KE KOPÍROVÁNÍ

Tento text lze stáhnout k volnému užití z www.vycvikkvp.cz. Je uložen v záložce „Ke stažení" po dobu tří měsíců od data vydání tohoto čísla časopisu Třídní učitel a vedení třídy. Pro ZŠ a SŠ zpracoval Mgr. Tomáš Holub.

Pracovní list: Bezpečně na internetu

BEZPEČNĚ NA INTERNETU

Naprostá většina z nás používá internet aktivně – má profil na sociální síti, chatuje, komentuje a vytváří obsah. Chceme být součástí světa, chceme být vidět, chceme být v kontaktu. Tím se však vystavujeme velkému riziku. Pojďme se podívat, jaká pravidla bychom měli dodržovat a proč.

JAK NA TOM JSEM? Jak moc ohrožený/á jsi ve virtuálním světě? Zaškrtni ANO/NE podle toho, jestli pro tebe dané tvrzení platí.

	ANO	NE
1) Hraju online hry a bavím se na chatu s ostatními hráči	☐	☐
2) Mám profil na některé sociální síti	☐	☐
3) ...a svůj profil mám veřejný (přístupný pro kohokoliv).....	☐	☐
4) Už jsem někdy vložil/a své video na videoportál jako YouTube či Musical.ly.....	☐	☐
5) Na sociální síti mám jako profilovku svou fotku	☐	☐
6) Navštěvuji nějaké internetové fórum a přispívám na ně	☐	☐
7) Seznamuji se přes internet s novými lidmi	☐	☐
8) Těm nejbližším kamarádům jsem prozradil/a své heslo či PIN	☐	☐

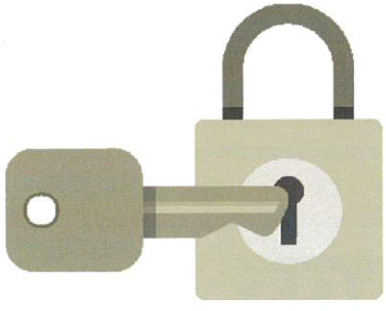
Vyhodnocení

Spočítej si odpovědi ANO. Čím víc takových odpovědí máš, tím větší riziko ti na internetu hrozí. Je potřeba si ale uvědomit, že nebezpečí číhá na každého, kdo internet aktivně používá ke komunikaci a sebeprezentaci.

6–8 = Nacházíš se v té neohroženější skupině! **3–5** = Dávej si bacha, nebezpečí číhá i na tebe…
1–2 = Nenech se zmást, ani ty nejsi v bezpečí. **0** = Klobouk dolů, v online světě jsi v bezpečí!

HESLA

Heslo je základní **ochranný prvek** zajišťující, aby se nikdo cizí nedostal do tvého účtu. Přesto se takové případy mohou stát, obvykle je to ale vlastním zaviněním. Respektuj proto uvedená doporučení.



Pravidla bezpečnosti – hesla

1) Dej si práci s originálním silným heslem

Heslo by mělo mít alespoň 8 různých znaků a kombinovat čísla i písmena, hesla typu „1234" jsou naopak velice slabá a tvůj účet nijak nezabezpečí, protože je uhádne každý.

2) Používej pro každý svůj účet/aplikaci jiné heslo

Neměj jedno heslo na vše, pokud by se někdo dostal k tvému heslu na sociální síť, měl by tak přístup i k tvé e-mailové schránce atd.

3) Nikdy své heslo nikomu cizímu neříkej ani je nikomu neposílej elektronicky

4) Svá hesla uchovávej v bezpečí

Někdy je těžké pamatovat si všechna hesla, nepiš si je však na místo, kde jsou všem na očích, ani je nenos např. v peněžence.

ŽIVOT bez závislostí

Pracovní list vypracoval Mgr. Tomáš Holub

OSOBNÍ ÚDAJE

Osobní údaje jsou informace, podle kterých můžeme být identifikováni, jedná se tedy o jméno, adresu, telefonní číslo, ale také například o fotografii, věk, datum narození. Mezi citlivé osobní údaje patří třeba rasový či etnický původ, sexuální orientace, zdravotní stav či politické názory – tedy vše, na základě čeho může být člověk diskriminován. S kamarády takové informace běžně sdílíme, problém však nastává, když se dostanou do nesprávných rukou – mohou být zneužity v rámci kyberšikany, kybergroomingu a dalších kyberzločinů (viz další stránka).

