V digitálním světě

MEDIÁLNÍ VZDĚLÁVÁNÍ S VYUŽITÍM AUDIOVIZUÁLNÍCH PROSTŘEDKŮ

PRO 1. STUPEŇ ZÁKLADNÍCH ŠKOL

METODICKÁ PŘÍRUČKA

JSNS.CZ

JEDEN SVĚT NA ŠKOLÁCH
Člověk v tísni, o.p.s.
Šafaříkova 24, 120 00 Praha 2
www.jsns.cz

Koncept: Paula Sisková, Sandra Telenská

Na přípravě publikace se dále podíleli:
Marianka Macková, Adéla Skálová, Karel Strachota, Kateřina Suchá, Tomáš Titěra, Michaela Trnková, Ester Pěkná Valchařová

Editorka: Hana Valentová

Jazyková úprava: Pavla Kučerová
Grafická úprava a sazba: Mowshe >0<

Rok vydání: 2020

ISBN: 978-80-7591-047-9

V digitálním světě

MEDIÁLNÍ VZDĚLÁVÁNÍ S VYUŽITÍM AUDIOVIZUÁLNÍCH PROSTŘEDKŮ

PRO 1. STUPEŇ ZÁKLADNÍCH ŠKOL

METODICKÁ PŘÍRUČKA

OBSAH

Vážení vyučující,

publikace ***V digitálním světě***, kterou právě držíte v ruce, a stejnojmenná sada audiovizuálních lekcí dostupných na portále JSNS představují další milník v našich mediálně-vzdělávacích aktivitách. Dosavadní širokou nabídku určenou pro středoškoláky a žáky 2. stupně základních škol nově rozšiřujeme o výukové materiály vhodné pro žáky 1. stupně základních škol. Takové materiály přitom v České republice dlouhodobě chybí navzdory narůstající potřebě začít s mediální výchovou co nejdříve.

Děti již v prvních letech života vstupují do prostoru internetu, který je pro ně přirozenou součástí světa, ve kterém dělají první kroky. Proto je důležité, aby blíže poznávaly prostředí, které pro ně vedle zajímavého a zábavného obsahu představuje také určitá rizika. Měli bychom je vést k obezřetnosti a digitální střídmosti.

Za základ sady ***V digitálním světě*** jsme s ohledem na cílovou skupinu zvolili atraktivní a hravý formát animovaného seriálu. Jednotlivé díly děti seznamují s pojmy, jako jsou vyhledávače, cookies nebo lajky, a zároveň přibližují jejich fungování. Další se zaměřují například na principy tvorby bezpečného hesla, rozebírají důvody rodičovské kontroly nebo nezbytnost ověřování informací. Značný prostor je věnován rizikovému chování na internetu. Ke každému dílu seriálu jsme připravili aktivity a pracovní listy určené přímo do vyučovací hodiny. Vznikaly ve spolupráci s vyučujícími, kteří je testovali se svými žáky. O jejich zkušenostech i reakcích dětí si můžete přečíst v úvodní kapitole publikace.

Věřím, že se nám podařilo připravit praktickou pomůcku, s jejíž pomocí můžete s mediální výchovou na 1. stupni začít. Budeme rádi, když nám dáte vědět, jak se vám s jednotlivými materiály pracovalo, a pošlete případně náměty na úpravy a rozšíření, které budeme moci v budoucnu zohlednit.

Děkuji všem, kdo se na její tvorbě podíleli, a také všem partnerům a podporovatelům.

Karel Strachota
ředitel JSNS

ZKUŠENOSTI VYUČUJÍCÍCH

Audiovizuální sadu* V digitálním světě *již vyzkoušeli vyučující v praxi. Přečtěte si, jak se jim s tématy a materiály pracovalo a jaké byly reakce žáků. Věříme, že i toto stručné sdílení zkušeností vás inspiruje k tomu, abyste sadu zařadili i do své výuky.

JAK SE VÁM S AUDIOVIZUÁLNÍ SADOU V DIGITÁLNÍM SVĚTĚ PRACOVALO A JAKÉ BYLY REAKCE VAŠICH ŽÁKŮ?

S audiovizuální sadou *V digitálním světě* se mně i žákům pracovalo výborně! Tuto sadu vnímám jako velmi důležitou, protože v této oblasti je pro učitele žáků 1. stupně zatím jen málo materiálů. Pro žáky je to téma, které velice dobře znají ze svého úhlu pohledu, ví, o čem mluví. Aktivity jsou přehledně připravené, žáky moc bavily.
Andrea Tláskalová, *ZŠ Zbiroh*

Sada je připravena k okamžitému použití po krátké přípravě. Někteří žáci 1. stupně se již velmi dobře orientují v aplikacích, nezaznamenal jsem ale povýšené jednání nad těmi, kteří s tématy teprve začínají. Všichni se dobře bavili, aniž si uvědomovali, že se posouvají dál.
Pavel Mikoláš, *ZŠ Benešova, Třebíč*

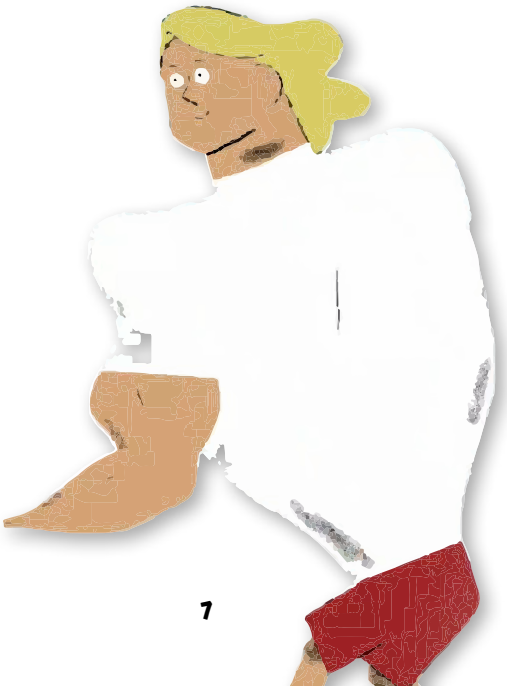
S audiovizuální sadou se mi pracovalo velmi dobře. Využila jsem ji v 5. ročníku, kde žáci neměli žádné obtíže s pochopením témat. Žáky i mě nejvíce zaujalo téma rodičovské kontroly. Někteří žáci se o něm zmínili i doma a rodiče chtěli poslat odkaz na video. Proto se domnívám, že sada dává nám, pedagogům, možnost oslovit nejen žáky, ale i jejich rodiče.
Během distanční výuky se žáci nenásilnou a zároveň zábavnou formou učili i jak s informacemi zacházet, umět si je ochránit, ověřit a použít ve výuce. Domnívám se, že to je důležitější, než umět nazpaměť vyjmenovaná slova.
Markéta Břešťanová, *Základní škola Červený vrch, Praha*

CO VZKÁŽETE VYUČUJÍCÍM, KTEŘÍ VÁHAJÍ, ZDA ZAČÍT PRACOVAT S AUDIOVIZUÁLNÍ SADOU V DIGITÁLNÍM SVĚTĚ?

