Jsem SAFE na netu.

Průvodce pro děti, mládež a rodiče

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Zlínský kraj

ŠIKULA
Dům dětí a mládeže Uh. Hradiště

ICM
Informační centrum pro mládež Uherské Hradiště

MAS STAROMĚSTSKO

MAP ORP UH II

ICM
Uherské Hradiště

INFORMAČNÍ CENTRUM PRO MLÁDEŽ
Masarykovo náměstí 21
686 01 Uherské Hradiště
Tel.: 572 525 526
E-mail: icm@icm.uh.cz
www.icm.uh.cz

NABÍZÍME:

- přehledy kroužků pro děti i dospělé
- nabídku letních táborů a brigád
- informace o možnostech studia
- informace o práci v zahraničí
- bezplatnou inzerci na webu a na nástěnce v ICM
- místo pro setkávání
- informace o akcích v regionu

SLUŽBY:

- internet a možnost užití PC
- kopírování, tisk, skenování
- tisk na 3D tiskárně
- prodej slevových karet ISIC, ITIC a ISIC Scholar

POŘÁDÁME:

- akce, soutěže, workshopy
- výukové programy
- OMG - výukový program O Mediální Gramotnosti pro školy
- Hradišťskou hledačku a šifrovačku - poznávání historického
- centra města UH zábavnou formou
- pravidelné besedy:
- **CESTY** - cestopisná beseda každé 3. úterý v měsíci
- **JAZYKOVÁ KAVÁRNA** - bezplatná anglická konverzace nad šálkem kávy

Informační centrum pro mládež Uherské Hradiště

icm865

ŠIKULA

DŮM DĚTÍ A MLÁDEŽE
UHERSKÉ HRADIŠTĚ
příspěvková organizace
Purkyňova 494,
686 06 Uherské Hradiště
tel.: 572 551 347, mobil: 737 923 842,
e-mail: info@ddmsikula.cz, www.ddmsikula.cz

„Šikula, váš kamarád ve volném čase.“

Co u nás můžete zažít? Jak super trávit volný čas? Co vám nabízíme?

Kroužky – pravidelné setkávání v kroužcích a kurzech s různým zaměřením

- **Sportovní a taneční** – sport, tance, geocaching, ...
- **Estetické** – výtvarka, keramika, tvoření, DIY móda,---
- **Společensko vědní** – fotografický, hra na hudební nástroje, kapela, jazykové,...
- **Přírodovědné** – kroužky o zvířátkách a se zvířátky, myslivecký, badatelský, cestovatelský, technický,...
- **Příprava na přijímací řízení na střední školy**
- **Kluby dětí a maminek**

Kroužky jsou určeny jak pro děti, tak pro dospělé. Určitě si vyberete z naší široké nabídky .

Akce – pravidelně nepravidelné „dění“ v Šikulovi – pořádáme soutěže, přehlídky, akce spojené s různými tématy, výstavy, atd.

Kurzy a vzdělávání – se zaměřením zejména pro dospělé na environmentální výchovu, kurzy vzdělávání externích pracovníků, kurzy pro táborníky, atd.

Výukové programy – programy jsou zaměřené na finanční gramotnost, environmentální výchovu, dopravní výchovu

Příměstské a pobytové tábory – nabízíme každoročně více než 30 táborů, kde si každý zájemce určitě najde ten svůj.

Bližší info na www.ddmsikula.cz a www.trnka.xf.cz a fc.

ÚVOD

Projekt **„Jsem SAFE na netu“** má za cíl tě naučit správným návykům internetové bezpečnosti.
Na internetu najdeš spoustu fajn věcí, které tě baví, nebo se ti hodí třeba do školy. Potkáváš tam kamarády, spolužáky, ale samozřejmě i úplně cizí lidi. Ne vždy ale víš zcela jistě, jestli ten člověk, se kterým si píšeš, je vážně ten, za koho se vydává. Musíš proto vědět, **na co si dát pozor a co dělat** v případě, že tě na internetu potká něco nepříjemného. **Ne každému můžeš věřit a ne všechno pochází z důvěryhodného zdroje**. Je proto dobré být opatrný na své osobní údaje a vždy si rozmyslet, co budeš na síti sdílet. Vždycky je lepší vědět, co se ti může stát a jak tomu předcházet. Někdy tě může i zdánlivě zcela neškodná věc přivést do hodně nepříjemné situace. Pokud se ti něco stane, nenechávej si to pro sebe. **Máš se vždycky komu svěřit**. Pokud se o tom nechceš bavit s rodiči, máš ještě spoustu dalších možností. **Nikdy v tom nejsi sám!** Proto jsme vydali tuto brožurku s důležitými informacemi a kontakty, na které se můžeš obrátit pro pomoc. Věříme, že to pro tebe i tvé rodiče bude zajímavé čtení a pomůže ti cítit se na internetu bezpečněji.

Brožura byla vydána v rámci projektu „Jsem SAFE na netu“. Vydal ji Dům dětí a mládeže Uherské Hradiště ve spolupráci s Informačním centrem pro mládež Uherské Hradiště v roce 2019 a byla finančně podpořena Zlínským krajem a projektem Místní akční plán ORP Uherské Hradiště II, registrační číslo CZ.02.3.68/0. 0/0.0/17_047/0008649, který je spolufinancovaný z prostředků EU, Operačního programu Výzkum, vývoj a vzdělávání, a státního rozpočtu.

Grafické zpracování a tisk: JOKER, spol. s.r.o.
Kresby: Lenka Kodrlová
Náklad: 2000 ks

KYBERŠIKANA

(kybernetická – počítačová šikana, angl. cyberbullying)

Jde o **druh šikany využívající informační a komunikační technologie** (počítače, tablety, mobilní telefony, sociální sítě, emaily apod.) **k ublížení druhému** (vydírání, ubližování, ztrapňování, obtěžování, ohrožování, zastrašování apod.). Aktéry kyberšikany jsou (obdobně jako u klasické šikany): **Agresor – Oběť – Přihlížející** (publikum).
Je to naprosto zásadní problém současné společnosti, hlavně mládeže.

ZNAKY KYBERŠIKANY:

Anonymita

Útočník zpravidla vystupuje anonymně, pod falešnými přezdívkami (nicky), vytváří jednoúčelové e mailové schránky nebo falešné profily na sociálních sítích, a díky tomuto pocitu anonymity je posílena jeho odvaha v použití agresivnější formy útoku. Z technologického hlediska je tato anonymita však pouze vzdušným zámkem, neboť odhalení takového útočníka dnes pro Policii ČR není velkým problémem. Problém může nastat z hlediska právní stránky, neboť kyberšikana není právně nijak vymezena, a je-li právně kvalifikována jako přestupek, nemá za současného právního stavu policejní orgán příliš možností, jak důkazní materiál (provozně lokalizační údaje) vyžádat.

Profil útočníka

Ve virtuálním světě neplatí pravidla klasické šikany – nezáleží zde na věku, pohlaví, fyzické síle útočníka, sociálním postavení apod. Převládají převážně znalosti a dovednosti v užívání informačních a komunikačních technologií.

Místo a čas útoku nelze předpokládat

Zatímco u klasické šikany lze předpokládat, kdy a kde k útoku dojde (o přestávce ve třídě, po vyučování před školou, v odpoledních hodinách na hřišti apod.), u kyberšikany útok může přijít kdykoliv a kdekoliv. Třeba o půlnoci a prostřednictvím různých kanálů: SMS, e-mailem, videem na videoportálu (např. youtube.com), příspěvkem na sociální síti.

V šíření kyberšikany pomáhá útočníkovi „publikum“

Zejména možnost sdílení nebo následné přeposílání závadových příspěvků zvyšuje intenzitu vedeného útoku. Útočníkovi tedy postačí příspěvek publikovat pouze jednou, o jeho opakování a šíření se často postará ono „publikum“. Jednání tohoto publika nepřímo ale velice důrazně zvyšuje negativní psychický dopad na oběť.

Není snadné rozeznat dopad kyberšikany na oběť

Vzhledem k tomu, že dopady kyberšikany jsou spíše v rovině psychické, je nesnadné je na oběti rozeznat nebo poznat oběť samotnou. Na rozdíl od klasické šikany u kyberšikany je o mnoho složitější vysledovat varovné signály – modřiny, potrhané a špinavé oblečení apod. Oběť se často uzavírá do sebe a přestává komunikovat s okolím, ať už ze strachu, že útočník zintenzivní své útoky, ze studu nebo strachu z nepochopení problému rodiči nebo učiteli.

Dlouhodobé působení na oběť

Klasickou šikanu může tvořit soubor jednotlivých útoků, které se mohou opakovat, ale útok jako takový má vždy svůj konec. Naopak útok vedený prostřednictvím informačních a komunikačních technologií v nadneseném slova smyslu nemusí skončit vůbec. Je-li oběť zesměšňována např. prostřednictvím sociální sítě, nemusí se jí podařit legitimními prostředky dosáhnout smazání inkriminovaného příspěvku nebo se po výmazu příspěvek může objevit znova a třeba prostřednictvím jiné sociální sítě a jiného agresora. V tomto případě lze hovořit o opakovatelnosti útoku jako takového a řešením není ani „odstěhování se“ z místa, kde byla oběť původně šikanována.

**To, co se internetu zveřejní,
již povětšinou nelze vzít zpět!**

Nejčastější projevy kyberšikany:

- Pomlouvání, urážení, zastrašování, ponižování a zesměšňování
- Pořizování audio a video záznamů, fotografií, jejich následná úprava a zveřejnění s cílem poškodit oběť
- Pořizování video záznamů spojené s předem připraveným fyzický útokem (Happy Slapping)
- Krádež identity a následné vystupování útočníka pod identitou oběti
- Odhalování cizích tajemství
- Vydírání pomocí informačních a komunikačních technologií
- Kyberstalking – obtěžování a pronásledování pomocí informačních a komunikačních technologií
- Další formy kyberšikany (provokování a napadání uživatelů v diskuzních fórech, ostrakizace atd.)

