše varovné signály.
- Bezpečie, ktoré nám poskytujú naši susedia, okolie, blízkosť rodičov či kamarátov mizne našou prítomnosťou na internete.
- Pri stretnutí s osobou cez internet nemáme možnosť nechať danú osobu posúdiť kamarátom, blízkej osobe. Pri fyzických stretnutiach si často nechávame poradiť, či je osoba sympatická, či sa zdá „v poriadku“ alebo či sa jej máme radšej vyhnúť. Samozrejme, nie vždy musia podobné rady od známych vystihnúť realitu, ale aspoň máme ďalší názor, ktorý nás môže varovať.

Grooming

Grooming (z anglického groom - pripraviť sa, upraviť sa) je zámerné vytváranie dôverného vzťahu dospelým človekom voči dieťaťu, príprava pôdy, vhodnej situácie s úmyslom mať následne sexuálny kontakt. Sexuálne obťažovanie málokedy začína z ničoho nič. Zväčša sa páchatelia zaoberajú touto myšlienkou a až neskôr, po dôkladnej príprave, ju aj realizujú.

Grooming môže obsahovať aktivity, ktoré sú samé o sebe legálne a beztrestné, ich nebezpečenstvo spočíva v tom, že neskôr vedú k sexuálnemu zneužívaniu. Typickým je získanie si dôvery dieťaťa a podobne aj osoby zodpovednej za dieťa. Výskumy totiž dokazujú, že dieťa menej často oznámi kriminálny čin, ak je spáchaný človekom, ktorého pozná a verí mu. Podobne aj blízky vzťah s rodičmi či rodinnými príslušníkmi vedie k tomu, že okolie je menej podozrievavé a nedôverčivé voči páchateľovi.

Príklady:

- neobvyklý záujem o priateľstvo dieťaťa,
- peňažné, či vecné dary bez zjavného dôvodu,
- vychádzky či stretnutia s dieťaťom mimo dozoru dospelých ,
- ukazovanie pornografie dieťaťu,
- rozhovory o sexuálnych témach, ktoré nie sú primerané veku dieťaťa,
- neprimerané zasahovanie do súkromia dieťaťa (napr. odprevádzanie do kúpeľne),
- fyzický kontakt s dieťaťom (objatia, bozky, hladkanie), aj keď oň nie je zo strany dieťaťa záujem,
- rozhovory s dieťaťom o témach, ktoré sa bežne riešia s dospelými (manželstvo,...).

Grooming cez internet, mobilný telefón

Internet a mobilný telefón považujú osoby, ktoré majú sklony k tomuto správaniu, za vhodný priestor, v ktorom sa môže odohrávať široká škála sexuálneho zneužívania. Poskytuje totiž dostatočnú anonymitu a možnosť zmeniť identitu. Môžu takto vystupovať ako dieťa, rovesník a dohodnúť si osobné stretnutie s vyhliadnutým dieťaťom.

Nová štúdia o kybernetickom priestore uskutočnená na University of Central Lancashire priniesla popis procesu, ktorý je využívaný pedofilmi pri kontakte detí cez internet, mobilný telefón s úmyslom neskoršieho sexuálneho obťažovania.

- **Priateľstvo.** Snaha nadviazať kontakt s dieťaťom na súkromnom čete, kde budú izolovaní od ostatných užívateľov. Dieťa je často žiadané o zaslanie „nesexuálnych“ fotografií z bežného života.
- **Vytváranie vzťahu.** Vytvorenie ilúzie u dieťaťa, ktoré má nejaký problém, že ho môže riešiť s ním ako s najlepším priateľom.
- **Zhodnocovanie rizika.** Vypytovanie sa dieťaťa, kde je umiestnený počítač, kto iný ho používa. Navádzajú dieťa aby si zmazalo históriu četu, jeho emaily, sms, mms správy. Takto znižujú riziko, že budú odhalení rodičmi alebo inou dospelou osobou.
- **Budovanie výnimočnosti.** Vytváranie vzájomného vzťahu plného lásky a dôvery, ktorý dieťa považuje za jedinečný, výnimočný. Získava si takto „kamaráta“, s ktorým môže riešiť problémy, ktoré ho trápia a znepokojujú.
- **Sexuálne reči.** Zaťahovanie dieťaťa do otvorenej konverzácie o sexualite. Osoba si už žiada fotografie so sexuálnym podtónom. V tomto bode sa zväčša pedofil snaží zorganizovať osobné stretnutie s dieťaťom.

Aké môžu byť znaky, že je dieťa obeťou groomingu alebo sexuálneho obťažovania:

- strach, bojí sa určitých ľudí alebo miest (vychovávateľ/ka, príbuzný/á...),
- problémy so spaním, nočné mory,
- nevysvetliteľné zmeny správania (veselé dieťa je zrazu smutné, zakríknuté, ustrašené),
- kresby, detské hry či túžby môžu obsahovať sexuálne motívy,
- strata chuti do jedla, problémy s trávením, žalúdočné problémy,
- simulovanie „dospeláckych“ sexuálnych praktík s hračkami, bábikami,
- nové názvy pre intímne časti tela, ktoré sa nedozvedelo v rodine,
- nové hračky, oblečenie alebo peniaze, ktoré nedostalo od rodičov,
- negatívny sebaobraz, nízka mienka o sebe, svojom tele.

Obchodovanie s ľuďmi

Obchodovanie s ľuďmi (human trafficking) je momentálne jedným z najvýnosnejších obchodov a najrozšírenejším druhom kriminality. Za účelom využitia vášho tela alebo služieb vás niekto premiestni z jedného miesta na druhé s prísľubom lepšej práce, manželstva alebo inej výhody používajúc nátlak, podvod, falošné údaje alebo silu. Ani v dnešnej dobe sa neostýchajú moderní otrokári ublížiť vám alebo vašej rodine.

Únos a obchodovanie s ľuďmi je aj dnes celosvetový problém. Každý si môže povedať: „mne sa to nemôže stať". Pravdou je, že sa to ľuďom stáva každý deň na celom svete. Páchatelia lákajú ľudí na vidinu lepšej práce v zahraničí a neskôr ich nútia vykonávať sexuálne služby, natáčať filmy alebo pracovať v neľudských podmienkach. Obchodníci, často celé skupiny, sľubujú uhradiť vstupné náklady ako sú cestovné, poistenie, ubytovanie či pracovné povolenie. Podozrivými môžu byť inzeráty napríklad modelingových agentúr, cestovných či au–pair agentúr. V niektorých oblastiach (prevažne Ázia a východná Európa) je rozvinuté aj tzv. manželstvo na objednávku, kedy si prostredníctvom internetu a mailov ženích vyberie nevestu, väčšinou z chudobných pomerov a túžiacu po lepšom živote. Táto sa však dostáva do rizika, že sa stane predmetom obchodu so ženami.

Obrovským problémom je obchodovanie s deťmi, odhaduje sa, že každoročne je unesených 1,2 milióna detí na celom svete. Využívajú sa ako zdroj lacnej pracovnej sily, na sexuálne služby alebo ako detskí vojaci. Únoscovia často využívajú nevedomosť a zlé sociálno-ekonomické podmienky detí a ich rodín, pre ktoré sú často nádejou na lepší život. Zraniteľnosť detí navyše podporujú mýty ako sexuálny styk s pannou môže vyliečiť HIV/AIDS.

Informačné technológie sa v tomto prípade ukazujú ako dvojsečná zbraň. Na jednej strane uľahčujú život miliónom ľudí v práci, škole, vo voľnom čase. Na druhej však uľahčujú aj obchod s ľuďmi. Prostredníctvom internetu si kriminálne skupiny môžu udržiavať kontakt, vymieňať údaje a plánovať svoje aktivity. Zároveň sa internet stáva priestorom pre nákup a predaj pornografie, vytváranie komunít konzumentov pornografie a ich komunikáciu. Prostredníctvom internetu si môže páchateľ vystopovať obete, zistiť situáciu v danej rodine, nadviazať kontakt a následne dohodnúť osobné stretnutie.

Nie vždy sú obete unesené neznámymi páchateľmi. Často ide o ľudí, ktorých poznajú: susedia, príbuzní, priatelia, kolegovia a podobne. Po únose sú obete väčšinou izolované od okolia, žijú alebo pracujú v neprípustných podmienkach. Keďže sú ďaleko od domova, často bez znalosti jazyka krajiny, majú sťaženú cestu na políciu, úrady alebo iné inštitúcie, kde by im mohli poskytnúť pomoc. Páchatelia im odnímajú doklady, fyzicky ich týrajú a vyhrážajú sa ublížením im alebo ich rodine.

Obete obchodovania s ľuďmi majú svoje práva! Aj keď ste v krajine nelegálne, môžete sa obrátiť na inštitúcie, ktoré vám pomôžu. Ide o poradenstvo, azylové domy, lekárske ošetrenia a nakoniec núdzový prevoz do domovskej krajiny. Okrem polície môžu pomoc poskytnúť inštitúcie ako nemocnice, kostoly či farnosti, požiarny zbor, azylové domy pre ženy, organizácie zaoberajúce sa pomocou imigrantom alebo veľvyslanectvo.

Legislatíva

Zákon č. 300/2005 Z.z. – Trestný zákon v znení neskorších predpisov

- *§179* Obchodovanie s ľuďmi - Kto s použitím podvodného konania, ľsti, obmedzovania osobnej slobody, násilia, hrozby násilia, hrozby inej ťažkej ujmy alebo iných foriem donucovania, prijatia alebo poskytnutia peňažného plnenia či iných výhod na dosiahnutie súhlasu osoby, na ktorú je iná osoba odkázaná, alebo zneužitia svojho postavenia alebo zneužitia bezbrannosti alebo inak zraniteľného postavenia zláka, prepraví, prechováva, odovzdá alebo prevezme iného, hoci aj s jeho súhlasom, na účel jeho prostitúcie alebo inej formy sexuálneho vykorisťovania vrátane pornografie, nútenej práce či nútenej služby, otroctva alebo praktík podobných otroctvu, nevoľníctva, odoberania orgánov, tkanív či bunky alebo iných foriem vykorisťovania alebo kto zláka, prepraví, prechováva, odovzdá alebo prevezme osobu mladšiu ako osemnásť rokov, hoci aj s jej súhlasom, na účel jej prostitúcie alebo inej formy sexuálneho vykorisťovania vrátane pornografie, nútenej práce či nútenej služby, otroctva alebo praktík podobných otroctvu, nevoľníctva, odoberania orgánov, tkanív či bunky alebo iných foriem vykorisťovania.
- *§180* Obchodovanie s deťmi – Kto v rozpore so všeobecne záväzným právnym predpisom zverí do moci iného dieťa na účel adopcie.
- *§181* Kto za odmenu zverí dieťa do moci iného na účel jeho využívania na detskú prácu alebo na iný účel.
- *§182* Pozbavenie osobnej slobody – Kto iného neoprávnene pozbaví osobnej slobody.
- *§183* Obmedzovanie osobnej slobody – Kto inému bez oprávnenia bráni užívať osobnú slobodu.
- *§184* Obmedzovanie slobody pobytu – Kto ľsťou alebo násilím, hrozbou násilia alebo inej ujmy
    a) iného neoprávnene núti k pobytu na určitom mieste alebo
    b) inému neoprávnene bráni k pobytu na určitom mieste.
- *§185* Branie rukojemníka – Kto sa zmocní rukojemníka a hrozí, že ho usmrtí alebo že mu spôsobí ujmu na zdraví alebo inú ujmu s cieľom donútiť iného, aby niečo konal, opomenul alebo strpel.

Informácie na internete

http://www.radaeuropy.sk/?obchodovanie-s-ludmi

www.wikipedia.sk – Online encyklopédia

Prevencia

- **Pedofil sa najčastejšie snaží svoju obeť získať spoločnými záujmami, porozumením, pochopením problémov a podobne.** Ďalšou fázou je, že sa s ňou chce stretnúť, možno si svoj vek necháva v tajnosti a ak nie, aj tak má dobré taktiky ako dieťa zmiasť. Najčastejšie využíva svoj starší vek ako výhodu, že im bude ako ocko, starší brat, starší kamarát, ktorý im bude pomáhať.
- **Nedávajte na internet alebo cez mobil žiadne fotografie, videá, na ktorých ste v plavkách, v spodnej bielizni, máte odhalené časti tela alebo pôsobíte eroticky.** Fotoalbumy, videoalbumy na internete alebo v mobiloch nie sú bezpečné, aj keď sa píše, že sú „súkromné“, „zamknuté“ a podobne. Obsah sa môže dostať na voľne dostupné miesta a vaše fotografie, videá uvidia všetci: rodičia, učitelia, spolužiaci ale aj osoby, ktoré vám môžu ublížiť. Fotografie z detstva môžu byť zneužité pedofilom, fotografie z rodinných osláv, dovoleniek prezradia rodinné, sociálne zázemie. Fotografie alebo videá, na ktorých je váš byt, dom, škola môžu identifikovať adresy vášho pobytu. Ostatné osobné fotografie zverejňujte v malom rozlíšení (max 200x200 pixlov/bodov), tak sťažíte ich zneužitie. Fotografie alebo videá môže byť zneužité aj za účelom poníženie, zahanbenie, zastrašenie alebo vydierania.

- **Najmenšie deti by mali navštevovať iba „detské“ stránky.** Na Slovensku iniciatíva „child-friendly“ zatiaľ neexistuje. Deťom priateľské stránky, čo je slovenský preklad, by napríklad nemali tolerovať poskytovanie osobných informácii bez povolenia rodičov, nemali by obsahovať nevhodný obsah pre ich vekovú kategóriu, mali by garantovať vek osôb v četoch a podobne.
- **Pri ceste do zahraničia urobte potrebné opatrenia, ktoré vám zaistia väčšiu bezpečnosť**:
    - zistite si adresu a telefonický kontakt na Slovenské veľvyslanectvo v danej krajine,
    - naučte sa meno, adresu a kontakt na osobu alebo miesto kde sa máte dostaviť,
    - skontrolujte cez neziskové organizácie (predovšetkým tie, ktoré sa zaoberajú násilím na ženách, ľudskými právami) či je daná agentúra alebo firma registrovaná, či s ňou nemajú zlé skúsenosti,
    - zistite si na internete referencie k jednotlivým agentúram, prípadne vyhľadajte podozrivé údaje o osobách,
    - povedzte vašim priateľom a rodine, že odchádzate a dajte im adresu a kontakt, kde vás môžu nájsť,
    - snažte sa nevydať pas alebo iné osobné doklady žiadnej ďalšej osobe,
    - urobte si kópiu vašich dokladov a schovajte ju, aj doklady, na bezpečné miesto,
    - naučte sa základné frázy, ktoré vás môžu zachrániť v jazyku krajiny kam cestujete,
    - kontaktujte po príchode vašu rodinu a priateľov, udržiavajte s nimi neustály kontakt, dohodnite si vhodné slovné spojenia, ktoré budú znamenať, že niečo nie je v poriadku.
- **Internet môže byť nebezpečný.** Oboznámte dieťa o tom, že tak ako v bežnom živote aj na internete alebo pri mobilnej komunikácii, číha nebezpečenstvo. Môžete použiť príklad s elektrinou. Je to rovnako ako internet potrebná a nenahraditeľná vec, ale je to rovnako ako internet pri nezodpovednom používaní nebezpečná vec pre vaše zdravie alebo dokonca pre život. Pri internete na rozdiel od elektriny stále chýba takáto skúsenosť, či skôr osveta.
- **Nikdy neviete, kto je v skutočnosti na druhej strane internetu alebo mobilu.** Na druhej strane môže byť človek, ktorý klame o svojom veku, pohlaví, záujmoch, vzhľade a podobne. Takýto ľudia chcú deťom veľmi ublížiť a sú to:
    - pedofili...
    - ľudia, ktorí chcú fotografie a videá detí...
    - navádzajú na užívanie drog...
    - navádzajú na šikanovanie, alebo šikanujú deti...
    - nenávidia určité skupiny ľudí...
    - správajú sa agresívne, násilne...
    - chcú sa s deťmi tajne stretnúť, ublížiť im, uniesť ich...
    - získať osobné údaje o dieťati, jeho rodine, kamarátoch...
    - chcú oklamať, podviesť dieťa...
    - návádzajú na sebapoškodzovanie...
- **Nie je bezpečné dávať na internet alebo cez mobil svoje osobné údaje.** Vysvetlite deťom, čo sú to osobné údaje a prečo je nebezpečné zverejňovať svoje pravé meno a priezvisko, svoju fotografiu, video, vek, emailovú adresu, telefónne číslo, adresu domov, adresu školy, majetkové pomery, prístupové mená a heslá alebo iné osobné údaje (záľuby, opis vzhľadu, povahy, znalosti, zručnosti, vzdelanie, obľúbené veci, túžby...). V prípade, že je nevyhnutné takéto údaje poskytnúť, musia o tom vedieť rodičia alebo učitelia.
- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- **S nikým, s kým sa dieťa zoznámilo iba cez internet alebo mobil, sa nesmie stretávať samé osobne.** Tak ako v reálnom živote nechodia deti na stretnutie s neznámou osobou bez sprievodu niekoho ďalšieho, najlepšie rodiča, alebo aspoň súrodenca, kamaráta, tak aj na stretnutie s neznámou osobou, s ktorou sa dieťa zoznámilo iba cez internet alebo mobil, je stretnutie veľmi nebezpečné. Ak už dieťa ide na stretnutie, tak vždy aspoň s kamarátom. Rodičom by malo oznámiť na aké stretnutie ide, za kým ide, kde a kedy sa plánuje vrátiť. Stretnutie by malo byť na verejnom mieste, kde je veľa ľudí. Znakom bezpečnejšieho stretnutia je, že tomu, čo pozýva, nevadí, že dieťa príde s rodičom alebo inou dospelou osobou. Ak mu to vadí, ten človek nemá čisté úmysly.
- **Buďte podozrievavý voči človeku, ktorý dieťa presviedča, aby zatajovalo svoje internetové kamarátstvo pred rodičmi, alebo vystupuje ako tínedžer, ale nevie väčšinu odpovedí na otázky,**

ktoré bežne rovesníci poznajú. Takýto človek chce deťom ublížiť, a preto klame a navádza, aby zatajili pozvanie na stretnutie s ním, aby si zmazali históriu četu, jeho emaily, sms, mms správy, a podobne.

- **Použitie lokalizačných služieb mobilného telefónu dieťaťa neznámou osobou je nebezpečné.** Vďaka lokalizácii môže ktorákoľvek osoba vyhľadať miesto pobytu dieťaťa, ak mu to samo z nevedomosti umožní.
- **Bluetooth spojenie cez mobilný telefón dieťaťa s neznámou osobou je nebezpečné.** Pomenujte mobilný telefón dieťaťa tak, aby z neho nebolo hneď jasné, že sa jedná o dieťa.
- **Nie všetko, čo je na internete, je pravda.** Vysvetlite deťom, nech neveria všetkému čo nájdu na internete. Informácie si je potrebné porovnať z viacerých zdrojov a v prípade nejasností sa poradiť s rodičmi alebo učiteľmi v škole.
- **Ak dieťa na internete alebo cez mobil niečo vyľaká, našlo niečo škaredé, desivé, niečo z čoho sa cíti trápne, zraňuje ho to alebo ohrozuje, vysvetlite mu, že to nie je jeho chyba.**
- **Ak sa dieťa cíti nepohodlne alebo trápne pri online konverzácii, má právo ju okamžite prerušiť a odísť z četovej miestnosti**. Ak sa pritom snažil človek zaviesť tému do sexuálnej oblasti nech dieťa o tom povie rodičom, alebo v škole učiteľom.
- **Váš domáci počítač (alebo hraciu konzolu) postavte do obývacej izby alebo na iné spoločné prístupové miesto v byte.** Najlepšie tak, aby rodič mal vždy výhľad na monitor**.** Nedávajte počítač do detských izieb. Majte dobrý prehľad o všetkých ďalších počítačoch, ktoré sú deťom prístupné.
- **Stanovte medzi deťmi a rodičmi jasné pravidlá pre používanie internetu**. Urobte si rozvrh na dni a presný čas, kedy má dieťa povolenie stráviť čas na internete, najlepšie v čase vašej prítomnosti. Podpísanú zmluvu vystavte v blízkosti počítača na viditeľnom mieste. Nezabudnite, ak si s vaším dieťaťom vytvoríte pravidlá o používaní internetu, stanovte si práva a povinnosti pre obe strany. Pravidla, by sa mali pravidelne aktualizovať. Vzor takejto „rodinnej zmluvy" nájdete na stránkach Zodpovedne.sk.
- **Najmenšie deti by nemali používať četovacie miestnosti bez moderátora, v ktorých môže byť dieťa najviac ohrozené.**
- **Vytvorte medzi dieťaťom a rodičom vzťah vzájomnej dôvery.** Majte prehľad o prezývkach (nickname) vašich detí, ktoré používajú na internete. Buďte opatrný, nebuďte dotieravý pri kontrole dieťaťa, vzájomná dôvera je veľmi dôležitá. Prílišná kontrola by mohla dieťa dohnať ku skrývaniu a zatajovaniu činností. Netrestajte dieťa za to, čo nie je jeho chyba, môže vám prestať dôverovať a mať strach a neistotu pri zdôverovaní sa s nejakým problémom. Je potrebné sa s deťmi veľa rozprávať, upozorniť ich na rôzne nebezpečenstvá, zaujímať sa a vedieť kde a ako trávia voľný čas, s kým telefonujú, emailujú, četujú, s kým sa stretávajú. Menšie deti si vyžadujú pravidelnú kontrolu. Ponúknite deťom adekvátne, zmysluplné a zaujímavé mimoškolské aktivity. Všímajte si viac svoje okolie. Nebuďte ľahostajní ani k cudzím deťom.
- **Dôveruj, ale preveruj.** Nie vždy sa dieťa zdôveruje rodičom, preto nezabudnite sledovať jeho nálady, zvyky, zmeny nálad a správanie, ktoré môže byť kľúčom k objasneniu príčiny. Kontrolujte, ktoré stránky navštevuje, s kým si píše emaily, hovorte s ním s kým a o čom si píše. Ak dieťa chodí na stránky s nevhodným obsahom, je možné pomocou filtra zakázať prístup na tieto stránky. Ak nechcete aby dieťa bolo vystavené riziku pri otváraní emailov, nainštalujte si program, ktorý povolí otvorenie emailu iba od známych ľudí zo zoznamu, adresáru. Pokiaľ to uznáte za vhodné, používajte monitorovacie nástroje, ktoré vám umožnia získať prehľad o chovaní vášho dieťaťa na internete.
- **Dbajte, aby dieťa hralo iba hry, ktoré sú určené správnej vekovej skupine a s vhodným obsahom.** Počítačové hry alebo hracie konzoly sú zatriedené podľa veku hráčov do skupín 3+, 4+, 6+, 7+, 12+, 16+, 18+. Obsahové ohrozenia hráčov sa delia na skupiny:
    - hra obsahuje vulgarizmy,
    - hra obsahuje diskriminačné prvky tj. obsahuje zobrazenia alebo materiály, ktoré môžu nabádať k diskriminácii,
    - hra znázorňuje užívanie drog,
    - hra môže pôsobiť na dieťa desivo až hrozivo,
    - hra znázorňuje nahotu alebo iné sexuálne správanie,

- hra zobrazuje násilie,
- hra, ktorá nabáda alebo vyučuje hazardné hry.

- **Pri výbere školy, mládežníckeho klubu, centra voľného času, letných táborov a podobne sa informujte, aké majú jednotlivé organizácie vypracované programy prevencie voči e-ohrozeniam.** Medzi e-ohrozenia patria:
  - Pedofília, pornografia (Pedofília, pornografia, sexturizmus, zverejňovanie erotiky...)
  - Závislosti (Drogy, anorexia, bulímia, sebapoškodzovanie, sekty, závislosť od internetu, mobilov, esemesiek, počítačových hier, návody na samovraždy, emo...),
  - Šikanovanie (Bullying, elektronické šikanovanie, zastrašovanie, ponižovanie, zosmiešňovanie, ohováranie, nadávanie, happy slapping...),
  - Diskriminácia (Xenofóbia, rasizmus, extréministické hnutia, totalitný režim...),
  - Násilie (Agresivita, klubové chuligánstvo, terorizmus, flaming, hate speech...),
  - Stretnutie s neznámou osobou (Internetové známosti, grooming, obchodovanie s ľuďmi...),
  - Poskytovanie osobných údajov (Poskytovanie kontaktných, osobných údajov, majetkové pomery, phishing...),
  - Internetové podvody (Počítačová kriminalita, falšovanie počítačových údajov, porušenia autorských a príbuzných práv...).
- **Neustále sa informujte, vzdelávajte, zlepšujte svoje zručnosti na internete, v mobilnej komunikácii a nových technológiách.** Súčasná generácia vyrastá s internetom a ich znalosti (aj jazykové), zručnosti sú vo väčšine prípadov lepšie ako u ich rodičov. Preto je potrebné snažiť sa s nimi aspoň držať krok a tak chrániť deti, seba a celú rodinu. Sledujte odbornú tlač, prípadne internetové stránky zaoberajúce sa danou problematikou.
- **Zvyšujte povedomie, šírte osvetu o zodpovednom používaní internetu, mobilu a nových technológií.**
- **Komunikujte s inými rodičmi, učiteľmi**, vymieňajte si informácie a poznatky.

Správajte sa Zodpovedne.sk! Na internete alebo pri mobilnej komunikácii sa správajte tak ako v ozajstnom živote. Vysvetlite deťom, aby, neurobili niečo, čo by v skutočnom živote nespravili. Pravidlá slušného správania sa na internete nazývajú netiketa.

Poskytovanie osobných údajov (Poskytovanie kontaktných, osobných údajov, majetkové pomery, phishing)

Poskytovanie kontaktných, osobných údajov, majetkové pomery

Podľa zákona o ochrane osobných údajov sú osobnými údajmi tie, ktoré sa týkajú určenej alebo určiteľnej osoby. Takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo najmä na základe jednej či viacerých charakteristík, znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu. Osobné údaje sú teda tie, ktoré umožnia presne identifikovať konkrétnu osobu.

Mnohokrát užívatelia internetu poskytnú svoje osobné údaje tretej strane bez toho, aby si boli vedomí rizík, ktorým sa vystavujú. Môže ísť o údaje zaslané mailom, okamžitými správami, zverejnené vo verejných četovým miestnostiach, prostredníctvom sms a podobne.

Údaje, ktoré môžu byť zneužité:

- Osobné a kontaktné údaje: meno, bydlisko, telefónne číslo, pracovisko, škola, vek, pohlavie. Najmä deti často udávajú svoj vek, pohlavie a dokonca aj adresu, čo môžu využiť osoby s nekalými zámermi.
- Bankové údaje: číslo účtu, heslo, informácie ku kreditným kartám. Často sa posielajú tieto údaje emailom alebo prostredníctvom okamžitých správ, je potom jednoduché sa dostať k prostriedkom na účte.
- Fotografie: z dovoleniek, erotické fotografie, alebo také, prostredníctvom ktorých vás môže niekto zahanbiť, strápniť alebo šikanovať. Môžu byť využité na vaše zosmiešnenie medzi kamarátmi, uverejnené na erotických webových stránkach, prezradia viac o sociálnej a ekonomickej situácii v rodine.
- Sociálno-ekonomické pomery: ako, kde a s kým žijete, príjem vás alebo rodičov, záľuby. Je možné zistiť, či žijete s oboma rodičmi, aký máte vzťah, koľko rodičia zarábajú, či máte doma drahé spotrebiče, techniku a podobne.

Je potrebné si uvedomiť, že k údajom na internete má prístup obrovské množstvo jeho používateľov. Pri komunikácii s cudzím človekom je vždy riziko, že je niekým iným ako sa vydáva. Preto je nutné dôkladne zvažovať informácie, ktoré o svojej osobe poskytneme akýmkoľvek spôsobom.

Deťom a mladým ľuďom je dobré vysvetliť riziká pri komunikácii cez internet tak, aby boli schopné sa brániť a vyhľadať pomoc v prípade, že sa stanú obeťou šikanovania, sexuálneho obťažovania, či iného nevhodného správania.

Pri dospelých je význam osvety v problematike poskytovania osobných údajov hlavne pri nakladaní s finančnými informáciami a bankovými účtami. Je možné sa tak vyhnúť zneužitiu údajov pri finančných podvodoch alebo manipulácii s účtami.