Kolegům-pedagogům vzkazuji, aby se nebáli vyzkoušet minimálně jednu lekci. Sami uvidí, že jejich žáci reagují na video velmi pozitivně a chtějí o tématech, která jsou jim blízká, mluvit. Nevadí, že my, učitelé, nevíme vše. Proč by nás zas něco nemohli naučit žáci? Důležité je o digitálním světě mluvit, aby se nám v něm děti neztratily. V reálném světě děti učíme odmala, co je správné a co je špatné. Měli bychom vědět, jak funguje i virtuální svět, a upozornit žáky na všechny nástrahy, které je tam čekají.
Markéta Břešťanová, *Základní škola Červený vrch, Praha*

Kolegyním a kolegům bych vzkázala, ať se témat nebojí, a to i když s nimi sami nemají mnoho zkušeností. Zjistila jsem, že toho moji žáci ví o dost víc než já, ale to vůbec nevadilo. Naopak mě žáci aktivně se vším seznamovali a vysvětlovali – dokonce mi chtěli zakládat účty :-). Žáci byli hodně otevření ke mně i k sobě navzájem. Potřeba byla jen dávat pozor na čas, protože žáci přicházeli stále s novými podněty a zážitky.
Andrea Tláskalová, *ZŠ Zbiroh*

Nebojte se začít, vše je srozumitelně a přehledně seřazené. Příprava vám nezabere mnoho času a vaši žáci vám jistě pomohou v průběhu lekce.
Pavel Mikoláš, *ZŠ Benešova, Třebíč*



3. METODIKA

ZÁKLADY PRÁCE SE SADOU V DIGITÁLNÍM SVĚTĚ

V této části nabízíme několik rad a doporučení, které se osvědčily při využívání sady V digitálním světě ve výuce. Vycházíme z osvědčené metodiky Jednoho světa na školách (JSNS), která se opírá o základy práce s audiovizuálními materiály[1]. Platí, že nejde o zásady a pravidla, které musí být za každé situace dodrženy, ale spíš o tipy a postřehy, které vám mohou při práci se sadou V digitálním světě pomoci.

CO JE SADA V DIGITÁLNÍM SVĚTĚ?

Sada *V digitálním světě* obsahuje jednotlivé audiovizuální lekce (AV lekce), které tvoří video a doprovodné materiály. Ty zahrnují například související dokumenty (pracovní listy, faktické informace k tématu zpracované odborníky apod.) a především v praxi vyzkoušené aktivity do hodin. Díky AV lekcím tak snadno připravíte pro své žáky a studenty atraktivní hodiny, které dané téma proberou v širším kontextu. AV lekce na rozmanitá témata najdete na našem audiovizuálním výukovém portálu jsns.cz.

CO SADA V DIGITÁLNÍM SVĚTĚ OBSAHUJE?

Tuto sadu jsme pojmenovali podle animovaného vzdělávacího seriálu *V digitálním světě*, který seznamuje děti s fungováním digitálního (online) světa a pravidly bezpečného chování v něm.

Sada vychází z tohoto seriálu a skládá se z 15 audiovizuálních lekcí zaměřených na základy mediální a digitální gramotnosti mladších žáků ZŠ. Základem každé AV lekce je jedna epizoda seriálu.

V rámci AV lekcí se se svými žáky seznámíte s pojmy, jako jsou vyhledávače, cookies nebo lajky. Zaměříte se na principy tvorby bezpečného hesla, rozeberete důvody rodičovské kontroly nebo nezbytnost ověřování informací. Otevřete i problematická témata, jako jsou například projevy nenávisti a rizikového chování na internetu.

V digitálním světě – původem francouzský animovaný seriál (v originále pod názvem #DansLaToile) je určen pro 6–12leté diváky. Hlavní hrdinové seriálu Mína a Filip přibližují dětem prostředí „nul a jedniček“ a seznamují je atraktivní formou se základními pojmy a nástroji digitálního světa. Seriál obsahuje 15 epizod, které jsou dostupné na **jsns.cz/v-digitalnim-svete**.

AV LEKCE JSOU ROZDĚLENY DO PĚTI TEMATICKÝCH BLOKŮ:

- **Digitální svět: Jak vznikl a jak funguje** (AV lekce: Výlet do historie, Digitální svět)
- **Jak na data** (AV lekce: Vyhledávače, Viry, Hesla, Cookies)
- **Jak na online zábavu** (AV lekce: Online hry, Závislost na internetu, Rodičovská kontrola)
- **Jak na sociální sítě** (AV lekce: Sociální sítě, Lajky, Jak mluvit na internetu, Tvořit na internetu)
- **Jak to všechno zvládat chytře a bezpečně** (AV lekce: Kyberšikana, Pravda, nebo ne?)

1 *Více o tom, jak využívat audiovizuální materiály ve výuce (zejména dokumentární film), najdete v naší metodické příručce* **Učíme s filmem**.

KE KAŽDÉMU DÍLU JSOU PRO VÁS PŘIPRAVENY NÁSLEDUJÍCÍ MATERIÁLY DO VÝUKY:

EPIZODA SERIÁLU V DIGITÁLNÍM SVĚTĚ

Epizoda má zpravidla 2 minuty.
Všechny epizody naleznete na audiovizuálním výukovém portálu jsns.cz/v-digitalnim-svete, kde si je můžete přehrát online.

AKTIVITA NA JEDNU VYUČOVACÍ HODINU

Návrh každé aktivity vytvořili pedagogové základních škol a je otestovaná v praxi při výuce s žáky.

PRACOVNÍ LIST PRO ŽÁKY

Pracovní listy jsou připravené přímo **k dané aktivitě a slouží jako materiál pro žáky**.

LIST PRO VYUČUJÍCÍ

Doprovodný informační materiál pro učitele, který vám bude oporou při vedení hodiny.

OTÁZKY A ODPOVĚDI

Přehled základních otázek a odpovědí k tématu, který sestavili odborníci. Materiál vám pomůže se v tématu zorientovat.