Kyberšikana je nebezpečná!

Účinky kyberšikany jsou mnohem silnější a následky mnohem závažnější než u klasické šikany.

- Oběť často neví, kdo a proč jí ubližuje
- Do šikany v kyberprostoru se zapojuje více agresorů
- Ponižující příspěvek nebo jiný druh kyberšikany je STÁLE na internetu, čímž oběť vystavuje stresu, jehož intenzita se nezmírňuje – nenastává úleva
- Velké množství uživatelů internetu může sledovat ponížení oběti
- Pocit bezmoci, oběť nabývá pocitu, že se nemá kam obrátit

Symptomy kyberšikanovaného dítěte:

- Dítě zásadně změní své návyky při používání PC, mobilu, sociální sítě atd. (např. časté užívání vystřídá střídmé, až minimální)
- Během a po pobytu na internetu je smutné, rozzlobené, zoufalé
- Při oznámení SMS prožívá negativní emoce, frustraci, vztek atd
- Brání se diskuzi o tom, co na počítači dělá, s kým si píše, kdo mu poslal SMS atd
- Omezuje dřívější vztahy s rodinou, kamarády, uzavírá se do sebe
- Redukuje své koníčky a záliby, nebo se do nich naopak pouští s velkou vervou
- Trpí poklesem pracovní výkonnosti, zhoršením prospěchu, problémy s chováním, potyčkami se spolužáky, drzým chováním k učitelům
- Vyhýbá se skupinovým aktivitám, shromáždění, kde hrozí, že se potká se spolužáky
- Vykazuje změny nálad, chování, spánku nebo jeví známky deprese a úzkosti
- Vymlouvá se na cokoli, jen aby nemuselo do školy (nejčastěji na bolesti břicha, hlavy, nevolnost atd.)
- Ze školy se naopak může začít vracet později než obvykle, bez zjevné příčiny
- Omezená chuť k jídlu až nechutenství
- Sklony k nespavosti, špatnému usínání a nočním můrám
- Vyhledávání blízkosti učitelů
- Působí vystrašeně, zakřikle, a přitom ve svém projevu může problematiku kyberšikany zlehčovat a ujišťovat o tom, že žádný problém není. Dítě se může za situaci stydět a snažit se ji za každou cenu neprozradit dalším aktérům
- Mohou se střídat chvíle apatie a agresivity
- Dítě se nedokáže soustředit, je roztěkané

K dalším faktorům zvyšujícím riziko kyberšikany patří také:

- Nezájem rodičů o výchovu a virtuální život potomka
- Nedostatečná, či žádná komunikace o činnostech na PC
- Počítač sloužící jako chůva dítěte bez zavedení pravidel a kontroly
- Neřízená komunikace a užívání sociálních sítí
- Vlastní nevhodné využívání moderních technologií, rodič před dítětem komunikuje s ostatními uživateli vulgárně, zveřejňuje nepatřičné příspěvky, osobní údaje atd
- Nezájem o preventivní programy řešící kyberšikanu na škole
- Psychické rozpoložení dítěte, přílišná agrese, přecitlivělost, přeceňování hodnocení ostatními a důraz na virtuální obraz

Zdroj: příručka Prevence a diagnostika symptomů oběti kyberšikany pro pediatry, autor: Mgr. Lukáš Látal, www.internetembezpecne.cz

AGRESOR

Při analýze chování pachatelů šikany jsme byli léta zvyklí úlohu a pozici pachatele zjednodušovat – pachatel byl jednoduše agresor, kterého bylo třeba potrestat. S příchodem kybernetických forem šikany se však situace stala složitější – u řady pachatelů dochází k tzv. přepínání rolí (z oběti na pachatele) a svůj útok vnímají jako oprávněnou pomstu za násilí, které vůči nim spáchal někdo jiný. U dalších pachatelů je pak kyberšikana spíše nezvládnutým žertem, který se vymknul kontrole (např. v prostředí sociálních sítí). Na pachatele kyberšikany se proto podíváme podrobněji.

Kdo jsou vlastně pachatelé?

Mezi pachateli najdeme stejně tak žáky s dobrým i špatným prospěchem, bohaté i chudé, děti chytřejší i méně chytré apod.

Pachatelem může být kdokoliv!

Pachatelé kyberšikany si zpravidla kladou za cíl zranit, vystrašit a ponížit oběť, a to buď veřejně, nebo v soukromí (Kohut, 2007), nicméně v posledních letech se objevuje stále více případů, kdy ke kyberšikaně došlo neúmyslně – pachatel nechtěl oběti ublížit, ale pouze se pobavit na její úkor (případně pobavit konkrétní skupinu – např. spolužáky). Bohužel postupně ztratil nad kyberšikanou kontrolu.

Základní klasifikace pachatelů kyberšikany vychází z charakteristiky agresorů v rámci tradiční šikany.

Agresory lze pro základní pochopení rozdělit na dvě skupiny:

1. Na jedné straně existují agresoři, kteří mají **nižší sebevědomí**, snížené sociální dovednosti, trpí pocity nejistoty, nedostatečného uznání a osamělostí (Shariff, 2008). V kolektivu bývají neoblíbeni a šikanování ostatních je reakcí na pocit vlastní nedostatečnosti a frustrace -šikanují, protože získaný pocit moci jim pomáhá kompenzovat jejich vlastní nedostatky (Černá, Dědková, Macháčková, Ševčíková, & Šmahel, 2013). Často tak šikanují proto, aby si upevnili svoji pozici ve skupině a uspokojili svou touhu po převaze a moci (Olweus, 1993).

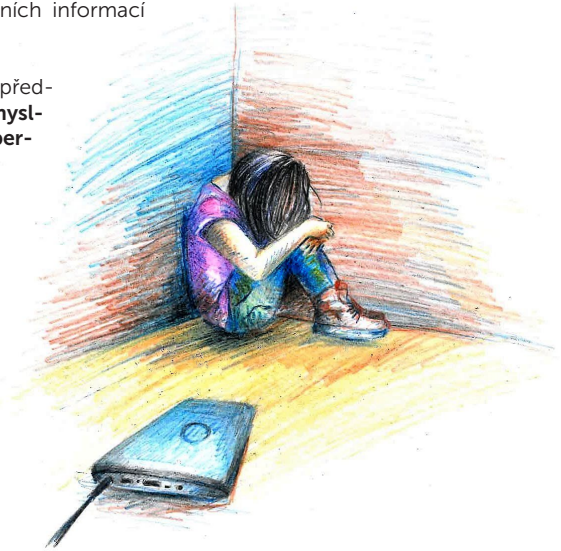
2. Na straně druhé však existují agresoři, kteří jsou naopak **v kolektivu uznávaní**, mají velký okruh přátel, vyšší sociální dovednosti i sebevědomí a tyto vlastnosti využívají k obratnému manipulování ostatních (Sutton, Smith, & Swettenham, 1999). Tento typ agresorů dokáže dobře odhadnout jednotlivé procesy ve skupině a využít je ve svůj prospěch – šikana je pak nástrojem pro získání dobrého postavení v kolektivu.

Mezi základní motivy, které se při šikanování uplatňují, patří:
(Kolář, 2011; Šmahaj, 2014)

a) motiv upoutání pozornosti – agresor se snaží být středem pozornosti, snaží si získat přízeň spolužáků,
b) motiv zahnání nudy – šikanování přináší agresorovi vzrušení a zábavu,
c) motiv Mengeleho – agresor zkoumá, co oběť vydrží, dochází ke stupňování těchto pokusů, a to jak na psychické, tak fyzické úrovni,
d) motiv prevence – častý pro oběti šikany, které přejdou do nového prostředí a ve snaze předejít šikanování začnou samy šikanovat, případně se přidají k nějakému agresorovi,
e) motiv vykonat něco velkého – tento motiv u neúspěšných žáků vyvolává pocit, že prostřednictvím šikanování jsou schopni výkonu a že se oni sami stávají příčinou významného děje.

Mezi **další motivy** (Ministerstvo školství, 2009) patří nuda, kulturní konflikty, spory ve třídě, rozpad přátelství, proměna třídního kolektivu, zveřejnění osobních informací apod.

Specifický typ představují tzv. **neúmyslní pachatelé kyberšikany**.



TYPY AGRESORŮ:

Typ Anděl pomsty („The Vengeful Angel")

Základem motivace prvního typu agresora je odplata, pomsta za příkoří, které se stalo samotnému pachateli nebo jeho přátelům. Pachatel sám sebe nevnímá jako někoho, kdo páchá šikanu či kyberšikanu, vnímá se jako ten, kdo napravuje spáchané křivdy a chrání sebe a ostatní před „padouchy", na které sám útočí. Anděl pomsty zahrnuje typické oběti tradiční šikany či kyberšikany, u kterých proběhlo přepnutí role a stali se z nich útočníci.

Typ („Power-Hungry" & „Revenge of the Nerds")

Typ agresora, který je označovaný jako „power-hungry aggressor", tedy agresor „bažící po moci", touží především dávat ostatním najevo svou autoritu a vnucovat jim svou vůli. Tito pachatelé chtějí ostatním ukázat, že jsou dostatečně silní přinutit ostatní dělat to, co sami chtějí, případně ostatní ovládat prostřednictvím strachu. Vyžadují publikum – publikum nemusí být početné, může být složeno z několika přátel nebo spolužáků. Potřebují, aby bylivnímáni jako silní a hroziví, často se svými aktivitami chlubí. Chtějí vyvolat reakci publika, a aby této reakce dosáhli, stupňují své útoky tak dlouho, než příslušnou odezvu vyvolají.