Phishing

Phishing (z anglického fishing – rybárčenie), označuje činnosť, pri ktorej sa snažia podvodníci nezákonným spôsobom alebo prostredníctvom podvodu vylákať od obete citlivé informácie ako prihlasovacie meno, heslo, bankové detaily vydávajúc sa za dôveryhodný a spoľahlivý zdroj.

Phishing prebieha hlavne prostredníctvom emailov a okamžitých správ. Často navádza užívateľa uvádzať údaje priamo na web stránky, aj keď sa tieto úkony dajú vybaviť aj prostredníctvom telefónu alebo osobne. Takáto stránka vyzerá ako verná kópia existujúcej dôveryhodnej stránky, preto sa užívateľ často nechá zmiasť a zadá požadované informácie.

Phishing sa môže prejavovať ako:

- Email, ktorý láka užívateľov napríklad k zmene hesla alebo jeho obnoveniu. Vizuál a obsah emailov vyzerá ako keby bol zaslaný od dôveryhodnej inštitúcie, známej banky.
- Email s uvedenými telefónnymi číslami, na ktorých je potrebné zmeniť údaje, heslo alebo doplniť informácie. Často krát sa podvodníci nachádzajú na úplne iných miestach ako naznačuje telefonická predvoľba – telefonický phishing.
- Aktívne linky priamo v emailoch na formuláre, ktoré vás lákajú kliknúť na ne.
- Email s informáciou, že na vašom účte bola zaznamenaná podozrivá transakcia a so žiadosťou o aktualizáciu alebo zmenu údajov.
- Email s informáciou, že v banke sa nepodarilo aktualizovať a overiť vaše údaje, aby ste tak spravili prostredníctvom uvedenej linky.
- Správy typu: ak neodpoviete, do 48 hodín váš účet bude zrušený. Využívajú nátlak a stres, ktorý u užívateľa spôsobí, že sa menej zamýšľa nad dôsledkami a oprávnenosťou podobných správ.
- Všeobecné oslovenia ako „Vážený zákazník“. Podozrivé emaily sa rozosielajú hromadne, preto neobsahujú vaše meno ani priezvisko.
- Často sa používajú logá a obrázky stiahnuté zo stránok pravých inštitúcií, aby presvedčili užívateľa, že ide o dôveryhodnú stránku.

Legislatíva

Zákon č. 300/2005 Z.z. – Trestný zákon

- § 196 – Porušovanie tajomstva prepravovaných správ – Kto úmyselne poruší

  b) tajomstvo informácie prenášanej prostredníctvom elektronickej komunikačnej služby, alebo

  c) tajomstvo neverejného prenosu počítačových dát do počítačového systému, z neho alebo v jeho rámci, vrátane elektromagnetického vyžarovania z počítačového systému, prenášajúceho takéto počítačové dáta

- § 198 – Kto v rozpore so všeobecne záväzným právnym predpisom vyrobí, sebe alebo inému zadováži alebo prechováva zariadenie spôsobilé na odpočúvanie informácií prenášaných prostredníctvom elektronickej komunikačnej služby
- § 221 – Podvod – Kto na škodu cudzieho majetku seba alebo iného obohatí tým, že uvedie niekoho do omylu alebo využije niečí omyl, a spôsobí tak na cudzom majetku škodu

Informácie na internete

www.dataprotection.gov.sk – Úrad na ochranu osobných údajov

www.wikipedia.sk – Online encyklopédia

Prevencia

- **Zvoľte si svoju prezývku (nickname) tak, aby sa vás podľa nej nedalo identifikovať.**
- **Zvoľte si zložité heslá.** Heslo by malo mať minimálne 7 znakov, kombináciu písmen a číslic, malých aj veľkých znakov. Heslo by nemalo obsahovať žiadne slovo zo slovníka slovenského ani iného jazyka, bežné kombinácie ako krstné mená; bežné číselné kombinácie; dátum narodenia; názvy miest, štátov, riek; nadávky; internetovo známe slová. Vyhýbajte sa použitia písmen Z a Y, lebo sa na klávesnici pletú. Heslá si podľa možnosti nezapisujte. Meňte si svoje heslá vždy, keď máte pocit, že ich dôveryhodnosť bola narušená.
- **Nepoužívajte jedno heslo na všetky stránky, služby na internete.**
- **Nikdy neposkytujte svoje prístupové heslá.** Osobné heslo chráni súkromie, drží sa v tajnosti a nikomu sa neprezrádza, dokonca ani svojmu najlepšiemu kamarátovi alebo niekomu, kto sa tvári úradne.
- **Nikdy neposielajte emailom, četom, sms a podobne svoje osobné údaje**: svoju fotografiu, video, vek, emailovú adresu, telefónne číslo, adresu domov, adresu školy, majetkové pomery, prístupové mená a heslá alebo iné osobné údaje (číslo kreditnej karty...). Neodpovedajte na emaily alebo pop-up okná, ktoré vás žiadajú o osobné alebo finančné údaje a neklikajte na uvedené linky. Seriózne inštitúcie od vás nebudú žiadať heslá ani iné citlivé informácie prostredníctvom emailu.
- **Nedávajte na internet alebo cez mobil žiadne fotografie, videá, na ktorých ste v plavkách, v spodnej bielizni, máte odhalené časti tela alebo pôsobíte eroticky.** Fotoalbumy, videoalbumy na internete alebo v mobiloch nie sú bezpečné, aj keď sa píše, že sú „súkromné“, „zamknuté“ a podobne. Obsah sa môže dostať na voľne dostupné miesta a vaše fotografie, videá uvidia všetci: rodičia, učitelia, spolužiaci ale aj osoby, ktoré vám môžu ublížiť. Fotografie z detstva môžu byť zneužité pedofilom, fotografie z rodinných osláv, dovoleniek prezradia rodinné, sociálne zázemie. Fotografie alebo videá, na ktorých je váš byt, dom, škola môžu identifikovať adresy vášho pobytu. Ostatné osobné fotografie zverejňujte v malom rozlíšení (max 200x200 pixlov/bodov), tak sťažíte ich zneužitie. Fotografie alebo videá môžu byť zneužité aj za účelom poníženia, zahanbenia, zastrašenia alebo vydierania.
- **Najmenšie deti by mali navštevovať iba „detské“ stránky.** Na Slovensku iniciatíva „child-friendly“ zatiaľ neexistuje. Deťom priateľské stránky, čo je slovenský preklad, by napríklad nemali tolerovať poskytovanie osobných informácii bez povolenia rodičov, nemali by obsahovať nevhodný obsah pre ich vekovú kategóriu, mali by garantovať vek osôb v četoch a podobne.
- **Kontrolujte svoje bankové výpisy a hláste každú podozrivú platbu, ktorou si nie ste istý**.
- **Informujte sa o ochrane osobných údajov „Privacy policy“.** Internetové stránky deklarujú pravidlá na ochranu údajov väčšinou v pätičke svojej stránky.
- **Nekopírujte linku do prehliadača priamo z emailu**. Často vyzerá, že vás odkáže na stránku banky, ale v skutočnosti vás pošle na úplne inú stránku. Ak potrebujete navštíviť danú stránku, naťukajte ju priamo do prehliadača bez kopírovania.
- **Používajte antivírové a antispyware softvéry, firewall a aktualizujte ich pravidelne**.
- **Buďte opatrný pri sťahovaní súborov aj keď prišli od známej osoby**. Môžu obsahovať vírusy, ktoré oslabia obranyschopnosť vášho počítača.
- **Internet môže byť nebezpečný.** Oboznámte dieťa o tom, že tak ako v bežnom živote aj na internete alebo pri mobilnej komunikácii, číha nebezpečenstvo. Môžete použiť príklad s elektrinou. Je to rovnako ako internet potrebná a nenahraditeľná vec, ale je to rovnako ako internet pri nezodpovednom používaní nebezpečná vec pre vaše zdravie alebo dokonca pre život. Pri internete na rozdiel od elektriny stále chýba takáto skúsenosť, či skôr osveta.
- **Nikdy neviete, kto je v skutočnosti na druhej strane internetu alebo mobilu.** Na druhej strane môže byť človek, ktorý klame o svojom veku, pohlaví, záujmoch, vzhľade a podobne. Takýto ľudia chcú deťom veľmi ublížiť a sú to:
    - pedofili...
    - ľudia, ktorí chcú fotografie a videá detí...
    - navádzajú na užívanie drog...
    - navádzajú na šikanovanie, alebo šikanujú deti...
    - nenávidia určité skupiny ľudí...

- správajú sa agresívne, násilne...
- chcú sa s deťmi tajne stretnúť, ublížiť im, uniesť ich...
- získať osobné údaje o dieťati, jeho rodine, kamarátoch...
- chcú oklamať, podviesť dieťa...
- návádzajú na sebapoškodzovanie...

- **Nie je bezpečné dávať na internet alebo cez mobil svoje osobné údaje.** Vysvetlite deťom, čo sú to osobné údaje a prečo je nebezpečné zverejňovať svoje pravé meno a priezvisko, svoju fotografiu, video, vek, emailovú adresu, telefónne číslo, adresu domov, adresu školy, majetkové pomery, prístupové mená a heslá alebo iné osobné údaje (záľuby, opis vzhľadu, povahy, znalosti, zručnosti, vzdelanie, obľúbené veci, túžby...). V prípade, že je nevyhnutné takéto údaje poskytnúť, musia o tom vedieť rodičia alebo učitelia.
- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- **S nikým, s kým sa dieťa zoznámilo iba cez internet alebo mobil, sa nesmie stretávať samé osobne.** Tak ako v reálnom živote nechodia deti na stretnutie s neznámou osobou bez sprievodu niekoho ďalšieho, najlepšie rodiča, alebo aspoň súrodenca, kamaráta, tak aj na stretnutie s neznámou osobou, s ktorou sa dieťa zoznámilo iba cez internet alebo mobil, je stretnutie veľmi nebezpečné. Ak už dieťa ide na stretnutie, tak vždy aspoň s kamarátom. Rodičom by malo oznámiť na aké stretnutie ide, za kým ide, kde a kedy sa plánuje vrátiť. Stretnutie by malo byť na verejnom mieste, kde je veľa ľudí. Znakom bezpečnejšieho stretnutia je, že tomu, čo pozýva, nevadí, že dieťa príde s rodičom alebo inou dospelou osobou. Ak mu to vadí, ten človek nemá čisté úmysly.
- **Buďte podozrievavý voči človeku, ktorý dieťa presviedča, aby zatajovalo svoje internetové kamarátstvo pred rodičmi, alebo vystupuje ako tínedžer, ale nevie väčšinu odpovedí na otázky, ktoré bežne rovesníci poznajú.** Takýto človek chce deťom ublížiť, a preto klame a navádza, aby zatajili pozvanie na stretnutie s ním, aby si zmazali históriu četu, jeho emaily, sms, mms správy, a podobne.
- **Použitie lokalizačných služieb mobilného telefónu dieťaťa neznámou osobou je nebezpečné**. Vďaka lokalizácii môže ktorákoľvek osoba vyhľadať miesto pobytu dieťaťa, ak mu to samo z nevedomosti umožní.
- **Bluetooth spojenie cez mobilný telefón dieťaťa s neznámou osobou je nebezpečné**. Pomenujte mobilný telefón dieťaťa tak, aby z neho nebolo hneď jasné, že sa jedná o dieťa.
- **Nie všetko, čo je na internete, je pravda.** Vysvetlite deťom, nech neveria všetkému čo nájdu na internete. Informácie si je potrebné porovnať z viacerých zdrojov a v prípade nejasností sa poradiť s rodičmi alebo učiteľmi v škole.
- **Ak dieťa na internete alebo cez mobil niečo vyľaká, našlo niečo škaredé, desivé, niečo z čoho sa cíti trápne, zraňuje ho to alebo ohrozuje, vysvetlite mu, že to nie je jeho chyba.**
- **Ak sa dieťa cíti nepohodlne alebo trápne pri online konverzácii, má právo ju okamžite prerušiť a odísť z četovej miestnosti**. Ak sa pritom snažil človek zaviesť tému do sexuálnej oblasti nech dieťa o tom povie rodičom, alebo v škole učiteľom.
- **Váš domáci počítač (alebo hraciu konzolu) postavte do obývacej izby alebo na iné spoločné prístupové miesto v byte.** Najlepšie tak, aby rodič mal vždy výhľad na monitor**.** Nedávajte počítač do detských izieb. Majte dobrý prehľad o všetkých ďalších počítačoch, ktoré sú deťom prístupné.
- **Stanovte medzi deťmi a rodičmi jasné pravidlá pre používanie internetu**. Urobte si rozvrh na dni a presný čas, kedy má dieťa povolenie stráviť čas na internete, najlepšie v čase vašej prítomnosti. Podpísanú zmluvu vystavte v blízkosti počítača na viditeľnom mieste. Nezabudnite, ak si s vaším dieťaťom vytvoríte pravidlá o používaní internetu, stanovte si práva a povinnosti pre obe strany. Pravidla, by sa mali pravidelne aktualizovať. Vzor takejto „rodinnej zmluvy“ nájdete na stránkach Zodpovedne.sk.
- **Najmenšie deti by nemali používať četovacie miestnosti bez moderátora, v ktorých môže byť dieťa najviac ohrozené.**
- **Vytvorte medzi dieťaťom a rodičom vzťah vzájomnej dôvery.** Majte prehľad o prezývkach (nickname) vašich detí, ktoré používajú na internete. Buďte opatrný, nebuďte dotieravý pri kontrole dieťaťa, vzájomná dôvera je veľmi dôležitá. Prílišná kontrola by mohla dieťa dohnať ku skrývaniu a zatajovaniu činností. Netrestajte dieťa za to, čo nie je jeho chyba, môže vám prestať dôverovať a mať strach a neistotu pri zdôverovaní sa s nejakým

problémom. Je potrebné sa s deťmi veľa rozprávať, upozorniť ich na rôzne nebezpečenstvá, zaujímať sa a vedieť kde a ako trávia voľný čas, s kým telefonujú, emailujú, četujú, s kým sa stretávajú. Menšie deti si vyžadujú pravidelnú kontrolu. Ponúknite deťom adekvátne, zmysluplné a zaujímavé mimoškolské aktivity. Všímajte si viac svoje okolie. Nebuďte ľahostajní ani k cudzím deťom.

- **Dôveruj, ale preveruj.** Nie vždy sa dieťa zdôveruje rodičom, preto nezabudnite sledovať jeho nálady, zvyky, zmeny nálad a správanie, ktoré môže byť kľúčom k objasneniu príčiny. Kontrolujte, ktoré stránky navštevuje, s kým si píše emaily, hovorte s ním s kým a o čom si píše. Ak dieťa chodí na stránky s nevhodným obsahom, je možné pomocou filtra zakázať prístup na tieto stránky. Ak nechcete aby dieťa bolo vystavené riziku pri otváraní emailov, nainštalujte si program, ktorý povolí otvorenie emailu iba od známych ľudí zo zoznamu, adresáru. Pokiaľ to uznáte za vhodné, používajte monitorovacie nástroje, ktoré vám umožnia získať prehľad o chovaní vášho dieťaťa na internete.
- **Dbajte, aby dieťa hralo iba hry, ktoré sú určené správnej vekovej skupine a s vhodným obsahom.** Počítačové hry alebo hracie konzoly sú zatriedené podľa veku hráčov do skupín 3+, 4+, 6+, 7+, 12+, 16+, 18+. Obsahové ohrozenia hráčov sa delia na skupiny:
    - hra obsahuje vulgarizmy,
    - hra obsahuje diskriminačné prvky tj. obsahuje zobrazenia alebo materiály, ktoré môžu nabádať k diskriminácii,
    - hra znázorňuje užívanie drog,
    - hra môže pôsobiť na dieťa desivo až hrozivo,
    - hra znázorňuje nahotu alebo iné sexuálne správanie,
    - hra zobrazuje násilie,
    - hra, ktorá nabáda alebo vyučuje hazardné hry.
- **Pri výbere školy, mládežníckeho klubu, centra voľného času, letných táborov a podobne sa informujte, aké majú jednotlivé organizácie vypracované programy prevencie voči e-ohrozeniam.** Medzi e-ohrozenia patria:
    - Pedofília, pornografia (Pedofília, pornografia, sexturizmus, zverejňovanie erotiky...)
    - Závislosti (Drogy, anorexia, bulímia, sebapoškodzovanie, sekty, závislosť od internetu, mobilov, esemesiek, počítačových hier, návody na samovraždy, emo...),
    - Šikanovanie (Bullying, elektronické šikanovanie, zastrašovanie, ponižovanie, zosmiešňovanie, ohováranie, nadávanie, happy slapping...),
    - Diskriminácia (Xenofóbia, rasizmus, extréministické hnutia, totalitný režim...),
    - Násilie (Agresivita, klubové chuligánstvo, terorizmus, flaming, hate speech...),
    - Stretnutie s neznámou osobou (Internetové známosti, grooming, obchodovanie s ľuďmi...),
    - Poskytovanie osobných údajov (Poskytovanie kontaktných, osobných údajov, majetkové pomery, phishing...),
    - Internetové podvody (Počítačová kriminalita, falšovanie počítačových údajov, porušenia autorských a príbuzných práv...).
- **Neustále sa informujte, vzdelávajte, zlepšujte svoje zručnosti na internete, v mobilnej komunikácii a nových technológiách.** Súčasná generácia vyrastá s internetom a ich znalosti (aj jazykové), zručnosti sú vo väčšine prípadov lepšie ako u ich rodičov. Preto je potrebné snažiť sa s nimi aspoň držať krok a tak chrániť deti, seba a celú rodinu. Sledujte odbornú tlač, prípadne internetové stránky zaoberajúce sa danou problematikou.
- **Zvyšujte povedomie, šírte osvetu o zodpovednom používaní internetu, mobilu a nových technológií.**
- **Komunikujte s inými rodičmi, učiteľmi**, vymieňajte si informácie a poznatky.

Správajte sa Zodpovedne.sk! Na internete alebo pri mobilnej komunikácii sa správajte tak ako v ozajstnom živote. Vysvetlite deťom, aby, neurobili niečo, čo by v skutočnom živote nespravili. Pravidlá slušného správania sa na internete nazývajú netiketa.

Internetové podvody (Počítačová kriminalita, falšovanie počítačových údajov, porušenia autorských a príbuzných práv)

Počítačová kriminalita, falšovanie počítačových údajov, porušenia autorských a príbuzných práv

Informačné technológie sú fenoménom, ktoré okrem praktických prínosov prinášajú aj negatívne javy. Tak ako mnohé iné nástroje, je aj počítačová technika použiteľná na účely, ktoré nie sú vždy v súlade so spoločenskými požiadavkami, ba často idú za hranice majoritou stanovených noriem. Príchod internetových technológií priniesol so sebou nárast aktivít, ktoré sú často klasifikovateľné ako protizákonné a v informatickom i právnom slangu dostali pomenovanie počítačová kriminalita alebo IT kriminalita. Pojem počítačová kriminalita bol položený Dohovorom o počítačovej kriminalite iniciovaný na úrovni Rady Európy roku 2001.

Dnes je možné vysloviť tvrdenie, že páchanie trestnej činnosti, ktorú je možné definovať ako tzv. "počítačovú kriminalitu", má narastajúcu tendenciu.

Rapídny nástup informačných technológií priniesol nárast určitých špecifických foriem páchania trestnej činnosti a to najmä z dôvodu rýchlosti, ktorou je možné vďaka výkonu jednotlivé úkony vykonať. Prečo práve internet priniesol rapídny nárast podobných aktivít?

Dôvodov je viacero, pokúsme sa pomenovať aspoň niektoré z nich:

- cenová dostupnosť technológií,
- pocit anonymity,
- technologická nenáročnosť,
- rýchlosť vykonania operácie.

Dohovor o počítačovej kriminalite zaviedol zaujímavú kategorizáciu činov namierených proti dôvernosti, dostupnosti a integrite počítačových systémov, sietí a počítačových údajov:

- **Trestné činy proti dôvernosti, hodnovernosti a dostupnosti počítačových údajov a systémov:**
  - nezákonný prístup do počítačového systému
  - nezákonné zachytávanie údajov
  - zasahovanie do údajov – poškodenie, vymazanie, zhoršenie kvality, pozmenenie údajov alebo zamedzenie prístupu k údajom
  - zasahovanie do systému – marenie funkčnosti počítačového systému
  - zneužívanie zariadení
- **Počítačové trestné činy:**
  - falšovanie počítačových údajov
  - počítačové podvody
- **Trestné činy týkajúce sa obsahu:**
  - trestné činy týkajúce sa detskej pornografie

- **Trestné činy týkajúce sa porušenia autorských a príbuzných práv**

Z pragmatického hľadiska je možné dnes rozdeliť IT kriminalitu na dve základné oblasti:

- **kde IT (počítače, softvérové vybavenie) sú prostriedkom t.j. práve pomocou výpočtovej techniky je páchaná trestná činnosť a teda počítač je len nástrojom pre dosiahnutie iného cieľa. Príkladmi môžu byť napríklad:**
  - pozmeňovanie a falšovanie peňazí a cenín
  - ohováranie, zastrašovanie, vydieranie
  - úverové podvody – fiktívne doklady
  - prechovávanie a šírenie dát v rozpore so zákonom (napr. pornografia)
- **kde IT aktíva sú cieľom aktivít považovateľných za trestnú činnosť:**
  - porušovanie autorského práva
  - využívanie SW bez/v rozpore s platnou licenciou
  - nelegálne šírenie SW a audiovizuálnych diel
  - hard disk loading
  - nelegálne šírenie televízneho signálu pomocou IT
  - cielené útoky zamerané voči dôvernosti, dostupnosti, integrite informačných systémov a dát, ktoré sú v nich spracované
  - zneužívanie a poškodzovanie dát na nosiči informácií
  - neoprávnené nakladanie s údajmi dôverného charakteru (napr. osobné údaje)

Legislatíva

Zákon č. 300/2005 Z.z. – Trestný zákon

- *§ 221* – Podvod – Kto na škodu cudzieho majetku seba alebo iného obohatí tým, že uvedie niekoho do omylu alebo využije niečí omyl, a spôsobí tak na cudzom majetku malú škodu
- *§ 226* – Neoprávnené obohatenie – Kto na škodu cudzieho majetku seba alebo iného obohatí tým, že neoprávneným zásahom do technického alebo programového vybavenia počítača, automatu alebo iného podobného prístroja alebo technického zariadenia slúžiaceho na automatizované uskutočňovanie predaja tovaru, zmenu alebo výber peňazí alebo na poskytovanie platených výkonov, služieb, informácií či iných plnení dosiahne, že tovar, služby, alebo informácie získa bez požadovanej úhrady alebo peniaze získa neoprávnene, a spôsobí tým na cudzom majetku malú škodu
- *§ 283* - Porušovanie autorského práva – Kto neoprávnene zasiahne do zákonom chránených práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo – obrazovému záznamu, rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze

Informácie na internete

www.infoconsult.sk - Prednášky z oblasti súdneho inžinierstva v problematike počítačovej kriminality

www.wikipedia.sk – Online encyklopédia

Prevencia

- **Majte prehľad o všetkých nástrojoch, cez ktoré vás môže internet alebo mobil ohroziť**:
  - SPAM (Nevyžiadaná pošta, falošné prosby o pomoc, reklamy, pyramídové hry, reťazové listy šťastia...),
  - Vírusy (Malware, klasické počítačové vírusy, internetové červy, emailové červy, trójske kone, dialery, spyware, adware, pop-up a hijackery, hoax, phishing, pharming, spoofing...),
  - Online obchodovanie (Online nakupovanie, internet banking, virtuálny účet...),
  - Čet (Instant messaging, blog, diskusné fórum...),

- Reklama (Reklama, targeting, druhy online reklamy, adware...),
- Hry (Online hry, hazardné hry, hracie konzoly, java hry, tipovanie a stávkovanie...),
- Sťahovanie (Download, porušenie autorských práv, softvérové pirátstvo, voľne dostupné materiály, riziká sťahovania...),
- Zoznamky (Zoznamky cez internet, vydávanie sa za niekoho iného, stretnutie s neznámou osobou, ochrana osobných údajov...),
- Mobily (SMS reklamný spam, zneužitie osobných údajov, krádež telefónu, obsah len pre dospelých, lokalizačné služby, tiesňové linky, audiotext, bluetooth, WiFi...),
- HOAX (Fámy, varovania pred vymyslenými vírusmi, fámy o mobilných telefónoch, petície a výzvy, podvodné emaily, žartovné správy...).

- **Stanovte si jasné pravidlá či deti budú alebo nebudú môcť utrácať peniaze na internete.** V prípade, že platobnú kartu používa dieťa, zvyšuje sa aj riziko úniku osobných údajov, údajov o karte a bankové informácie.
- **Používajte antivírové a antispyware softvéry, firewall a aktualizujte ich pravidelne**.
- **Buďte opatrný pri sťahovaní súborov aj keď prišli od známej osoby**. Môžu obsahovať vírusy, ktoré oslabia obranyschopnosť vášho počítača.
- **Internet môže byť nebezpečný.** Oboznámte dieťa o tom, že tak ako v bežnom živote aj na internete alebo pri mobilnej komunikácii, číha nebezpečenstvo. Môžete použiť príklad s elektrinou. Je to rovnako ako internet potrebná a nenahraditeľná vec, ale je to rovnako ako internet pri nezodpovednom používaní nebezpečná vec pre vaše zdravie alebo dokonca pre život. Pri internete na rozdiel od elektriny stále chýba takáto skúsenosť, či skôr osveta.
- **Nikdy neviete, kto je v skutočnosti na druhej strane internetu alebo mobilu.** Na druhej strane môže byť človek, ktorý klame o svojom veku, pohlaví, záujmoch, vzhľade a podobne. Takýto ľudia chcú deťom veľmi ublížiť a sú to:
  - pedofili...
  - ľudia, ktorí chcú fotografie a videá detí...
  - navádzajú na užívanie drog...
  - navádzajú na šikanovanie, alebo šikanujú deti...
  - nenávidia určité skupiny ľudí...
  - správajú sa agresívne, násilne...
  - chcú sa s deťmi tajne stretnúť, ublížiť im, uniesť ich...
  - získať osobné údaje o dieťati, jeho rodine, kamarátoch...
  - chcú oklamať, podviesť dieťa...
  - návádzajú na sebapoškodzovanie...
- **Nie je bezpečné dávať na internet alebo cez mobil svoje osobné údaje.** Vysvetlite deťom, čo sú to osobné údaje a prečo je nebezpečné zverejňovať svoje pravé meno a priezvisko, svoju fotografiu, video, vek, emailovú adresu, telefónne číslo, adresu domov, adresu školy, majetkové pomery, prístupové mená a heslá alebo iné osobné údaje (záľuby, opis vzhľadu, povahy, znalosti, zručnosti, vzdelanie, obľúbené veci, túžby...). V prípade, že je nevyhnutné takéto údaje poskytnúť, musia o tom vedieť rodičia alebo učitelia.
- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- **S nikým, s kým sa dieťa zoznámilo iba cez internet alebo mobil, sa nesmie stretávať samé osobne.** Tak ako v reálnom živote nechodia deti na stretnutie s neznámou osobou bez sprievodu niekoho ďalšieho, najlepšie rodiča, alebo aspoň súrodenca, kamaráta, tak aj na stretnutie s neznámou osobou, s ktorou sa dieťa zoznámilo iba cez internet alebo mobil, je stretnutie veľmi nebezpečné. Ak už dieťa ide na stretnutie, tak vždy aspoň s kamarátom. Rodičom by malo oznámiť na aké stretnutie ide, za kým ide, kde a kedy sa plánuje vrátiť. Stretnutie by malo byť na verejnom mieste, kde je veľa ľudí. Znakom bezpečnejšieho stretnutia je, že tomu, čo pozýva, nevadí, že dieťa príde s rodičom alebo inou dospelou osobou. Ak mu to vadí, ten človek nemá čisté úmysly.
- **Buďte podozrievavý voči človeku, ktorý dieťa presviedča, aby zatajovalo svoje internetové kamarátstvo pred rodičmi, alebo vystupuje ako tínedžer, ale nevie väčšinu odpovedí na otázky, ktoré bežne rovesníci poznajú.** Takýto človek chce deťom ublížiť, a preto klame a navádza, aby zatajili pozvanie na stretnutie s ním, aby si zmazali históriu četu, jeho emaily, sms, mms správy, a podobne.