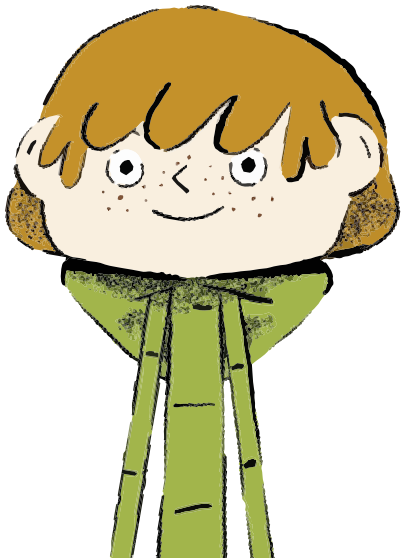
Seriál *V digitálním světě* vám také může pomoci naplnit **průřezové téma mediální výchova Rámcového vzdělávacího programu (RVP)**. RVP na 1. stupni ZŠ stanovuje několik očekávaných výstupů a předpokládá, že žák umí reflektovat, jakým způsobem média provázejí jeho den a den jeho rodiny, rozeznává zvolené výrazové prostředky nebo rozdíly mezi seriózním a bulvárním zpravodajstvím.

Provázanost s RVP najdete u každé aktivity v záhlaví příslušného listu.

JAK POSTUPOVAT PŘI PRÁCI SE SADOU V DIGITÁLNÍM SVĚTĚ

Přečtěte si praktické tipy a doporučení pro práci se sadou *V digitálním světě* (najdete je v této publikaci na str 12).

1. Před prací s první epizodou zařaďte „nultou“ hodinu, během níž v úvodním neformálním průzkumu zjistíte úroveň digitální a mediální gramotnosti svých žáků (jak provést úvodní průzkum třídy naleznete v této publikaci na str. 14).
2. Vyberte si epizodu seriálu, která se vám tematicky hodí. Téma může vzejít z provedeného úvodního průzkumu třídy nebo z jiné aktuální potřeby vztahující se k probírané látce apod. Anebo můžete postupovat jednoduše podle tematických oblastí.
3. Udělejte úvodní evokaci před projekcí a navnaďte žáky na téma epizody otázkami, které se vztahují k tématu epizody. Návrh několika vhodných otázek najdete v úvodu každé AV lekce.
4. Pusťte vybranou epizodu, klidně opakovaně, aby žáci lépe pochopili její obsah.
5. Udělejte reflexi emocí metodou jednoho slova. Zjistěte, jaké dojmy ve třídě projekce vyvolala a jestli vaši žáci všemu rozuměli (více o metodě jednoho slova naleznete v této publikaci na str 17).
6. Věnujte se dalším krokům popsaným v AV lekci – vyplňte s žáky pracovní list, diskutujte nad jejich odpověďmi, zeptejte se na jejich zkušenosti apod. Nezapomeňte na závěr na reflexi aktivity. Tipy, jak úspěšně shrnout proběhlou lekci, najdete vždy na konci aktivity.
7. Gratulujeme, máte hotovo! A můžete pokračovat ve výuce s další lekcí.



PRAKTICKÉ TIPY A DOPORUČENÍ

NEŽ ZAČNETE PROMÍTAT ANEB JAK SE PŘIPRAVIT NA HODINU

1. UDĚLEJTE ÚVODNÍ PRŮZKUM VAŠÍ TŘÍDY

Než začnete seriál *V digitálním světě* a sadu aktivit využívat, **doporučujeme provést úvodní průzkum a získat přehled o digitální a mediální gramotnosti třídy,** se kterou chcete pracovat. Úvodní průzkum (monitoring) můžete provést v rámci tzv. nulté hodiny k tématu. Zjistíte, že s některými tématy už možná mají žáci zkušenosti, u jiných budete mít možnost téma otevřít ještě dříve, než se s ním žáci setkají v rámci AV lekce.

Více informací najdete v této publikaci v kapitole 3. Úvodní průzkum: Jak jsou na tom vaši žáci.

2. ZHLÉDNĚTE EPIZODU PŘED PROJEKCÍ

Na epizodu se sami podívejte ještě dříve, než ji budete pouštět žákům. Ověříte si tak, zda svou náplní odpovídá naladění a možnostem třídy (z hlediska zájmu žáků, úrovně znalostí apod.) i kritériím, která musíte naplnit (ŠVP, učební plán aj.). Zhlédnutí vám pomůže promyslet i podobu lekce.

3. PROJDĚTE SI MATERIÁLY K LEKCI A PŘIPRAVTE SI HODINU

V návaznosti na zhlédnutí epizody si projděte materiály ke každé lekci. Materiály jsou kompletně připravené, doporučujeme si je však pečlivě prostudovat a v případě potřeby si je můžete upravit dle potřeby.

4. PROČTĚTE SI INFORMACE O PROMÍTANÉM TÉMATU

Součástí materiálů jsou i další doprovodné informace k tématu, abyste se v něm dobře orientovali. S tím vám pomůže informační text Otázky a odpovědi. Najdete jej na konci každé lekce a přiblíží vám nejdůležitější témata, kterým se epizoda věnuje.

5. PŘIPRAVTE SI TECHNIKU A ZKONTROLUJTE RYCHLOST INTERNETOVÉHO PŘIPOJENÍ

Věnujte pozornost i technickým aspektům projekce: důležitý je dobrý obraz (doporučujeme místnost zatemnit) a dostatečně hlasitý zvuk. Případné technické problémy snižují pozornost žáků a projekci znehodnotí.

Epizody seriálu *V digitálním světě* najdete online na internetovém portálu JSNS.CZ, kde si je můžete rovnou přehrát. Potřebovat k tomu budete funkční internetové připojení, protože videa se z důvodu ochrany autorských práv nedají stáhnout. Pokud vám technika není blízká, nebojte se říci si o pomoc kolegům.

BĚHEM VÝUKY

1. PŘED PROMÍTNUTÍM EPIZODY ZAŘAĎTE EVOKAČNÍ AKTIVITU

Jednotlivé lekce jsou vystavěny podle modelu E-U-R, tedy evokace, uvědomění a reflexe. První část, tedy evokace, slouží k tomu, aby si žáci mohli nové informace zařadit do kontextu svých dosavadních znalostí a zkušeností, aby se zaktivizovali před samostatnou prací a aby se namotivovali pro vstup do nového tématu. Náměty k evokačním aktivitám jsou vždy uvedeny jako první bod v postupu provázejícím lekcí. Při závěrečné reflexi aktivity se pak můžete k momentům z evokační fáze vracet a nechat je žáky doplnit o nově zjištěné poznatky.

2. PUSŤTE EPIZODY VÍCEKRÁT

Jednotlivé epizody seriálu *V digitálním světě* mají pouze několik minut. Někdy se žáci při promítání takto krátkého videa nestihnou dostatečně soustředit a unikne jim tak hlavní sdělení. Pokud je to možné, doporučujeme snímek přehrát nejméně dvakrát.

3. OVĚŘTE, ŽE ŽÁCI PŘÍBĚH POCHOPILI

Pro další úspěch lekce je důležité, aby žáci příběh epizody pochopili. Vždy proto krátce ověřte, že žáci rozumí, co se v epizodě odehrálo. Můžete žákům položit několik otázek zaměřených na chápání hlavního sdělení epizody. Další možností je vyzvat žáky k tomu, aby sami zkusili děj filmu převyprávět.