Typ Zlé dívky („Mean Girls")

Pachatel tohoto typu provozuje kyberšikanu zejména proto, že se nudí a hledá zábavu. Agresory jsou v tomto případě nejčastěji dívky. Ty se pak v útocích zaměřují nejčastěji na jiné dívky, méně často na chlapce. Kyberšikana realizovaná tímto typem agresora je obvykle páchána ve skupině, případně je skupinou alespoň plánována. Tento typ kyberšikany vyžaduje publikum (agresoři chtějí, aby publikum vědělo, že mají dostatek sil šikanovat ostatní). Cílem útočníků je především pobavit se – a to na úkor vyhlédnutých obětí. Pachatelé touží po obdivu a jejich útoky jsou přiživovány pasivitou přihlížejících, kteří v průběhu kyberšikany nezasáhnou.

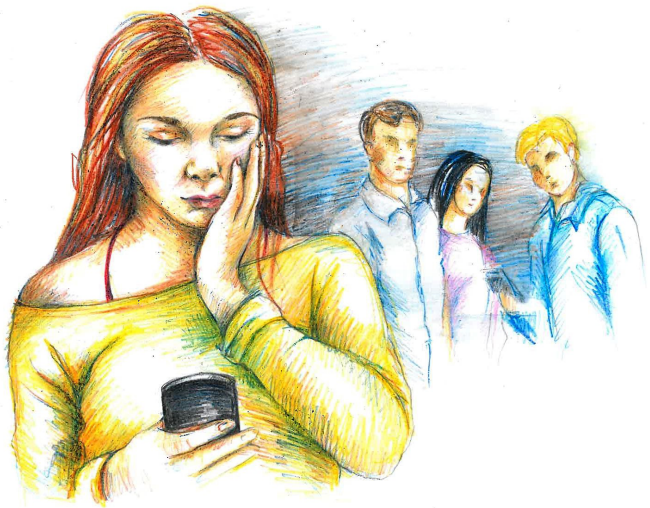
Neúmyslný pachatel („Inadvertent Cyberbully")

Neúmyslný pachatel sám sebe nevnímá jako agresora, do kyberšikany se zapojuje bezděčně, neplánovaně, neúmyslně. Tito pachatelé mají ve zvyku reagovat ve vzteku, nebo když jsou frustrováni, nepřemýšlejí o následcích svého jednání (Vašutová et al., 2010). Často na internetu vystupují pod cizí identitou, pod kterou mohou posílat typické šikanující zprávy ostatním uživatelům. Jejich motivy se dají definovat slovy „můžu" a „legrace". Neúmyslní pachatelé kyberšikany často věří, že bylo jejich chování neškodné, pouze se bavili nebo si s obětí pohrávali.

Jak je to s těmi jedničkáři?

Z výzkumů vyplývá, že z toho, jak je žák či student ve škole úspěšný, nelze vyvozovat, že nebude týrat ostatní vrstevníky a nebude původcem kyberšikany. Z tohoto důvodu není snadné původce kyberšikany v komunitě dětí identifikovat a v řadě případů byli učitelé i rodiče šokováni, že někteří velmi dobří žáci či studenti mohou být do šikany či kyberšikany zapojeni. Je mýtem, že by původci kyberšikany byli mezi učiteli a dětmi všeobecně známí („známé firmy").

Zdroj: www.e-bezpeci.cz



JAK SE CHRÁNIT PŘED KYBERŠIKANOU?

- Respektovat ostatní, nevyvolávat zbytečné konflikty ve skutečném ani virtuálním světě
- Nesdělovat citlivé informace, které by mohly být zneužity: nezveřejňovat osobní údaje, osobní fotografie, hesla k elektronickým účtům, nesvěřovat se se svými problémy, neřešit svou sexualitu atd. Umístěním na internet nad těmito materiály ztrácíme kontrolu
- Nebýt přehnaně důvěřivý (výzkumy ukazují, že většina lidí ve virtuální komunikaci lže)
- Seznámit se s pravidly služeb internetu a GSM sítí
- Seznámit se s riziky, která souvisí s elektronickou komunikací

JAK SE BRÁNIT KYBERÚTOKŮM?

- **UKONČIT** – přestat komunikovat s útočníkem, nemstít se
- **BLOKOVAT** – zamezit útočníkovi přístup k oběti i k dané službě (kontaktovat poskytovatele služby, zablokovat si přijímání útočníkových zpráv nebo hovorů, změnit svou virtuální identitu)
- **ODHALIT PACHATELE** – pokud je to možné (např. podle profilu)
- **OZNÁMIT** – oznámit útok dospělým, schovat si důkazy pro vyšetřování (např. zprávy videozáznamy, odkazy na weby, blogy)

Zdroj: www.e-bezpeci.cz

NEJČASTĚJŠÍ DRUHY KYBERŠIKANY:

Existuje v zásadě několik „standardizovaných" druhů kyberšikany.

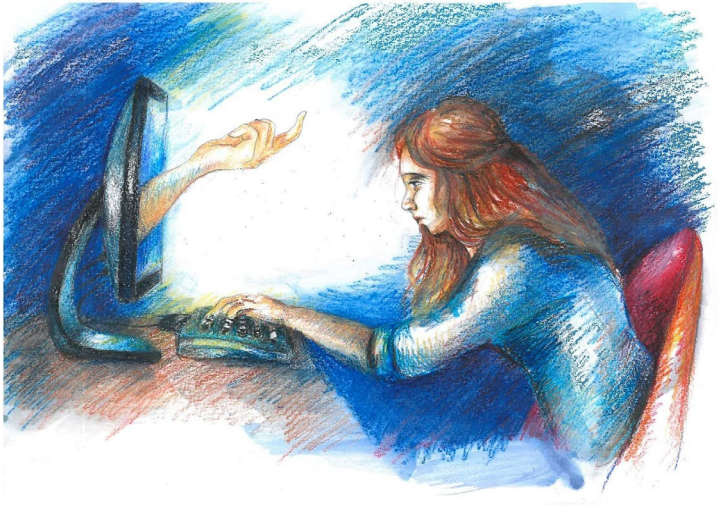
„Fanouškovská stránka" na Facebooku, Instagramu, ale třeba i ve formě samostatné webové stránky má za cíl systematickou, dlouhodobou a stupňující se dehonestaci a šikanu oběti. Útočníci vytvoří stránku, kde zveřejňují různé srážející komentáře, fotomontáže a podobně. Někdy na stránku hodí i tzv. Google bombu – tj. odkazují na ni z nesouvisejících stránek, např. z diskusí pod články, čímž zlepšují její pozici ve vyhledávači. Naštěstí Evropská komise rozhodla o právu občanů EU na ochranu proti těmto praktikám, takže je možné Google i další vyhledávače požádat o vymazání dané stránky z výsledků vyhledávání. U stránky na Facebooku či Instagramu je zase nutné požádat o její zablokování.

Sdílení nelichotivých fotek (a fotomontáží) či videí na sociálních sítích nebo třeba e-mailem je další forma kyberšikany. Útočníci fotky často získávají přímo ze sociálních sítí oběti, v horším případě z její soukromé konverzace, kdy zejména dívky neuváženě posílají své vyzývavé fotky chlapcům, o které mají zájem. Ti je někdy, například z pomsty, neváhají zveřejnit. Někdy se je dokonce snaží od dívek vylákat. Nelichotivé fotky se mohou zrodit i na různých party a v neposlední řadě se objevují fotky a videa zachycující skutečnou šikanu, jež pak přerůstají v kyberšikanu. To se týká i mnoha známých českých případů útoků dětí na učitele.

Sdílení lží online je další častá praktika. Mohou to být i relativně „nevinné" lži, že ten či onen chodí s tím a tím. Nejhrozivějším příkladem kyberšikany tohoto druhu byly právě zmíněné „roztahovačky", kde byly zveřejňovány fotografie nezletilých dívek doplněné o informace například o tom, jak jsou či nejsou náruživé. Fotografie často byly ukradeny z jejich vlastních profilů na Facebooku. Lživé a šikanující přitom mohou být i příspěvky v diskusích.

Sdílení osobní komunikace, korespondence a dokumentů je jednou z nejzávažnějších forem kyberšikany. Oběti to vnímají jako největší proniknutí do svého soukromí. Přitom cizí deníčky a milostné dopisy se čítávaly nahlas už od nepaměti. V kyberprostoru je to však jiné – co se zde jednou objeví, nikdy nezmizí. Celá věc je o to bolestnější, že vše obvykle nepochází od samotné oběti, ale od někoho blízkého, komu oběť důvěřovala. Například od bývalého partnera.

Zdroj: www.vimkamklikam.cz



KYBERGROOMING

Kybergrooming lze vysvětlit jako psychickou manipulaci dítěte dospělým prostřednictvím moderních komunikačních technologií s cílem získat důvěru oběti, vylákat ji na osobní schůzku a zpravidla sexuálně zneužít.

Kybergrooming se nejčastěji vyskytuje v rámci instant messengerů (Facebook Messenger, Skype), sociálních sítí (Facebook, Twitter, Badoo), internetových seznamek (libimseti.cz) a různých blogovacích stránek.

Obětí kybergroomingu se může stát prakticky kdokoliv, zpravidla se ale jedná o dívky ve věku 11-17 let, často užívající informační a komunikační technologie, trpící nedostatkem sebedůvěry, pocitem osamění. Jsou otevřené manipulaci a neznalé rizik internetové komunikace.