- **Použitie lokalizačných služieb mobilného telefónu dieťaťa neznámou osobou je nebezpečné**. Vďaka lokalizácii môže ktorákoľvek osoba vyhľadať miesto pobytu dieťaťa, ak mu to samo z nevedomosti umožní.
- **Bluetooth spojenie cez mobilný telefón dieťaťa s neznámou osobou je nebezpečné**. Pomenujte mobilný telefón dieťaťa tak, aby z neho nebolo hneď jasné, že sa jedná o dieťa.
- **Nie všetko, čo je na internete, je pravda.** Vysvetlite deťom, nech neveria všetkému čo nájdu na internete. Informácie si je potrebné porovnať z viacerých zdrojov a v prípade nejasností sa poradiť s rodičmi alebo učiteľmi v škole.
- **Ak dieťa na internete alebo cez mobil niečo vyľaká, našlo niečo škaredé, desivé, niečo z čoho sa cíti trápne, zraňuje ho to alebo ohrozuje, vysvetlite mu, že to nie je jeho chyba.**
- **Ak sa dieťa cíti nepohodlne alebo trápne pri online konverzácii, má právo ju okamžite prerušiť a odísť z četovej miestnosti**. Ak sa pritom snažil človek zaviesť tému do sexuálnej oblasti nech dieťa o tom povie rodičom, alebo v škole učiteľom.
- **Váš domáci počítač (alebo hraciu konzolu) postavte do obývacej izby alebo na iné spoločné prístupové miesto v byte.** Najlepšie tak, aby rodič mal vždy výhľad na monitor**.** Nedávajte počítač do detských izieb. Majte dobrý prehľad o všetkých ďalších počítačoch, ktoré sú deťom prístupné.
- **Stanovte medzi deťmi a rodičmi jasné pravidlá pre používanie internetu**. Urobte si rozvrh na dni a presný čas, kedy má dieťa povolenie stráviť čas na internete, najlepšie v čase vašej prítomnosti. Podpísanú zmluvu vystavte v blízkosti počítača na viditeľnom mieste. Nezabudnite, ak si s vaším dieťaťom vytvoríte pravidlá o používaní internetu, stanovte si práva a povinnosti pre obe strany. Pravidla, by sa mali pravidelne aktualizovať. Vzor takejto „rodinnej zmluvy" nájdete na stránkach Zodpovedne.sk.
- **Najmenšie deti by nemali používať četovacie miestnosti bez moderátora, v ktorých môže byť dieťa najviac ohrozené.**
- **Vytvorte medzi dieťaťom a rodičom vzťah vzájomnej dôvery.** Majte prehľad o prezývkach (nickname) vašich detí, ktoré používajú na internete. Buďte opatrný, nebuďte dotieravý pri kontrole dieťaťa, vzájomná dôvera je veľmi dôležitá. Prílišná kontrola by mohla dieťa dohnať ku skrývaniu a zatajovaniu činností. Netrestajte dieťa za to, čo nie je jeho chyba, môže vám prestať dôverovať a mať strach a neistotu pri zdôverovaní sa s nejakým problémom. Je potrebné sa s deťmi veľa rozprávať, upozorniť ich na rôzne nebezpečenstvá, zaujímať sa a vedieť kde a ako trávia voľný čas, s kým telefonujú, emailujú, četujú, s kým sa stretávajú. Menšie deti si vyžadujú pravidelnú kontrolu. Ponúknite deťom adekvátne, zmysluplné a zaujímavé mimoškolské aktivity. Všímajte si viac svoje okolie. Nebuďte ľahostajní ani k cudzím deťom.
- **Dôveruj, ale preveruj.** Nie vždy sa dieťa zdôveruje rodičom, preto nezabudnite sledovať jeho nálady, zvyky, zmeny nálad a správanie, ktoré môže byť kľúčom k objasneniu príčiny. Kontrolujte, ktoré stránky navštevuje, s kým si píše emaily, hovorte s ním s kým a o čom si píše. Ak dieťa chodí na stránky s nevhodným obsahom, je možné pomocou filtra zakázať prístup na tieto stránky. Ak nechcete aby dieťa bolo vystavené riziku pri otváraní emailov, nainštalujte si program, ktorý povolí otvorenie emailu iba od známych ľudí zo zoznamu, adresáru. Pokiaľ to uznáte za vhodné, používajte monitorovacie nástroje, ktoré vám umožnia získať prehľad o chovaní vášho dieťaťa na internete.
- **Dbajte, aby dieťa hralo iba hry, ktoré sú určené správnej vekovej skupine a s vhodným obsahom.** Počítačové hry alebo hracie konzoly sú zatriedené podľa veku hráčov do skupín 3+, 4+, 6+, 7+, 12+, 16+, 18+. Obsahové ohrozenia hráčov sa delia na skupiny:
    - hra obsahuje vulgarizmy,
    - hra obsahuje diskriminačné prvky tj. obsahuje zobrazenia alebo materiály, ktoré môžu nabádať k diskriminácii,
    - hra znázorňuje užívanie drog,
    - hra môže pôsobiť na dieťa desivo až hrozivo,
    - hra znázorňuje nahotu alebo iné sexuálne správanie,
    - hra zobrazuje násilie,
    - hra, ktorá nabáda alebo vyučuje hazardné hry.

- **Pri výbere školy, mládežníckeho klubu, centra voľného času, letných táborov a podobne sa informujte, aké majú jednotlivé organizácie vypracované programy prevencie voči e-ohrozeniam.** Medzi e-ohrozenia patria:
    - Pedofilia, pornografia (Pedofilia, pornografia, sexturizmus, zverejňovanie erotiky...)
    - Závislosti (Drogy, anorexia, bulímia, sebapoškodzovanie, sekty, závislosť od internetu, mobilov, esemesiek, počítačových hier, návody na samovraždy, emo...),
    - Šikanovanie (Bullying, elektronické šikanovanie, zastrašovanie, ponižovanie, zosmiešňovanie, ohováranie, nadávanie, happy slapping...),
    - Diskriminácia (Xenofóbia, rasizmus, extréministické hnutia, totalitný režim...),
    - Násilie (Agresivita, klubové chuligánstvo, terorizmus, flaming, hate speech...),
    - Stretnutie s neznámou osobou (Internetové známosti, grooming, obchodovanie s ľuďmi...),
    - Poskytovanie osobných údajov (Poskytovanie kontaktných, osobných údajov, majetkové pomery, phishing...),
    - Internetové podvody (Počítačová kriminalita, falšovanie počítačových údajov, porušenia autorských a príbuzných práv...).
- **Neustále sa informujte, vzdelávajte, zlepšujte svoje zručnosti na internete, v mobilnej komunikácii a nových technológiách.** Súčasná generácia vyrastá s internetom a ich znalosti (aj jazykové), zručnosti sú vo väčšine prípadov lepšie ako u ich rodičov. Preto je potrebné snažiť sa s nimi aspoň držať krok a tak chrániť deti, seba a celú rodinu. Sledujte odbornú tlač, prípadne internetové stránky zaoberajúce sa danou problematikou.
- **Zvyšujte povedomie, šírte osvetu o zodpovednom používaní internetu, mobilu a nových technológií.**
- **Komunikujte s inými rodičmi, učiteľmi**, vymieňajte si informácie a poznatky.
- **Správajte sa Zodpovedne.sk!** Na internete alebo pri mobilnej komunikácii sa správajte tak ako v ozajstnom živote. Vysvetlite deťom, aby, neurobili niečo, čo by v skutočnom živote nespravili. Pravidlá slušného správania sa na internete nazývajú netiketa.

SPAM (Nevyžiadaná pošta, falošné prosby o pomoc, reklamy, pyramídové hry, reťazové listy šťastia)

Nevyžiadaná pošta

SPAM: nevyžiadaná pošta, spočíva v rozosielaní jednej a tej istej správy viacerým prijímateľom súčasne, ktorí o ňu nestoja. Môže obsahovať lacné reklamy, elektronické letáky, vírusy, phishing - podvody, hoax - poplašné správy a iné ohrozenia z internetu.

Na úvod jedna perlička z histórie. Málokto vie, že spam je registrovaná značka Hormel Corporation, ktorá označuje mäsový výrobok („Spiced Pork And Ham“ - korenené bravčové mäso a šunka), populárny počas 2. svetovej vojny. A ako súvisia nevyžiadané správy s bravčovým mäsom? Podľa viacerých zdrojov sa tak stalo podľa populárnej zábavnej relácie britskej televíznej stanice BBC („Monty Python’s Flying Circus“ - Lietajúci cirkus Montyho Pythona) od komediálnej skupiny „Monty Python’s“, kde SPAM bol v 12. časti druhej série hlavnou, aj keď nežiadanou, ingredienciou všetkých jedál v reštaurácii.

(http://www.youtube.com/watch?v=wZ7YedEopp4)

S problémom spammingu majú najdlhšie skúsenosti užívatelia siete USENET, ktorí sa združovali v diskusných skupinách – tzv. newsgroup. Spamming spočíval v rozosielaní jednej a tej istej správy do viacerých diskusných skupín súčasne. Správa sa pritom netýkala témy v oslovených diskusných skupinách. Formálne sa takýmto aktivitám začalo hovoriť „Excessive Multi-Posting“ (skratkou EMP), ale užívatelia si zvykli skôr na označenie „spam“, resp. „spamming“. So vznikom internetu sa tento negatívny jav rozširoval a začal zasahovať ďalšie sieťové služby – hlavne email. Spam však neobišiel ani ďalšie služby internetu – možno sa s ním stretnúť aj v prostredí online diskusií, realizovaných službami čet alebo rýchleho posielania správ. Všeobecne pri všetkých službách, ktoré fungujú na distribučnom princípe a oslovujú viac príjemcov súčasne. Tento fenomén robí vrásky na čele prevádzkovateľom aj užívateľom internetu. Na jednej strane zaťažuje prenosové linky a poštové servery, na druhej strane obťažuje užívateľov.

Za prvý komerčný spam je považovaný email z roku 1994, informujúci o lotérii o zelenú kartu. Táto správa vyvolala obrovskú vlnu spamu, ktorá sa šíri dodnes.

Podľa najnovšej štúdie spoločnosti Barracuda Networks (výrobca hardvérových riešení pre detekciu a filtrovanie spamu) má z 20 emailov len jediný legitímny obsah, zvyšných 19 tvorí spam. Podiel spamu už každoročne prudko stúpa a zatiaľ sa tento problém nepodarilo nikomu vyriešiť. Istý čas sa dokonca rozprávalo o spoplatnení mailu symbolickými sumami, to by však spôsobovalo množstvo problémov a hlavne by to bolo proti filozofii slobodného internetu. Faktom zostáva, že v roku 2007 tvoril spam rekordných 95% mailovej komunikácie. Na porovnanie, v roku 2006 to bolo 85% a v roku 2001 len 5%. Spameri stále zdokonaľujú svoje techniky a nevyžiadaná pošta je len ťažko odlíšiteľná od normálnej komunikácie. Na Slovensku je rozosielanie nevyžiadaných správ prostredníctvom elektronických médií protizákonné a národný regulátor má právo takéto aktivity pokutovať do výšky až 10 miliónov Sk.

Existuje veľa spôsobov, ako nám spam môže začať otravovať život. Uvedieme si tie najzákladnejšie, ale žiaľ osvedčené spôsoby. Prvý je menej úspešný, funguje na základe vygenerovania emailovej adresy podľa určitých kritérií. Ak takáto adresa existuje, uloží sa a pri posielaní ďalšieho otravného mailu sa nemusí znova generovať. Druhý spôsob je skenovanie webových stránok na emailové adresy. Skener prejde kód HTML, a keď nájde náznak emailovej adresy, napr.. <a href=“mailto:lalala@lalala.com“>, uloží si nájdenú adresu do súboru s adresami, na ktoré rozposiela emaily. Posledným a najpoužívanejším spôsobom je získavanie adries z emailových diskusných skupín tzv. mailing listov. Spamer si „objedná” mailing list na svoju adresu a adresy všetkých prispievateľov si uloží do distribučného zoznamu. Existuje aj obdoba tohto spôsobu, kde namiesto emailových newsletterov spamer prehľadáva Usenet newsgroup-y alebo diskusné skupiny webových stránok.

Najväčšie percento spamov predstavujú správy, ktoré majú komerčno-reklamný charakter (v angličtine „Unsolicited Commercial Email“, UCE). Väčšinou ide o záležitosti „pochybného“ charakteru.

Príklady:

- návody na rýchle zbohatnutie,
- výzvy k účasti v multi-level marketingu (MLM) a pyramídovým hrám,
- ponuky erotických telefonátov a inzeráty pornografických www serverov,
- ponuky služieb masového rozosielania emailov,
- ponuky akcií neznámych začínajúcich firiem,
- ponuky zázračných liekov a liečebných postupov,
- ponuky nelegálneho softvéru,
- výzvy k zaslaniu malej čiastky,
- falošné poplašné správy,
- recesie.

Proti spammingová ochrana je založená na viacerých líniách.

Prvá z nich by mala byť už u poskytovateľa mailových služieb, ktorý by mal aplikovať účinný antispamový filter na poštových serveroch. Antispamový filter je nástroj, ktorý už pri príchode správy

na poštový server vyhodnotí, či ide o spam alebo nie. Na vyhodnotenie obsahu správy sa používajú rôzne techniky – testovanie správy na určité slová a slovné spojenia (viagra, penis, university diploma...), hľadanie rozporov v adrese odosielateľa, zle napísaný dátum v hlavičke, prípadne porovnanie adresy odosielateľa s databázou serverov (blacklisting), ktoré sú označené ako zdroje spamu.

Ďalšou oblasťou boja proti spamu sú domáce alebo firemné počítače. Väčšina známych emailových klientov (Thunderbird, Opera Mail, a i.) má v sebe integrovaný nástroj na ochranu proti spamu. Na internete sa tiež dajú nájsť desiatky nástrojov na ochranu – od freeware až po platené verzie. Veľmi dôležitá je aj ostražitosť pri zverejňovaní vlastnej emailovej adresy na verejne prístupných serveroch, odkiaľ ju spameri jednoducho získajú. Jednou z možností je mať dve a viac emailových adries. Jedna z nich by mohla byť vytvorená na verejnom poštovom servery a pri požiadavke na zaregistrovanie na rôznych stránkach by sa mala používať práve táto. Mnohé verejné servery sa pri registrácií opýtajú napr. na záujmy alebo obsahujú zaškrtávacie políčko s ponukou zasielania informácií o fungovaní a službách servera, noviniek a zmien, a pod. A potom sa nám nechcená pošta len tak sype. Druhú adresu by mali poznať len ľudia, ktorým ju chceme zverejniť. Slúžila by len súkromné resp. firemné účely. No ak už musíme uverejniť svoju emailovú adresu, napr. na svoju webovú stránku, môžeme použiť rôzne „finty“, ako nahradenie symbolu @ (slovom zavináč). Väčšina ľudí pochopí, že ide o emailovú adresu.

Prečo sa vám niekedy zdá, že vám od niekoho niektoré maily prídu po niekoľkých hodinách? Spamové filtre na serveroch pracujú tak, že veľa pokusov o doručenie spamu rovno odmietnu prijímať a vložia to do zvláštnej zložky s pomenovaním napr. „SPAM“, inak nazývanej aj karanténa. Do tejto zložky môže nahliadať obsluha poštového servera (administrátor) a doslova ručne dotrieďovať. Skutočné spamy zmaže a skutočné maily uvoľní ich adresátovi (greylisting). Preto niektoré maily adresátovi nedôjdu alebo sa značne oneskoria.

Ako sa vyhnúť tomu, aby váš mail bol chybne označený ako SPAM alebo aby bol aspoň rýchlo od spamu odlíšený?

- vyplňujte „Predmet (Subject) správy“; vyberajte pritom také slovné spojenia a výrazy, ktoré sú neopakovateľné; nepoužívajte napr. „Pozor! Dôležité!“, pretože práve takéto slová obsahuje skoro každý spam,
- nepoužívajte mailové systémy, ktoré vám do mailu vkladajú textovú reklamu,
- dôležitejšie správy si nechajte príjemcom potvrdiť,
- vyskúšajte radšej viac verejných mailových systémov, niektoré z nich sú až príliš často zaraďované medzi „spamové“,
- nepoužívajte jednoriadkové konverzácie mailom ako náhradu četu.

Dlhodobým koncepčným riešením boja proti spammingu je určite osveta a hlavne informovanosť začínajúcich používateľov emailových schránok. Tí totiž málokedy vedia, že to kvantum zbytočných správ, ktoré sa nachádzajú v ich schránkach, tam nemuselo byť a nevedia, že je to spam. Väčšinou túto správu preskočia. Takto ani ten najvýkonnejší spamový filter nedokáže zistiť, že je to spam. Je teda potrebné, zvyšovať povedomie laickej verejnosti pravdivými informáciami o spame a možnostiach,

ako sa mu brániť. Napríklad aj na školách v rámci hodín informatiky, v podnikoch rôznymi školeniami, a pod.

So spamom sa v súčasnosti stretávame aj v mobilnej komunikácii. Najčastejšie sú to reklamné SMS, MMS-ky.

Prevencia

- **Spam nikdy neotvárajte, nepotvrdzujte príjem, neodpisujte a zmažte ho natrvalo (aj v koši).**
- **Vyberajte si kvalitného poskytovateľa webových, emailových služieb** s antispamovým filtrom, najlepšie takým, ktorý spam presúva do osobitného adresára.
- Voľte poskytovateľa webových, emailových služieb s antispamovým filtrom, najlepšie takým, ktorý sa vie sa sám „naučiť" nové pravidlá a tak účinnejšie filtruje vašu prichádzajúcu poštu. **Antispamový filter priebežne kontrolujte**, lebo sa stáva, že filtre označia za spam aj správu, ktorá spamom nie je.
- Vyberajte si menej frekventovaných poskytovateľov webových, emailových služieb. Poprední poskytovatelia sú spamom bombardovaní neustále. Majú mnoho používateľov a tak je väčšia šanca, že spameri „trafia" vašu emailovú adresu. Pri menej frekventovaných poskytovateľoch emailových služieb dbajte na ich kvalitu. **Výber poskytovateľa webových, emailových služieb je vždy kompromisom.**
- **Vyberajte si kvalitného emailového klienta** (softvér na sťahovanie pošty, napr. Thunderbird, Eudora, Outlook...) so vstavaným antispamovým filtrom, prípadne jeho plug-in. Tu platia podobné požiadavky, ako na antispamový filter u poskytovateľa webových, emailových služieb, ale s väčšou možnosťou administrácie z vašej strany.
- **Nainštalujte si antispamový filter** sami, ak ho váš emailový klient neobsahuje. Mnohí výrobcovia vyvíjajú nové produkty, kde v jednom balíku sú integrované firewall, antivírusové, antispyvérové a antispamové programy, preto si zistite čo obsahuje váš balík softvéru.
- **Pravidelne aktualizujte databázu antispamového softvéru**.
- Žiadny antispamový filter nie je dokonalý, preto **buďte v otváraní emailov vždy opatrný.**
- V prípade prvej nevyžiadanej správy, označte túto správu ako spam, neotvárajte, nepotvrdzujte príjem, neodpisujte a zmažte ju. V prípade ďalších nevyžiadaných správ od toho istého odosielateľa, nepotvrdzujte príjem, neotvárajte, neodpisujte, **kontaktujte svojho administrátora a upozornite ho na nefunkčnosť antispamového filtra.**
- Ak posielate svoj email viacerým prijímateľom, nastavte si odoslanie tak, aby **prijímatelia nedostali všetky emailové adresy** (napr. v programe Outlook použijete „skrytá kópia").
- **Utajte svoju emailovú adresu.** Utajte svoju emailovú adresu tak, že nahradíte symbol @ slovom „zavinac", „at" alebo „cat". Programátori stránok utajte emailové adresy, nepoužívajte funkciu „mailto:".
- Nezverejňujte svoju emailovú adresu na rôznych fórach, inzertných a kontaktných stránkach a pod. V prípade, že sa tomu nedá vyhnúť, **zriaďte si ďalšiu emailovú adresu, ktorú budete publikovať**.
- **Utajte svoje mobilné číslo.** Proti SMS, MMS spamu je najúčinnejšie neposkytovať mobilné číslo neznámym osobám, firmám a inštitúciám.
- **Správajte sa Zodpovedne.sk!**

Vírusy (Malware, klasické počítačové vírusy, internetové červy, emailové červy, trójske kone, dialery, spyware, adware, spam, pop-up a hijackery, hoax, phishing, pharming, spoofing)

Malware

MALWARE: *škodlivý/zhubný program*, všeobecné označenie škodlivého softvéru. Patria sem napríklad vírusy, trójske kone, spyware a adware.

Na pomenovanie celej skupiny škodlivého softvéru sme použili výraz „vírusy“. Je to asi najrozšírenejšie pomenovanie, aj keď nie je celkom presné. Vírusy sú len jedno z mála nebezpečenstiev, ktoré ohrozujú náš počítač a naše osobné údaje uložené v počítači, resp. na sieti. Vírusy sú podskupinou tzv. malware – „malicious software“, čo v preklade znamená škodlivý softvér. Malware sa do počítača dostáva zvyčajne cez internet, hlavne pri prezeraní stránok s nie dobre zabezpečeným systémom (najčastejšie stránok s crackmi alebo stránok s erotickým obsahom).

Malware môžeme rozdeliť do týchto kategórií:

- Klasické počítačové vírusy
- Internetové červy
- Emailové červy
- Trójske kone
- Dialery
- Spyware
- Adware
- Spam
- PopUp a Hijackery
- Hoax
- Phishing
- Pharming
- Spoofing

Klasické počítačové vírusy

Sú to škodlivé programy, ktoré sa nedokážu rozmnožovať samé. Pre svoje rozširovanie potrebujú, podobne ako biologický vírus, hostiteľa, teda iný program najčastejšie s koncovkou .exe, .com, .sys, .dll, prípadne dokumenty balíka MS Office. Tieto vírusy sa nazývajú súborové vírusy. Inou skupinou sú tzv. boot vírusy, ktoré bývajú uložené v boot sektore, čo je prvý sektor diskety alebo pevného disku, kde sa nachádza spúšťacia časť operačného systému. Tieto vírusy sa spúšťajú pri každom čítaní z infikovanej diskety a tak isto pri každom spustení operačného systému v infikovanom počítači. Existujú aj kombinované vírusy nachádzajúce sa naraz v súboroch i v boot sektoroch, označujú sa tiež ako *multipartitné* vírusy.

Okrem samotnej reprodukcie sa vírus môže navonok prejavovať nejakou formou, napríklad môže vypisovať rôzne nečakané hlásenia, vytvárať na obrazovke grafické efekty alebo aj zvukovo sa prejaviť. Vírusy mávajú často deštruktívnu formu prejavu - napádajú systémové súbory operačného systému, kvôli čomu dochádza k „mrznutiu“ alebo celkovému znefunkčneniu daného systému, mažú súbory alebo adresáre, menia obsah súborov, šifrovanie dát, prípadne poškodzujú hardvér (prepísaním BIOSu na základnej doske). Vírusy majú zväčša väzbu na čas, alebo dátum, spúšťajú sa a pôsobia v určitých hodinách, dňoch (typickým príkladom bol v minulosti vírus Černobyľ).

Medzi novšie druhy vírusov patria tzv. neviditeľné vírusy označované ako stealth. Majú schopnosť skryť sa pred užívateľom, preto ich niektoré antivírusové programy nie sú schopné zaregistrovať. Takisto dokáže odvíriť vlastné súbory pri požiadavke o otvorenie súboru a po dokončení procesu ich znova infikovať.

Ďalším druhom vírusov sú vírusy polymorfné, ktoré samé dokážu meniť časť svojho kódu, a preto žiadna kópia tela vírusu nie je totožná s inou kópiou. Detekcia takýchto vírusov je oveľa ťažšia.

Internetové červy

V pôvodnom význame je červ tá časť vírusu, ktorá je zodpovedná za jeho šírenie. Kým klasickým súborovým vírusom trvalo mesiace až roky, kým sa rozšírili, internetovým červom na to stačí niekoľko dní, niekedy dokonca niekoľko minút. Kým súborový vírus vyžaduje zásah užívateľa, aby sa dostal z jedného počítača na druhý pomocou média (stiahnutím z internetu, CD, DVD alebo iný nosič), internetový červ sa dokáže rozšíriť sám pomocou počítačovej siete. Funguje tak, že sa pokúša pripojiť na každý možný počítač v počítačovej sieti a na svoj prenos využiť slabé miesto zle zabezpečeného počítača (predovšetkým vďaka chybám v operačnom systéme, či chybám v iných programoch poskytujúcich sieťové služby). Na tomto počítači sa červ aktivuje a znovu sa skúša šíriť do ďalších počítačov. Počet nakazených počítačov teda stúpa exponenciálne. Šíreniu červov sa dá zabrániť dobrým zabezpečením počítačovej siete, pretože napadnutiu vnútornej siete z internetu dnes už dokážeme ľahko zabrániť.

Emailové červy

Rozdelenie vírusov do spomínaných kategórií (klasické, červy a trójske kone) nie je úplne jednoznačné. Typickým príkladom sú emailové vírusy, ktoré by sa dali zaradiť medzi červy, pretože sa šíria cez internet, ale i medzi klasické vírusy a trójske kone, pretože sa aktivujú otvorením spustiteľného programu v prílohe emailu. Po aktivovaní takéhoto vírusu sa tento dokáže napríklad rozposlať na všetky emailové adresy zaznamenané v programe MS Outlook a MS Outlook Express a tým pôsobiť ako mail poslaný od priateľa resp. známej osoby. Takže ak užívateľ poľaví v ostražitosti, jedným kliknutím môže rozšíriť tento vírus ďalším užívateľom.

Trójske kone

Trójsky kôň je škodlivý kód pribalený k zdanlivo neškodnému, užitočnému softvéru. Od vírusov a červov sa líši tým, že sa nereprodukuje a v infikovanom počítači sa nachádza len v jednej kópii. Trójske kone môžu mať najrôznejšie účinky. Veľakrát môžu i priamo ohroziť počítač podobne ako vírusy vykonaním škodlivej akcie – formátovanie pevného disku, prepisovanie dát, a pod.

Najzákernejším druhom trójskych koňov sú takzvané droppery. Tieto v pravidelných intervaloch vpúšťajú do systému najrôznejší malware. Môžu obsahovať klasické vírusy, červy ale i spyware. Takto vpustený červ potom napadne sieť z vnútra, pričom je veľmi ťažké odhaliť zdroj nákazy.

Odhalenie trójskeho koňa sťažuje i technika nazývaná rootkits (voľne preložené ako nástroje správcu). Touto technikou sa trójsky kôň dokáže v systéme zamaskovať, takže to navonok vyzerá, že je všetko v poriadku.

Ďalšou nebezpečnou akciou, ktorú môžu trójske kone vykonávať, je otvorenie tzv. backdoor (v preklade zadné vrátka). Cez tieto zadné vrátka sa vie útočník, autor trójskeho koňa, dostať do systému bez toho, aby poznal prístupové meno a heslo.

Dialery

Programy, ktoré menia telefonické pripojenie počítača. Spôsobujú presmerovanie na linky s vyššou tarifikáciou, hlavne na audiotextové a zahraničné čísla. Mnohí užívatelia internetu pripojený pomocou dial-up na nich doplatili vysokými faktúrami za telefón.

Spyware

Je softvér skrývajúci sa vo vašom počítači bez vášho vedomia. Využíva sa na zbieranie informácii o počítači (hardvéri, softvéri), o vašich surfovacích návykoch, heslách, emailových adresách a samozrejme aj o vašich osobných údajoch - mene, veku, a pod.

Adware

Je softvér, ktorý automaticky zobrazuje, prehráva alebo sťahuje reklamný materiál do počítača po svojej inštalácii alebo pri používaní tohto softvéru. Často ho používajú firmy, ktoré poskytujú služby typu zarábaj cez internet. Vtedy používateľ "prenajme" časť monitora, kde sa budú zobrazovať reklamné bannery.

Spam

Je to nevyžiadaná pošta, spočíva v rozosielaní jednej a tej istej správy viacerým prijímateľom súčasne, ktorí o ňu nestoja. Môže obsahovať lacné reklamy, elektronické letáky, vírusy, phishing - podvody, hoax - poplašné správy a iné ohrozenia z internetu.