4. NEZAPOMÍNEJTE NA REFLEXI EMOCÍ PO PROJEKCI

Velmi důležitou součástí práce s audiovizuálními materiály je reflexe emocí a dojmů po projekci. Žáci mohou bezprostředně po zhlédnutí reagovat, vyjádřit se, co je zaujalo, a pojmenovat dojmy, které v nich epizoda zanechala. Platí, že v reflexi emocí neexistuje správná odpověď: každý může mít jiné pocity a dojmy a je podstatné, aby všichni dostali příležitosti je sdělit. Reflexe emocí vám pomůže i v dalším vedení lekce, jelikož již budou ošetřeny ty nejsilnější pocity a dojmy, které v žácích po zhlédnutí filmu rezonují. Pro účely této sady se osvědčilo provést reflexi metodou jednoho slova (více o metodě si přečtěte v této publikaci na str. 17).

5. NA KONCI SHRŇTE PRŮBĚH CELÉ LEKCE (REFLEXE AKTIVITY)

V samém závěru lekce je dobré shrnout s žáky celou aktivitu. Společně s žáky zkuste přijít na to, k čemu jste došli, a říct si, s čím by měli žáci z hodiny odcházet. Slouží k tomu sada otázek, kterou naleznete na konci každé aktivity (v rámečku Reflexe aktivity).

NA CO JE DOBRÉ PAMATOVAT

1.
UČTE ŽÁKY DISKUTOVAT

Umět diskutovat a vést diskusi je velmi praktická a přínosná dovednost. Pomáhá žákům si navzájem naslouchat, klást si otázky a hledat na ně odpovědi. Rozvíjejte proto v komunikačních dovednostech sebe i své žáky.

2.
POZOR NA OČEKÁVÁNÍ

Na začátku nemusí výsledek práce se žáky odpovídat původnímu očekávání. Důvodů může být několik (např. neochota žáků diskutovat nebo málo zkušeností s tématem). Zdánlivě odmítavé projevy žáků (např. agresivní výkřiky, znevažování situace) jsou však také určitou formou odpovědi, se kterou můžete dále pracovat a citlivě ji usměrňovat. Nenechte se proto hned odradit, vše má svůj čas.

3.
PŘIPUSŤTE, ŽE NEVÍTE VŠECHNO

Během sledování jednotlivých epizod se mohou objevit nejrůznější otázky. Pokud někdy neznáte odpověď, je to zcela přirozené. Není pak slabostí před žáky připustit, že nevíte všechno.

Otázky a nejasnosti, které vyvstanou během diskuse, mohou posloužit jako podnět pro domácí úkol či vypracování projektu. Žáci mohou vyhledat odpovědi a sdílet je pak s ostatními.

4.
NENUŤTE VŠECHNY DĚLAT VŠECHNO

Do realizace aktivit není vhodné žáky nutit. Může se stát, že některá aktivita bude některým žákům nepříjemná. Buďte připraveni žákům nabídnout alternativní možnost splnění zadání, například formou samostatné práce namísto práce ve skupině nebo písemného vyjádření namísto verbálního.

5.
BUĎTE SVÝM ŽÁKŮM PARTNEREM

Klíčem k úspěchu je osobnost vyučujícího. Snažte se být žákům přirozenou autoritou i partnerem. Žáci ocení empatii, možnost diskuse, projevený zájem o jejich názor i respekt k jejich postojům.

ÚVODNÍ PRŮZKUM: JAK JSOU NA TOM VAŠI ŽÁCI

Než začnete seriál V digitálním světě a sadu aktivit využívat, doporučujeme provést úvodní průzkum (monitoring) mezi žáky a získat tak přehled o digitální a mediální gramotnosti třídy, se kterou chcete pracovat.

Rozdíly mezi třídami i školami totiž mohou být velké. Roli hraje mnoho faktorů: například názor rodičů na používání technologií (zda dětem přístup k technologiím omezují, nebo ne, jak se s dětmi o používání technologií baví) či ekonomická situace rodiny (zda mají technologie vůbec k dispozici) apod.

PROČ SE VYPLATÍ PRŮZKUMU VĚNOVAT ČAS?

Úvodní průzkum, například v rámci „nulté hodiny“, vám jako vyučujícímu nejen pomůže zjistit, jak na tom jsou vaši žáci z hlediska fungování digitálního světa, ale rovněž se díky němu budete snáze rozhodovat, kterým z pěti tematických oblastí z AV sady se nejvíce věnovat. Možná zjistíte, že v některém tématu se žáci již orientují a dokážou sami rozpoznat rizikové chování.

DEJTE ŽÁKŮM SLOVO

Úvodnímu průzkumu doporučujeme věnovat dostatek času a dát tak žákům prostor diskutovat o jejich zkušenostech. Žáci také pravděpodobně ocení váš zájem o jejich prožitky v pro ně atraktivní oblasti. Ochota žáků naslouchat a spolupracovat na aktivitách rozvíjejících digitální a mediální gramotnost se dle našich zkušeností díky tomu určitě zvýší.

JAK NA ÚVODNÍ PRŮZKUM – PTEJTE SE

Připravili jsme pro vás návrhy aktivit, jak při úvodním průzkumu postupovat. Základem každé aktivity jsou otázky, které žákům v různé formě pokládáte.

Vnímejte je jako inspiraci, není nutné dodržet přesné pořadí a projít všechny otázky, naopak může být přínosnější hlouběji se věnovat oblastem, které žáky zaujmou nebo naopak ve kterých budou tápat.

NÁMĚTY PRO ÚVODNÍ PRŮZKUM TŘÍDY V TÉMATECH PUBLIKACE

1. DIGITÁLNÍ SVĚT: JAK VZNIKL A JAK FUNGUJE

EPIZODY: VÝLET DO HISTORIE, DIGITÁLNÍ SVĚT

První tematická oblast se zabývá základy fungování internetu. Tato témata mohou být hůře uchopitelná pro žáky, kteří internet příliš nepoužívají. Je proto vhodné zjistit, jak moc aktivními uživateli žáci jsou.

JAK POSTUPOVAT

Vyzvěte žáky, ať se rozestaví podél nejdelší zdi v místnosti podle toho, kolik času tráví na internetu, ať už na počítači, nebo mobilu. Uveďte, že levá strana znamená „málo času“ a pravá strana „hodně času“. Zkuste obě krajní hodnoty nijak nespecifikovat a nechat žáky se rozestavit dle jejich vlastního mínění. Následně se žáků ptejte, proč se postavili zrovna na dané místo a kolik času si myslí, že tráví na internetu. Možná se ukáže, že co je pro jednoho málo, je pro druhého už příliš. Nechte žáky porovnávat se mezi sebou a sledujte jejich reakce.