Kybergroomer je zpravidla sexuální útočník využívající informační a komunikační technologie k prosazení svého cíle. Často se vydává za jinou osobu, než ve skutečnosti je, dle vybrané oběti. Pokud se snaží spřátelit se s 12 letou dívkou, vydává se za 14 letého chlapce. Významnou vlastností kybergroomera (není však pravidlem) je trpělivost – vydrží si s obětí psát i několik měsíců, jen aby pevně získal její důvěru.

Typický průběh kybergroomingu

- Vzbuzení důvěry a snaha izolovat oběť od okolí
- Podplácení dárky, penězi, budování přátelského vztahu
- Získání nebezpečných materiálů k případnému vydírání
- Emocionální závislost oběti na útočníkovi
- Osobní schůzka
- Sexuální obtěžování, zneužití

Nenechávejte své děti na internetu bez dozoru!

Jak kybergroomingu předejít?
Předejít kybergroomingu můžou rodiče důslednou kontrolou činnosti svých dětí v internetovém prostředí. V tomto případě je třeba odložit předsudky o narušování soukromí svého dítěte a na celou věc nahlížet tak, jako by bylo dítě hlídáno v hustém silničním provozu. Zde by každý rodič své dítě držel pevně za ruku a raději vodil – v internetovém provozu by to mělo být obdobné!

KYBERSTALKING

Kyberstalking lze jednoduše nazvat nebezpečným pronásledováním. Útočník využívá informační a komunikační technologie k dlouhodobému, opakovanému a stupňovanému kontaktování – pronásledování své oběti, ve které chce úmyslně vyvolat pocit strachu o své soukromí, zdraví nebo život.

Některé formy kyberstalkingu:
- zasílání zpráv SMS
- telefonáty a prozvánění
- zasílání zpráv prostřednictvím messengerů a e-mailů
- opakované komentování příspěvků oběti na sociálních sítích
- vkládání příspěvků na profily sociálních sítí oběti
- krádež identity oběti – následné vystupování jejím jménem
- kontaktování oběti pod falešnou identitou (několika falešnými identitami)
- monitorování počítače oběti speciálními programy (keyloggery apod.)
- zveřejňování informací ze života oběti
- obtěžující kontaktování přátel oběti aj.

Některé motivy kyberstalkera:
- obtěžovat, vyhrožovat a vydírat oběť
- demonstrovat svou sílu
- poškodit oběť před společností
- opětovné navázání vztahu po odmítnutí aj.

Zprávy ani další případný materiál (fotografie, audiovizuální záznamy apod.) je důležité nemazat a policii předložit jako důkaz!

Jak se bránit?
Kyberstalkingu lze předcházet již ochranou svých dat na internetu.

- užívat kvalitní a silná hesla a dodržovat pravidla tvorby bezpečného hesla
- věnovat pozornost informacím na sociálních sítích, které mohou vidět osoby mimo okruh přátel
- dodržovat pravidla bezpečného užívání internetu (zabezpečení připojení, počítače, mobilního telefonu atd.)
- v případě, že se skutečně oběť bude cítit ohrožena na svém soukromí, zdraví nebo dokonce životě, je třeba věc neprodleně oznámit na Policii ČR

Kyberstalking a právo
Kyberstalking lze za určitých podmínek právně kvalifikovat jako trestný čin Nebezpečné pronásledování podle § 354 trestního zákoníku. Mezi základní podmínky patří, že útočník musí oběť dlouhodobě vytrvale prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktovat a toto jednání je způsobilé vzbudit v oběti důvodnou obavu o její život nebo zdraví nebo o život a zdraví osob jí blízkých. Okolností přitěžující dle § 354 odst. 2 písm. a) TZK je ta skutečnost, že uvedený čin je spáchán na dítěti.

Zdroj: www.internetembezpecne.cz

SEXTING

Slovo sexting je spojení slov sex a textování a znamená posílání textového, fotografického, audio a video obsahu se sexuálním podtextem prostřednictvím informačních a komunikačních technologií.
Takový obsah, zasílaný převážně v rámci milostného vztahu, je zejména po jeho ukončení zneužit k poškození druhé strany jeho zveřejněním nebo výhrůžkou jeho zveřejnění.
Sexting, v němž figurují nezletilé a mladistvé osoby, může být z právního hlediska kvalifikován i jako trestný čin.
Jedná se o velmi rizikové chování!

Rizika sextingu:

- potencionální útočník obdrží citlivý materiál, který může v budoucnu zneužít
- v případě zveřejnění citlivého materiálu na internetu je prakticky nemožné tento materiál „smazat" – může být zneužit i po velice dlouhé době od zveřejnění
- trestní odpovědnost za šíření sextingu
- sexting se často stává prostředkem pro vydírání dětí v rámci tzv. kybergroomingu

Sextingem potencionální útočník obdrží citlivý materiál, který může v budoucnu zneužít!

Bohužel, takto zaslaný obsah (video, fotografie, text) se může stát „časovanou bombou" – data si již ve světě internetu žijí svůj vlastní „život", a není možná kontrola nad tím, kdo jej sdílel, kdo si jej kam uložil anebo kdo, kdy a kde jej opět předvede reálnému světu.

JAK SE BRÁNIT?
Jedinou a účinnou obranou proti zveřejnění sextingového obsahu je takový nepořizovat a neposílat! Ani kamarádům a známým!

Zdroj: www.internetembezpecne.cz

WEBCAM TROLLING

V poslední době se na internetu objevuje nový fenomén nazývaný webcam trolling. Především děti jsou podvodem lákány na erotické videohovory přes oblíbené komunikační nástroje.

Získané intimní záběry pak podvodníci umisťují na internet, nebo je využívají k manipulaci a vydírání.

Podvodníci mohou člověka **napálit velice jednoduše**. Stačí, aby si na internetu zakoupili speciální program, který dokáže vytvářet virtuální webkameru. Ta se chová jako skutečná webkamera, místo sebe sama ale díky ní útočník může nechat zobrazit předehrané záběry atraktivních dívek nebo mladých chlapců (videosmyčku) v chatovacích programech, jako je například Skype či ICQ.

S nainstalovaným doplňkem, který je možné na černém trhu sehnat už za 200 korun, pak může oslovit libovolného člověka. Komunikace pak zpravidla probíhá v duchu lechtivých témat a **útočník čeká, až mu protistrana ukáže svoje intimní partie**. Oběť zpravidla ani netuší, že je hovor nahráván a že video může být zneužito.

„Nejrozšířenější jsou servery s videosekvencemi dětí, hlavně pak chlapců ve věku 13-18 let," uvedl Martin Kožíšek, manažer pro internetovou bezpečnost společnosti Seznam.cz.
„Chování obětí naznačuje, že jsou jedinci vyzváni dívkou nebo dívkami k erotickému pokecu, následují výzvy k ukázání intimních partií, případně onanii. Existují videa, kdy se požadavky útočníků specializují na konkrétní sexuální praktiky a obzvláště velký počet zhlédnutí pak mají videa, kde je zobrazeno více obětí najednou," konstatoval Kožíšek.

„**Oběti jsou zmanipulovány** takovým způsobem, že v několikaminutové stopáži dokážou plnit příkazy útočníků a i heterosexuální jedinci jsou ochotni na videokameru s kamarády vyzkoušet různé sexuální praktiky se stejným pohlavím," varoval manažer pro internetovou bezpečnost společnosti Seznam.cz.

Odhalit podvodníka není jednoduché.

K získání intimních materiálů používají útočníci tak sofistikované metody, že je velmi obtížné je odhalit. Pozornější uživatelé si mohou všimnout absence zvuku ve videu.

„Pokud se uživatel či uživatelka na druhé straně webkamery například začne vymlouvat, že nemá mikrofon a nemůže tedy v reálném čase odpovídat, pravděpodobně se jedná o podvod. **Většina dostupných videosmyček totiž neobsahuje záznam zvuku**, zobrazené osoby pak na kameru zásadně nemluví, naopak komunikují s vámi pomocí textového chatu," doplnil Kožíšek.
„Další možností, jak prověřit, zdali se jedná o podvrh či skutečný přenos, je požádat osobu na webkameře, aby svou identitu potvrdila nějakým textovým vzkazem v reálném čase, který bude vidět na webkameře, například napíše na kus papíru své jméno, dnešní datum a nějaký domluvený vzkaz. Tak lze identitu komunikujících snadno potvrdit," poradil Kamil Kopecký, který na Univerzitě Palackého v Olomouci vede projekt E-Bezpečí.