Proč je věk osobním údajem?
Podle jednoho osobního údaje tě obvykle nikdo nepozná, ale podle více takových údajů (třeba z vícero zdrojů) již ano.

CVIČENÍ

Urči, které údaje bys neměl/a uvádět na svém profilu.

a) jméno a příjmení
b) velikost bot
c) věk
d) adresa bydliště
e) přezdívka
f) fotografie svého obličeje
g) domácí zvíře
h) plat rodičů
i) barva vlasů
j) telefonní číslo
k) PIN k mobilu
l) údaje o kamarádovi

Vyhodnocení najdeš na poslední stránce.

Pravidla bezpečnosti – osobní údaje

1) Nepoužívejte na sociální síti své pravé jméno (ale přezdívku)

2) Místo profilové fotografie sebe použijte např. obrázek zvířete či nějaké kreslené postavičky
Ale pozor, nepoužívejte ani fotku někoho jiného, i když by šlo o fotografii někoho cizího staženou z internetu. Požádej své kamarády, aby bez tvého svolení nezveřejňovali tvé fotky ani tě na nich neoznačovali.

3) Nezveřejňuj na internetu své telefonní číslo ani adresu (e-mailovou či bydliště)
Kontaktní údaje neposílej ani elektronicky, dávej je kamarádům jen při osobním setkání, důrazně je požádej, aby je sami od sebe nešířili bez tvého svolení.

4) Nastav si soukromí svého účtu na sociální síti
Věnuj čas nastavení soukromí – kdo může vidět tvůj profil, kdo ti může psát, kdo si může prohlížet tvé fotografie. Čím soukromější budeš mít svůj profil, tím víc budeš v bezpečí.

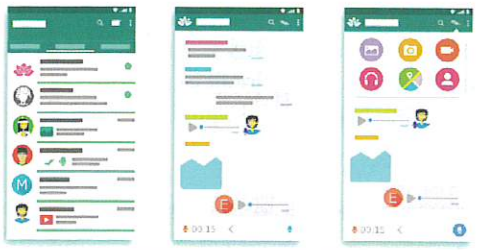
5) Když si nejsi jistý/á, co můžeš zveřejnit, polož si jednoduchou otázku:
„Sdělil bych tuto informaci náhodnému cizímu člověku venku na ulici?“
Na internetu chceme zaujmout, ale měli bychom se řídit stejnými zásadami jako ve skutečném světě, kde jsme mnohem opatrnější a méně sdílní.

ŽIVOT bez závislostí

Pracovní list vypracoval Mgr. Tomáš Holub

ONLINE KOMUNIKACE

Řada lidí hledá kamarádství na internetu, tam se skrývá ale i spousta **falešných profilů** osob, které se vydávají za někoho jiného s cílem získat **intimní materiál** (za účelem následného vydírání) či jinak ublížit. A jelikož si nikdy nemůžeš být jist, jestli je na druhé straně doopravdy tvůj kamarád, nejen v kontaktu s cizím člověkem je potřeba být ve střehu.



Kyberzločiny

Kyberšikana – ubližování pomocí elektronických médií (mobilní telefon, počítač, internet, sociální sítě, chat ad.).

Kyberstalking – nebezpečné a obtěžující pronásledování pomocí mobilního telefonu/počítače (telefonování, psaní zpráv a e-mailů).

Kybergrooming – snaha o manipulaci obětí za účelem osobního setkání a následného sexuálního zneužití či jiného využití.

Kyberphishing – podvodné získávání přístupových údajů například k bankovnímu účtu.

CO TÍM SLEDUJE?!

I nevinná otázka může mít skrytý podtext – obzvláště u kybergroomingu. Přečti si následující výňatky z online konverzace a urči, proč to dotyčný píše: vydírání (1), zisk informace (2), zisk intimního/kompromitujícího materiálu (3), ujištění o bezpečnosti komunikace (4), izolace oběti (5). (Ke každé větě připiš číslo ze závorky)

a) „Pošleš mi fotku? Já pro tebe mám taky jednu povedenou.“ .....
b) „Máš kluka/holku? A co kámoši?“ .....
c) „A to tvoji rodiče pracují každý den od osmi do pěti? To je fuška…“ .....
d) „Bydlíš v Praze? A kde? Já Prahu moc neznám.“ .....
e) „A to máš svůj počítač, nebo společný se sourozencem/rodinou?
Já mám naštěstí PC ve svém pokojíčku.“ .....
f) „Rád si s tebou píšu, ale kámoši by mohli žárlit. Že to nikomu neřekneš?“ .....
g) „Tohle by dospělí nepochopili, ale já jo, mně se můžeš svěřit.“ .....
h) „Jestli mi nepošleš další fotku, tak pošlu tvým rodičům všechnu naši konverzaci
i s těmi obrázky!“ .....