Poznámka: Spousta současných telefonů disponuje funkcí sledování času stráveného používáním zařízení. Můžete následně žáky vyzvat, aby svůj časový odhad porovnali s daty ze svého telefonu. Lišily se jejich odhady příliš? Byli žáci příliš pesimističtí, nebo naopak optimističtí?

Velkou vypovídající hodnotu o času stráveném na internetu může mít i samotný přístup k zařízení. Můžete se žáků zeptat, kolik jich vlastní chytrý telefon a zda mají přístup k wifi nebo mobilním datům. Další otázka může znít, kdo má doma přístup i k dalšímu zařízení, například tabletu nebo počítači. Můžete očekávat, že lepší ponětí o fungování internetu budou mít žáci, kteří mají doma přístup k (vlastnímu) tabletu nebo počítači.

2. JAK NA DATA

EPIZODY: VYHLEDÁVAČE, VIRY, HESLA, COOKIES

Po seznámení se základy fungování digitálního světa se ve druhé tematické oblasti pouštíme více do detailů role dat a jejich zabezpečení. Je dost možné, že v této kapitole se objeví pro žáky neznámé termíny. V rámci úvodního průzkumu můžete zmapovat, jak dobře se žáci v problematice zabezpečení dat na internetu orientují.

JAK POSTUPOVAT

Zkuste žákům položit níže uvedené otázky. Buď s nimi můžete vést řízenou diskusi, nebo jednotlivé otázky napište na malé papírky a poschovávejte je před začátkem hodiny v učebně. Kdo papírek najde, může otázku zbytku třídy přečíst.

- Jak vypadá bezpečné heslo?
- Je lepší mít jedno heslo na všechny možné internetové účty, nebo jich mít více?
- Jak se bránit před viry na internetu?
- Co jsou to cookies?
- Které internetové vyhledávače znáte?
- Co byste napsali do vyhledávače, když byste chtěli vědět, jaké je dnes počasí v Českých Budějovicích?

Sledujte, do jaké míry se odpovědi žáků shodují se zákonitostmi fungování internetu, na kterých panuje obecná shoda: zda žáci dokážou navrhnout bezpečná hesla, zda mají povědomí o ochraně proti virům (používání antivirových programů, vestavěné funkce prohlížečů varující před podezřelým obsahem, bezpečný pohyb na internetu) nebo zda tuší, že jsou o jejich pohybu na internetu sbírána data. Jejich úrovni poznání můžete následně přizpůsobit průběh lekcí ze druhé tematické oblasti.

Poznámka: V této fázi není nutné se pouštět u probíraných témat do hloubky, nechte případné otázky a řešení otevřené a vraťte se k nim v dané AV lekci, kde jsou pro tento účel připraveny konkrétní aktivity.

3. JAK NA ONLINE ZÁBAVU

EPIZODY: ONLINE HRY, ZÁVISLOST NA INTERNETU, RODIČOVSKÁ KONTROLA

Žáci 1. stupně ve většině případů používají internet primárně jako zdroj zábavy. Témata třetí tematické oblasti jim tedy budou jistě blízká. Abyste žáky navnadili na kritickou perspektivu, kterou jim chcete lekcemi nabídnout, nechte je prostřednictvím následující aktivity zmapovat terén ve třídě, co se týče jejich přístupu k online zábavě.

JAK POSTUPOVAT

Na tabuli napište nebo promítněte následující výroky. Úkolem žáků bude najít ve třídě alespoň jednoho člověka, který se s daným výrokem může ztotožnit, a zaznamenat si jeho jméno. Cílem je mít napsáno ke každému výroku jméno alespoň jednoho spolužáka, pro kterého daná věta platí.

Najdi někoho...

... kdo každý den hraje hry na počítači nebo mobilu.
... kdo alespoň jednou týdně hraje hry se spoluhráči online.
... kdo má doma herní konzoli.
... kdo má od rodičů stanovený časový limit na používání počítače nebo mobilu.
... kdo má od rodičů v počítači nebo mobilu nainstalovaný program, který blokuje nevhodný obsah.
... s kým rodiče hrají počítačové hry nebo se společně dívají na videa na internetu a povídají si o nich.
... s kým se rodiče někdy baví o tom, že ne vše, co vidí v počítačových hrách nebo videích na internetu, je skutečné.
... jehož rodiče hrají hry na počítači nebo na mobilu.

Poté, co vyprší časový limit, se zeptejte žáků, kdo zvládl napsat jméno ke každému výroku. Následně se u každého výroku ptejte, na koho daná věta sedí. Můžete žáky vybídnout k rozvedení jejich odpovědí, abyste získali přehled o rozmanitosti jejich zkušeností z oblasti online zábavy a rodičovské kontroly. Pokud je vám tento způsob práce blízký, využijte mobilní zařízení žáků, nechte si ukázat aplikace, které používají, nebo hry, které hrají.

4. JAK NA SOCIÁLNÍ SÍTĚ

EPIZODY: SOCIÁLNÍ SÍTĚ, LAJKY, JAK MLUVIT NA INTERNETU, TVOŘIT NA INTERNETU

Ačkoliv většina sociálních sítí umožňuje vytvoření účtu až od 13 let, jistě někteří vaši žáci některé z těchto služeb využívají. Než abyste se jich sami ptali na používání každé z nich, můžete je nechat zjistit tyto informace od sebe navzájem.

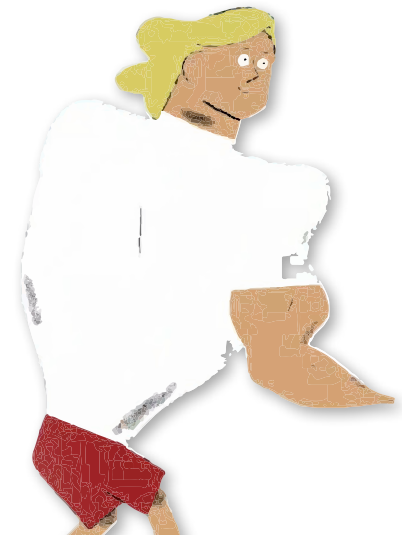
JAK POSTUPOVAT

Nechte žáky se posadit na židle do kruhu. Jeden žák bude stát uprostřed a dávat ostatním pokyny: „Ať si vymění místo ti, kdo…“, následováno popisem činnosti nebo chování vážícího se k používání sociálních sítí s tím, že daný výrok by měl platit i pro onoho „vyvolávače“ – například: „Ať si vymění místo ti, kdo používají TikTok“. V tu chvíli se ze svých míst zvednou ti, kdo TikTok používají, a pokusí se zasednout jinou židli. O to samé se pokouší i ten, kdo výrok pronesl. Ten, kdo zůstane bez židle, se stává mluvčím uprostřed a v dalším kole vyvolává.