Zdroj: www.novinky.cz

NETOLISMUS

Termín netolismus (příp. netholismus) lze vysvětlit pojmem závislost – v tomto případě závislost na virtuálních drogách, mezi které můžeme zařadit sociální sítě, počítačové hry, různé internetové služby, ale i užívání samotných zařízení jako např. mobilní telefon, televize apod. Takto závislou osobu označujeme slovem netholik.
Pojem droga – virtuální droga – je uveden záměrně, neboť je-li pojem návyková látka nahrazen za návykový proces, je snazší spatřit podobnost obou světů: pro neustálou potřebu sledovat nové statusy na Facebooku, nutkavost odpovídat přátelům na zprávy nebo netrpělivě čekat na jejich odpověď, sledovat displej telefonu, zda nepřišla nějaká zpráva, i bez notifikace zanedbávat své potřeby a povinnosti – tyto potřeby nalezneme i u osoby závislé na návykových látkách. Netolismus v pojetí závislosti na virtuálních drogách nebyl do současné doby oficiálně uznán ani diagnostikován, avšak v prostředí psychologů se dostává do popředí zájmu. Obecně se však dle dostupných pramenů psychologové neshodli na skutečnosti, zda lze závislost na internetu (a dalších virtuálních drogách) měřit, resp. zda vůbec existuje. Přesto lze dohledat mnoho studií, které uvádějí přesná procentuální čísla osob postižených netolismem v rámci zkoumaného vzorku osob. Způsob diagnózy však povětšinou není uveden. Přesnost takové studie je tedy diskutabilní. Z praxe jsou však známé případy netoliků, kterým jejich závislost změnila život nebo dokonce život vzala. I přes tyto případy z praxe však mnozí rodiče této hrozbě nevěnují dostatečnou pozornost. Ponechávají své děti nekontrolovaně napospas virtuálnímu světu v podobě časově nadměrného užívání počítače, tabletu nebo mobilního telefonu.
V případě muže netolika se závislost nejčastěji projevuje v nadměrném hraní počítačových her a sledováním pornografie, případě ženy netoličky se tato závislost nejčastěji projevujenadměrným užíváním sociálních sítí a internetových diskusních fór.

Dítě, které nenalezne zábrany k nadměrnému užívání informačních a komunikačních technologií ve svém rodiči – vzoru (který doufejme sám netolismem netrpí), takové zábrany nalézá velmi těžko (spíše vůbec) a snadněji netolismu podléhá. V kombinaci s nedostatkem životních zkušeností, naivitou, důvěřivostí, neopatrností a neznalostí zásad bezpečného užívaní internetu a komunikace na něm se tak lehce může stát obětí virtuálního predátora.

Pokud k výše uvedeným atributům dále doplníme dítě, které těžce navazuje přátelské vztahy, je introvertní, je sociálně vyloučeno z okruhů školních i mimoškolních vrstevníků, propadá netolismu velice snadno. Virtuální život je prostě snazší, ale zabere mnoho hodin strávených ve virtuálním světě. V tomto případě je však na místě hovořit o patologickém netolismu spočívajícím v prohlubování asociálního chování jedince. Neúspěchy v reálném životě jsou kompenzovány v tom virtuálním, čímž se nadále prohlubuje ona propast dělící tyto dva životy.

DRUHY NETOLISMU:

- **Závislost na virtuální sexualitě**
  Kompulzivní používání webových stránek pornografického zaměření.
- **Závislost na virtuálních vztazích**
  Nadměrné věnování se virtuálním vztahům (online seznamky, sociální sítě).
- **Internetové kompulze**
  Např. hraní online her, internetové nakupování, internetové sázení, virální videa atd.
- **Přetížení informacemi**
  Např. nadměrné surfování nebo nadměrné hledání v databázích.
- **Závislost na počítači (mobilním telefonu)**
  Nadměrné využívání počítače – zejména nadměrné hraní her.

(podle K. Young, 2004, doplněno autorem)

Znaky netolismu:

VÝZNAČNOST
Určitá aktivita se stane nejdůležitější v životě člověka a začíná ovládat jeho myšlení, cítění a chování.

ZMĚNY NÁLADY
Změny nálady v důsledku zapojení se do určité aktivity, které mohou být vnímány jako vyrovnávací strategie za účelem uklidnění se.

TOLERANCE
Proces, při kterém je nutno stále více aktivity k dosažení předchozí míry uspokojení. V praxi tedy např. roste délka času tráveného online.

ODVYKACÍ SYMPTOMY
Ukončení či omezení aktivity se projevuje abstinenčními symptomy.

RELAPS
Tendence opakovat dřívější vzorce závislostního chování.

Kdy jde o netolismus?
Nosnými znaky jsou zejména neschopnost jedince mít kontrolu nad svým užíváním internetu – zejména jeho nadužíváním a změny nálady v případě nemožnosti jej užívat.

(Shapira, Goldsmith, Keck, Khosla, & McElroy, 2000).

Obecné příznaky netolismu:

ZTRÁTA KONTROLY NAD ČASEM
Zvyšuje se tolerance, brzké vstávání či naopak ponocování z důvodu potřeby být online.

PSYCHICKÉ PROJEVY
Pocit prázdnoty, když člověk není u počítače či mobilu, rostoucí nervozita a neklid, když člověk nepoužívá počítač delší dobu, přemýšlení o počítači, když ho člověk zrovna nepoužívá, zatajování informací o závislosti, počítač/mobil jako únik od osobních problémů atd...

PSYCHOSOCIÁLNÍ PROJEVY
Narušení vztahů s rodinou, ztráta dřívějších přátel.

PROJEVY SPOJENÉ S PRACÍ
Méně vykonané práce, zanedbávání učení, zhoršující se prospěch.

NOMOFOBIE
Nomofobie (angl. Nomophobia – zkratka z „no mobile phobia"), ač by se nemuselo zdát, s netolismem úzce souvisí, zejména podstatou v závislosti na mobilním telefonu. Uvádí se, že se jedná o jednoho z velkých stresorů konce 20. a počátku 21. století, při kterém postižený jedinec trpí strachem ze ztráty mobilního signálu, tj. např. z nedostatečného pokrytí v některých oblastech (na horách), vybití baterie či ztráty samotného telefonu apod.
Dle vyjádření odborníků může nomofobie postihovat až 53 % všech uživatelů mobilních telefonů.

Zdroj: www.internetembezpecne.cz

Mobilní telefony mají v životě teenagerů výsadní postavení a tak není divu, že se ani jim kyberšikana nevyhnula. Naopak, s používáním mobilních telefonů se dokonce rozvinuly specifické praktiky šikany:

OUTING

Je nový pojem, který sice mezi teenagery často neuslyšíte, s jeho projevy se ale setkáte častěji: jde o fotografování a natáčení oběti v intimních a trapných situacích, například při převlékání nebo na toaletě, a následné zveřejnění takových materiálů, nejčastěji na internetu. Pachatelé outingu se někdy dokonce mohou snažit oběť vydírat a přimět ji, aby choulostivé informace o sobě zveřejnila sama.

HAPPY SLAPPING

Nic netušící oběť je fyzicky napadena skupinou útočníků. Další z pachatelů zároveň celý útok natáčí většinou pomocí videokamery v mobilním telefonu. Záznam se potom obvykle rozšíří na internetu nebo ho pachatelé rozesílají na mobilní telefony kamarádů svých a kamarádů oběti. Oběť je tak traumatizována několikanásobně: jak samotným útokem, tak i následným ponižujícím zveřejněním videa.

Existuje několik typů videí obsahujících násilí. Některá jsou jen zinscenována, jiná jsou tvořena úryvky z filmů, ostatní jsou nahrávky skutečných násilných činů. Stále častěji se na internetu objevují i videa zachycující znásilnění nebo smrt.

A asi není nutné připomínat, že jde o trestný čin!

Samotné mobily nejsou příčinou šikany, násilí je společenský fenomén, který nesouvisí s rozvojem technologií: teenageři procházejí obdobím, kdy chtějí zkoušet nové věci, zkoušet hranice, ukázat se před partou a být v něčem zajímaví. Často si přitom neuvědomí, že už dávno překročili mantinely nevinné legrace.

Kyberšikana tak často bývá nevědomá a neúmyslná, zraňuje ale úplně stejně.

Zdroj: www.bezpecne-online.saferinternet.cz

BEZPEČNÉ HESLO

Heslo je pro uživatele informačních a komunikačních technologií prvotní a základní ochrannou hradbou proti případným útočníkům, a proto je třeba heslu věnovat nemalou pozornost.

Co je nutné dodržet:

- délka hesla minimálně 8 znaků (doporučení 12 – 14 znaků)
- kombinace číslic, malých a velkých písmen a speciálního znaku(!, #, $, & apod.)

Určitě nepoužívat snadno uhodnutelná hesla:

- běžná slova samostatně
- jména blízkých osob
- jméno domácího mazlíčka
- datum narození
- běžná posloupnost čísel (123456, 11111111 apod.)
- očekávané náhrady znaků – např. A → 4, O → 0, S → $, I → 1

Existuje mnoho programů specializovaných na prolomení hesla (passwordcrackery) užívajících různých metod prolomení (slovníkový útok, bruteforce útok atd.).

Slovníkový útok – program nejprve vyzkouší zadanou sadu nejužívanějších hesel, kterou připraví útočník. Úspěšnost útoku je tedy závislá na kvalitě zadané sady slov (slovníku). Seznamy nejpoužívanějších hesel jsou na internetu volně ke stažení. Slovníkový útok má velice vysokou úspěšnost!

Metoda brute-force – tedy metoda hrubou silou, využívá všechny možné kombinace znaků, a je tedy značně závislá na výkonu počítače.

Zdroj: www.internetembezpecne.cz

Desatero bezpečného internetu

Drž se zásad o bezpečnosti na internetu a zbytečně neriskuj!

Pro bezpečí na internetu ti stačí dodržet jen pár důležitých, ale přitom jednoduchých zásad!

1.
Nedávej nikomu adresu ani telefon. Nevíš, kdo se skrývá za monitorem na druhé straně.

2.
Neposílej nikomu, koho neznáš, svou fotografii a už vůbec ne intimní. Svou intimní fotku neposílej ani kamarádovi nebo kamarádce - nikdy nevíš, co s ní může někdy udělat.

3.
Udržuj hesla (k e-mailu i jiné) v tajnosti, nesděluj je ani blízkému kamarádovi.

4.
Nikdy neodpovídej na neslušné, hrubé nebo vulgární maily a vzkazy. Ignoruj je.

5 .
Nedomlouvej si schůzku přes internet, aniž bys o tom řekl někomu jinému.