Vyhodnocení najdeš na poslední stránce.

Nejznámější případ kybergroomingu v ČR:

V roce 2013 byli odsouzeni dva skautští vedoucí (přezdívky Piškot a Meluzín) k 10 letům odnětí svobody za zneužití 39 chlapců, které vydírali pomocí falešného profilu dívky – oslovili chlapce na sociální síti, psali si s ním a manipulací ho přiměli k zaslání nahé fotografie (sami mu nejdříve poslali fotografii dívky staženou z internetu, aby si získali jeho důvěru), tou poté chlapce vydírali a nutili k výrobě dalších pornografických materiálů a některé též k pohlavnímu styku.

ŽIVOT bez závislostí

Pracovní list vypracoval Mgr. Tomáš Holub

Pravidla bezpečnosti – online komunikace

1) Ověř si identitu
Opravdu se jedná o tvého kamaráda či osobu ve tvém věku? Při jakékoliv pochybnosti chtěj hned ověření ve formě fotografie dotyčného (selfie), jak drží papír s napsanou větou, kterou si vymyslíš. Raději ukonči komunikaci, pokud přijde nějaká výmluva („Zrovna se mi rozbil foťák v mobilu...“).

2) Všímej si nesrovnalostí v komunikaci
Pokud dotyčný, se kterým si píšeš, často mění uváděný věk, školu, zájmy atd., měl/a bys zbystřit, evidentně používá několik falešných identit, se kterými oslovuje své oběti.

3) Přemýšlej, proč to chce dotyčná osoba vědět
Ptá se tě, jestli jsi zrovna sám/sama? Kde jsou tvoji rodiče? Třeba se jen snaží zjistit, jestli je pro něj komunikace s tebou bezpečná.

4) Nepřistupuj na tajemství
Pokud se tě někdo snaží přemluvit k tomu, abys o kontaktu s ním nikomu neříkal/a, je to jasné znamení, že to s tebou dotyčný člověk nemyslí dobře.

5) Neprovozuj sexting
Psaní si intimních zpráv či posílání nahatých fotek se snadno vymstí, následuje vydírání zveřejněním těchto materiálů, proto nikomu nic takového neposílej a nesdílej – ani když jste spolu ve vztahu!

6) Neboj se komunikaci ukončit a svěřit se
Ať už je ti v online komunikaci nepříjemné cokoliv (vulgarity, násilné obrázky, vydírání atd.), nezdráhej se kontakt ukončit a svěřit se rodičům či se obrať na Linku bezpečí (116 111).

7) Na osobní schůzku jen s doprovodem
Pokud se máš poprvé sejít s „online kamarádem“ naživo, vždy jen v doprovodu rodiče! Kamarád či kamarádka si nemusí vědět rady v situaci, kdy tě chce někdo unést. Nenastupuj ani k nikomu do auta (častá výmluva je: „On na tebe čeká u školy, já jsem jeho táta, mám tě k němu dovézt.“)

POSLEDNÍ RADA ZÁVĚREM – CO DĚLAT V ROLI OBĚTI

Čím víc jsme aktivní online, tím víc bychom si měli hlídat své soukromí a řídit se zásadami bezpečného chování na internetu. Důležité je také pracovat na svém kritickém myšlení, abychom nenaletěli podvodníkům a dokázali včas rozpoznat varovné signály. Pokud se přece jen setkáš s kyberšikanou, kybergroomingem či jiným kyberzločinem, nikdy si to nenech pro sebe – čím déle budeš v roli oběti, tím větší následky to na tebe bude mít.

Zachovej klid, zajisti důkazy (ulož konverzaci/fotky atd.), ukonči konverzaci, svěř se rodičům a společně kontaktujte policii!

ŽIVOT bez závislostí

Pracovní list vypracoval Mgr. Tomáš Holub