Můžete nechat žáky si otázky vymýšlet, nebo jim dát k dispozici následující seznam možností:

Ať si vymění místo ti, kdo…
… používají nějakou konkrétní sociální síť.
… sami postují fotky, videa nebo texty na nějaké konkrétní sociální síti.
… ví, co jsou to lajky.
… si našli na sociální síti nějakého nového kamaráda.
… mají mezi svými „přáteli“ či sledujícími nebo sledovanými na sociálních sítích lidi, které osobně neznají.
… mají rodiče či prarodiče, kteří používají nějakou konkrétní sociální síť.

Když už žáci vyčerpají všechny své nápady na otázky, navažte na aktivitu reflexí. Můžete se vrátit k otázkám, na něž vás reakce žáků překvapily, například se můžete doptat, co přesně žáci dělají na sociálních sítích, které aktivně využívají. Uděláte si tak lepší představu o potenciálním rizikovém chování, které bude později dobré probrat v rámci příslušné AV lekce. Jednou z otázek v reflexi také může být, zda žáci vědí, jaká je věková hranice pro založení účtů na sociálních sítích (v naprosté většině případů je to 13 let) a proč je takto nastavena.



5. JAK TO VŠECHNO ZVLÁDAT CHYTŘE A BEZPEČNĚ

EPIZODY: KYBERŠIKANA, PRAVDA, NEBO NE?

Poslední tematická oblast se zabývá problematikou kyberšikany a dezinformací na internetu. Jelikož je téma kyberšikany velmi komplexní a vyžaduje citlivý a neuspěchaný přístup, doporučujeme jej v rámci úvodního průzkumu neotevírat, jelikož by nemuselo zbýt dostatek času pro ošetření případných negativních emocí, které by mohlo vyvolat.

Můžete však žáky navnadit na téma fake news a zeptat se jich, jestli někdy na internetu naletěli nějaké nepravdivé informaci. Pokud ano, můžete žáky nechat informaci dohledat nebo si článek, obrázek či video promítnout na tabuli a společně se zamyslet, jak by šlo poznat, že se nejedná o pravdivou informaci.

Pokud se nikdo z žáků nejprve nepřihlásí, zkuste je motivovat vlastním příkladem, kdy jste uvěřili nějaké informaci, která se pak ukázala jako nepravdivá. Pokud žádnou takovou zkušenost nemáte nebo daný příklad není vhodný pro žáky na 1. stupni, vyberte některý z často sdílených hoaxů či dezinformací například na webech www.hoax.cz nebo www.manipulatori.cz, dobře u mladších žáků také fungují smyšlené zprávy z webu Pravdivé zprávy (www.cool.iprima.cz/pravdive-zpravy). Smyslem této aktivity je navodit bezpečné prostředí pro následné diskuse o problematice dezinformací na internetu a umožnit žákům uvědomit si, že „naletět“ nepravdivé informaci může při troše nepozornosti opravdu každý.

JAK NA REFLEXI PO PROJEKCI

Bezprostředně pro projekci doporučujeme vždy provést tzv. reflexi. Ta je přínosná pro žáky i pro vás jako vyučujícího, protože vám naznačí, jak žáci o tématu přemýšlejí, což vám pomůže při dalším vedení hodiny.

PROČ MÁ SMYSL PROVÁDĚT REFLEXI

- Žáci se učí naslouchat jeden druhému.
- Každý dostává příležitost, aby se mohl vyjádřit.
- Reflexe vede žáky k respektu a k pochopení, že na věci je možné se dívat z různých úhlů.

Při reflexi pracujeme s prvními dojmy a emocemi, které v žácích zhlédnutá epizoda vyvolala. Výjimečně se může stát, že žáci budou i mlčet – i to je ale druh reakce, který musíme brát v úvahu. Platí, že smyslem reflexe není dojmy hodnotit; neříkáme, který je správný a který nikoliv, respektujeme individuální pohled každého žáka.

Existuje mnoho technik, kterými je možné reflexi provádět. My vás seznámíme s velmi jednoduchou a praktickou metodou, kdy každý řekne jedno jediné slovo popisující jeho pocit či dojem.

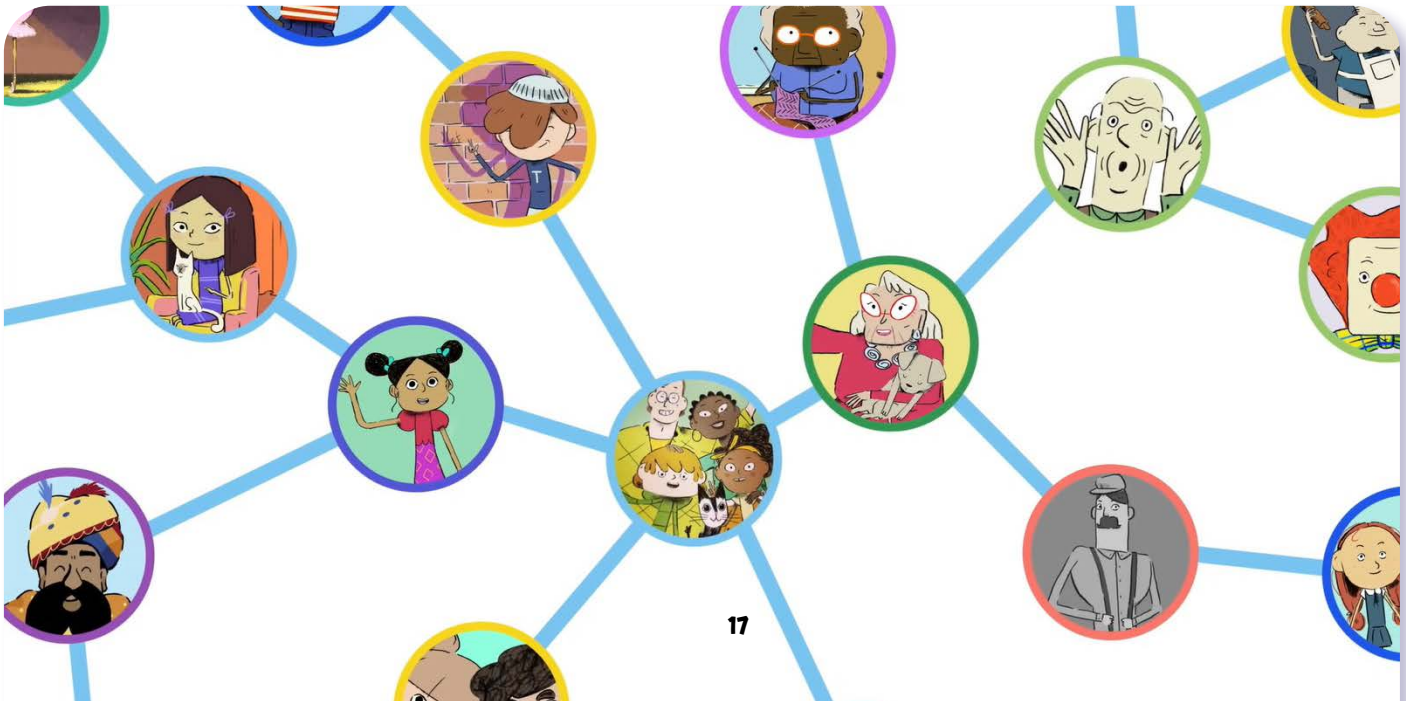
Pokud vás téma reflexe zaujalo, podívejte se na další metody reflexe, které doporučujeme při práci s audiovizuálními materiály: <jsns.cz/lekce/reflexe-po-projekci>.