6.
Pokud narazíš na obrázek, video nebo e-mail, který tě šokuje, opusť webovou stránku.

7.
Svěř se dospělému, pokud tě stránky nebo něčí vzkazy uvedou do rozpaků, nebo tě dokonce vyděsí.

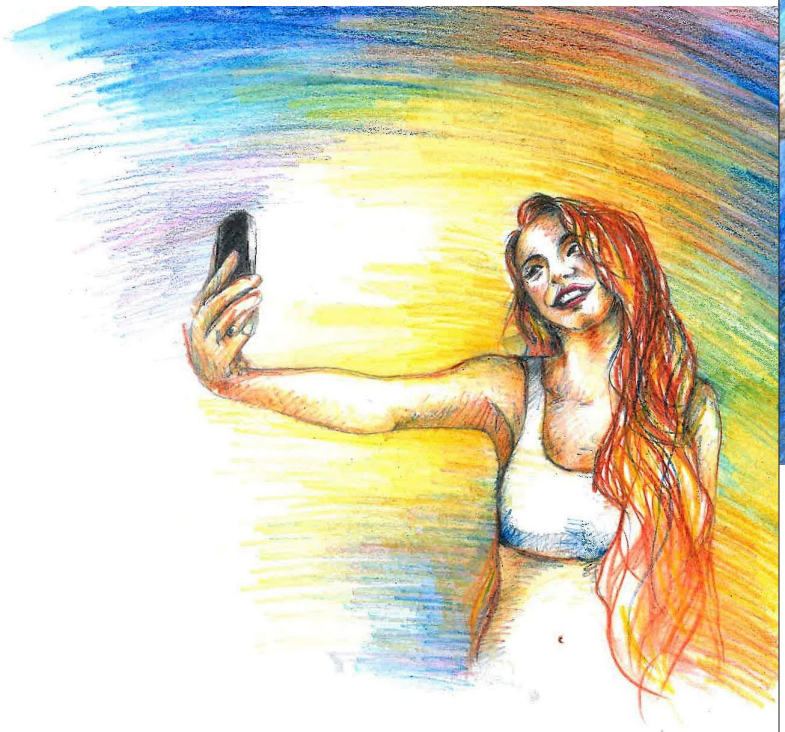
8.
Nedej šanci virům. Neotevírej přílohu zprávy, která přišla z neznámé adresy.

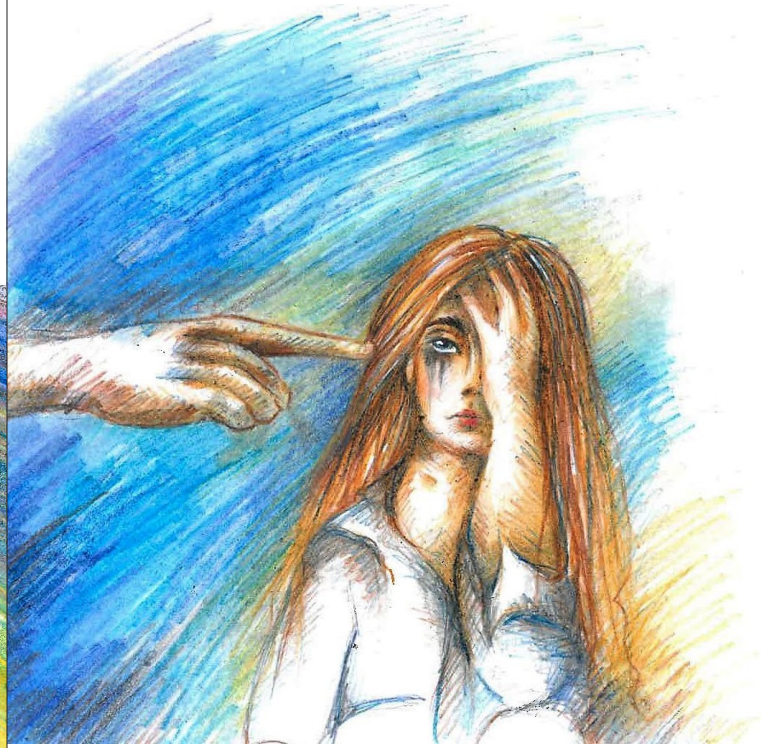
9.
Nevěř každé informaci, kterou na internetu získáš.

10.
Když se s někým nechceš bavit, nebav se.

Zdroj: www.bezpecnyinternet.cz

To, co se internetu zveřejní ...





... již povětšinou nelze vzít zpět!

ZÁKONY:

Víš, že svým příspěvkem či jen komentářem na sociálních sítích můžeš naplnit skutkovou podstatu hned několika paragrafů trestního zákoníku?

§181 – **Poškození cizích práv**
§184 – **Pomluva**
§345 – **Křivé obvinění**
§355 – **Hanobení**
§356 – **Podněcování k nenávisti**
§357 – **Šíření poplašné zprávy**
§364 – **Podněcování k trestnému činu**
§ 365 – **Schvalování trestného činu**
§404 – **Projev sympatií k hnutí směřujícímu k potlačování práv a svobod člověka**

KYBERŠIKANA:

- Pachatel se tímto jednáním může dopouštět například následujících trestných činů: ublížení na zdraví, vydírání, pomluva, násilí proti skupině nebo jednotlivci apod.
- Za tyto trestné činy může být potrestán odnětím svobody až na 4 roky.

KYBERGROOMING:

- Pod toto jednání mohou být zahrnuty následující trestné činy: obchodování s lidmi, vydírání, pohlavní zneužívání, nebezpečné pronásledování apod.
- Za spáchání těchto trestných činů mohou pachateli hrozit až 4 roky vězení.

SEXTING:

- Jedná se o závažný skutek, který může zanechat vážné následky na oběti.
- Patří sem následující trestné činy: znásilnění, pohlavní zneužití, výroba a jiné nakládání s dětskou pornografií, omezování osobní svobody, nebezpečné pronásledování apod.
- Výše trestu je 1 – 8 let.

ZNEUŽITÍ OSOBNÍCH ÚDAJŮ:

- Osoba, která zneužije naše osobní údaje, se může dopustit trestných činů: vydírání, útisk, neoprávněné nakládání s osobními údaji, poškození cizích práv, podvod apod.
- Výše trestu je 1 – 4 roky.

Kde hledat pomoc?

- **Linka bezpečí**
  www.linkabezpeci.cz; 116 111
- **Policie 158**
- **Pedagogicko – psychologická poradna**
  www.poradnazl.cz; 572 551 352 (UH)
- **Občansko právní poradny**
  www.uhradiste.charita.cz/nase-sluzby/obcanskaporadna- uherske-hradiste ; 606 453 502 (UH)
- **Středisko výchovné péče**
  www.svphelp.cz ; 572 564 520 (UH)

CO JE TO HOAX ?

Anglické slovo HOAX [:houks:] v překladu znamená: Falešnou zprávu, Mystifikaci, Novinářskou kachnu, Podvod, Poplašnou zprávu, Výmysl, Žert, kanadský žertík.

V počítačovém světě slovem HOAX nejčastěji označujeme poplašnou zprávu, která varuje před neexistujícím nebezpečným virem.

JAK HOAX POZNÁME?

Typický text poplašné zprávy obsahuje většinou tyto body:

Snaží se přesvědčit svojí důležitostí
Šokující informace, nové nebezpečí, naléhavá pomoc...

Důvěryhodné zdroje varují
Ve většině případů se pisatel poplašné zprávy snaží přesvědčit, že varování přišlo od důvěryhodných zdrojů („FBI varuje...", „Microsoft upozorňuje", „Zdravotnická organizace zjistila" atd...).

Nebo naopak tajná informace unikla
Údajná informace, o které oficiální média mlčí a nesmí se o ní mluvit, ale autor zprávy ji objevil a vyzývá k jejímu sdílení.

Výzva k dalšímu rozeslání
Tento bod HOAX vždy obsahuje! Je takovým hnacím motorem pro další šíření. Mnoho nezkušených uživatelů se nechá zprávou napálit a bez přemýšlení výzvu uposlechnou. Právě proto se tyto nesmysly lavinovitě šíří.

Jako hoax můžeme také označit šířenou zprávu, která obsahuje nepřesné, zkreslující informace, účelově upravené polopravdy nebo směsku polopravd a lží.

V praxi můžeme použít následující pravidlo:
Jestliže zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, je to podezřelé a s největší pravděpodobností HOAX. Občas to také může být původně opravdová prosba o pomoc, ale i ty svého největšího šíření dosáhnou v době, kdy jsou již neaktuální.

Pokud podobnou zprávu obdržíte a nemáte jistotu, můžete si prohlédnout některý ze seznamů HOAXů a určitě tam obdobu doručené zprávy najdete. Také pravděpodobnost, že byste stopnutím podezřelého e-mailu někomu uškodili, je minimální. Šířením hoaxů a jiných řetězových e-mailů se uživatel proviňuje proti pravidlům Netikety - pravidel chování na Internetu.

NEJČASTĚJŠÍ TYPY POPLAŠNÝCH E-MAILŮ:

- Varování před smyšlenými viry a různými útoky na počítač
- Popis jiného nereálného nebezpečí
- Zprávy varují před vymyšleným nebezpečím z běžného života - mimo oblast výpočetní techniky. Často obsahují směs lží a polopravd, které nezasvěcený člověk nemůže s jistotou posoudit.
- Falešné prosby o pomoc
- Kdysi skutečná prosba o pomoc, většinou se masově rozšíří až po její aktuálnosti. Typickým příkladem jsou prosby o darování krve pro nemocného člověka.
- Trapný pokus o žert, který útočí na základní lidské city.
- Fámy o mobilních telefonech
- Vymyšlené, zkreslené nebo neúplné informace o mobilních telefonech. Většinou bývají také masově šířené.