PopUp a Hijackery

Do uvedenej kategórie patria programy vložené do webových stránok, ktoré otvárajú neželané okná s reklamou. Tieto okná sú najčastejšie také „agresívne“, že pri pokuse zatvoriť ich, sa otvoria ďalšie. Takéto programy sa nachádzajú na stránkach s pornografickými materiálmi, hudbou, či zvonení do mobilov. PopUp okná však dnes už blokuje väčšina moderných prehliadačov. Ak vystavíte váš počítač takémuto útoku, odporúča sa odpojiť od internetu a až potom pozatvárať okná, a samozrejme na stránky takéhoto typu radšej nechodiť. Niektoré druhy malware (tzv. Hijackers, v preklade únoscovia) spôsobujú „samovoľné“ otváranie okien prehliadača i v čase, keď používateľ žiadne webové stránky neotvára, prípadne menia nastavenie vašej domovskej stránky, stránok s chybovými hláseniami prehliadača a vyhľadávacie stránky na svoje vlastné. Nepríjemné je to, že znemožnia nastavenie týchto stránok späť.

Hoax

Falošná správa/poplašná správa/podvod, ktorý varuje napríklad pred neexistujúcim nebezpečným vírusom. Najčastejšie sa môžeme stretnúť s falošnými prosbami o pomoc, fámami o mobilných telefónoch, petíciami a výzvami, reťazovými listami šťastia, atď.

Phishing

Týmto slovom sa označujú podvodné emaily, ktoré sú rozosielané na veľký počet adries. Na prvý pohľad vyzerá táto pošta ako napríklad informácie z banky. Príjemca je pod nátlakom hrozby nútený vyplniť osobné údaje (čísla účtu, kódy k internetovému bankovníctvu, pin pre platbu). Tieto údaje sú potom zneužívané.

Pharming

Podvodné internetové stránky, princíp týchto stránok spočíva v presmerovaní názvu www stránky na inú adresu, miesto pôvodnej stránky sa zobrazí jej dokonalá napodobenina. Zväčša sa jedná o podvodné web-stránky bánk, ktoré od vás žiadajú vyplnenie napr. kódov z viacerých pozícii GRID karty, heslá vašich účtov a pod.

Spoofing

Podvodná metóda, ktorú používajú útočníci na zmenu totožnosti odosielaných správ. Jednou z týchto metód je náhrada emailovej adresy pri phishingu. Ďalšia spočíva v podvrhu IP adresy pri pharmingu. Najviac nebezpečnou je však metóda nazývaná man-in-the-middle. Táto metóda spočíva v narušení komunikácie medzi klientom a bankou, pri ktorej útočník naruší šifrovací systém verejného a súkromného kľúča, označovaný ako certifikát banky, ktorý sa používa pri komunikácií.

Zraniteľnosť systémov

Počítačové systémy sú zraniteľné najmä kvôli týmto dôvodom:

- **Homogenita systémov** – väčšina počítačov v sieti je vybavená rovnakým operačným systémom, rovnakým prehliadačom Internetu a poštovým klientom. Toto umožňuje malwaru rýchle šírenie, lebo ak narazí na jednu bezpečnostnú dieru, je vysoká pravdepodobnosť, že ostatné počítače budú na tom podobne.
- **Chybovosť** – väčšina programov obsahuje bezpečnostné chyby, niektoré sú tak závažné, že malware dokáže jednoducho vniknúť do systému a spôsobiť tak nemalé škody.
- **Nepotvrdený kód** – pri vložení prenosného média ako je napr. CD, DVD, USB disk alebo iné prenosné médium, sa ihneď aktivuje program, ktorý môže obsahovať malware. Jedno z riešení je zakázať automatické spustenie pri vložení CD alebo DVD do mechaniky.

Prevencia

- Zálohujte všetky svoje údaje na disky chránené proti zápisu. Zálohovaním dát sa vyhnete i strate dát následkom výpadku prúdu alebo tvrdého reštartu.
- **Používajte menej rozšírený operačný systém, prehliadač a poštového klienta**. Väčšina malwaru pracuje pod operačným systémom MS Windows, prehliadačom Internet Explorer a poštovým klientom Outlook. Pravidelne si aktualizujte operačný systém.
- **Zabezpečte svoj počítač proti neoprávnenému vniknutiu**. Tento krok môžete urobiť použitím tzv. firewall, ktorý vytvára ochrannú stenu medzi vaším počítačom a potenciálne škodlivým obsahom na internete.
- V prípade, že využívate pripojenie k internetu cez dial-up, **kontrolujte aké číslo pri pripájaní počítač vytáča,** používajte programy, ktoré zabraňujú dialerom v zmene čísla (napr. Connection Meter, OptimAccess Dial a pod.), a **v prípade, že máte pochybnosti o vytočenom čísle, odpojte sa od internetu**, preverte počítač antivírusovým programom, reštartujte ho a vyskúšajte sa pripojiť odznova.
- **Zabezpečte svoje bezdrôtové WiFi siete.**
- **Nenavštevujte nezabezpečené stránky.** Snažte sa vyhnúť stránkam s pornografiou, stránkam s mp3 hudbou, filmami, licenčnými kľúčmi a pod. Nesťahujte žiadne programy, ktorých činnosť by mohla byť v rozpore s autorskými zákonmi.
- **Pred stiahnutím každého freeware programu si pozorne prečítajte, či jeho súčasťou nie je niektorý z uvedených nebezpečných programov.** Pozorne si prečítajte podmienky používania programu a vyhnite sa všetkým programom, ktoré podmieňujú svoju inštaláciu nainštalovaním tzv. Third Party Components (komponenty od tretích strán) a tiež tým, ktoré sa v zmluve zbavujú zodpovednosti.
- **Nezverejňujte svoju emailovú adresu**. Vaša emailová adresa je váš osobný údaj. Veľmi dobre si rozmyslite, do akého formulára ju vyplníte. Používajte radšej niekoľko adries (jednu pre priateľov a druhú na vyplňovanie do formulárov).
- **Neotvárajte neznáme prílohy**. Ak neotvoríte spustiteľnú prílohu emailu, nemôžete dostať emailový vírus. Preto radšej všetky cudzojazyčné emaily vymazávajte. Vírus však môžete dostať i od rodiny či priateľov bez toho, aby vedeli, že vám taký email poslali. Pred otvorením podozrivej prílohy emailu si radšej overte, či vám ju dotyčný chcel poslať.
- **Nespúšťajte neoverené makrá v dokumentoch**. V súčasnosti sa i makrá podpisujú digitálnym podpisom. Preto si pred jeho spustením overte platnosť digitálneho podpisu a neaktivujte neznáme makro.

- **Udržujte všetky súčasti systému aktuálne, používajte najnovšiu verziu prehliadača a poštového klienta**. Aktualizovaním súčastí systému odstraňujete jeho nedostatky, ktoré by škodlivé programy mohli využiť.
- **Chráňte svoj počítač aktuálnym antivírusovým systémom**. Aby bola ochrana účinná, antivírusové systémy sa aktualizujú i niekoľkokrát za deň.
- **Chráňte svoj počítač anti-spyware programom**. Tieto programy sa aktualizujú rovnako ako antivírusové systémy.
- **Zvážte, ktoré priečinky budete zdieľať v sieti**. Nastavte na všetky zdieľané priečinky príslušné oprávnenia a chráňte k nim prístup heslom.
- **Vypnite automatické spúšťanie programu po vložení média (CD, DVD, USB DISK)**.
- **Chráňte vstup do počítača heslom.** Nedovoľte neznámej osobe, aby sa dostala do vášho počítača.
- **Majte prehľad kto a ako využíva váš počítač.** Veľa užívateľov využívajúcich cudzí počítač prejavuje menšiu zodpovednosť ako pri vlastnom počítači, preto sa treba dohodnúť na konkrétnych pravidlách a určiť vopred aké súbory budú otvárané/používané a predtým ich skontrolovať pomocou antivírusového programu.
- **Zálohujte svoje dáta.** Zálohovaním predídete škodám, ktoré vzniknú pri chybe alebo poškodení hardvéru alebo softvéru.
- **Nepodliehajte panike.** Ak je počítač zavírený a antivírus neposkytuje možnosť súbory odvíriť, alebo si užívateľ nevie poradiť s iným problémom, treba k tomuto problému pristupovať s rozvahou, nerobiť unáhlené kroky. Užívateľ by mal požiadať o odvírenie počítača profesionálov, prípadne sa s nimi aspoň poradiť.
- **Správajte sa Zodpovedne.sk!**

Online obchodovanie (Online nakupovanie, internet banking, virtuálny účet)

Online nakupovanie

Čo všetko sa dá nakúpiť online? Všetko! Dokonca aj tovar, ktorý nie je na území Slovenska povolené predávať, alebo je predávaný len na vlastnú zodpovednosť. K takémuto tovaru patria napríklad lieky, čaje, kozmetika atď.

Na Slovensku sa v súčasnosti najviac predávajú knihy, cd a dvd nosiče s hudbou, hrami alebo softvérmi, oblečenie, pc komponenty, lístky na kultúrne podujatia ale aj letenky.

Online si môžete kúpiť úplne nový či používaný tovar, môžete sa zúčastniť aj online aukcií.

V neposlednom rade, ak máte niečo na predaj vy, môžete to ponúknuť na rôznych inzertných stránkach, ktoré po registrácii umožňujú podávať inzeráty zadarmo.

Online nakupovanie má viacero výhod oproti klasickému nakupovaniu v tzv. kamennom obchode:

- Nakupovanie z pohodlia domova - nemusíte vstávať od svojho počítača a ani čakať v radoch. A navyše nakupovať môžete aj za hranicami štátu.
- Otvorené non-stop.
- Výber spôsobu platby (pomocou internet bankingu, priamym vložením sumy na účet v banke, dobierkou, hotovosťou pri dodávke kuriérom, na splátky, faktúrou, prostredníctvom kreditných kariet, pomocou virtuálneho účtu, atď.).
- V niektorých prípadoch je tovar doručený až do domu alebo kancelárie, často aj zdarma, ale môžete si ho vyzdvihnúť aj osobne v dohodnutom čase na dohodnutom mieste.
- Mnohokrát nižšie ceny.
- V mnohých prípadoch je možné objednávku stornovať do 24 hodín alebo nepoužitý a zabalený výrobok vrátiť do 7 dní bez udania dôvodu.
- Na všetky nové výrobky kupované v rámci Slovenska sa vzťahuje zákonom stanovená 2-ročná záručná lehota. V prípade poruchy je oprava zadarmo garantovaná v autorizovanom servise v mieste vášho bydliska.
- Pri online nákupe nemusíte zadávať číslo vašej platobnej karty, heslá k účtom ani žiadne osobné údaje, ktoré by mohli byť zneužité, je treba uviesť iba adresu doručenia, telefónny kontakt a email.
- Pravidelné zasielanie informácií o stave objednávky na váš email.
- Anonymita pri nakupovaní.
- Doplnkové služby - väčšina online obchodov má prepracovaný systém zákazníckeho servisu. V prvom rade takýto predajca odpovedá na akékoľvek otázky týkajúce sa predaja ponúkaného tovaru. Pomáha pri vytváraní objednávky, ale aj pri vyhľadávaní menej dostupného tovaru. V prípade potreby umožní aj vybavenie splátkového úveru na diaľku bez nutnosti osobného navštívenia predajne. Na vaše vyžiadanie vás bude informovať o rôznych akciách a novinkách buď telefonicky alebo mailom.

- Online nakupovanie má však aj niekoľko nevýhod:
- Podstatnou nevýhodou je, že si tovar pred nákupom nemôžete ohmatať, poriadne popozerať ani vyskúšať. Oplatí sa preto obzrieť si ho v klasickom obchode a potom za výhodnejších a pohodlnejších podmienok kúpiť online.
- Prienik do súkromia – viaceré internetové obchody vyžadujú pred nákupom registráciu, či už pre samotný nákup alebo pre marketingový prieskum. Tieto údaje môžu byť posunuté ďalej iným spoločnostiam a môžu byť zneužité.
- Finančné podvody – zákazník sa môže stať obeťou internetového podvodu aj u spoľahlivého predajcu v prípade napadnutia serveru neznámym páchateľom (hackerom) alebo nečestným zamestnancom. Môže pritom nie len jednorázovo prísť o svoje peniaze, ale jeho osobné údaje môžu byť ďalej zneužívané. Hovorí sa o tzv. kradnutí totožnosti, kedy podvodník využíva osobné údaje obete napr. na vytvorenie novej kreditnej karty.
- Dodacia lehota závisí od dostupnosti tovaru. Zatiaľ, čo v klasickom obchode si po zaplatení môžete tovar rovno odniesť domov, cez online nakupovanie to môže trvať od niekoľkých hodín, v prípade, že je tovar na sklade, až do niekoľkých týždňov, ak ide o špecifický málo dostupný produkt.
- Môžete natrafiť na nespoľahlivých predajcov, či už ide o firmy alebo o jednotlivcov. Tovar, ktorý od nich kúpite nezodpovedá dohodnutému tovaru a máte problém ho reklamovať. V druhom prípade po zaplatení vám tovar nie je vôbec dodaný a vaše peniaze si márne pýtate naspäť.

Internet banking

Internet banking (IB) je služba poskytovaná k bežným účtom, ktorú dnes ponúka väčšina bánk vo svete. Umožňuje sledovať stav účtov, zadávať príkazy pre domáce aj zahraničné platby, prípadne pre trvalé platby a inkaso, sledovať zostatky a pohyby na kreditných kartách a mnoho ďalších možností z pohodlia vášho domova cez internet pomocou bežného prehliadača. Podstatná výhoda IB je, že váš účet môžete obsluhovať kedykoľvek z ktoréhokoľvek miesta na svete, kde je možné pripojenie na Internet. Pomocou IB ušetríte čas, ale aj peniaze za účtovné položky, ktoré sú na pobočkách banky spoplatnené vyššími sumami.

Aby bol IB bezpečný je nutné urobiť určité opatrenia zo strany banky ako aj zo strany majiteľa účtu so službou IB. Banka zabezpečuje ochranu súkromia klienta, ochranu identifikácie a použitie najnovších technológií pre zabezpečenie počítačov vo vnútri banky.

Ochrana súkromia zahŕňa bezpečné spojenie pri prihlásení do IB. Bezpečné spojenie rozpoznáte podľa adresy URL, ktorá sa začína https://meno.banky.sk alebo podľa symbolu visiaceho zámku, či zlomeného kľúča v pravom dolnom rohu vášho prehliadača. V IB sa využíva technológia šifrovania Secure Sockets Layer (SSL) na zašifrovanie vašich osobných údajov predtým, ako sú odoslané z vášho počítača. Tým sa zabezpečí, že ich počas prenosu nikto iný neprečíta. Ak sa po používaní IB zabudnete odhlásiť, alebo váš počítač je určitú dobu neaktívny, systémy banky vás automaticky odhlásia. Stránky zobrazené počas bezpečného spojenia sa neukladajú do dočasných súborov na vašom počítači.

Na ochranu identifikácie sa používa viacfaktorová identifikácia a autentifikácia (PID, HESLO + GRID alebo SECURid karta alebo SMSKOD). Taktiež sa po určitom počte neúspešných pokusov o prihlásenie do IB využíva automatické zablokovanie. Ak ho chcete znovu aktivovať je potrebné kontaktovať vašu banku.

Všetky počítače banky sú zabezpečené pred nechceným prienikom zvonka. Všetky majú operačné systémy aktualizované najnovšími bezpečnostnými záplatami, antivírusový softvér je takisto aktualizovaný v určitých intervaloch a používajú sa firewally (ochranná stena medzi počítačom a potenciálne škodlivým obsahom na internete) na zabránenie neautorizovaného vniknutia.Od majiteľa účtu sa očakáva obdobná opatrnosť. Je potrebné mať zabezpečený počítač ako aj chrániť si svoje súkromie.

Čo sa týka samotného počítača, je potrebné mať nainštalovaný antivírusový softvér a pravidelne ho aktualizovať, používať anti-spyware softvér, používať firewall a nainštalovať si najnovšie bezpečnostné aktualizácie a záplaty operačného systému.

Čo sa týka vášho súkromia, v prvom rade sa nepripájajte k službe IB na verejných miestach, napr. v internetových kaviarňach či knižniciach a pod. Vždy sa po ukončení služby IB odhláste.

Dávajte si pozor na online podvody. Najznámejšie sú tri typy bankových krádeží: pharming, phishing a MITM. Pfarming spočíva v presmerovaní názvu www stránky na inú podvodnú adresu. Po ich otvorení neskúsený majiteľ účtu ani nerozozná, že ide len o dokonalú napodobeninu stránky jeho banky. Väčšinou si podvodník takouto formou vypýta kódy z viacerých, prípadne všetkých, pozícií vašej GRID karty. Pamätajte si, že žiadna banka od svojich klientov pri jednom prihlásení nikdy nežiada viacnásobne zadať napr. kódy na GRID karte. Phishing je druhý zo spôsobov ako získať vaše osobné údaje pomocou emailov, instant messaging-u alebo pomocou sms v mobilnom telefóne. Takéto správy sa tvária ako produkty finančných inštitúcií a obsahujú odkaz, na ktorom si máte zmeniť heslo a zaslať ho podvodníkovi, ktorý sa vydáva za vašu banku, prípadne vás odkážu na už vyššie spomínanú napodobeninu stránky. Preto si vždy overte pravosť takejto správy a neotvárajte stránku cez odkaz v pošte. Vždy priamo zadajte webovú adresu, alebo použite záložku Obľúbené. Nikdy neposielajte dôverné údaje emailom, sms správou ani pomocou instant messaging-u! Najviac nebezpečnou je metóda nazývaná MITM (man-in-the-middle v preklade „muž v strede“). Táto metóda spočíva v narušení komunikácie medzi klientom a bankou. Použiť metódu MITM však nie je jednoduché, pretože na narušenie komunikácie je potrebné získanie kľúča (označovaný aj ako certifikát) banky, ktorý sa často mení. Je preto dôležité nastaviť váš internetový prehliadač tak, aby overoval, či je certifikát ešte platný.

Nevyžiadané emailové správy s prílohami otvárajte len veľmi opatrne. Nikdy neotvárajte emailovú prílohu, ktorá obsahuje súbor s príponou .exe, .pif alebo .vbs, keďže tieto sú zvyčajne využívané vírusmi. Každý súbor s dvojitou príponou je pravdepodobne vírus a mal by byť vymazaný.

Chráňte svoj počítač heslom, zabránite tak neautorizovanému prístupu k vašim osobným informáciám. Vypnite vo svojom prehliadači funkciu "AutoComplete" (automatické dokončovanie – funkcia, ktorá pri písaní do formulárového políčka automaticky ponúka výber slov podľa už napísaných písmen). To zabráni „nepovolaným“ vidieť vaše osobné údaje, ktoré ste zadali, niekedy aj spolu s heslami. Udržujte heslo v tajnosti, neprezrádzajte ho, buďte pri jeho tvorbe originálny, aby bolo dostatočne zložité, nepoužívajte napr. mená a dátumy narodení členov vašej rodiny, alebo iné jednoduché číselné kombinácie a slová. Nepoužívajte rovnaké heslá pri IB a zároveň pri prihlasovaní na freemailové služby. Heslá si podľa možnosti nezapisujte. Meňte si svoje heslá vždy, keď máte pocit, že ich dôveryhodnosť bola narušená. Snažte sa na Internet banking nevyužívať zdieľané počítače.

Chráňte svoje dôverné informácie aj keď ste offline. Čítajte bankové výpisy k účtom a kreditným kartám, v prípade nezrovnalosti v transakciách, okamžite upozornite banku. Upozornite banku aj na každú zmenu vo vašich osobných údajoch. Svoje bankové dokumenty, ako napríklad výpisy z účtov, uložte na bezpečnom mieste. Ak plánujete zrušiť kartu alebo ak uplynie doba jej platnosti, znehodnoťte ju prestrihnutím na polovicu cez číslo účtu a magnetický prúžok. Buďte opatrný pri každej osobnej informácii, ktorú odhadzujete.

Virtuálny účet

Najznámejším virtuálnym účtom na svete je PayPal, ktorý od roku 2002 patrí americkej spoločnosti eBay. V súčasnosti je možné ho využiť v 55 krajinách sveta, vrátané Slovenska. Jeho hlavnou výhodou je možnosť platby aj v zahraničných e-obchodoch bez vysokých poplatkov za prevod na zahraničný účet a bez časovej náročnosti. Skrátka ide o prevod peňazí rýchlo a lacno. Možnosť platby pomocou PayPal ponúkajú aj slovenské banky, ktoré neposkytujú vlastný virtuálny účet alebo naopak poskytujú PayPal spolu so svojim virtuálnym účtom. Na Slovensku sú známejšie virtuálne účty eCommerce od Všeobecnej úverovej banky, TatraPay a CardPay od Tatrabanky, SporoPay od Slovenskej sporiteľne atď.

Ako funguje virtuálny účet? Na jednej strane musí existovať dohoda medzi bankou ponúkajúcou tento spôsob platby a samotným e-obchodníkom. Na druhej strane musí mať potenciálny zákazník vedený účet v banke a aktívnu službu IB. Potom si zákazník môže po vybratí tovaru zvoliť tento spôsob platby a je tak automaticky presmerovaný na službu IB. Od IB sa tento spôsob líši tým, že zákazníkovi odpadá vypĺňanie formulára pre platobný príkaz, lebo samotná banka po overení jeho identity, mu tento formulár ponúkne vyplnený. Od zákazníka sa potom očakáva iba zadať, z ktorého účtu budú peniaze stiahnuté ak vlastní viac účtov a záverečné potvrdenie pre platobný príkaz pomocou kódu na GRID karte. Platba je po odsúhlasení hneď prevedená na účet e-obchodníka a rovnako zákazník je spätne presmerovaný na stránku internetového obchodníka. Informáciu o realizácii platby obdrží klient aj obchodník ihneď vo forme emailovej správy.

Druhý zásadný rozdiel oproti IB je garancia vrátenia peňazí v prípade nespokojnosti s tovarom a v prípade, že e-obchodník tovar vôbec nedodal. Banka totiž po obdržaní sťažností od zákazníka hneď rieši problém s e-obchodom bez toho, aby si to musel zákazník s danou firmou vybavovať sám. V prípade nepoctivosti zo strany e-obchodu banka zmrazí tomuto obchodu účet, zruší s ním dohodu a vymaže ho zo zoznamu schválených obchodov.

Prevencia

- **Vyberte si seriózneho predajcu,** prečítajte si príspevky iných užívateľov, čím viac ich je k dispozícii, tým lepší obraz si môžete o spoľahlivosti obchodu vytvoriť.
- **Skontrolujte, či internetový obchod uvádza kompletné kontaktné údaje,** najmä telefonické kontakty, email, fyzickú adresu, obchodné meno spoločnosti.
- **Preštudujte si dodacie podmienky** - vždy si predtým, ako tovar objednáte, skontrolujte dodacie lehoty, aby ste mali istotu, že tovar dorazí načas. V prípade, že vás obchod priebežne neinformuje o stave vašej objednávky, prípadne máte pochybnosti, priebežne obchod kontaktujte, najlepšie telefonicky.
- **Preštudujte si reklamačný poriadok predajcu.**
- **Pri platbe dbajte na správnosť zadávaných údajov.**
- **Vytlačte a uschovajte všetky dokumenty**.
- **Zvažujte celkové náklady** - pred nákupom si vždy overte náklady na dopravu tovaru (resp. možnosť osobného odberu tovaru). Od určitej sumy býva často doprava bez poplatku.
- **Poznajte vaše práva** - či už ide o záručnú dobu alebo možnosť reklamácie.
- **Strážte si svoje osobné údaje** - neposkytujte o sebe informácie, ktoré nie je nutné zverejňovať a nikdy nikomu nedávajte svoje vstupné heslá pre internetové služby.
- **Vyhýbajte sa používaniu služby IB na verejných a zdieľaných počítačoch**. Ak sa tomu nedá vyhnúť, tak sa vždy po ukončení odhláste.
- **Zabezpečte si svoj počítač** antivírusovým programom, zároveň pravidelne aktualizujte vírusovú databázu, používajte anti-spyware program a firewall, nainštalujte si potrebné aktualizácie a záplaty operačného systému.
- **Komunikujte bezpečným spôsobom.** Seriózne web stránky, hlavne pre internet banking, bežia na serveroch, ktoré používajú tzv. SSL certifikát. Poskytujú informácie o tom, ako chránia vaše finančné informácie (heslá, čísla účtov, atď.) počas ich prenosu a uskladnenia. Hľadajte znak nezlomeného kľúča alebo uzavretého zámku, ktorý informuje o tom, že prenos týchto dát je šifrovaný alebo skontrolujte, či je na začiatku URL adresy „https“.
- Po prihlásení **skontrolujte, či sú v zozname všetky vaše účty**, z ktorých môžete zadávať v Internet bankingu platobné príkazy.
- V prípade, že niečo z vyššie spomínaných vecí nesedí, **nezadávajte Vaše PID a heslo, ale kontaktujte svoju banku!** Môže ísť o tzv. pharming – presmerovanie na falošnú stránku!
- **Ak ste už heslo zadali, urýchlene si ho zmeňte v Internet bankingu!**
- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- Aktivujte si **službu posielania sms alebo emailov**, ktorá vás budete okamžite informovať o debetoch a kreditoch na vašom účte, prípadne o každom vstupe do služby internet banking.
- **Správajte sa Zodpovedne.sk!**

Čet (Instant messaging, blog, diskusné fórum)

ČET: rozhovor, písomná konverzácia dvoch alebo viacerých ľudí v reálnom čase prostredníctvom počítačovej siete. Pomocou nej môžeme zároveň posielať prílohy (textové súbory, obrázky, video súbory, ...). Je to prevzaté slovo z anglického CHAT, ktoré sa v slovenčine udomácnilo a píše sa foneticky ČET. Skloňuje sa podľa vzoru dub. V lokáli jednotného čísla má príponu –e, teda na čete, o čete. Toto slovo skloňujeme takto: čet – z četu (uveriť) četu (čítať) čet – na/o čete – s četom, v množnom čísle: čety – z četov (uveriť) četom – (čítať) čety – na četoch – s četmi.

BLOG: weblog, „internetový denníček“, sú to teda zápisky, názory, myšlienky, skúsenosti, dojmy publikované na internete. Užívatelia sa stretávajú na tematických blogoch, kde spolu komunikujú na danú tému. Blogy môžu byť verejné i súkromné.

FÓRUM: otvorená diskusia, miesto, kde môže každý vyjadrovať svoj názor. Internetové fóra niekedy vyžadujú registráciu, pre možnosť pridania príspevku. Fóra sú založené pre určitú záujmovú skupinu, kde si ľudia vymieňajú poznatky, znalosti, skúsenosti, aby si pomohli.

Čet a instang messaging

Čet je interaktívny spôsob komunikácie dvoch alebo viacerých ľudí súčasne. Slovo čet znamená klebetiť, z toho vyplýva nezáväznosť komunikácie, ale je možné ho v nutných prípadoch použiť aj na riešenie pracovných záležitostí alebo iných dôležitých vecí. Zásadnou nevýhodou četu je, že aj druhý účastník konverzácie musí byť online. Čety podľa spôsobu komunikácie môžeme rozdeliť na:

- Čet cez instant Messenger (Skype, ICQ, atď.), čiže program na prácu so správami. Ak chcú dvaja alebo viacerí ľudia komunikovať, musia ho mať nainštalovaný vo svojom počítači.
- Webčet (4ever.sk, pokec.azet.sk, fun-online.sk atď), na ktorý by mal stačiť len internetový prehliadač, prípadne sa vyžaduje nainštalovanie nejakého pluginu, podpora javy a pod. Webčety možno používať napríklad v internetovej kaviarni, kde nie je dovolené nainštalovať instant messenger.

Zásadný rozdiel je v bezpečnosti. Treba mať na zreteli, že prenos správ pomocou četu nie je šifrovaný. Na webčete sa preto neodporúča riešiť osobné a diskrétne záležitosti, tieto informácie by mohli byť ľahko zneužité.

Webčet zvykne byť rozdelený do rôznych záujmových kategórií, tzv. miestností. Užívateľ si môže dokonca vytvoriť aj svoju vlastnú miestnosť a vstup do nej povoliť všetkým alebo len vybraným ľuďom.