METODA REFLEXE – JEDNO SLOVO

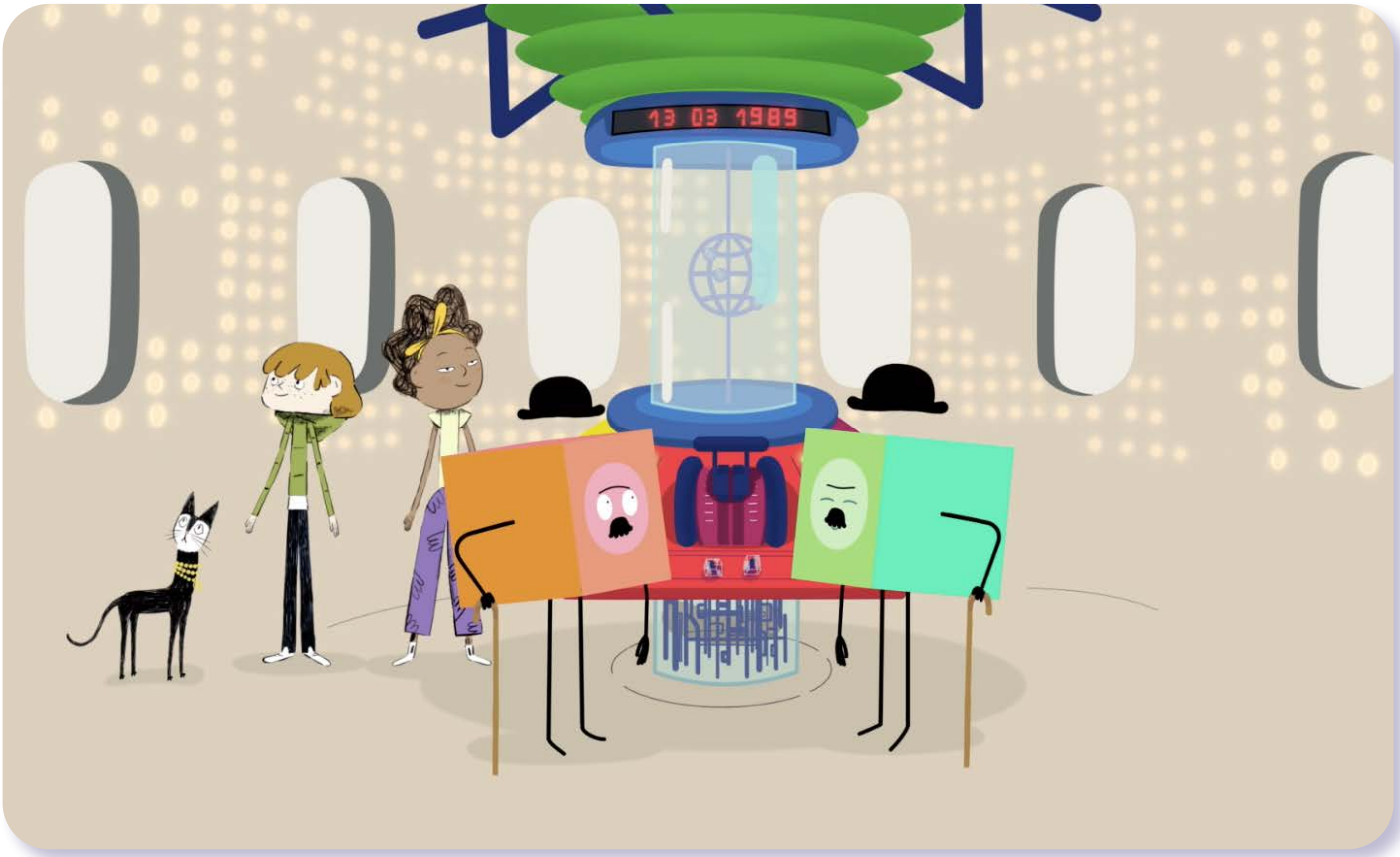
Pojmenovat jedním slovem svůj pocit či dojem nebo to, co nám po zhlédnutí filmu „zůstalo v hlavě“, většinou dokážou všichni. Výjimečně se stává, že žák jen zavrtí hlavou nebo řekne, že vůbec neví. V takovém případě na něj netlačíme. Je ale možné se k němu vrátit ve chvíli, kdy už všichni promluvili, a dát mu dodatečně prostor k vyjádření.

JAK PRO PROJEKCI POSTUPOVAT

1. Vyzveme žáky, aby řekli jedno slovo, které nejlépe ilustruje jejich dojem, pocit, nový poznatek nebo náladu ze zhlédnuté epizody.
2. Žáci odpovídají postupně a nejlépe popořadě, aby bylo přehledně vidět, kdo už mluvil.
3. Jednotlivá slova zapisujeme na tabuli, ale nijak nekomentujeme. Můžeme každé slovo při zápisu zopakovat, aby bylo srozumitelné pro všechny. Uvidíme pak přehledně, jak epizoda působila na třídu jako celek, které dojmy či poznatky se opakovaly apod.
4. V případě, že někdo nechce odpovídat, vrátíme se k němu na konci.
5. Žáci mohou opakovat stejná slova. Zapisujeme pak u daného slova čárky jako symbol pro opakování. Nicméně pobídneme je k nové formulaci či pojmenování dalšího dojmu z filmu.
6. Poté, co všichni odpověděli, můžeme žáky vyzvat k doplnění komentářů k uvedeným slovům. Můžeme se také přímo zeptat na slova, která nás zaujala a která je dobré rozvést.



4. AUDIOVIZUÁLNÍ LEKCE DO VÝUKY



V digitálním světě

Výlet do historie

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Kostičky Ping a Pong berou Mínu, Filipa a Kocoura strojem času na výlet do historie internetu. Za zvuku připojujícího se modemu se nestačí divit, jak pomalu se dříve internetové stránky načítaly. A jak vůbec vznikl internet? Vědce nejdříve napadlo, že by bylo výhodné propojit počítače, aby mohly sdílet informace. Časem se funkce rozšířila i na elektronickou poštu a posílání krátkých textových zpráv. Síť dostala jméno World Wide Web a její tvůrci ji následně darovali veřejnosti s myšlenkou bezplatného sdílení informací.