Petice a výzvy

Smyšlená petice jako žert.
Nedomyšlená snaha boje za určitou věc. Petice šířená e-mailem často neobsahuje potřebné údaje podepisujících se (pokud je lze takto označit), aby petice byla platná. Naopak, jestliže ke jménu připojíte další osobní údaje, dáváte je k dispozici komukoliv, kdo email dostane. Zpráva s vašimi údaji se šíří pyramidovitě v mnoha různých variantách na další adresy. Kdykoliv může být změněn i text údajné petice a váš podpis může být pod něčím, s čím nesouhlasíte.

Pyramidové hry a různé nabídky na snadné výdělky

Většinou to jsou různé obdoby pyramidových her. Podle našich zákonů jsou pyramidové hry zakázány, proto se je organizátoři snaží maskovat jako prodej různých produktů. Tyto nabídky mají stejný základ: koupím produkt od zapojeného účastníka(ů), tím již zapojené členy posunu o pozici výš a snažím se přesvědčit jiné, aby produkt koupili a moji pozici také vylepšili. Pokud je trh nasycen - a to díky pyramidovému způsobu je poměrně rychle - poslední mají minimální šanci, že někdo další se připojí, a jsou to pouze jejich peníze, které pomohly alespoň částečně vrátit náklady zapojeným předchůdcům. Nabídky na odměnu nebo slevu na služby za hromadné rozeslání e-mailů. Pořádně si rozmyslete, jestli je slíbená odměna dostatečnou kompenzací za obtěžování vašich přátel.

Řetězové dopisy štěstí

Čínské modlitby a různé dopisy štěstí šířené z pověrčivosti nebo z neznalosti.

Žertovné zprávy

Různé žertovné zprávy, které si posílají kamarádi a známí. Ne všichni mají stejný smysl pro humor, a proto není vhodné je hromadně šířit na všechny adresy.

UKÁZKY VYLOŽENĚ PODVODNÝCH E-MAILŮ:

Nigerijské podvodné e-maily (SCAM 419)

Podvodníci rozesílají e-maily s lákavými nabídkami na velkou sumu peněz. Údajnými odesílateli jsou například vdovy po bohatém podnikateli, které žádají o pomoc při převodu peněz ze země. Jako odměna za pomoc je slíbeno až několik miliónů dolarů. Hlavní trik podvodu je v tom, že nachytaná oběť je nucena postupně platit několikatisícové poplatky na údajné výdaje spojené s převodem peněz, který je stále pod různými záminkami odkládán.

Podvodné loterie

Uživatelům je rozeslán e-mail, že vyhráli vysokou cenu v mezinárodní loterii. Do údajného slosování se dostali například výběrem e-mailových adres z celého světa a právě ta jejich vyhrála. Když se šťastlivec o svoji výhru přihlásí, dozví se, že musí před vyplacením výhry zaplatit manipulační poplatek ve výši několika desítek až tisíce EUR. Tento poplatek samozřejmě není možné strhnout z vyplácené výhry. I když naivní šťastlivec zaplatí, žádnou výhru neobdrží. Vymáhání výhry je nereálné a šance na vrácení peněz nulová.

PHISHING (rybaření)

Na velké množství adres jsou rozeslány **podvodné dopisy**, které na první pohled vypadají jako informace z určité banky. Tyto dopisy plně využívají tzv. sociální inženýrství. Příjemce je informován o údajné nutnosti vyplnit údaje v připraveném formuláři, jinak mu může být zablokován účet, nebo jinak omezena možnost využití svých finančních prostředků. V e-mailu bývá uveden odkaz na připravené stránky s formulářem, které jakoby odkazovaly na server banky. Ve skutečnosti je uživatel přesměrován na cizí server, ale vytvořený ve stejném stylu, jako jsou stránky příslušné instituce.
Chycený uživatel nepozná rozdíl a může vyplnit předvolená políčka, kde jsou po něm požadovány důvěrné informace - čísla účtu, kódy k internetovému bankovnictví, pin pro platbu atd. Takto získané údaje mohou podvodníci velice snadno zneužít.

Zdroj: www.novinky.cz

CO JSOU TO FAKE NEWS?

Přestože je internet vynikající nástroj pro vyjádření názoru, čím dál víc se potvrzuje, že lidé snadno dokážou zaměnit názory za jasná a potvrzená fakta a následkem toho šířit falešné zprávy. Mnoho webových stránek vydělává na tom, že lidé často klikají na jakýkoli obsah téměř automaticky. Stalo se vám někdy, že jste sdíleli článek, aniž byste ho četli celý? Než se rozhodnete sdílet nebo „lajkovat" nějaký článek, je důležité zjistit, o čem opravdu je, a pečlivě zvážit, zda stojí za sdílení. Kvalita internetu je závislá na tom, jaký obsah zveřejníme a šíříme. Výraz „fake news" (falešné zprávy) je používán mnoha lidmi již několik let. Vědí ale, jak takové zprávy opravdu vypadají? Tento výraz bývá používán velmi neurčitě, takže zaslouží bližší prozkoumání.

Senzacechtivé falešné zprávy často slouží ke generování kliků na webové stránce za účelem zvýšení příjmu z reklam. Také se ale používají k ovlivnění veřejného mínění. I když byste se zřejmě zasmáli a zprávy o existenci netopýřího chlapce byste si v bulvárním tisku vůbec nevšimli, internet dokáže být rafinovanější. Co si počít, když dokonce i seriózní společnosti, jakou je New Yorker, využívají k získání bezmyšlenkovitých kliků sloupky se satirickými zprávami? Lidé se při troše snahy mohou naučit rozpoznávat internetové falešné zprávy o něco lépe. Pojďme se podívat na příklad smyšlené důležité zprávy.

Byla transplantována lidská hlava?
Ne, opravdu nebyla, informuje deník Guardian. Poté, co italský lékař Sergio Canavero prohlásil, že takovou operaci provádí, objevily se na různých webech s falešnými zprávami články o úspěšné transplantaci hlavy. Pokud byste něco takového uviděli, klikli byste na to? To je učebnicová ukázka falešné zprávy.

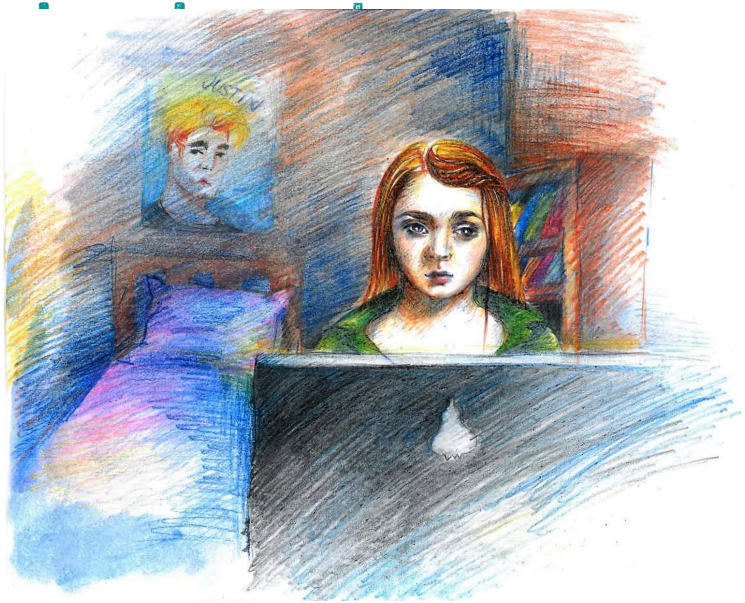
Zdroj: www.blog.avast.com

DEEP FAKE (video)

Falešné zprávy dostávají postupně nový a dokonalejší rozměr. Od smyšlených informací a konspiračních teorií, přes upravené fotografie až po videa, kde významný politik věrohodně pronáší to, co ve skutečnosti nikdy neřekl. Po fake news přijde fáze „hlubokých lží" – deep fake. Je jen otázkou času, kdy se upravená či zcela zfalšovaná videa českých politiků či jiných veřejně známých osob začnou šířit sociálními sítěmi a konspiračními weby i v České republice. Na to, jak je díky novým technologiím stále snadnější manipulovat obsahem, upozornil mezi prvními americký komik Jordan Peele. Ten díky počítačovému programu doslova vložil svá ústa do tváře Baracka Obamy a „donutil" jej tak věrohodně říkat to, co nikdy neřekl. Například se velmi nevybíravě vyjádřit o Donaldu Trumpovi.

Zdroj: www.forum24.cz

Nenechávejte své děti na internetu



SLOVO RODIČŮM

Proto, abyste mohli maximálně zabránit situaci ohrožujícívaše dítě, je nutné umět rozpoznat rizika. Čím lépe víte, co ho může na internetu potkat, tím lépe můžete na situaci reagovat a vašemu dítěti pomoci. Seznamte se s riziky s používáním internetu spojenými a citlivě s nimi seznamte i vaše dítě. Pokud vaše dítě s riziky předem seznámíte, nebezpečnou situaci může detekovat samo, a třeba se jí tak i vyhnout.

Následující záležitosti doporučujeme s dítětem probrat i v případě, že se dítě s obtěžováním přes internet nesetkalo:

- Nepředávejte své osobní údaje a osobní záležitosti, např. fotografie, aniž byste pečlivě zvážili následky. Přátelství přes internet může skončit, a když se tak stane, osobní údaje mohou být odeslány nesprávným lidem.
- Každý má právo na to, aby s ním bylo na internetu jednáno s úctou.
- Chat, e-mail nebo počítač můžete vypnout, kdykoli chcete.
- Děti by měly mít možnost mluvit se svými rodiči o negativních zkušenostech.