Typické pre četovanie je používanie prezývok (nickov), čo zabezpečuje anonymitu četujúcich. Či četujúci užívateľ odhalí svoju skutočnú totožnosť, vek, pohlavie, či iné informácie je len jeho vlastné rozhodnutie. Môže byť zábavné vydávať sa za niekoho kým nie ste, ale rovnako nikdy neviete, kto je ten na druhej strane. Musíte preto poznať mieru a nezachádzať priďaleko.

V bežnej komunikácii okrem samotného rozhovoru využívame aj neverbálnu komunikáciu, gestikuláciu, postoj tela, a pod., čo veľa napovie o našom charaktere a momentálnej nálade. Samotný text pri četovaní však nie vždy vystihuje náladu komunikujúcich, preto sa vo veľkej miere používajú rôzne skratky a grafické symboly – emotikony. Moderné technológie však umožňujú aj iné formy komunikácie, konkrétne audiočet a videočet, na ktoré stačí doplnkové vybavenie domáceho PC (slúchadlá alebo reproduktory, mikrofón, webkamera).

Ako možno četovanie využiť?

- Na súkromne účely (zábava, trávenie voľného času, nezáväzné rozhovory, rady, informácie o rôznych akciách, zoznámenie, a pod.)
- Na pracovné alebo obchodné účely (hotline linky pre zákazníkov, práca na diaľku, video konferencie, reklama, komunikácia s kolegami, a pod.)
- Riziká četovania
- Anonymita. Nikoho nemôžete prinútiť, aby písal iba to, čo je pravda. Profil môže byť vyplnený nepravdivo, priložené fotky skresľujúce. Treba byť opatrný aj v prípade, že sa do četu zapojí človek, ktorý má založený nový účet. Novou identitou sa môže snažiť zakryť svoje predchádzajúce pôsobenie v čete, pri ktorom mu bol zrušený, zablokovaný účet alebo sa snaží vytvorením viacerých identít znásobiť šance pre získanie nových obetí. Kým si píšete, môžete sa odpojiť hneď, ako vám prestane byť četovanie príjemné. Ak sa chcete spoznať aj osobne, platí to isté, čo aj pri online zoznamkách, vyberte si radšej ľudí zo svojho okolia a necestujte na stretnutie do neznámych miest. V známom a hlavne verejnom prostredí sa človek cíti bezpečnejšie. Na prvé stretnutie nikdy nechoďte sami. Dajte si jasné poznávacie znamenie. Pokiaľ vás dotyčný na prvý pohľad odradí alebo vyľaká, môžete jednoducho odísť.
- Zneužitie údajov. Nikdy neuvádzajte počas četovania vaše osobné údaje, heslá, PIN a pod., ktoré je možné zneužiť. Nájdu sa aj ľudia, ktorí zneužijú vaše osobné údaje (použijú vaše pravé meno a priezvisko, vašu fotografiu) na vyplnenie profilu a vystupujú v čete vo vašom mene. V takomto prípade kontaktujte správcu servera a požiadajte ho o zablokovanie alebo zrušenie účtu.
- Príspevky s nevhodným obsahom. Nie je až také zriedkavé ak sa medzi četujúcimi objaví niekto, kto ostatných bezdôvodne uráža a posmieva sa im, možno tým ventiluje svoje neúspechy v osobnom živote alebo v kariére, rovnako sa môžeme stretnúť aj s rasistickými a extrémistickými názormi. Z tohto dôvodu bývajú niektoré četovacie miestnosti moderované. Moderátor upozorňuje nevhodne prispievajúcich užívateľov a v prípade nutnosti im dokonca zakáže prispievať.
- Zdravotné riziko a potenciálna závislosť. Akákoľvek dlhé vysedávanie pri počítači zaťažuje chrbticu, oči a nervovú sústavu. Oveľa horšie riziko je, že četovanie môže prejsť do závislosti, alebo že človek, ktorý sa vydáva za niekoho fiktívneho sa začne so svojou virtuálnou identitou stotožňovať.

Blog

Blog je určitá forma komunikácie, čosi ako internetový zápisník, miesto, kde autor zdieľa informácie, názory, myšlienky, skúsenosti, dojmy s ostatnými, dokonca aj neznámymi ľuďmi. Môže byť tematicky zameraný (politika, sociálna situácia, webdizajn, príroda, a pod.).

Obdobný spôsob komunikácie existoval aj v predblogovej ére, väčšinou ale znamenal udržiavanie vlastnej webovej stránky. Ale zatiaľ čo na klasickom webe sa obsah mení len sporadicky, na blog autor prispieva viac-menej pravidelne. Väčšinou je ku každému článku diskusia, čo umožňuje spätnú väzbu a komunikáciu s ľuďmi, ktorí blog čítajú.

Oproti spravodajským serverom je blog písaný s určitou dávkou subjektivity a prevažne jedným autorom. Na spravodajských serveroch publikujú viacerí jednotlivci objektívne fakty a poznatky. Blogovanie je o tom, čo ľudia chcú povedať a nie o tom, ako to zabezpečiť. Preto vznikajú špecializované servery, kde si užívatelia svoj blog založia, vytvárajú články, čítajú ich a o nič viac sa nestarajú.

Diskusné fórum

Viaceré špecializované stránky poskytujú svojím návštevníkom možnosť diskusie na určitú tému, na položenie otázky, odpovedanie, vyjadrovanie vlastného názoru, kritizovanie, ale aj na poskytovanie rád, odporúčaní a pod.

Samotné fórum je rozdelené do niekoľkých kategórií podľa témy, čo by sa dalo teoreticky porovnať s rozdelením četu na viaceré miestnosti. V porovnaní s četom ide o komunikáciu, ktorá neprebieha v reálnom čase, ale formou sporadických príspevkov. To znamená, že nie je nutné, aby účastníci diskusie boli online. Fórum môže byť moderované a podobne ako pri čete sa v ňom s obľubou využívajú aj emotikony a skratky.

Prevencia

- **Služba instant messaging nie je šifrovaná**, preto ju nevyužívajte na prenos informácii, ako sú čísla kreditných kariet, heslá, čísla účtov, adresy, či iné citlivé údaje.
- **Pri zdieľaní akýchkoľvek súkromných informácii neznámej osobe, s ktorou ste sa zoznámili cez službu instant messaging, buďte veľmi opatrní**. Dokonca i zdanlivo nevinné informácie, ako je meno vášho zamestnávateľa, by mohli byť podvodníkmi použité proti vám.
- **Zablokujte prístup neznámym ľuďom**. Ak vám to software dovolí, nastavte systém tak, aby vás mohli kontaktovať len ľudia, ktorých máte v zozname.
- **Nevyplňujte svoj internetový profil**, pokiaľ ste nútení vložiť do systému údaje, používajte fiktívne informácie.
- **Buď opatrný pri četovaní s človekom, ktorý má nový profil.** Novou identitou sa môže snažiť zakryť svoje predchádzajúce pôsobenie v čete, pri ktorom mu bol zrušený, zablokovaný účet alebo sa snaží vytvorením viacerých identít znásobiť šance pre získanie nových obetí.
- **Ak zistíte, že boli zneužité vaše osobné údaje** (napr. fotografia) alebo niekto v čete vystupuje vo vašom mene, kontaktujte okamžite správcu servera, aby jeho účet zablokoval. Dôkazový materiál si uschovajte.
- **Pri prihlasovaní do systému instant messaging nepoužívajte svoje systémové, či emailové heslo**.
- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- **Deaktivujte si automatické sťahovanie.**

- **Neklikajte na linky poslané cez instant messenger**, hlavne ak ide o neznámeho adresáta, ktorý vás vyzýva napr. na zmenu prístupového hesla k vašim účtom. Môže isť o bankový podvod.
- **Neotvárajte pochybné súbory poslané pomocou instant messengera**, hlavne ak majú dve koncovky (napr. exe, .com, a pod.), môže ísť o infiltráciu.
- **Nezaťažujte zbytočne linky posielaním tzv. hoaxu**. Správu, ktorá vás vyzýva k ďalšiemu preposielaniu ľuďom z vášho zoznamu kontaktov, si pre istotu overte v databáze hoaxov.
- **Aktualizujte svoj instant messaging software.**
- **S nikým, s kým sa dieťa zoznámilo iba cez internet alebo mobil, sa nesmie stretávať samé osobne.** Tak ako v reálnom živote nechodia deti na stretnutie s neznámou osobou bez sprievodu niekoho ďalšieho, najlepšie rodiča, alebo aspoň súrodenca, kamaráta, tak aj na stretnutie s neznámou osobou, s ktorou sa dieťa zoznámilo iba cez internet alebo mobil, je stretnutie veľmi nebezpečné. Ak už dieťa ide na stretnutie, tak vždy aspoň s kamarátom. Rodičom oznámiť na aké stretnutie ide, za kým ide, kde a kedy sa plánuje vrátiť. Stretnutie by malo byť na verejnom mieste, kde je veľa ľudí. Znakom bezpečnejšieho stretnutia je, že tomu, čo pozýva, nevadí, že dieťa príde s rodičom alebo inou dospelou osobou. Ak mu to vadí, ten človek nemá čisté úmysly.
- **Buďte podozrievavý voči človeku, ktorý dieťa presviedča, aby zatajovalo svoje internetové kamarátstvo pred rodičmi, alebo vystupuje ako tínedžer, ale nevie väčšinu odpovedí na otázky, ktoré bežne rovesníci poznajú.** Takýto človek chce deťom ublížiť a preto klame a navádza, aby zatajili pozvanie na stretnutie s ním, aby si zmazali históriu četu, jeho emaily, sms-mms správy a podobne.
- **Ak sa dieťa cíti nepohodlne alebo trápne pri online konverzácii, má právo ju okamžite prerušiť a odísť z četovej miestnosti**. Ak sa pritom snažil človek zaviesť tému do sexuálnej oblasti nech dieťa o tom povie rodičom, alebo v škole učiteľom.
- **Váš domáci počítač (alebo hraciu konzolu) postavte do obývacej izby alebo na iné spoločné prístupové miesto v byte.** Najlepšie tak, aby rodič mal vždy výhľad na monitor**.** Nedávajte počítač do detských izieb. Majte dobrý prehľad o všetkých ďalších počítačoch, ktoré sú deťom prístupné.
- **Stanovte medzi deťmi a rodičmi jasné pravidlá pre používanie internetu**. Urobte si rozvrh na dni a presný čas, kedy má dieťa povolenie stráviť čas na internete, najlepšie v čase vašej prítomnosti. Podpísanú zmluvu vystavte niekde pri monitore počítača. Nezabudnite, ak si s vaším dieťaťom vytvoríte pravidlá o používaní internetu, stanovte si práva a povinnosti pre obe strany. Pravidla, by sa mali pravidelne aktualizovať. Vzor takejto „rodinnej zmluvy" nájdete na stránkach Zodpovedne.sk
- **Najmenšie deti by nemali používať četovacie miestnosti bez moderátora, v ktorých môže byť dieťa najviac ohrozené.**
- **Vytvorte medzi dieťaťom a rodičom vzťah vzájomnej dôvery.** Majte prehľad o prezývkach (nickname) vašich detí, ktoré používajú na internete. Buďte opatrný, nebuďte dotieravý pri kontrole dieťaťa, vzájomná dôvera je veľmi dôležitá. Prílišná kontrola by mohla dieťa dohnať ku skrývaniu a zatajovaniu činností. Netrestajte dieťa za to, čo nie je jeho chyba, môže vám prestať dôverovať a mať strach a neistotu pri zdôverovaní sa s nejakým problémom. Je potrebné sa s deťmi veľa rozprávať, upozorniť ich na rôzne nebezpečenstvá, zaujímať sa a vedieť kde a ako trávia voľný čas, s kým telefonujú, emailujú, četujú, s kým sa stretávajú. Menšie deti si vyžadujú pravidelnú kontrolu. Ponúknite deťom adekvátne, zmysluplné a zaujímavé mimoškolské aktivity. Všímajte si viac svoje okolie. Nebuďte ľahostajní ani k cudzím deťom.
- **Správajte sa Zodpovedne.sk!**

Reklama (Reklama, targeting, druhy online reklamy, adware)

ADWARE: advertising-supported software, je softvér, ktorý automaticky zobrazuje, prehráva alebo sťahuje reklamný materiál do počítača po svojej inštalácii alebo pri používaní tohto softvéru. Často ho používajú firmy, ktoré poskytujú služby typu zarábaj cez internet. Vtedy používateľ "prenajme" časť monitora, kde sa budú zobrazovať reklamné bannery.

BANNER: obrázková reklama, reklama na internete, má väčšinou formu obrázku (formát gif, png, či jpg), alebo je spracovaná v technológii FLASH. Je to teda pohyblivá forma reklamy umiestnená na internete.

ADVERTISING BREAKS: reklama zaradená v dobe medzi načítaním jednotlivých websites alebo stránok na webe.

Reklama

Reklamou je dnes zaplavený celý svet, od billboardov pri cestách, cez rádiá a televíziu, až po letákmi preplnené poštové schránky. Niekedy sa možno zdá, že bez reklamy by ľudia nevedeli, čo a kde majú kúpiť. Rozmach internetu si samozrejme vyžiadal aj umiestňovanie reklám priamo na webe.

Reklama môže byť niekedy aj celkom vkusným spestrením tej ktorej stránky, ale môže nás svojou vtieravosťou aj odrádzať. Je to však na druhej strane určitým prostriedkom na zaplatenie používania webových stránok. Ak by sme mali v súčasnosti platiť za každú informáciu, ktorú sme na internete našli, tak by sme to riadne pocítili na svojich úsporách. Reklamy to zaplatia za nás! Preto ich v podstate musíme akceptovať.

Od klasických reklám v televízii a rádiu sa líšia hlavne interaktivitou, kreativitou a targetingom. Interaktivita je veľmi výhodná pre ľudí, ktorých reklama zaujme. Ak by zahliadli reklamu na ten istý tovar v televízii, alebo by len začuli pár informácií o ňom v rádiu, nič by to nepovedalo o všetkých podrobnostiach a o cene produktu. Na internete sa jedným kliknutím dostaneme naopak ku všetkému, čo nás o danom tovare zaujíma. Na základe týchto informácií sa potenciálny zákazník rozhodne, či sa mu oplatí ísť si pozrieť objekt svojho záujmu priamo do predajne alebo by cestu tam meral zbytočne, lebo mu nevyhovuje „to a to“.

Grafická pestrosť internetovej reklamy býva často obohatená ešte o ďalšie prvky, ktoré sa nám nedostanú pri pozeraní televízie. Napríklad pri nadídení myškou na reklamu sa začnú meniť farby alebo sa vykoná nejaká akcia, zmena, pohyb a pod.

Targeting

Pod targetingom sa myslí zacielenie na určitú cieľovú skupinu užívateľov internetu. Rozlišujeme priamy, technický a multidimenzionálny targeting.

Pri priamom targetingu je reklama zobrazovaná užívateľom, ktorí si ju vyslovene žiadajú. Je im zasielaná viac-menej pravidelne a týka sa oblasti ich záujmu.

Pri technickom targetingu sa zobrazuje reklama napr. podľa typu operačného systému, verzie prehliadača, IP adresy, krajiny pôvodu užívateľa a pod. Znamená to, že napríklad na slovenských stránkach sa budú zobrazovať slovenské reklamy. Z užívateľovej IP adresy sa dá zistiť, z ktorého mesta alebo kraja pochádza, a tak sa mu bude zobrazovať reklama firiem, ktoré v tomto meste, resp. kraji, sídlia. Napríklad reklama košickej firmy nebude zobrazovaná u užívateľov v bratislavskom kraji.

Multidimenzionálny targeting umožňuje zobrazovať reklamu podľa tematiky webovej stránky. To znamená, že webová stránka zameraná na šport bude obsahovať reklamy na športové potreby. V prípade, že užívateľ zadá v niektorom prihlasovacom formulári vek alebo pohlavie budú sa mu zobrazovať reklamy, ktoré by mohli byť pre neho potenciálne zaujímavé. Napríklad ženám okolo 35 sa zobrazí reklama na prípravok na chudnutie, zatiaľ čo 18 ročnému hráčovi akčných hier reklama na novú hraciu konzolu.

Druhy online reklamy

BANNER - obrázková reklama, má väčšinou formu obrázku alebo je spracovaná v technológii flash.

Základné znaky bannerov:

- integrácia do webovej stránky
- pravouhlý formát
- možnosť interaktivity pre užívateľa

BUTTON - banner menších rozmerov.

ANIMOVANÝ BANNER - využíva gif animácie, reklama sa zobrazuje ako malý film, je to najčastejšie využívaný druh banneru, ale aj napriek tomu nie je možnosť interaktivity zmenená oproti statickému banneru.

HTML BANNER - oproti klasickému banneru obsahuje tento druh okrem grafiky aj rozličné príkazy HTML, ktoré umožňujú využitie interaktívnych prvkov ako pull-down menu, či políčka na výber, a tým pádom prichádza k podstatnému rozšíreniu možností odskoku na inú stránku, keďže užívateľ má na výber viac možností.

NANOSITE BANNER - mini web stránka, po kliknutí na banner sa nezobrazí nová stránka, ale ďalšia reklama na tom istom mieste. Využívajú ho firmy, ktoré nemajú vlastné webstránky.

RICH-MEDIA BANNER - „multimediálny banner", využíva doplnky a serverové rozšírenia ako audio, video, 3D a pod.

INTERSTITIALS - pred tým, ako sa užívateľovi načíta stránka, ktorej adresu si zvolil v prehliadači, uvidí na niekoľko sekúnd reklamnú stránku. Táto reklama má jednu vlastnosť úplne zhodnú s rádiom či televíziou, a síce, že sa jej užívateľ nemôže vyhnúť.

POP-UP - reklama sa nezobrazí priamo v prehliadači užívateľa, ale v novom vyskakujúcom okne, ktoré sa otvorí automaticky.

DIRECT EMAIL - možnosť priameho zacieleniau, reklama na vyžiadanie užívateľa.

NEWSLETTER - pravidelný emailový bulletin, zasielaný na vyžiadanie užívateľa.

COMET CURSOR - druh reklamy, ktorý dáva klasickej šípke nový vzhľad.

SUPERSTITIALS - efektívna a dynamická reklama, ktorá navonok pôsobí ako televízny spot. Vyrába sa vo formáte Flash 3, ktorý jej umožňuje animovaný vzhľad podobný filmu a využívanie zvuku.

Adware

Je softvér, ktorý automaticky zobrazuje, prehráva alebo sťahuje reklamný materiál do počítača po svojej inštalácii alebo pri používaní tohto softvéru. Často ho používajú firmy, ktoré poskytujú služby typu zarábaj cez internet. Vtedy používateľ "prenajme" časť monitora, kde sa budú zobrazovať reklamné bannery.

Prevencia

- **Chráňte sa pred adware**, ktorý sa vás snaží donútiť k návšteve komerčných serverov, najmä spojených s hazardnými hrami a pornografiou. Tieto stránky nemávajú dostatočné zabezpečenie, čo môže ohroziť váš počítač rôznymi typmi malware.
- **Používajte antivírusové, anti-spamové a anti-adware programy a pravidelne ich aktualizujte.**
- **Používajte internetový prehliadač alebo jeho plugin umožňujúci blokovanie reklamného materiálu.**
- **Správajte sa Zodpovedne.sk!**

Hry (Online hry, hazardné hry, hracie konzoly, java hry, tipovanie a stávkovanie, PEGI, PEGI online)

Online hry, hazardné hry, hracie konzoly, java hry, tipovanie a stávkovanie, PEGI, PEGI online

Môže počítačová hra ovplyvniť zdravý vývoj dieťaťa?

Či sa nám to páči alebo nie, socializáciu detí postupne preberá na svoje plecia elektronika v podobe médií akými sú televízia, rádio, internet, počítačové hry.

Človek je od prírody tvor hravý. Hra je sprievodným javom celej našej spoločnosti. Líši sa kultúrou, zvykmi, tradíciami. Jej podstata je však stále rovnaká. Dieťa sa pomocou hry pripravuje na svoje budúce pôsobenie (napodobňovanie), dospelému prináša relax, uvoľnenie, zábavu, pohodu. Preto je hra v každej svojej forme veľmi dôležitý nástroj socializácie jedinca. Hrou sa dieťa naučí omnoho viac ako mechanickým memorovaním. Počítačová hra poskytuje deťom vnemy takmer pre všetky zmysly. Má však počítačová hra okrem zábavy aj iný vplyv?

Psychologická obec sa v názore na televízne a počítačové násilie delí stále na dve časti. Jedna hovorí, že násilie v televízii a v počítačových hrách nemá vplyv na vývoj človeka a nemalo by sa obmedzovať, druhá skupina psychológov zase zastáva názor, že tento vplyv je veľmi silný a významný.

V mnohom nám môžu pomôcť výskumy, ktoré sa zaoberajú vplyvom televízneho násilia, a to nielen na detského diváka. Tieto prebiehajú už niekoľko rokov a nezvratne deklarujú nevhodnosť akčných a násilníckych scén vo filmoch, kde sa dôsledky častého sledovania takýchto filmov hlavne u detského diváka môžu prejaviť až o 10 a viac rokov. Toto zistenie je alarmujúce, lebo rozdiel medzi filmom a počítačovou hrou je značný. Pri filme sa dieťa stáva len pasívnym pozorovateľom deja, pričom pri počítačovej hre sa dieťa aktívne zapája do interaktívneho deja, tvorí a mení ho. Je vždy jej hlavným hrdinom.

Prieskum, ktorý som spracoval s názvom Počítačové hry ako rizikový faktor socializácie dieťaťa vo veku 10-15 rokov, mi poskytol informáciu, podľa ktorej až 40 % opýtaných respondentov (chlapcov) a takmer 28 % opýtaných dievčat hrá nevhodné počítačové hry. Ide hlavne o hry s agresívnym násilným nábojom, hry podporujúce nenávisť, rasizmus, intoleranciu, sexuálnu neviazanosť s obsahom proti ľudskosti či morálke.

Súčasťou tohto prieskumu bola aj snaha o zistenie hodnotového aspektu šiestich najhranejších počítačových hier, v ktorom z prosociálnych hodnôt, akými sú darovanie, útecha, pomoc, solidarita, odpustenie, trpezlivosť, ohľaduplnosť, asertivita a delenie si našla uplatnenie iba pomoc. Tá sa tu nechápe ako pomoc nezištná, ale skôr ako určitý spôsob kooperatívy medzi hráčmi, ktorí si navzájom pomáhajú pri zdolávaní prekážok alebo pri porážke nepriateľa. Je len samozrejmé, že v rámci

vytvárania hodnotového systému je prosociálne správanie veľmi dôležité. Počítačové hry, ktoré sme analyzovali, v sebe neukrývajú takmer žiadne z prosociálnych hodnôt.

Niekto môže namietať, že napr. rozprávky, na ktorých sme boli my skôr narodení vychovávaní a ktoré výrazne ovplyvnili našu socializáciu, obsahujú tiež prvky násilia. Avšak všetci tí, ktorí porovnávajú počítačové hry alebo akčné filmy s rozprávkami, si neuvedomujú, že útočné formy správania sú v rozprávkach spracované práve v prosociálnom kontexte. V rozprávkach a klasických dielach dobrodružnej literatúry je násilná smrť alebo krutý trest formou odplaty za spáchané zlo alebo násilie na nevinných, je teda súčasťou katarzie príbehu, vedie dieťa k poznaniu, že zlo je potrestané a pomáha mu premôcť strach. Zlo a jeho potrestanie je v rozprávkach symbolom predstavujúcim spravodlivosť – vždy víťazí dobro nad zlom.

Jeden z psychoterapeutických smerov hovorí, že si každý z nás utvára svoj vlastný svet. Každý podľa vlastných skúseností, a keď sú deti a mládež hojne vystavovaní vplyvu násilia v televízii, hrách či drastickým rozprávkam, tak je tým ich svet nejako ovplyvnený, takzvane si „nastavujú kontext“. Začnú to chápať ako určitú normu. A ak sa naučia napríklad vo svojom virtuálnom svete, teda napríklad v počítačovom svete, uvoľňovať svoju agresiu tým, že budú strieľať po ostatných, určitým spôsobom sa to podpíše aj na ich bežnej norme správania. Rizikové pre dieťa je aj to, že keď v počítačovej hre niekoho rozstrieľa a potom si hru pustí znova, postava „vstane z mŕtvych“ a akoby sa nič nestalo.

Na základe štúdia odbornej literatúry a zovšeobecnenia vlastných skúseností treba uvažovať o nasledovných negatívnych dôsledkoch pedagogicky neusmerneného hrania počítačových hier:

- ochudobňovanie reči a jej vulgarizácia (hlavne počítačové herne),
- neurotizmus,
- propagácia násilia,
- utváranie predsudkov,
- dočasná (úplná) strata záujmu o okolitý svet,
- dočasná (úplná) strata kontaktu s okolitým svetom,
- oslabenie vôľových schopností,
- oslabenie schopnosti empatie,
- rozvoj komplexu moci,
- strata objektívneho posudzovania reality,
- strata prosociálnosti.

Môže sa hranie počítačovej hry skončiť závislosťou?

Pri analýze počítačovej hry a jej využívaní v detskom veku je potrebné zobrať do úvahy aj riziko vzniku patologického hráčstva. Vedie k tomu poznanie vekových zvláštností detí pubescentného veku, prirodzená potreba hier v detskom veku, lákavosť hier a ich rafinované psychologické spracovanie, nedostatočné legislatívne a organizačné zabezpečenie ochrany detí v tejto oblasti. Ak sa tieto objektívne dané okolnosti spoja so zanedbávajúcou výchovou, nedostatkom úprimných vzťahov v rodine či nedostatkom času, ochoty alebo schopností výchovne sa zaoberať dieťaťom, vzniká riziko ohrozenia dieťaťa, ktoré v prvom štádiu môžeme nazvať ako zanietenosť pre hru. Dieťa sa tak pre emocionálnu a sociálnu izoláciu môže vzdialiť od plnenia prirodzených vývinových, socializačných úloh a rozvíjania morálnych a vôľových vlastností.

Počítačové hry pôsobia na nezrelú detskú psychiku oveľa viac ako na zrelú psychiku dospelého človeka. Detská psychika je viac zraniteľná a podlieha oveľa rýchlejšie rozvoju všetkých druhov závislostí.

Počítačová hra spĺňa všetkých šesť znakov závislostí, akými sú silná túžba alebo pocit popudu, ťažkosti so sebaovládaním, odvykací stav, rast tolerancie, postupné zanedbávanie iných potešení alebo záujmov a pokračovanie aj napriek jasnému dôkazu škodlivých následkov. Z vlastnej skúsenosti môžem tvrdiť, že pri počítačových hrách je len veľmi ťažké zistiť presný moment prechodu od „normálneho“ hrania cez zanietenosť hraním až po vznikajúcu „závislosť“ od hry. Z detstva si v podstate nespomínam na žiadnu klasickú hru, ktorá by ma natoľko zaujala, aby som nevenoval pozornosť iným činnostiam. Ten ohromný pocit akejsi sebarealizácie a sebauspokojenia, na ktorom treba v reálnom živote tvrdo pracovať, sa dá v počítačovej hre dosiahnuť za niekoľko minút. V každom prípade čas, ktorý dieťa venuje hraniu, treba obmedziť a určiť si jasné pravidlá. So zvyšovaním „časovej dávky“ sa zvyšuje aj potenciálna závislosť. Zaujímavý je fakt, že nelátkové závislosti, akými sú gamblovanie, závislosť od internetu, závislosť od esemesiek, ale aj počítačových hier, sú z hľadiska vzdelania alebo intelektových schopností postihnutých ľudí posunuté k tým vyšším hodnotám. Intelekt týchto ľudí je nadpriemerný, nejde o hlúposť, ale o túžbu navodiť si určitý stav. Postihnutý vlastne s hracím automatom alebo počítačovou hrou zvádza boj. On ho potrebuje poraziť, je tam určitá adrenalínová, kompetetívna, súťaživá zložka.

PEGI

Pre zaistenie ochrany detí mladších ako 18 rokov vyvinula organizácia Interactive Software Federation of Europe (Európska interaktívna softvérová federácia – ISFE), čo je obchodné zoskupenie, ku ktorému patrí väčšina firiem zaoberajúcich sa hrami, jednotný vekový klasifikačný systém, aplikovateľný v celej Európe, s názvom PEGI. Slúži na to, aby sa deti nestretli s hrami, ktoré nie sú pre ich vekovú kategóriu vhodné.