Upozorněte děti na rizika zasílání svých osobních nebo citlivých informací. Fenoménem dnešní doby je používání multimédií, a to i komunikace prostřednictvím videa. Pamatujte, že stejně jako u fotografií, může dojít velmi často ke zneužití záznamu, zejména jeho šíření, pokud obsahuje citlivý materiál.

Použití osobních údajů podléhá:

- Zákonu o ochraně osobních údajů
- Předpisům souvisejícím se soukromím a elektronickou komunikací
- Úřadu pro ochranu osobních údajů

Pamatujte si, že své osobní údaje nemusíte poskytovat, pokud nevíte, kdo je požaduje a k jakému účelu budou použity.

Zdroj: www.bezpecnyinternet.cz

Nebojte se! Ačkoliv výchova dětí v digitálním věku může vypadat jako neřešitelný problém, není zas tak těžké zajistit vašemu dítěti v online světě bezpečí a zároveň mu dopřát informace a zkušenosti, které bude v budoucnu tolik potřebovat. A ještě si u toho spolu můžete užít spoustu zábavy.

Zdroj: Oficiální stránky manuálu pro rodiče Dítě v síti, https://www.flowee.cz/ediceflowee/dite-v-siti
(pro zájemce k zapůjčení v ICM UH)

ŠEST RAD, NEŽ BUDETE COKOLI SDÍLET

Zde je několik oblastí, na které je třeba myslet, když surfujete v digitálním oceánu a narazíte na lákavý obsah, který byste mohli sdílet.

1. Z jakého zdroje obsah pochází? Už jste o něm slyšeli a vypadá seriózně? Je tento obsah vážný, nebo se jedná spíš o satiru?

2. Je za tím víc než jen poutavý titulek a vystihuje titulek obsah článku? Zjistěte, zda se vůbec jedná o článek. Zbystřete, pokud je obsah krátký a máte dojem, že není na ničem založený.

3. Nevzbuzuje ve vás obsah článku strach? Mohli jste se stát cílem na základě vaší historie hledání a nyní je s vámi manipulováno pomocí falešných článků, jejichž cílem je vyvolat ve vás strach.

4. Jedná se o aktuální informaci? Zkontrolujte datum, abyste neztratili nervy (případně o ně nepřipravili někoho jiného) kvůli zprávě staré dva roky – ať už skutečné, nebo falešné.

5. Dávejte pozor, na co v článku kliknete. Pokud v něm jsou odkazy, mohlo by se jednat o phishing nebo o pokus přesměrovat vás na nebezpečný web, který by mohl infikovat vaše zařízení.

6. Ověřte daný obsah na webech s dobrou pověstí, například org, jejichž cílem je odhalovat internetové lži.

Zdroj: www.blog.avast.com

Zajímavé odkazy:

www.internetembezpecne.cz
www.e-bezpeci.cz
www.televizeseznam.cz/porad/seznam-se-bezpecne
www.jsns.cz
www.nebudobet.cz
www.jsmetu.org
www.linkabezpeci.cz/poradna/dalsi/internet/
www.poradna.e-bezpeci.cz
www.bezpecnyinternet.cz/poradna/default.aspx
www.budsafeonline.cz
www.bezpecne-online.saferinternet.cz
www.replug.me

Knihy:

Nejlepší kniha o fake news, dezinformacích a manipulacích!!!;
Autoři: Miloš Gregor, Petra Vejvodová, Zvol si info;
Máme v ICM - můžeš si přijít přečíst!
Svět médií – Tvořivé náměty pro výuku průřezových témat na 2. stupni ZŠ
Digitální detox; Autor: Orianna Fieldingová

Dokumentární film o zneužívání dětí na internetu **„V síti“**
Režisér: Vít Klusák
Premiéra v českých kinech je naplánována na 8. března 2020

KYBERŠIKANA ZABÍJÍ ANEB REÁLNÉ PŘÍPADY

Ryan Halligan (1989–2003) měl ve škole problémy se spolužáky snad každý den. Vyhlídla si ho partička „bijců", která ho ponižovala a mlátila pro své potěšení. **Ryan byl klasickou slabou obětí**, která si nechala všechno líbit. Až jednoho dne došla jeho otci trpělivost a přihlásil ho na hodiny kickboxu. Po několika lekcích se skutečně postavil vůdci dětských gaunerů a dojšlo ke rvačce. Sice dostal nakládačku – přece jen čtyři na jednoho je trochu moc – ale **získal si respekt**. Trýznitelé mu už dali pokoj. **Ale chystali pomstu**. V létě 2003 **trávil** třináctiletý Ryan **většinu svého času na internetu**. Tam navázal známost s dívkou, která chodila na stejnou školu. **Zamiloval se a svěřil se jí s intimními informacemi o sobě**, včetně znamínek a jizev, které má na těle. Rozhodně **netušil**, že dívka je nasazená vůdcem dětského gangu a ve skutečnosti svou lásku jen předstírá. Začal školní rok a Ryan s hrůzou zjistil, že všechny **detaily**, které o sobě dívce napsal, jsou **zveřejněny** na školním serveru. Včetně komentářů jeho „lásky", která Ryana označila za gaye. **Celá škola se bavila** a třináctiletý kluk byl doslova společensky odepsaný.
7. října 2003. Celá rodina Halliganových se uložila ke spánku. „Běž už taky spát, Ryane", řekla matka svému synovi, který seděl u svého počítače. „Hned, ještě si tady něco dodělám, dobrou noc, mami". Řekl Ryan a **matka netuší, že jsou to poslední slova, která od něho uslyší**. Chlapec počkal ještě hodinu, než si byl jistý, že všichni spí. Pak se potichu zavřel v koupelně. Tam se ve vší tichosti oběsil. Podle pitevní zprávy se škrtil na provaze asi pět minut.

Týden po pohřbu našel John Halligan v počítači svého syna celou korespondenci a všechny urážlivé útoky od svých spolužáků. Na pevném disku byl totiž neúmyslně instalovaný program, který vše archivoval. V den sebevraždy je tam uložená konverzace, kdy Ryan prohlašuje, že jde spáchat sebevraždu. Jeho spolužáci na to odpovídají, že se těší, až si to přečtou v zítřejších novinách. Pro otce mrtvého dítěte to bylo nejtěžší čtení na světě.

Megan Meierová (1992–2006) plakala ve svém pokoji. Její matka Christie Meierová byla okamžitě u ní. Věděla moc dobře, že Megan **trpěla od třetí třídy depresemi ze svého vzhledu** a proto ji také přihlásila na katolickou školu Neposkvrněného početí panny Marie. Tam její dcera nosila školní uniformu. Žádný make up ani šperky. Megan se cítila šťastná, proto byl její pláč pro matku tak neobvyklý. Co se stalo? Její kluk, s nímž **se seznámila na internetu a nikdy ho neviděla**, jí poslal zprávu, že je nejodpornějším stvořením na světě. Matka dceru uklidňovala a vypnula její počítač. Bylo 15. října 2006 a o dva dny později se třináctiletá Megan oběsila v koupelně. Když si třináctiletá Megan **založila účet na stránkách MySpace**, oslovil ji šestnáctiletý Josh Evans. Vyměňovali si fotografie a **konverzovali pouze prostřednictvím internetu**. Megan se nový kluk moc líbil a chlubila se jeho fotografií spolužačkám v dívčí škole. Josh tvrdil, že se jeho rodina právě přestěhovala a proto nemá ještě telefonní číslo. **Virtuální láska** jako z Romea a Julie trvala několik týdnů a Megan se vznášela štěstím. Proto nerozuměla slovům plných nenávisti, která si četla 15. října. Přes zákaz matky se snažila s Joshem komunikovat a zjistit, co se stalo. Prý se chovala hnusně ke svým přátelům a poslední věta, kterou jí Josh 17. října napsal, zněla: **„Svět by byl bez tebe daleko lepší!"**

Za šest týdnů po smrti Megan byli její rodiče policií informováni, kdo se skrýval za identitou Joshe Evanse. Pokud byste čekali nějakého zakomplexovaného puberťáka, jste na omylu. Padesátiletá Lori Drewová si na MySpace založila falešný účet jen proto, aby mohla Megan deptat. A jaký měla důvod? Megan přestala kamarádit s její dcerou Sarah. Zřejmě si myslíte, že paní Drewová má ze smrti třináctileté dívky nepřekonatelné výčitky svědomí. Omyl. Její jediná reakce na celou záležitost je, že se jednalo jen o nevinný žert. Nemohla prý tušit, že se Megan psychicky složí kvůli nějakému vymyšlenému klukovi.

Zdroj: www. bystron.blog.idnes.cz

JEDEN SVĚT

FESTIVAL DOKUMENTÁRNÍCH FILMŮ O LIDSKÝCH PRÁVECH

KAŽDÉ JARO TAKÉ V KINĚ HVĚZDA UHERSKÉ HRADIŠTĚ

- ŠKOLNÍ PROJEKCE DOPLNĚNÁ BESEDOU S ODBORNÍKY
- MOŽNOST SETKÁNÍ S FILMOVÝMI TVŮRCI A REŽISÉRY!
- VEŠKERÉ DOTAZY RÁDI ZODPOVÍME. INFO@MKUH.CZ

městská kina UHERSKÉ HRADIŠTĚ · kinoHVĚZDA · EUROPA CINEMAS MEDIA PROGRAMME OF THE EUROPEAN UNION · MINISTERSTVO KULTURY · ISIC.CZ