PEGI zlučuje dva rozdielne a predsa navzájom sa doplňujúce komponenty: po prvé je to veková klasifikácia 3+, 4+, 7+, 6+, 12+, 16+, 18+, po druhé jeden alebo viac popisovačov hry. Tieto ikony, zobrazené na zadnej strane balenia, naznačujú obsah predmetnej hry. V závislosti od typu hry môže byť zobrazených až sedem takýchto popisovačov. Rizikovosť daného obsahu hry je zosúladená s vekovou klasifikáciou hry. Kombinácia vekovej klasifikácie a popisovačov hry umožní rodičom a iným osobám kupujúcim hry pre deti, aby sa uistili, že sa vybraná hra hodí pre vek budúceho hráča.

V rámci systému PEGI existujú dva typy piktogramov pre označovanie hier podľa:

- obsahov
- vekovej kategórie


Hra obsahuje vulgarizmy


Hra obsahuje diskriminačné prvky. Obsahuje zobrazenia alebo materiály, ktoré môžu nabádať k diskriminácii.


Hra znázorňuje (obsahuje) užívanie drog


Hra môže pôsobiť na dieťa desivo až hrozivo


Hra znázorňuje nahotu alebo iné sexuálne správanie


Hra zobrazuje násilie


Hra, ktorá nabáda alebo vyučuje hazardné hry


Odporúčaný vek 3+ hra je vhodná od troch rokov úplne pre každého


Odporúčaný vek 4+ hra je vhodná od troch rokov úplne pre každého


Odporúčaný vek 6+ hra je vhodná od troch rokov úplne pre každého


Odporúčaný vek 7+ hra je vhodná od sedem rokov pre každého. Deti do sedem rokov sa môžu hrať pod dohľadom dospelého


Odporúčaný vek 12+ hra je vhodná od dvanásť rokov pre každého


Odporúčaný vek 16+ hra je vhodná od šestnásť rokov pre každého, väčšinou je treba rátať so zobrazením násilia, hrôzy, problematiky drog a pod.

 Odporúčaný vek 18+ hry len pre dospelých, ktoré by deti do šestnásť rokov rozhodne nemali hrať

(www.pegi.info)

PEGI online

PEGI online je nová edícia PEGI systému. Jej cieľom je zabezpečiť lepšiu ochranu mládeže pred nevyhovujúcimi PC hrami prevádzkovanými online a zároveň pomôcť rodičom, aby pochopili riziko a potenciálnu škodu, ktorú tieto hry môžu mať za následok.

PEGI online je založená na nasledujúcich princípoch:

- PEGI Online bezpečnostný kód a rámcový kontrakt, podpísaný všetkými zúčastnenými
- PEGI Online Logo, ktoré bude vyobrazené držiteľmi licencie
- web stránka uvádzajúca informácie pre žiadateľov, ale aj pre širokú verejnosť
- nezávislá administratíva, pomoc a riešenie konfliktov.

Licencia zobrazovať PEGI Online Logo je garantovaná PEGI Online administrátorom akémukoľvek správcovi online hier, ktorý spĺňa všetky požiadavky a odporúčania ukotvené v PEGI Online bezpečnostnom kóde(POSC). Tieto odporúčania zároveň zahŕňajú aj povinnosť udržiavať web stránku bez akéhokoľvek nelegálneho a útočného obsahu, neželaného internetového odkazu, ako aj povinnosť zabezpečiť opatrenia na ochranu mládeže a ich súkromia, do ktorého hranie online hier zasahuje.

PEGI Online Logo sa bude objavovať na obale hry, ak je predávaná vo forme CD či DVD, alebo je umiestnená priamo na internetovej stránke. Logo ukáže, či hra môže alebo nemôže byť hraná online, a taktiež či daná hra, alebo stránka je pod kontrolou operátora, ktorý má za úlohu ochranu mládeže.

Hry, ktoré nie sú hrané online, ale na konzolách alebo PC, budú naďalej hodnotené súčasným PEGI systémom, alebo iným, už existujúcim európsky uznaným hodnotiacim systémom.

Systém PEGI je však dobrovoľný a pokiaľ krajina nemá vhodnú legislatívu, ktorá by riešila ochranu detí pred nevhodným obsahom počítačových hier, javí sa tento systém ako nedokonalý, resp. len informatívny, postavený čisto na dobrovoľnosti a ochote vydavateľa a tiež predajcu informovať kupujúceho o obsahu hry.

Slovenská legislatíva sa tejto problematike venuje vo vyhláške Ministerstva kultúry Slovenskej republiky č. 589/2007 Z. z. s účinnosťou od 1. januára 2008.

Zelené piktogramy označujú vhodnosť a červené naopak nevhodnosť obsahu. Okrem krúžkov s číslom vekovej hranice - 7, 12, 15 a 18 rokov, sem patrí aj tvár zeleného macka - znak vhodnosti pre deti do 12 rokov a zelené "u" - označujúce prístupnosť pre všetkých maloletých. Výnimku tvoria zvukové

nosiče, ktoré budú informovať len o nevhodnom obsahu pre deti a mládež. Označenie o nevhodnosti dostanú napríklad nahrávky, ktoré obsahujú vulgárne slová, či texty zľahčujúce závislosť, násilie či neznášanlivosť.

Audiovizuálne diela, multimediálne diela a programy alebo iné zložky televíznej programovej služby sa klasifikujú ako nevhodné a neprístupné pre vekovú skupinu maloletých do 18 rokov, ak obsahujú:

- zobrazenie násilia, najmä zobrazenie krutého ubližovania alebo násilnej smrti človeka, obzvlášť bez pocitov ľútosti, zobrazenie fyzicky týraných osôb alebo psychicky týraných osôb, zobrazenie prejavov skupín s patologickými normami správania, prezentáciu nebezpečných situácií alebo zámerne vytváraného rizika ako atraktívnej formy zábavy,
- slovnú agresivitu, vulgárny jazyk, obscénne vyjadrovanie alebo obscénne gestá,
- zobrazenie prejavov neznášanlivosti alebo nenávisti, xenofóbie, rasizmu, náboženskej diskriminácie a neznášanlivosti, násilia voči etnickým alebo iným menšinám, zobrazenie šikanovania,
- zobrazenie alebo prezentovanie závislosti, akou je alkoholizmus, fajčenie, drogová alebo hráčska závislosť formou zábavy, zobrazenie používania zbrane ako útočného prostriedku alebo promiskuitného sexuálneho správania formou zábavy,
- zobrazenie erotických pomôcok alebo erotických scén, ktoré sú vyrobené výlučne na prezentáciu erotiky a erotických tém,
- sexuálne scény alebo sexuálne správanie, ktoré sú prezentované ako forma zábavy, scény spojené s prejavmi sexuálneho násilia alebo sexuálnymi deviáciami, alebo
- zobrazenie zámerne vyvolávajúce pocity strachu alebo úzkosti v žánri horor.

Audiovizuálne diela, multimediálne diela a programy alebo iné zložky televíznej programovej služby sa klasifikujú ako nevhodné pre vekovú skupinu maloletých do 15 rokov, ak obsahujú:

- zobrazenie fyzickej agresivity a s ňou súvisiace násilné akty končiace sa smrťou alebo vážnymi následkami, detaily následkov násilných činov,
- b) týranie zvierat,
- c) sexuálne scény, ktoré sú súčasťou dejovej línie,
- zobrazenie alebo prezentovanie formy závislosti, akou je alkoholizmus, fajčenie, drogová alebo hráčska závislosť alebo používanie zbrane ako útočného prostriedku, v ktorom sa formou spracovania niektorá forma závislosti alebo používanie zbrane ako útočného prostriedku schvaľuje, zľahčuje alebo sa vyzdvihuje do popredia, alebo
- zobrazenie správania s vysokým rizikom ublíženia na zdraví, pričom toto riziko sa prezentuje ako atraktívne alebo zábavné a správanie je prezentované bez upozornenia na nebezpečenstvo a možné následky tohto správania.

Audiovizuálne diela, multimediálne diela a programy alebo iné zložky televíznej programovej služby sa

klasifikujú ako nevhodné pre vekovú skupinu maloletých do 12 rokov, ak obsahujú:

- zobrazenie spôsobujúce pocity strachu a depresie,
- zobrazenie vytvárajúce predstavu málo bezpečného a neistého prostredia alebo zobrazujúce bezmocnosť dospelých voči vonkajšiemu svetu a silám, ktoré ohrozujú rodinné prostredie, alebo zobrazenie iným spôsobom nevhodné vo vzťahu k emočnej a sociálnej zrelosti maloletých, ak prezentujú ohrozenie rodiny alebo rodičovských vzťahov a vzhľadom na vek maloletých je predpoklad neadekvátnej interpretácie zobrazeného obsahu,

- zobrazenie reálneho násilia, najmä zobrazenie následkov na obetiach násilných trestných činov vrátane zobrazenia následkov na obetiach v dôsledku živelných pohrôm, dopravných alebo leteckých nešťastí, najmä obrazy zranení, krvi, telesných znetvorení a utrpenia,
- zobrazenie negatívnych skúseností detí a následkov násilia alebo nešťastia na deťoch, zobrazenie ranených alebo umierajúcich detí a detí ako obetí alebo ako svedkov kriminálnych činov, ktoré by ako zrkadlový obraz mohli vyvolať u detí efekt obete reálneho sveta,
- zobrazenie náhlych a neočakávaných zmien živých bytostí, zobrazenie neprirodzenej premeny organizmov alebo zobrazenie paranormálnych alebo iných mimovnemových javov v kontexte sci-fi,
- zobrazenie nahoty, ktoré nie je bežné v rodinnom prostredí a na verejnosti a ktoré by mohlo vyprovokovať záujem o sexuálne vzťahy a predčasné prebudenie sexuálnych pudov maloletých detí, alebo
- zobrazenie konania v situáciách, v ktorých je možnosť ublíženia na zdraví nedostatočne zreteľná, zobrazenie rizikových športových disciplín alebo fantazijných predstáv o nadľudských hrdinských výkonoch človeka mimo reálneho sveta, ktorých neadekvátna interpretácia vzhľadom na vek môže vyvolať u maloletých efekt napodobňovania.

Audiovizuálne diela, multimediálne diela a programy alebo iné zložky televíznej programovej služby sa

klasifikujú ako nevhodné pre vekovú skupinu maloletých do 7 rokov, ak obsahujú:

- agresívne útočiace zvieratá vyvolávajúce strach, napríklad agresívne útočiaci netopier, had alebo pavúk,
- zobrazenie prostredia v tmavých a pochmúrnych farbách alebo scény s príliš hlučnou hudbou alebo náhlymi zvukovými zmenami,
- vynútené násilie voči bezmocným, najmä voči deťom alebo zvieratám, alebo
- zobrazenie ohrozenia rodičovských vzťahov alebo rodiny.

Grafický symbol číslo	Klasifikácia podľa jednotného systému označovania	Grafický symbol jednotného systému označovania	Rozmery grafického symbolu
1.	nevhodné pre vekovú skupinu maloletých do 7 rokov		televízna programová služba: 41 x 41 pixlov obal, nosič: 1 cm x 1 cm
2.	nevhodné pre vekovú skupinu maloletých do 12 rokov		televízna programová služba: 41 x 41 pixlov obal, nosič: 1 cm x 1 cm
3.	nevhodné pre vekovú skupinu maloletých do 15 rokov		televízna programová služba: 41 x 41 pixlov obal, nosič: 1 cm x 1 cm
4.	nevhodné a neprístupné pre vekovú skupinu maloletých do 18 rokov		televízna programová služba: 41 x 41 pixlov obal, nosič: 1 cm x 1 cm
5.	vhodné pre vekovú skupinu maloletých do 12 rokov		televízna programová služba: 41 x 41 pixlov obal, nosič: 1 cm x 1 cm
6.	vhodné pre všetky vekové skupiny maloletých		televízna programová služba: 41 x 41 pixlov obal, nosič: 1 cm x 1 cm
7.	výchovno-vzdelávacie vhodné pre vekovú skupinu maloletých do 7 rokov		televízna programová služba: 41 x 41 pixlov obal, nosič: 1 cm x 1 cm
8.	výchovno-vzdelávacie vhodné pre vekovú skupinu maloletých od 7 rokov		televízna programová služba: 41 x 41 pixlov obal, nosič: 1 cm x 1 cm
9.	výchovno-vzdelávacie vhodné pre vekovú skupinu maloletých od 12 rokov		televízna programová služba: 41 x 41 pixlov obal, nosič: 1 cm x 1 cm
10.	výchovno-vzdelávacie vhodné pre vekovú skupinu maloletých od 15 rokov		televízna programová služba: 41 x 41 pixlov obal, nosič: 1 cm x 1 cm

Ale zákon nie je všetko. Ústrednú úlohu tu hrá stále rodina. Hru si totiž môže každé šikovnejšie dieťa stiahnuť z internetu alebo nahrať od kamaráta. Preto tu má práve výchovný vplyv rodiny nezastupiteľné miesto. Je vhodné, aby rodič neumiestňoval počítač do detskej izby alebo na miesto, kde nie je možná kontrola dieťaťa.

Tiež je vhodné vedieť, násilnícku počítačovú hru dieťaťu zakázať. Dieťa sa možno pôjde hrať ku kamarátovi, ale už bude mať vedomie o určitých hodnotách, ktoré sú vlastné jeho rodičom. Aj keď poruší rodičovský zákaz, vedomie, že takúto hru rodičia odmietajú, je krajne dôležité pre jeho výchovu a vzdelanie.

V neposlednom rade je dôležité, aby sa rodič nesnažil vyhnúť svojim povinnostiam voči dieťaťu práve kúpou počítača alebo počítačovej hry, po ktorej dieťa túži, len aby bol „pokoj“. Tým rodina stráca

svoju primárnu úlohu. „Ak sa dieťa pýta matke na ruky a ona mu namiesto toho dá čokoládu, v jeho mozgu sa vytvorí spojenie na celý život, že čokoláda je náhrada za telesný a citový kontakt s blízkym človekom, za lásku.“

Prepadnutie počítačovej hre má na svedomí vlastne súhrn istých nedostatkov či zlyhaní, a to tak na úrovni rodiny, ako aj v osobnom živote. Je to istá neschopnosť rodiny ponúknuť dieťaťu alternatívu za počítač a počítačovú hru.

Počítačové hry sú všade okolo nás. To nie je len osobný počítač. Sú to hracie konzoly (Gameboy, GameBoy Advance, GameBoy Color, GameCube, GameGear, Handheld, Mega Drive, NDS, N-GAGE, Nintendo, Nintendo 64, Playstation1, 2, 3, PSP, PSOne, Sega Dreamcast, Xbox, Xbox360), ale aj mobilné telefóny. Hrajú sa mladí aj starí, cestou do práce, doma, na dovolenke, v škole...

Ale počítačové hry, samozrejme, nie sú len o bezduchom virtuálnom krviprelievaní. Na pultoch predajcov sa objavujú aj hry, ktoré naozaj rozširujú rozhľad, upevňujú logické myslenie, cvičia postreh, zlepšujú priestorovú orientáciu, modelujú situácie , do ktorých by sa dieťa nemohlo v reálnom živote dostať. Ide o rôzne ekonomické simulátory, kde hráč stavia vlastné mesto alebo zoologickú záhradu či lunapark, stará sa o „svojich“ obyvateľov, prípadne sa sám podieľa na chode rodiny. Tiež sa sem radia rôzne logické hry či typické detské „plošinovky“ (skákačky, behačky...).

Nadmerné trávenie voľného času pri počítačovej hre ostáva však aj tu pálčivým problémom. Dieťaťu do života dá isto viac svedomitá príprava do školy ako dlhé vysedávanie pred monitorom. Je to podobné, ako keby dieťaťa hralo 3 hodiny denne napr. sedmové karty, ktorých hra tiež rozvíja logické myslenie... Asi by ho to však ďaleko neposunulo.

Na to, aby sme zistili, ako hra vplýva na hráča a aký má výchovný vplyv, si ju treba hlavne zahrať. Pozerať sa nestačí. Výrobcovia počítačových hier, počítačov a virtuálnej zábavy sa čoraz viac snažia zdokonaliť hry tak, aby poskytli čo najlepšiu ilúziu. Ilúziu, ktorá sa dnes ponúka na každom kroku a ktorú ľudia tak veľmi potrebujú pre život. Svedčia o tom takmer všetky tuctové relácie tak na štátnych, ako aj komerčných televíznych kanáloch. Za čias starovekého Ríma ľudia potrebovali pre život „chlieb a hry“. Dovolím si tento výrok upraviť na dnešnú realitu. Ľudia totiž potrebujú pre životu „chlieb a ilúzie...“ A tie počítačové sú čoraz dokonalejšie.

Prevencia

- **Vyberajte len hry, ktoré sú označené popisovačmi a zodpovedajú vekovo a obsahovo deťom.** Najmenšie deti by nemali hrávať hry, v ktorých sa strieľa na živé tvory.
- **Oboznámte deti o škodlivosti hrania násilníckych alebo inak nevhodných počítačových hier.**
- **Majte prehľad o nainštalovaných hrách.**
- **Ak si chce vaše dieťa kúpiť hru, tak iba vo vašom sprievode, prípadne v sprievode inej zodpovednej dospelej osoby.**

- **Otvorene zakážte hranie nevhodných počítačových hier** (v dieťati sa vytvorí vedomie o určitých hodnotách, ktoré sú vlastne jeho rodičom).
- **Váš domáci počítač (alebo hraciu konzolu) postavte do obývacej izby alebo na iné spoločné prístupové miesto v byte.** Najlepšie tak, aby rodič mal vždy výhľad na monitor**.** Nedávajte počítač do detských izieb. Majte dobrý prehľad o všetkých ďalších počítačoch, ktoré sú deťom prístupné.
- **Stanovte medzi deťmi a rodičmi jasné pravidlá pre používanie internetu.** Urobte si rozvrh na dni a presný čas, kedy má dieťa povolenie stráviť čas na internete, najlepšie v čase vašej prítomnosti. Podpísanú zmluvu vystavte niekde pri monitore počítača. Nezabudnite, ak si s vaším dieťaťom vytvoríte pravidlá o používaní internetu, stanovte si práva a povinnosti pre obe strany. Pravidla, by sa mali pravidelne aktualizovať. Vzor takejto „rodinnej zmluvy" nájdete na stránkach Zodpovedne.sk
- **Vytvorte medzi dieťaťom a rodičom vzťah vzájomnej dôvery.** Majte prehľad o prezývkach (nickname) vašich detí, ktoré používajú na internete. Buďte opatrný, nebuďte dotieravý pri kontrole dieťaťa, vzájomná dôvera je veľmi dôležitá. Prílišná kontrola by mohla dieťa dohnať ku skrývaniu a zatajovaniu činností. Netrestajte dieťa za to, čo nie je jeho chyba, môže vám prestať dôverovať a mať strach a neistotu pri zdôverovaní sa s nejakým problémom. Je potrebné sa s deťmi veľa rozprávať, upozorniť ich na rôzne nebezpečenstvá, zaujímať sa a vedieť kde a ako trávia voľný čas, s kým telefonujú, emailujú, četujú, s kým sa stretávajú. Menšie deti si vyžadujú pravidelnú kontrolu. Ponúknite deťom adekvátne, zmysluplné a zaujímavé mimoškolské aktivity. Všímajte si viac svoje okolie. Nebuďte ľahostajní ani k cudzím deťom.
- **Vytvorte svojpomocné rodičovské spolky či združenia** (aj elektronických) za účelom odovzdávania si potrebných informácii, skúsenosti...
- **Správajte sa Zodpovedne.sk!**

Sťahovanie z internetu (Download, porušenie autorských práv, softvérové pirátstvo, voľne dostupné materiály, riziká sťahovania z internetu)

Download

DOWLOAD: *„sťahovanie“* – doslova nahrať dole. Ide o prenos dát z internetu smerom k užívateľovi. Opak upload.

Porušovanie autorských práv

Porušovanie práv duševného vlastníctva v jeho rôznych formách je dnes určite jedným z dominantných foriem porušovania práva v oblasti informačných technológií, a to v celosvetovom meradle.

Podľa súčasne platnej legislatívy Slovenskej republiky (Autorský zákon, 618/2003 Z.z., a §283 Trestného zákona) je porušovanie autorského práva považované za trestný čin s vážnymi dôsledkami – možnosť odňatia slobody do 5 rokov, vysoké pokuty alebo prepadnutie majetku.

Pritom je nutné mať na zreteli, že porušovateľovi autorského práva môže byť v občianskom procese určená aj náhrada škody spôsobenej nelegálnym používaním alebo šírením diela.

Z pohľadu informačných technológií sú dnes za autorské diela považované:

- počítačové programy,
- databázy,
- zdrojové kódy počítačových programov,
- podkladové materiály pre tvorbu programu,
- multimediálne diela,
- literárne diela v digitalizovanej forme,
- hudobné diela v digitalizovanej forme,
- filmové diela v digitalizovanej forme.

Najčastejšími formami porušovania autorských práv v oblasti informačných technológií sú určite nasledovné:

- používanie programov v rozpore s licenčnou zmluvou,
- používanie programov bez platnej licencie (nezakúpené softvérové produkty),
- používanie programov formou tzv. nadužívania licencií – používajú sa inštalácie programov na väčšom počte počítačov než pre aký bola zakúpená platná licencia,
- používanie programov v rozpore s licenciou napr. prevádzkovanie softvéru v internetových kaviarňach bez platnej licencie na verejné prevádzkovanie,

- neoprávnené šírenie počítačových programov a iných autorských diel (multimediálne diela, literárne diela, a pod.),
- duplikovanie médií obsahujúcich produkty podliehajúce autorským právam,
- prevádzkovanie internetových stránok ponúkajúcich stiahnutie nelegálnych kópií licenčného softvéru či iných diel,
- prevádzkovanie a využívanie peer-to-peer sietí umožňujúcich neautorizovaný prenos programov či iných produktov požívajúcich autorsko-právnu ochranu,
- osobitnou kategóriou je tzv. hard disk loading - predaj počítačov s predinštalovaným programovým vybavením, kedy predajca v snahe získať alebo zvýhodniť zákazníka poskytne spolu s predávaným hardvérom aj nelegálne kópie operačného systému, či aplikačných programov,
- plagiátorstvo - tvorba a šírenie počítačových programov, ktoré parazitujú na dobrom mene už zabehnutých produktov kopírovaním ich dizajnu, mena alebo funkcionality. V tom to prípade však nemusí ísť len o porušovanie autorských práv, podobné kauzy často zasahujú do oblasti porušovania priemyselného vlastníctva.

Softvérové pirátstvo

Aké sú dôvody, že softvérové pirátstvo je tak rozšíreným a to v celosvetovom meradle? Aspoň niekoľko základných dôvodov:

- nízka úroveň všeobecno-právneho povedomia,
- vysoké náklady na obstaranie legálnej licencie,
- ľahká replikovateľnosť spôsobená základnými vlastnosťami softvéru (SW),
- kópia je vytvoriteľná v rovnakej kvalite ako originál,
- vytvorením kópie nedochádza k obmedzeniu strany vlastniacej originál,
- existencia nekontrolovateľného komunikačného kanálu umožňujúceho získanie pirátskeho SW,
- zneužívanie fenoménu SW pirátstva ako prostriedku konkurenčného boja medzi predajcami výpočtovej techniky – „zabudnuté“ inštalácie SW na disku predávaného počítača ako výhoda pri nákupe nového počítača u konkurenčného predajcu,
- zložitá kontrolovateľnosť vytvára priestor pre rôzne „podnikateľské“ aktivity súvisiace s nelegálnym rozmnožovaním a predajom SW,
- možno až prehnane dynamický vývoj nových verzií vyžadujúci pomerne časté a nákladné investície,
- dynamický vývoj prináša so sebou aj ďalší sekundárny jav – chybovosť, ktorá je síce online u väčšiny vývojárskych spoločností odstraňovaná, ale u používateľa vyvoláva efekt znechutenia a odmietavého stanoviska k vynakladaniu prostriedkov na legálnu aktualizáciu,
- reálny stav ekonomík – najmä v krajinách bývalého socialistického bloku väčšina používateľov (ziskové i neziskové organizácie, štátna správa, školstvo, ...) rieši často existenčné, či prevádzkové otázky, pri ktorých otázka riešenia licenčnej politiky má nižšiu prioritu.

Voľne dostupné materiály

Na internete sa nachádza množstvo voľne dostupného materiálu, na ktorý sa nevzťahujú autorské práva. Medzi takéto patrí:

- študijný materiál, ktorý zverejní samotný autor na svojej www stránke alebo ich pridá do zoznamu materiálov na stránky typu www.referaty.sk, www.tahaky-referaty.sk, a pod.,
- informácie zverejnené na voľne dostupných online encyklopédiách, napr. http://wikipedia.org/,
- trial verzie programov – verzie komerčných programov, ktorých použitie je obmedzené časom alebo počtom spustení,
- demo verzie programov – verzie komerčných programov, ktorých použitie nie je časovo obmedzené, ale nefungujú všetky ich aplikácie, najčastejšie nefunguje ukladanie zmien,
- beta verzie – skúšobné verzie komerčných programov oslobodené od licencie, za účelom ich testovania a vychytávania chýb pred samotným spustením plných verzií programov, ktoré už obsahujú licenciu,
- shareware – nekomerčný plnohodnotný program, ktorý je zadarmo použiteľný určitú dobu, alebo určitý počet spustení, potom je potrebné zakúpiť si licenciu, lebo po uplynutí stanoveného času prestáva program fungovať,
- freeware – „slobodný softvér“, ktorého “sloboda“ sa určuje na viacerých úrovniach:
    - je použiteľný na rôzne účely,
    - je voľne šíriteľný, ale nie za poplatok,
    - so súhlasom autora môže byť aj upravovateľný ,
    - po vylepšení je možné poskytnúť ho širokej verejnosti, pričom autorské práva musia byť zachované.

  Rôzne freeware programy môžu byť obmedzené v niektorej z týchto úrovní.
- open source – „voľný zdroj“, vo všeobecnosti akákoľvek informácia alebo zdrojový kód programov voľne a bezplatne dostupný verejnosti. Programy, ktoré sú open source, je možné upravovať podľa vlastných predstáv, šíriť ďalej, či dokonca predávať. Takéto programy sú buď bez autorských práv, čiže *public domain*, alebo majú tzv. *GPL* licenciu, kde je meno pôvodného autora stále uvedené.

Riziká sťahovania z internetu

Za predpokladu, že sa neangažujete v počítačovom pirátstve, plagiátorstve, či nezneužívate bezplatne licencované softvérové produkty, vám nehrozí žiadny právny postih. Je však dôležité upozorniť, že zapájanie sa do rôznych peer-to-peer sietí(využívanie programov pomocou ktorých je možné sťahovať z internetu rôzne programy a multimediálne diela) je z pohľadu ochrany autorského práva problematické, nakoľko pri sťahovaní rôznych autorských produktov (SW, hudba, filmové diela, atď.) zároveň umožňujete, aby z Vášho počítača iní účastníci p2p siete sťahovali produkty, ktoré môžu podliehať autorskoprávnej ochrane, alebo ich obsah môže byť protizákonný (napr. detská pornografia, materiály propagujúce rasizmus, xenofóbiu, fašizmus a iné). Pritom o skutočnom obsahu sťahovaných (ďalej takýmto spôsobom šírených) nemusíte mať na základe názvu týchto produktov vôbec vedomosť.

Ak radi využívate voľne dostupné programy, či multimediálne diela ponúkané na rôznych stránkach, majte na zreteli riziko ohrozenia vášho počítača a zneužitia vašich osobných údajov. Väčšina takýchto stránok nemá dostatočné zabezpečenie, a tak sa vám môže stať, že s obľúbenou pesničkou si stiahnete zároveň aj nejaký vírus, červa, a pod. Tieto infiltrácie môžu narobiť riadnu škodu samotnému počítaču. Môžu vám pozmeniť niektoré dokumenty, alebo ich vymazať a v horšom prípade môže dôjsť k naformátovaniu harddisku. Iné ohrozenie plynie zo zneužitia vašich osobných údajov, hesiel, emailovej adresy a pod. A to hlavne v prípade trójskeho koňa a keylogera, či tzv. spyware.

Niektoré stránky ponúkajú možnosť sťahovania až po predchádzajúcom zaregistrovaní sa. Vtedy je potrebné skontrolovať, ktoré údaje si od vás formulár vypýta. Často sa stáva, že musíte spolu s registráciou súhlasiť napr. so zasielaním reklám, lebo v podstate tie stránky z reklamy žijú. Reklamy vám potom budú zahlcovať vašu mailovú schránku, preto do formulárov uvádzajte radšej jednu

mailovú adresu, ktorá bude slúžiť na „neosobnú“ poštu, a druhú mailovú adresu si strážte pre komunikáciu s priateľmi, či zamestnávateľom.

Inou možnosťou je sťahovanie z lokálnych sietí v prípade zdieľaných súborov. Vtedy je potrebné dbať na správne sieťové nastavenia vo vašom počítači.

Prevencia

- **Nezneužívajte produkty chránené autorskými právami**.
- **Nastavte si správne sieťové parametre vo vašom počítači**.
- **Zabezpečte si pripojenie do vašej siete heslom.**
- **Chráňte svoj počítač aktuálnym antivírusovým systémom**. Aby bola ochrana účinná, antivírusové systémy sa aktualizujú i niekoľkokrát za deň.
- **Chráňte svoj počítač proti špionážnym programom**. Tieto programy sa aktualizujú rovnako ako antivírusové systémy.
- **Zvážte, ktoré priečinky budete zdieľať v sieti**. Nastavte na všetky zdieľané priečinky príslušné oprávnenia a chráňte k nim prístup heslom.
- Nezverejňujte svoju emailovú adresu na rôznych fórach, inzertných a kontaktných stránkach a pod. V prípade, že sa tomu nedá vyhnúť, **zriaďte si ďalšiu emailovú adresu, ktorú budete publikovať**.
- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- **Správajte sa Zodpovedne.sk!**

Zoznamky (Zoznamky cez internet, vydávanie sa za niekoho iného, stretnutie s neznámou osobou, ochrana osobných údajov)

Zoznamky cez internet

Dnes existuje množstvo zoznamovacích portálov, ktoré umožňujú nadviazať priateľstvá, či partnerské zväzky širokej skupine ľudí. Možnosť zoznámenia cez internet využijú hlavne plachí ľudia s nízkym sebavedomím, handicapovaní, osamelí, ale aj starší ľudia, ktorým vyhovuje hlavne anonymita na sieti. Rovnako však zoznamky využívajú aj mladí a atraktívni ľudia, ktorí si napríklad chcú skrátiť čas a využívajú zoznamky ako druh zábavy. Online zoznamovanie je v podstate modernejšou obdobou zoznamovacích inzerátov. Oproti nim má tú výhodu, že je rýchlejšie, pohodlnejšie a pestrejšie. Najčastejšie uvádzané dôvody na online zoznámenia sú: veľa práce a málo času. Ale čakanie na odpoveď si môžete skrátiť listovaním v profiloch iných inzerentov. Za jeden deň môžete osloviť toľkých ľudí, koľko sa vám páči a pritom sa vyhnúť odmietnutiu z očí do očí. Ak použijete filter, je veľká pravdepodobnosť, že nájdete skupinu ľudí, ktorá bude najviac vyhovovať vašim požiadavkám. Zo začiatku to bude možno len na komunikovanie a neskôr možno...

Vydávanie sa za niekoho iného

Predovšetkým treba zvážiť, čo o sebe chcete uverejniť a rovnako brať do úvahy, čo o sebe uverejnia ostatní. Anonymita internetu má svoje čaro, ktoré umožňuje schovať nedostatky, ale na druhej strane má aj svoje tienisté stránky. Sú ľudia, ktorí hneď na začiatku vsadia na svoju úprimnosť, ale aj takí, ktorí sa radšej zamaskujú, či už z opatrnosti alebo pre zábavu. Niekto hľadá vážny vzťah, iný si chce len písať, ďalší len tak zabaviť sa, niektorí vás vyzlečú cez monitor, ak sa dáte... Ak niekomu nevidíte do tváre, neviete, či práve neklame. Na internete je ľahké „vodiť niekoho za nos“ a vydávať sa za niekoho iného. Preto sa odporúča brať internetové zoznamovanie trochu ako hru. Určite je vhodnejšie odpovedať na inzeráty s fotkami. Aj keď podľa fotiek je ťažké urobiť si celkový dojem o človeku, ale ak vám aspoň trocha záleží na prvom dojme, iste je to pomoc.

Stretnutie s neznámou osobou

Ak sa zoznamujete s odstupom a nadhľadom, je to len výhoda. Nemali by ste si písať s ľuďmi, ktorí majú pochybne vyplnený profil. Ak sa chcete spoznať aj osobne, vyberte si radšej ľudí zo svojho okolia a necestujte na stretnutie do neznámych miest. V známom a hlavne verejnom prostredí sa človek cíti bezpečnejšie. Na prvé stretnutie nikdy nechoďte sami. Dajte si jasné poznávacie znamenie. Pokiaľ vás dotyčný na prvý pohľad odradí alebo vyľaká, môžete jednoducho odísť. Napriek všetkým nástrahám môže mať zoznámenie cez internet aj šťastný koniec, ale je potrebné k takémuto nadviazaniu vzťahu pristupovať opatrne.

Ochrana osobných údajov

Kvalitní poskytovatelia zoznamovacích portálov si sú vedomí, že existujú reálne možné ohrozenia, či sa už jedná o porušovanie právnej legislatívy, ochrany súkromia a autorských práv alebo zneužitia osobných údajov svojich užívateľov. Z týchto dôvodov majú poskytovatelia vypracované práva a povinnosti poskytovateľa služieb, ale aj práva a povinnosti užívateľov, s ktorými je treba pri registrácii súhlasiť, ináč nebudú služby poskytované.

Chráňte si vaše osobné údaje, fyzickú aj emailovú adresu, telefónne čísla, heslá, pin, čísla účtov a pod., lebo okrem sklamania v láske, či priateľstve, sa môžete stať aj obeťou najrôznejších trestných činov prevádzaných pomocou internetu. Môže ísť jednak šírenie rôznych počítačových infiltrácií (vírusy, červy, spam, nechcená reklama a pod.), ale aj o „vyčistenie" vašich účtov.

Tiež je dôležité si uvedomiť reálne nebezpečenstvo od ľudí, ktorí sa vás na zoznamke pýtajú na veľmi citlivé záležitosti z vášho osobného života. Uvedomte si, že ak vás vyzve na stretnutie neznámy človek, ktorý o vás vie, že ste opustený, nemáte žiadnych priateľov, či blízku rodinu alebo, že ste sa len pred časom prisťahovali, a ani to tu dobre nepoznáte, môže ísť o človeka, ktorý si hľadá svoju obeť! Zvlášť nebezpečné je, ak sa cez internet zoznamujú deti, ľahko sa môžu stať obeťou pedofilov!

Prevencia

- **Vyberte si kvalitného poskytovateľa služieb**, ktorý zabezpečí nielen ochranu osobných údajov, ale aj ochranu proti nevyžiadanej pošte, antivírusovú ochranu, atď.
- **Zabezpečte si svoje fotoalbumy heslom.** Nikdy neviete ako a kedy môžu byť vaše fotografie zneužité treťou stranou.
- **Nie je bezpečné dávať na internet alebo cez mobil svoje osobné údaje.** Vysvetlite deťom, čo sú to osobné údaje a prečo je nebezpečné zverejňovať svoje pravé meno a priezvisko, svoju fotografiu, video, vek, emailovú adresu, telefónne číslo, adresu domov, adresu školy, majetkové pomery, prístupové mená a heslá alebo iné osobné údaje (záľuby, opis vzhľadu, povahy, znalosti, zručnosti, vzdelanie, obľúbené veci, túžby...). V prípade, že je nevyhnutné takéto údaje poskytnúť, musia o tom vedieť rodičia alebo v škole učitelia.
- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- **S nikým, s kým sa dieťa zoznámilo iba cez internet alebo mobil, sa nesmie stretávať samé osobne.** Tak ako v reálnom živote nechodia deti na stretnutie s neznámou osobou bez sprievodu niekoho ďalšieho, najlepšie rodiča, alebo aspoň súrodenca, kamaráta, tak aj na stretnutie s neznámou osobou, s ktorou sa dieťa zoznámilo iba cez internet alebo mobil, je stretnutie veľmi nebezpečné. Ak už dieťa ide na stretnutie, tak vždy aspoň s kamarátom. Rodičom oznámiť na aké stretnutie ide, za kým ide, kde a kedy sa plánuje vrátiť. Stretnutie by malo byť na verejnom mieste, kde je veľa ľudí. Znakom bezpečnejšieho stretnutia je, že tomu, čo pozýva, nevadí, že dieťa príde s rodičom alebo inou dospelou osobou. Ak mu to vadí, ten človek nemá čisté úmysly.
- **Buďte podozrievavý voči človeku, ktorý dieťa presviedča, aby zatajovalo svoje internetové kamarátstvo pred rodičmi, alebo vystupuje ako tínedžer, ale nevie väčšinu odpovedí na otázky, ktoré bežne rovesníci poznajú.** Takýto človek chce deťom ublížiť a preto klame a navádza, aby zatajili pozvanie na stretnutie s ním, aby si zmazali históriu četu, jeho emaily, sms-mms správy a podobne.
- **Nie všetko, čo je na internete, je pravda.** Vysvetlite deťom, nech neveria všetkému čo nájdu na internete. Informácie si je potrebné porovnať z viacerých zdrojov a v prípade nejasností sa poradiť s rodičmi alebo učiteľmi v škole.
- **Váš domáci počítač (alebo hraciu konzolu) postavte do obývacej izby alebo na iné spoločné prístupové miesto v byte.** Najlepšie tak, aby rodič mal vždy výhľad na monitor. Nedávajte počítač do detských izieb. Majte dobrý prehľad o všetkých ďalších počítačoch, ktoré sú deťom prístupné.
- **Stanovte medzi deťmi a rodičmi jasné pravidlá pre používanie internetu.** Urobte si rozvrh na dni a presný čas, kedy má dieťa povolenie stráviť čas na internete, najlepšie v čase vašej prítomnosti. Podpísanú zmluvu vystavte niekde pri monitore počítača. Nezabudnite, ak si s vaším dieťaťom vytvoríte pravidlá o používaní internetu, stanovte si práva a povinnosti pre obe strany. Pravidla, by sa mali pravidelne aktualizovať. Vzor takejto „rodinnej zmluvy" nájdete na stránkach Zodpovedne.sk.
- **Vytvorte medzi dieťaťom a rodičom vzťah vzájomnej dôvery.** Majte prehľad o prezývkach (nickname) vašich detí, ktoré používajú na internete. Buďte opatrný, nebuďte dotieravý pri kontrole dieťaťa, vzájomná dôvera je veľmi dôležitá. Prílišná kontrola by mohla dieťa dohnať ku skrývaniu a zatajovaniu činností. Netrestajte dieťa za to, čo nie je jeho chyba, môže vám

prestať dôverovať a mať strach a neistotu pri zdôverovaní sa s nejakým problémom. Je potrebné sa s deťmi veľa rozprávať, upozorniť ich na rôzne nebezpečenstvá, zaujímať sa a vedieť kde a ako trávia voľný čas, s kým telefonujú, emailujú, četujú, s kým sa stretávajú. Menšie deti si vyžadujú pravidelnú kontrolu. Ponúknite deťom adekvátne, zmysluplné a zaujímavé mimoškolské aktivity. Všímajte si viac svoje okolie. Nebuďte ľahostajní ani k cudzím deťom.

Správajte sa Zodpovedne.sk!

Mobily (SMS reklamný spam, zneužitie osobných údajov, krádež telefónu, obsah len pre dospelých, lokalizačné služby, zneužívanie tiesňových liniek, audiotext, bezdrôtové technológie)

Už dávno neplatí, že mobilné telefóny sa využívajú iba na telefonovanie alebo posielanie textových správ. Vývoj technológií aj v tejto oblasti umožňuje používanie mobilov na množstvo aktivít, ktoré boli v minulosti prostredníctvom mobilných telefónov neprístupné. Vo veľkej miere súvisí tento posun so spojením výhod mobilných telefónov a možností internetu, ide napríklad o:

- posielanie emailov,
- komunikácia pomocou rýchlej pošty,
- sťahovanie fotografií, videí,
- aktualizovanie online fotoalbumov,
- sťahovanie a počúvanie hudby,
- spravovanie bankových účtov,
- realizácia platieb, bankových prevodov..

Pri týchto činnostiach sa môžu užívatelia dostať do kontaktu s ohrozeniami, ktoré sú prítomné aj pri používaní internetu.

SMS reklamný spam

Pre spoločnosti je posielanie reklamných sms správ spôsob, ktorým môžu lacno a efektívne komunikovať so svojimi potenciálnymi zákazníkmi a získavať popularitu. Je to určite lacnejšie ako posielanie listov a má to tú výhodu, že SMS správu si každý prečíta, minimálne jej začiatok.

Môžeme hovoriť o dvoch druhoch reklamných sms správ – o vyžiadaných a nevyžiadaných. Vyžiadané správy chcete dostávať, prinášajú vám úžitok alebo informácie o produktoch, o ktoré sa zaujímate. Proti nevyžiadaným správam sa začalo výraznejšie bojovať vo Veľkej Británii, kde sa zákazníci masívne sťažovali na obťažovanie reklamnými sms.

Ak si neželáte dostávať reklamné sms správy o službách vášho operátora, kontaktujte ho a požiadajte o zrušenie zasielania týchto správ. Podobne zvážte zadávanie vášho telefónneho čísla do rôznych formulárov pri online nakupovaní alebo registrácii, prípadne zaškrtnite okienko, že si neprajete dostávať reklamné správy danej spoločnosti.

Aj napriek tomu je možné, že sa k vášmu číslu dostane spoločnosť, ktorá vám bude posielať reklamné správy. Ak sa v nich neuvádza spôsob zrušenia ich prijímania, pokúste sa zistiť informácie o odosielateľovi cez internet alebo telefónny zoznam a požiadať o zrušenie telefonicky, prípadne listom.

Zneužitie osobných údajov

Fotografie alebo videá sú často urobené bez vedomia a povolenia danej osoby a následne sú sprístupnené na internete alebo posielané prostredníctvom mobilného telefónu. Takto sa dostanú k nesprávnym osobám aj obrázky, ktoré boli urobené zo zábavy pre kamarátov a môžu ubližovať danej osobe, strápňovať ju, čo si veľakrát deti a mladí ľudia neuvedomujú pri hraní sa s fotkami druhých.

Majte svoj mobilný telefón neustále pod dohľadom, nenechávajte ho ležať na stole v reštaurácii, v škole, v kancelárii a podobne. Inak sa môže k vašim kontaktom a ďalším údajom dostať osoba, ktorej neboli určené a ktorá ich môže zneužiť.

K číslam, sms správam alebo fotografiám sa môže cudzí človek dostať aj cez bluetooth, a to tak, že o tom ani nebudete vedieť. Snažte sa preto nebyť pripojený sústavne alebo sa aspoň označiť ako neviditeľný.

Nechcený kontakt

Aj mobilné telefóny sú jedným z prostriedkov, ktoré sa využívajú na vyhrážanie, šikanovanie, sexuálne obťažovanie, urážanie a podobne.

Podľa belgického výskumu na tému kyberšikany u mládeže 56,7% respondentov uviedlo, že boli obeťami šikanovania cez internet alebo mobil, 49,3% priznalo, že sami boli realizátormi takéhoto konania a 78,6% opýtaných bolo svedkom niektorej formy elektronického šikanovania. Medzi najčastejšie formy šikanovania cez internet a mobilné telefóny patria podľa spomínaného výskumu vyhrážky, podvody, šírenie výmyslov a klebiet, prelomenie hesla k pošte a znemožnenie prístupu k emailom.

Pri mobilných telefónoch sa môžete stretnúť s nasledujúcimi činnosťami, ktoré sú považované za šikanovanie, obťažovanie:

- agresívne alebo výhražné sms správy (doručené aj opakovane),
- prijímanie extrémne veľkého množstva správ od jedného odosielateľa,
- útočné, urážajúce fotografie, videá,
- neustále nevyžiadané správy.

Medzi základné tipy, ktorými môžete napomôcť zastaveniu obťažovania patria:

- ignorovanie takýchto správ,

- archivovanie prijatých správ a ich odovzdanie polícii,
- dočasné pozastavenie prijímania správ a v kritických situáciách zmena telefónneho čísla. Je potom ale potrebné dbať na to, aby ste nové číslo nesprístupnili širokému okruhu ľudí, napríklad na internete a aby ste ho dávali len ľuďom, ktorých poznáte.

Je rovnako dôležité, aby deti a mladí ľudia vedeli a rozumeli, že nemusia znášať nepríjemné hovory alebo správy, že ich môžu ukončiť a ignorovať. Na druhej strane je potrebné im vysvetliť, že posielanie takýchto správ ďalším osobám nie je vhodným spôsobom zábavy a krátenia si voľného času.

Nízka kontrola

Rodičia nemajú veľký dosah na deti počas používania mobilného telefónu a ťažko môžu kontrolovať ich činnosť a komunikáciu. Je preto potrebné s deťmi otvorene hovoriť o možných rizikách používania mobilných telefónov.

Ak budú mať jasné stanovisko od rodičov k šikanovaniu a obťažovaniu môžu na jednej strane sami odhaliť takéto správanie voči svojej osobe a brániť sa. Zároveň ich toto zadefinovanie môže odradiť od podobného vlastného správania a pokusov s odosielaním správ.

Je vhodné stanoviť si tiež finančné limity pre používanie mobilných telefónov a podobne ako pri internete aj pravidlá, ktorými sa budú deti riadiť. Jednou z možností ako kontrolovať účty dieťaťa je napríklad zavedenie paušálu.

Krádež telefónu

Situácia, kedy telefonujete, píšete sms na ulici, prípadne si dáte telefón do vrecka na kabáte alebo nohavíc je ideálnou na to, aby vám telefón ukradli. V takomto prípade čo najskôr kontaktujte svojho operátora aby zablokoval vašu SIM kartu a hovory z telefónu. Vyhnete sa tak vysokým telefónnym účtom alebo zneužitiu vašich čísiel a iných údajov.

Zároveň túto udalosť čo najrýchlejšie nahláste polícii. Tej môže pomôcť pri pátraní po mobilnom telefóne jeho výrobné číslo (IMEI: International Mobile Equipment Identity, 15-miestne medzinárodné identifikačné číslo mobilných zariadení), ktoré je možné zistiť stlačením *#06# na telefóne. Každý telefón ma svoje jedinečné číslo, prostredníctvom ktorého je možné ho zablokovať.

Ak viete poskytnúť bližšie detaily o vašom telefóne, ako napríklad kde bol poškriabaný, či mal niečo zlomené a podobne zvyšujete svoje šance na jeho vystopovanie.

Obsah len pre dospelých

Prostredníctvom mobilného telefónu a pripojenia na internet sa dnes môžu aj maloletí užívatelia dostať k materiálom, ktoré sú určené iba pre dospelé osoby.

Začiatkom februára 2008 slovenskí mobilní operátori podpísali Národný kódex bezpečného používania mobilných služieb. Ten ich zaväzuje, že najneskôr 31.12.2009 budú ponúkať mobilný obsah určený len pre dospelých so zabezpečením možnosti kontroly prístupu (napríklad na požiadanie rodičov bude prístup k tomuto obsahu úplne zneprístupnený) prostredníctvom metód, v rámci ktorých bude jednoznačne overená totožnosť a vek užívateľa. Operátori sa tiež spoločne zaviazali poskytovať základné informácie a poradenstvo o využívaní elektronických komunikačných služieb a obsahu, ako aj o opatreniach, ktoré môžu rodičia urobiť na ochranu svojich detí. Prostredníctvom nových služieb budú mať rodičia možnosť kontroly a ochrany detí pri používaní mobilných telefónov.

Lokalizačné služby

Niektorí operátori umožňujú zistiť polohu najbližších bankomatov, nákupných centier, pôšt a podobne. Stačí zaslať sms správu v určitom znení napr. „bankomat“ na skrátené číslo a vzápätí príde spätná sms správa s informáciou o najbližších bankomatoch. O konkrétnych kľúčových slovách ako aj skrátených číslach, kde treba zaslať sms správu sa informujte u jednotlivých operátorov.

Lokalizačné služby sa však používajú hlavne na to, aby bolo možné lokalizovať ľudí, ktorí dali svoj súhlas na lokalizovanie rodine, zamestnávateľovi, priateľom. Možnosti ako lokalizovať osobu sú u rôznych operátorov rôzne. Princíp však ostáva ten istý. Je potrebné zaslať sms správu v znení, ktoré vyžaduje konkrétny operátor na skrátené číslo. Ďalej je potrebné, aby vyhľadávaný užívateľ potvrdil sms správou, či súhlasí s tým, aby bol lokalizovaný. Ak tak neurobí do určitého časového limitu, alebo s tým nesúhlasí, nie je možné zistiť jeho polohu. Ak súhlasí, užívateľovi, ktorý ho hľadá príde sms správa s približnou polohou a vzdialenosťou. V prípade, že použijete vyhľadávanie mobilu cez internet, zobrazí sa vám poloha hľadaného na mape.

Zneužívanie tiesňových liniek

Vlastníctvo mobilného telefónu vedie často ľudí k neoprávneným volaniam na tiesňové linky alebo linky pomoci. Takto blokujú operátorov pre tých, ktorí pomoc reálne potrebujú, a ktorým by včasné dovolanie sa mohlo zachrániť zdravie alebo život.

Napriek mnohým apelom od pracovníkov tiesňových liniek sa s týmto problémom stretávajú stále vo veľkej miere. Je preto potrebné vysvetľovať deťom a mladým ľuďom význam týchto liniek a nebezpečenstvo, ktorému vystavujú ľudí v núdzi svojím neopodstatneným volaním.

Audiotext

Jedným z rizík, ktoré hrozí v prípade, že má dieťa telefón na paušál sú volania na audiotextové čísla. Týmto ťažko odolávajú hlavne deti, ktoré sa zapájajú do rôznych súťaží, kvízov vo vidine výhry alebo zo zábavy. Je preto potrebné im pred používaním mobilného telefónu vysvetliť, že ide o čísla, ktoré sú

vysoko spoplatňované. Rovnako pomôže aj dôverný vzťah medzi rodičmi a deťmi, aby sa nebáli priznať takéto konanie a predísť ešte vyšším nákladom v budúcnosti.

Bezdrôtové technológie

Bluetooth
Je to technológia pre bezdrôtovú komunikáciu, vďaka ktorej sa dá prepojiť dve rôzne zariadenia v okruhu cca 10 metrov a prenosová rýchlosť dosahuje 1 MB/s.

Prostredníctvom nej je možné prenášať dáta, obrázky či hudbu, spájať rôzne zariadenia a vzájomne komunikovať. Dnes už bluetooth môžete nájsť vo veľa druhoch elektronických zariadení, napr. mobilné telefóny, počítače, klávesnice, tlačiarne, videokamery, slúchadlá, reproduktory, atď.

Bluetooth je možné využiť na výmenu údajov medzi počítačmi, mobilnými telefónmi na bezdrôtovú tlač, pripojenie komponentov k počítaču, pripojenie hands–free setov k telefónu a podobne. Kedysi bolo bluetooth výbavou len drahých telefónov, dnes už je možné si ho zaobstarať aj v lacnejších alebo akciových modeloch. Zvyšujú sa tak možnosti prenosu informácií prostredníctvom mobilných telefónov a tým aj riziko, že sa k nim dostane nepovolaná osoba.

V prípade, že telefón nemá bluetooth dobre zabezpečený môže dôjsť k odcudzeniu telefónnych čísel zo zoznamu, prečítaniu alebo odoslaniu sms správ či vytočeniu vybraného čísla zo zoznamu. A to všetko bez toho, aby si bol majiteľ telefónu niečoho vedomý.

Pre využívanie bluetooth je potrebné spárovať dve zariadenia, zadať spoločný kód a potvrdiť spojenie. Ak je kód správny, je možné vzájomne komunikovať medzi zariadeniami, posielať si dokumenty alebo obrázky.

Ak máte zapnutý bluetooth neustále, je možné, že si vás vyhľadá cudzia osoba a osloví vás. Zvážte, či budete nadväzovať komunikáciu s osobou, ktorú nepoznáte. Pri aktívnom bluetooth môžete zvýšiť ochranu v bluetooth nastaveniach tým, že si zvolíte možnosť, aby bol váš telefón neviditeľný pre iné bluetooth zariadenia alebo telefóny.

WiFi
Podobne ako bluetooth ide o bezdrôtovú technológiu komunikácie. Na rozdiel od bluetooth má väčší dosah a vyššiu prenosovú rýchlosť, vďaka ktorej je možné komunikovať efektívnejšie a rýchlejšie. Dnes sa často využíva na pripojenie k internetu prostredníctvom prístupového bodu, pričom oblasť, ktorá je pokrytá viacerými prístupovými bodmi sa nazýva „hot spot“. Môžete sa s nimi stretnúť v kaviarňach, v centrách miest, v obchodných centrách, na letiskách a podobne.

Napriek tomu, že veľa ľudí využíva mobilný telefón väčšinou na písanie správ alebo telefonovanie, nachádzajú si pridávané služby k mobilom svojich priaznivcov. Jednou z týchto služieb je aj prístup na internet cez mobil, ktorý umožňuje aj technológia WiFi.

Zároveň je takto možné bez káblov prepojiť svoj mobil s počítačom. Pre zvýšenie bezpečnosti vašich údajov pri používaní internetu cez verejné prístupové body je potrebné si byť vedomý rizík a toho, že pripojenie na internet nie je úplne bezpečné.

Ak používate takéto pripojenie, takmer všetko, čo píšete u seba v počítači alebo mobile môže byť videné niekým iným. Preto pokiaľ udávate na akúkoľvek stránku vaše meno, heslo alebo iné osobné údaje, overte si, či ste na bezpečnej stránke. Uvidíte to tak, že v linke stránky je miesto bežného http uvedené https. Takto budú vaše údaje zašifrované a prenesené bezpečnejšie.

Niektoré stránky však po prihlásení zmenia svoj mód zo zabezpečeného na štandardný, teda údaje, ktoré uvádzate po prihlásení je už možné odchytiť ďalšou osobou.

Podobne ako si dávate pozor pri vyberaní peňazí z bankomatu, buďte opatrný aj pri zadávaní hesiel alebo uvádzaní dôležitých informácií na verejnosti. Vždy sa môže nájsť niekto, kto vám bude stáť za chrbtom alebo sedieť obďaleč a sledovať vašu činnosť.

Zabezpečenie WiFi sietí

V prípade, že ste si vytvorili WiFi sieť, alebo ste pripojený do siete WiFi technológiou, je potrebné si ju správne zabezpečiť, aby nedošlo k neautorizovanému pripojeniu do vašej siete, a tým napr. k nárastu vašich poplatkov za pripojenie k internetu alebo zneužitiu vašich osobných údajov. Zabezpečenie WiFi je možné urobiť viacerými spôsobmi:

- Skrytie alebo zmena názvu siete, tzv. SSID (Services Set Identifier), čo znamená zabránenie vysielaniu názvu siete do okolia AP (Acces point – prístupový bod). Taktiež je dobré zmeniť názov siete na akýkoľvek iný názov rozdielny od „default“.
- Filtrovanie pomocou adries MAC (Media Access Control). Ak chceme dovoliť pripojenie určitému počtu počítačov zaradíme si ich MAC adresy (fyzické adresy sieťových kariet dané výrobcom) do zoznamu povolených adries. Takýto typ zabezpečenia nazývame aj *autentifikáciou* – riadením prístupu do siete.
- Autentifikácia zdieľaným kľúčom (shared key), ak sa chce niekto pripojiť do vašej siete, musí poznať vami zadaný kľúč, pomocou ktorého prebehne autentifikácia a následné pripojenie. Táto metóda je ďalej rozšírená o šifrovanie prenosu kľúča. Dáta sú šifrované pomocou kľúča WEP (Wired Equivalent Privacy) alebo WPA (WiFi Protected Access), ktoré vyriešilo niektoré bezpečnostné slabiny WEP.

Skontrolujte si ešte pred samotným pripojením na internet, či máte nastavený správne firewall aj na iné siete a pripojenie ako je vaša domáca alebo pracovná. Pomôže vám chrániť si údaje pred ďalšími ľuďmi, ktorí využívajú WiFi pripojenie.

Prevencia

- **Rešpektujte ostatných, ich názor a priania**. Aj tu platí, nerobte iným to, čo nechcete, aby robili oni vám.
- **Telefónne čísla vašich známych neposkytujte bez ich vedomia.** Nikdy neviete, kam a ku komu sa nakoniec dostane, a na čo môže byť zneužité.
- **Nefotografujte a nenahrávajte ľudí bez ich povolenia, a tiež si dobre rozmyslite ako, a kým sa necháte odfotiť.** Ak sa necháte odfotiť zo zábavy, nezabúdajte na to, že tieto fotky sa môžu dostať prostredníctvom mobilov alebo internetu aj k ľuďom, ktorí ich môžu zneužiť.
- **Stanovte finančný limit.** Používanie internetu na mobilnom telefóne môže byť finančne náročné. Ak sa dohodnete s dieťaťom na jeho používaní, stanovte si maximálne možný prenos dát alebo maximálny poplatok za používanie internetu.
- **Nereagujte na sms správy, ktoré vás navádzajú k dobytiu kreditu neznámej osoby**, často krát sú spojené s prísľubom vykonania nejakej služby, ktorá sa v skutočnosti nikdy nezrealizuje.
- **Vysvetlite deťom, čo sú audiotextové čísla.** Ak si budú uvedomovať, že sú vysoko spoplatňované, môžete sa vyhnúť nepríjemným prekvapeniam po doručení účtu.
- **Oboznámte dieťa s účelom tiesňových liniek, liniek pomoci predtým, ako mu dáte mobilný telefón.** Môžete predísť pokusom o žart alebo volaniam zo zábavy, ktoré blokujú operátorov pre tých, ktorí skutočne pomoc potrebujú.
- **Zabezpečte dieťaťu mobilný telefón s paušálom.** Môžete tak kontrolovať výpisy hovorov a sms správ. Nevýhodou môže byť prekročenie voľných minút a tým vyššie náklady.
- **Naučte sa jazyk sms.** V správach sa používa množstvo skratiek a symbolov, ktorých neznalosť môže spôsobiť, že neporozumiete obsahu. (Napríklad: O5 si NPCHP – Opäť si nepochopil).
- **Hovorte s dieťaťom o možných rizikách.** Ak sa dostane cudzia osoba k údajom dieťaťa, je možné, že bude dostávať neslušné sms, mms správy, perverzné fotografie alebo ho bude táto inak obťažovať. Je potrebné, aby dieťa vedelo, že ak dostane takúto nechcenú správu, nie je to v poriadku, má sa vám zveriť a riešiť s vašou pomocou danú situáciu.
- **Neodpovedajte na pravidelne sa opakujúce správy alebo hovory od cudzej osoby.** Často ide o náhodu, že si osoba vybrala vaše číslo a jej jediným cieľom môže byť provokácia, nadviazanie kontaktu. Ak neodpoviete, nebude mať na čo nadväzovať a stratí záujem.
- **Ak obťažovanie alebo vyhrážanie cez sms správy a volania neprestáva, zmeňte svoje telefónne číslo.** Nové číslo neposkytujte cudzím osobám a neuvádzajte ho na internete. Vaše staré číslo sa určitý čas nebude používať a v tejto dobe sa k nemu môžete vrátiť.
- **Uložte si všetky výhražné, perverzné sms správy, obrázky.** V prípade, že dostávate vy alebo vaše dieťa výhražné alebo posmešné správy, je potrebné zájsť na políciu a predložiť všetky uchované správy, ktoré ste dostali.
- **Nahrajte si telefonáty na mobil.** Ak ide o telefonické hovory, je dobré si ich nahrať ak to telefón dovoľuje a predložiť polícii nahrávky.
- **Vyberte si operátora, ktorý poskytuje služby na ochranu vás a vášho dieťaťa.**
- **Nedovoľte ľuďom, ktorých nepoznáte používať váš mobil.** Môžu vám ho ukradnúť, zneužiť vaše osobné údaje alebo zavolať na audio textové číslo, z ktorého majú oni príjem a vám prídu vysoké účty za telefonovanie.
- **Nevystavujte svoj mobil na obdiv okoloidúcim.** Keď ho nepoužívate, má byť vo vrecku alebo ruksaku, inak sa môže ľahko stať, že vám ho ukradnú. Krádež mobilných telefónov je bežným činom, často krát ho sprevádza zranenie majiteľa alebo poškodenie jeho osobných vecí.
- **V prípade krádeže pomôžu polícii vystopovať váš mobilný telefón údaje o ňom.** Zaznamenajte si výrobné číslo telefónu. Toto môžete zistiť stlačením *#06# na telefóne, pričom sa vám zobrazí 15 miestne číslo.
- **Nikdy neviete, kto je v skutočnosti na druhej strane internetu alebo mobilu.** Na druhej strane môže byť človek, ktorý klame o svojom veku, pohlaví, záujmoch, vzhľade a podobne. Takýto ľudia chcú deťom veľmi ublížiť a sú to:
    - pedofili...
    - ľudia, ktorí chcú fotografie a videá detí...
    - navádzajú na užívanie drog...
    - navádzajú na šikanovanie, alebo šikanujú deti...
    - nenávidia určité skupiny ľudí...

- správajú sa agresívne, násilne...
- chcú sa s deťmi tajne stretnúť, ublížiť im, uniesť ich...
- získať osobné údaje o dieťati, jeho rodine, kamarátoch...
- chcú oklamať, podviesť dieťa...
- návádzajú na sebapoškodzovanie...

- **Nie je bezpečné dávať na internet alebo cez mobil svoje osobné údaje.** Vysvetlite deťom, čo sú to osobné údaje a prečo je nebezpečné zverejňovať svoje pravé meno a priezvisko, svoju fotografiu, video, vek, emailovú adresu, telefónne číslo, adresu domov, adresu školy, majetkové pomery, prístupové mená a heslá alebo iné osobné údaje (záľuby, opis vzhľadu, povahy, znalosti, zručnosti, vzdelanie, obľúbené veci, túžby...). V prípade, že je nevyhnutné takéto údaje poskytnúť, musia o tom vedieť rodičia alebo učitelia.
- **Pri kontrolných otázkach, ktoré sa používajú ako pomoc pri strate hesla, zvoľte odpoveď, ktorú okrem vás nikto nepozná.**
- **S nikým, s kým sa dieťa zoznámilo iba cez internet alebo mobil, sa nesmie stretávať samé osobne.** Tak ako v reálnom živote nechodia deti na stretnutie s neznámou osobou bez sprievodu niekoho ďalšieho, najlepšie rodiča, alebo aspoň súrodenca, kamaráta, tak aj na stretnutie s neznámou osobou, s ktorou sa dieťa zoznámilo iba cez internet alebo mobil, je stretnutie veľmi nebezpečné. Ak už dieťa ide na stretnutie, tak vždy aspoň s kamarátom. Rodičom by malo oznámiť na aké stretnutie ide, za kým ide, kde a kedy sa plánuje vrátiť. Stretnutie by malo byť na verejnom mieste, kde je veľa ľudí. Znakom bezpečnejšieho stretnutia je, že tomu, čo pozýva, nevadí, že dieťa príde s rodičom alebo inou dospelou osobou. Ak mu to vadí, ten človek nemá čisté úmysly.
- **Buďte podozrievavý voči človeku, ktorý dieťa presviedča, aby zatajovalo svoje internetové kamarátstvo pred rodičmi, alebo vystupuje ako tínedžer, ale nevie väčšinu odpovedí na otázky, ktoré bežne rovesníci poznajú.** Takýto človek chce deťom ublížiť, a preto klame a navádza, aby zatajili pozvanie na stretnutie s ním, aby si zmazali históriu četu, jeho emaily, sms, mms správy, a podobne.
- **Použitie lokalizačných služieb mobilného telefónu dieťaťa neznámou osobou je nebezpečné**. Vďaka lokalizácii môže ktorákoľvek osoba vyhľadať miesto pobytu dieťaťa, ak mu to samo z nevedomosti umožní.
- **Bluetooth spojenie cez mobilný telefón dieťaťa s neznámou osobou je nebezpečné**. Pomenujte mobilný telefón dieťaťa tak, aby z neho nebolo hneď jasné, že sa jedná o dieťa.
- **Používajte pri verejných WiFi sieťach bezpečné stránky.** Ak vkladáte osobné údaje, preverte si, či má stránka v názve miesto bežného http uvedené https.
- **Nie všetko, čo je na internete, je pravda.** Vysvetlite deťom, nech neveria všetkému čo nájdu na internete. Informácie si je potrebné porovnať z viacerých zdrojov a v prípade nejasností sa poradiť s rodičmi alebo učiteľmi v škole.
- **Ak dieťa na internete alebo cez mobil niečo vyľaká, našlo niečo škaredé, desivé, niečo z čoho sa cíti trápne, zraňuje ho to alebo ohrozuje, vysvetlite mu, že to nie je jeho chyba.**
- **Správajte sa Zodpovedne.sk!**

HOAX (Fámy, varovania pred vymyslenými vírusmi, fámy o mobilných telefónoch, petície a výzvy, podvodné emaily, žartovné správy)

Fámy, varovania pred vymyslenými vírusmi, fámy o mobilných telefónoch, petície a výzvy, podvodné emaily, žartovné správy

HOAX: *falošná správa/poplašná správa/podvod,* ktorá varuje napríklad pred neexistujúcim nebezpečným vírusom. Najčastejšie sa môžeme stretnúť s falošnými prosbami o pomoc, fámami o mobilných telefónoch, petíciami a výzvami, reťazovými listami šťastia, atď.

Slovo hoax pochádza z časov, kedy sa o počítačoch ešte ani nechyrovalo. Vzniklo vraj skrátením formulky „hókus-pókus“ už v 17. storočí. Túto formulku si vtedajšie reformované cirkvi prisvojili a upravili z latinského *„Hoc est corpus meum*“, čo v preklade znamená „toto je telo moje“, na výsmech katolíckej cirkvi, ktorá sa túto formulu modlieva počas liturgických obradov.

Poplašné správy či pokusy o reťazové listy majú svoje historické korene dávno pred expanziou internetu. Možno si spomínate na listy šťastia alebo listy sľubujúce zbohatnutie, ktoré bolo treba odoslať minimálne piatim svojim priateľom, aby sa nepretrhla reťaz, atď. V digitálnom svete internetu, mobilov to funguje rovnako, mení sa vlastne len médium prenosu správ.

Za prvý „pravý“ hoax je považovaná správa z októbra 1988 o nebezpečnom víruse a spôsobe ochrany pred ním. Od vtedy sa množstvo poplašných správ rozšírilo do takej miery, že si to vynútilo založiť databázy hoaxov.

Hoax podobne ako spam zapĺňa naše emailové schránky, ale otravuje nás napr. aj formou instant messaging (ICQ, Skype, atď.) a sms správami. Od spamu sa líši hlavne tým, že ho rozposielajú nevinní užívatelia, ktorý si myslia, že ide o dôležitú správu alebo, že poslaním emailu každému, koho majú vo svojich kontaktoch, môžu niekomu pomôcť, či dokonca zarobiť si peniaze. Je mnoho dôvodov, ktoré mohli viesť pôvodného autora k napísaniu poplašnej správy, zväčša však ide iba o zábavu z jeho strany. V mnohých správach sú úplné absurdnosti, to však nebráni tomu, aby sa správa vďaka ľudskej hlúposti nešírila ďalej.

Aby sme vedeli spoľahlivo určiť, či daná správa je alebo nie je hoax, je potrebné si všímať jej formu a obsah. Hoax má niekoľko charakteristických čŕt:

- **Naliehavosť a popis nebezpečenstva –** naliehavo popisuje riziko neexistujúceho nebezpečenstva, v prípade vírusu býva uvádzaný aj spôsob šírenia.

- **Ničivé účinky vírusov** - tu záleží prevažne na autorovej fantázii. Ničivé účinky môžu byť celkom obyčajné, napríklad sformátovanie disku alebo aj menej dôveryhodné – roztočenie harddisku opačným smerom, výbuch počítača, atď.
- **Zdanlivá dôveryhodnosť** - vo väčšine prípadov sa autor poplašnej správy snaží presvedčiť, že varovanie prišlo z dôveryhodných zdrojov ("IBM a FBI varujú" alebo "Microsoft upozorňuje" atď.)
- **Ďalším znakom je prosba o okamžité rozoslanie takéhoto varovania všetkým známym a priateľom** - veľa neskúsených užívateľov reaguje na správu bez premýšľania. Práve preto sa tieto nezmysly šíria ako lavína.

Ak Vám prišla takáto pochybná správa a chcete mať istotu, že ide o hoax skúste si pozrieť niektorú databázu hoaxov (Quatloos, Virushoaxbusters, Snopes.com, www.hoax.cz, Symantec, F-Secure, McAfee, Trend Micro). Vo väčšine prípadov tam nájdete, ak nie totožnú, tak veľmi podobnú verziu správy. Rovnako sa nemusíte obávať, že „prerušením“ reťaze Vás postihne nejaké nešťastie, navyše šírením hoaxov a iných reťazových emailov sa užívateľ previňuje proti pravidlám netikety.

Niekedy však môže ísť o reálnu správu, tú je však vhodné rozosielať len pri úplnej istote, že je pravdivá, napr. keď osobne poznáte odosielateľa a viete, že:

- rozumie tomu čo píše,
- správa pochádza priamo od neho (nie je preposlaná),
- zvykne písať pravdu.

Prečo je hoax škodlivý?

- **Obťažuje prijímateľov** - opakovaný príjem nezmyselných správ je nepríjemný a zdržuje, hlavne v dobe epidémie. Vtedy sa v emailových schránkach môže objaviť rovnaká správa aj niekoľkokrát denne.
- **Strata dôveryhodnosti** - rozposielaním hoaxu obchodným partnerom svoju prestíž určite nezvýšite. Šírenie poplašných správ štátnymi úradníkmi, hoci len v rámci zábavy, nie je dobrou vizitkou úradu. Vrcholom je, ak sa takáto správa pochádzajúca zo zdroja, ktorý je všeobecne považovaný za dôveryhodný, dostane na verejnosť.
- **Zbytočné zaťažovanie liniek a serverov** – napriek tomu, že výkony serverov a rýchlosti ich vzájomného prepojenia neustále narastajú, zvyšuje sa aj zaťaženie siete. Je to dané zvyšujúcim sa počtom užívateľov, ale aj väčším počtom šíriacich sa počítačových červov. Veľké množstvo hoaxov rozosielajú užívatelia spôsobom „poslať ďalej“ a na všetky adresy uvedené v kontaktoch.
- **Šírením hoaxu môžete vyzradiť dôverné informácie** - ak sa hoax rozosiela spôsobom „poslať ďalej“, teda aj s hlavičkami, v ktorých je celý zoznam emailových adries, dáva sa k dispozícii obrovský zoznam emailových adries náhodným prijímateľom. Nikdy neviete, ku komu sa tieto adresy kvôli takémuto spôsobu dostanú. Dajú sa tak ľahko zneužiť napríklad spamermi a nežiadaná pošta je hneď na ceste aj do každej schránky z vášho zoznamu. Nepríjemná situácia by mohla nastať, ak by sa zoznam adries vašich obchodných partnerov a klientov dostal ku konkurencii.

Medzi najčastejšie typy hoaxov, s ktorými sa dnes stretávame patria:

- **Varovania pred vymyslenými vírusmi a rôznymi útokmi na počítač.**
- **Popis iného nereálneho nebezpečenstva** - mimo oblasť výpočtovej techniky, (napr. nešťastie v rodinnom živote, pohroma, atď.)
- **Falošné prosby o pomoc** – môže sa stať, že v minulosti pravdivá prosba o pomoc sa začne masovo šíriť, až keď je už dávno neaktuálna. Často sa stáva, že sa takáto správa preposiela dokonca v určitých periódach aj niekoľko rokov za sebou. Príkladom môžu byť prosby o darovanie krvi, darovanie malej čiastky na nejaký neexistujúci účet, atď.
- **Fámy o mobilných telefónoch** - typu nevolajte na toto číslo, vaše účty porastú do závratných výšok. Vymyslené, skreslené alebo neúplné informácie ohľadne mobilných telefónov.
- **Petície a výzvy.**

- **Podvodné emaily (napr. z Nigérie) -** s lákavými ponukami na veľkú sumu peňazí (napr. pomoc pri prevode majetku alebo peňazí).
- **Pyramídové hry a rôzne ponuky na jednoduché obohatenie sa.**
- **Reťazové listy šťastia -** šírené z poverčivosti alebo z neznalosti.
- **Žartovné správy -** ktoré si medzi sebou posielajú kamaráti a známi.

Prevencia

- V praxi sa dá použiť pravidlo: **Ak správa obsahuje výzvu k hromadnému rozosielaniu na ďalšie adresy, je to s najväčšou pravdepodobnosťou hoax.**
- **Overte si pravdivosť uvádzaných informácií,** napríklad aj na niektorom zo serverov s databázami hoaxov.
- **Buďte „emailovo" rozvážny**, nereagujte a neposielajte ďalej každý podozrivý email, ktorý vám bol doručený, hlavne ak sa objaví viackrát za deň a vždy od iného odosielateľa.
- **Robte osvetu!** Jeden zo spôsobov je kontaktovať odosielateľov a vysvetliť im, čo Vám vlastne poslali, prečo je to zlé a svoje tvrdenia podoprieť odkazmi na databázy hoaxov.
- **Správajte sa Zodpovedne.sk!**

Monitorovacie, filtrovacie programy

Monitorovacie programy a filtre nepatria medzi ohrozenia, napriek tomu je však dobré vedieť, že žiadny filter nie je dokonalý. Je potrebné kontrolovať jeho funkčnosť, poprípade zabezpečiť si aktuálnu verziu. Filtre sa dajú rôznymi spôsobmi obísť alebo vyradiť z funkčnosti. Rodič tak môže nadobudnúť falošnú istotu, že nainštalovaním filtra je jeho dieťa dokonale chránené. Navyše takéto technické opatrenie môže viesť k zhoršeniu vzťahov medzi deťmi a ich rodičmi.

Monitorovacie programy umožnia spätne skontrolovať pohyb dieťaťa na internete, pozrieť si stránky, ktoré navštívilo, alebo chcelo navštíviť, získať prehľad aké súbory sťahovalo z internetu, koľko času strávilo na konkrétnych stránkach. Pomocou vzdialeného prístupu a ovládania sa dá kontrolovať surfovanie na domácom počítači z počítača, v ktorom je program nainštalovaný kedykoľvek (napr. z práce).

Filtre

Filtre zabezpečujú, aby sa dieťa nedostalo na internetové stránky, ktoré obsahujú nevhodný materiál. Pomocou filtrov je možné nastaviť blokovanie stránok, ktoré obsahujú vybrané slová, ale aj obrázky (napr. sex, porno...). Niektoré filtre tiež blokujú prístup do četových miestností, internetových diskusií, kontrolujú emaily a dáta sťahované cez peer-to-peer programy. Filter je možné si nainštalovať do svojho počítača alebo využívať filtre prevádzkované verejne internetovými poskytovateľmi, ktorý bude kontrolovať stránky miesto vás.

Filter pracuje na princípe:

- skenovania a blokovania stránok, ktoré obsahujú určité výrazy,
- blokovania stránok s obsahom sexuálnych a násilných materiálov,
- obmedzenia pohybu dieťaťa na vopred zvolené stránky a podstránky, ktoré spĺňajú kritériá bezpečnosti,

- zákazu pohybu po internetových stránkach s výnimkou povolených stránok a ich podstránok.

Na čo prihliadať pri výbere filtra:

- Jednoduchosť používania – filtre majú byť schopné používať aj osoby s nižšími počítačovými znalosťami.
- Efektivita filtrovania – rovnováha medzi blokovaním nevhodných stránok a prístupom k potrebným informáciám. Dôležitá je možnosť prispôsobiť filter potrebám každého člena rodiny.
- Mechanizmus filtrovania – najlepšie programy kombinujú techniky filtrovania (filtrovanie web stránok, filtrovanie kľúčových slov a dynamické filtrovanie - filtrovanie postavené na báze hodnotenia.
- Monitorovanie činností – lepšie filtre ponúkajú možnosť monitorovania činnosti na internete jednotlivých členov domácnosti (aké stránky navštívili, poslané emaily, navštívené četové miestnosti, sťahované súbory z internetu, čas strávený na jednotlivých webových stránkach...).
- Klientské/serverové filtre – mala by existovať možnosť nastavenia filtra v domácom počítači alebo prostredníctvom providera a jeho servera, prípadne kombinácie oboch možností.
- Filtrovanie vo viacerých jazykoch – možnosť nastaviť filtre a kľúčové slová vo viacerých jazykoch zabraňuje deťom obísť blokovanie zadaním slov v inom jazyku.
- Blokovanie všetkých prístupových ciest – internetových stránok, četových miestností, emailov, peer-to-peer programov, pop-up okien.

Podľa niektorých odborníkov nemusí byť používanie filtrov postavených na princípe filtrovania kľúčových slov (výrazov) tým najlepším riešením. Blokujú totiž nielen nevhodné stránky (napr. porno stránky), ale aj tie, kde sa vyskytne téma s filtrovaným slovom. Ak napríklad nastavíme blokovanie stránok, na ktorých sa vyskytuje slovo „sex“, zablokujeme aj tie, ktoré sa venujú prevencii sexuálnych chorôb, radám ako sa vyhnúť sexuálnemu obťažovaniu, antikoncepcii a podobne.

Predovšetkým mladí ľudia vyhľadávajú prostredníctvom internetu informácie o takýchto chúlostivých témach, o ktorých vedia iba ťažko komunikovať s rodičmi. Okrem toho filtre spomaľujú počítače, čo spolu s obmedzeným prístupom k informáciám často vedie k obchádzaniu filtrov a používaniu internetu za chrbtom rodičov.

Nesprávne nainštalovaný a nastavený filtrový softvér vyvoláva u rodičov falošný pocit bezpečia, čo môže oslabiť pozornosť a znížiť starostlivosť o správanie dieťaťa na internete. Aj keď sú filtre nainštalované, neznamená to, že rodičia alebo učitelia nemusia deti vzdelávať a upozorňovať na riziká používania internetu.

Rodičovská kontrola

Ak potrebujete sledovať, čo robia vaše deti na počítači alebo ak chcete obmedziť dobu ich pobytu pri počítači, či zakázať prístup na niektoré internetové stránky, prípadne blokovať niektoré programy, môžete využiť možnosti rodičovskej kontroly.

Cieľ je jasný, cesty k nemu sú však mnohým rodičom nejasné – je vôbec možné vhodným spôsobom kontrolovať, kde surfujú naše deti, čo z rôznych stránok sťahujú, a je vôbec možné nejakým spôsobom zasiahnuť?

Možností je niekoľko, ale v základe je možné rozdeliť ich do dvoch skupín:

- Opatrenia organizačného charakteru – stanovte medzi deťmi a rodičmi jasné pravidlá pre používanie internetu. Urobte si rozvrh na dni a presný čas, kedy má dieťa povolenie tráviť čas na internete, najlepšie v čase vašej prítomnosti. Podpísanú zmluvu vystavte v blízkosti počítača na viditeľnom mieste. Nezabudnite, ak si s vaším dieťaťom vytvoríte pravidlá o používaní internetu, stanovte si práva a povinnosti pre obe strany. Pravidlá, by sa mali pravidelne aktualizovať. Vzor takejto „rodinnej zmluvy" nájdete na stránkach Zodpovedne.sk.
- Opatrenia s aplikovaním technických foriem – využitím hardvérových zariadení alebo vhodného softvéru.

Voľne dostupný softvér

K dispozícii je množstvo rôznych aplikačných programov, ktoré poskytujú služby filtrovania resp. monitorovania aktivít na internete.

K9 Web Protection

Softvér umožňujúci filtrovanie web stránok zobrazovaných na vašom počítači ako aj limitovanie času stráveného za počítačom. Pomocou neho je možné:

- kontrolovať web stránky podľa obsahu – zakázať prezeranie pornografických stránok, nakupovať v online obchodoch a pod., ako aj zakázať prezeranie stránok, kde sa vyskytuje nežiaduci výraz, či slovné spojenie,
- limitovať čas strávený pri počítači a na internete,
- odosielať správy o činnosti vášho počítača na váš email – to umožňuje kontrolovať činnosť vášho počítača aj keď ste mimo domova alebo mimo pracoviska z rôznych kútov sveta.

Ďalšie informácie nájdete na linke:

http://www.k9webprotection.com

ParentalControl Bar

Voľne šíriteľný program, fungujúci ako prídavný panel pre Internet Explorer. Pomocou neho je možné:

- používa preddefinované filtre pre témy ako sex, nadávky, urážky, násilie, s možnosťou nastavenia filtra pre konkrétny účel,
- umožňuje zadávať aj vlastné adresy web-stránok, blokovať k nim prístup.

Ďalšie informácie nájdete na linke:

http://parentalcontrolbar.org

Internet Explorer

Internetový prehliadač Internet Explorer má v sebe zabudovaný mechanizmus kontrolovaného riadenia prístupu k obsahu internetu systému ICRA3 (http://www.icra.org). Umožňuje filtrovať prístup k stránkam obsahujúcim neželanú kategóriu informácií. Zároveň umožňuje prehliadanie tzv. schválených lokalít.

Ďalšie informácie nájdete na linke:

http://www.microsoft.com

Komerčné riešenia

PassManager, AreaGuard, OptimAccess

Dvojúrovňové riešenie umožňujúce vykonávanie monitorovania činnosti PC s operačným systémom MS Windows (všetky verzie) a zavádzanie reštrikcií (obmedzení) pre prácu s PC, využívaním internetu. Pomocou týchto programov je možné:

- **Monitorovanie:**
  - umožňuje získať prehľady o
  - čase, ktorý strávi dieťa pri počítači
  - spúšťaných aplikáciách
  - navštevovaných webových stránkach
  - sťahovaných súboroch (súboroch prijímaných ako príloha emailu)
  - tlačených dokumentoch
  - používanie výmenných médií
  - a rad ďalších
- **Reštrikcie:**
  - zákaz prístupu na definované web-stránky
  - povolenie prístupu na konkrétne stránky
  - riadenie prístupu k aplikáciám (spúšťateľné len povolené aplikácie)
  - ochrana nastavení vybraných aplikácií
  - rad ďalších

Ďalšie informácie nájdete na linkách:

www.sodatsw.cz www.infoconsult.sk

Operačný systém Microsoft Windows Vista

Obsahuje novú funkciu rodičovská kontrola, ktorou môžu rodičia obmedziť aktivity svojich detí pri počítači:

- Rodič môže presne určiť stránky, ktoré budú môcť ich deti navštevovať, a z ktorých budú môcť sťahovať dáta.
- Rodič môže kontrolovať čas, ktorý strávi dieťa pred počítačom tým, že softvérovo určí čas, v ktorom bude môcť dieťa využívať počítač.
- Rodič bude môcť blokovať prístup k jednotlivým programom, taktiež hrám, ktoré nie sú určené pre vekovú skupinu, v ktorej sa dieťa nachádza.

- Rodič môže zistiť aktivity dieťaťa na PC pomocou výpisov, v ktorých bude zaznamenané, aké stránky dieťa navštívilo, koľko emailov prijalo, s kým bolo v kontakte pri četovaní prostredníctvom IM programu (ICQ, Skype, atď.).

Ďalšie informácie nájdete na linke:

http://www.microsoft.com

Žiadny filter však nie je taký dokonalý, aby dokázal blokovať všetky nevhodné stránky. Okrem toho sa obsah na internete mení a dopĺňa tak rýchlo, že sa filtrovacie programy iba veľmi ťažko môžu stíhať aktualizovať. Preto je nutné, aby sa deti vzdelávali aj v oblasti používania internetu a vedeli reagovať v prípade nebezpečenstva, nevhodného obsahu stránok a podobne. Rodičia by nemali podobné riešenia vnímať ako náhradu za prístup k deťom, tieto riešenia by mali byť pre nich len pomocníkom pre získanie prehľadu v návykoch ich detí pri surfovaní na internete.

Autormi materiálu sú: Ondrej Bialko, Miroslav Drobný, Eva Dzurindová, Katarína Gondová, Silvia Guničová, Stanislava Chlastáková, Vladimír Kanás, Andrea Kerestešová, Lívia Kramárová, Patrik Krauspe, Michal Lavrinčík, Peter Lupták, Silvia Nagyová, Jaroslav Oster, Tibor Papp, Mária Pšenáková, Peter Stopiak, Katarína Trlicová, Kristián Ujváry, Ľudmila Václavová a ďalší.

Za obsah projektov zodpovedajú výlučne jeho realizátori a nemusí vyjadrovať názor Európskeho spoločenstva.