CÍLE LEKCE

1. dozvědět se více o tom, jak vznikl internet
2. uvědomit si, jak se informace sdílely v minulosti
3. porovnat rozdíly mezi současností a přítomností z hlediska šíření informací

DOPORUČENÝ VĚK

8+ LET

AKTIVITA: Výlet do historie !!!

ANOTACE

Žáci si v úvodu hodiny vyrobí jednoduchý provázkový telefon. Díky časové ose pochopí, že internet je mladý fenomén. Ve dvojicích se zamyslí, jak lidé zjišťovali a sdíleli informace v době bez internetu. Pojmenují výhody a nevýhody světa bez internetu a s internetem.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV, VDO

KLÍČOVÉ KOMPETENCE

ZV a GV: k učení, k řešení problémů, komunikativní, sociální a personální, občanské

CÍLE

Žáci:
- si uvědomí, jak se informace sdílely v minulosti
- se dozví, kdy internet vznikl
- zhodnotí výhody a nevýhody dnešního rychlého přenosu informací

DÉLKA

45 min. (včetně projekce)

POMŮCKY

- MATERIÁL
- 2 kelímky pro každou dvojici, např. od jogurtu
- klubko s provázkem
- nůžky
- kolíčky nebo kancelářské sponky
- menší kartičky (prázdné)
- PRACOVNÍ LIST 1A a 1B do dvojic
- LIST PRO VYUČUJÍCÍ 1
- LIST PRO VYUČUJÍCÍ 2

POSTUP

1. Žáky **rozdělíme do dvojic**. V úvodu hodiny si každá dvojice vyrobí provázkový telefon. Dvojice pracuje se dvěma kelímky. Do obou uděláme na dně dírku, kterou protáhneme provázek a uděláme uzly. Kelímky natáhneme od sebe – do jednoho mluvíme a v druhém posloucháme. Provázek musí být pečlivě natažený a nesmí se ničeho dotýkat, jinak by se přenos zvuku nepodařil. Můžeme společně zhodnotit, nakolik je tento způsob komunikace a přenosu informací vhodný i pro každodenní situace.

2. Následuje **projekce epizody seriálu**.
Ověříme, zda žáci epizodě porozuměli. Ptáme se:
Kam se vypravili Mína a Filip? Jak vypadala první internetová stránka? Líbilo se jim na výletě?
Poznámka: Pokud je to potřeba, snímek můžeme přehrát opakovaně.

3. Společně s žáky **vytvoříme časovou osu**, ze které by mělo být patrné, že internet (a digitální revoluce) je v dějinách lidstva velmi mladý fenomén. Můžeme opět pracovat s pomocí provázku na zemi. Na natažený provázek můžeme v přiměřených vzdálenostech zobrazujících časové intervaly připnout kartičky s událostmi – návrhy, co je možné zobrazit na časové ose, najdete v LISTU PRO VYUČUJÍCÍ 1.

4. Žáci opět vytvoří stejné dvojice, které spolu pracovaly v úvodu hodiny. Všechny vzniklé dvojice **rozdělíme do dvou skupin – A a B**. Do každé dvojice rozdáme PRACOVNÍ LIST. Dvojice **skupiny A** mají za úkol vymyslet co nejvíc způsobů, **jak zjistit zadanou informaci bez použití internetu** a online nástrojů. Dvojice **skupiny B** mají za úkol vymyslet co nejvíc způsobů, jak offline **informaci šířit**.

5. V dalším kroku dvojice stejné skupiny **sdílí svoje návrhy**.
Poznámka: Je možné využít **metodu sněhové koule** – spojíme první dvě dvojice se stejným úkolem, které mezi sebou sdílí svoje návrhy, postupně „nabalujeme“ další dvojice. Na závěr zástupce skupiny A a skupiny B představí své návrhy.
Návrhy řešení mohou vypadat například takto:
Skupina A: Zeptám se rodiče nebo učitele, vyhledám v encyklopedii – doma, ve škole, v knihovně...
Skupina B: Zatelefonuju z pevné linky, zajedu za babičkou na kole a informaci jí řeknu osobně, pošlu telegram nebo fax.

REFLEXE AKTIVITY

Reflexi necháme proběhnout formou diskuse. Ptáme se: *Jaké výhody nebo nevýhody mělo zjišťování a předávání informací v době před internetem? Jaké dnes?*
Okruhy témat, které by bylo možné v reflexi zmínit, najdete v LISTU PRO VYUČUJÍCÍ 2.

Doporučujeme seznámit se také s **informačním materiálem OTÁZKY A ODPOVĚDI**.
Poznámka: Dá se předpokládat, že žáci budou potřebovat vysvětlit, jak fungovala pevná linka, ukázat obrázek telefonu, vysvětlit, co byl telegram a fax nebo co je encyklopedie.

ZKUŠENOSTI Z PRAXE

Aktivitu jsem vyzkoušel v běžné třídě, bez zkušeností s mediální výchovou. Dětem se líbila grafika i hudba ze seriálu, chtěly ihned vidět i další díly.
Pro žáky bylo nové zjištění, že telefon je mnohem starší, než si představovali. Překvapilo mě, že sami uváděli mnoho nevýhod dnešní internetové doby. Uvědomovali si cenu technologií v minulosti a její nedostupnost, formulovali závislost na množství zbytečných informací v současné době. Při hledání odpovědi na otázku, kdo vynalezl telefon, si neuvědomili možnost zavolat pevnou linkou a neuvedli možnost využít knižní encyklopedie.
Pavel Mikoláš, *ZŠ Benešova, Třebíč*

PRACOVNÍ LIST

Skupina A:

Představte si, že žijete v roce 1989 a NEMÁTE tedy k dispozici ani počítač s internetem, ani chytrý telefon.

Vymyslete co nejvíce způsobů, jak byste zjistili, KDO VYNALEZL TELEFON.

Skupina B:

Představte si, že žijete v roce 1989 a NEMÁTE tedy k dispozici ani počítač s internetem, ani chytrý telefon. Narodil se vám sourozenec.

Vymyslete co nejvíce způsobů, jak to DÁT VĚDĚT BABIČCE, která žije v jiném městě.

LIST PRO VYUČUJÍCÍ 1

Na časové ose můžete zobrazit například tyto události:

21. století
- Aktuální rok
- Rozšíření smartphonů: kolem 2010
- Narodil/a jsem se: 2008/2009/2010/

20. století
- Narodili se rodiče
- Vznik internetu: 60./70. léta
- Narodili se prarodiče
- Vznik Československa: 1918

19. století
- Začátek výroby automobilů: 1885
- Vynález telefonu: 1876

Středověk
- Vynález knihtisku: 1455

Začátek letopočtu

První písmo: kolem 3000 př. n. l.

Vznik lidstva: před 200 až 400 tisíci let

Vymírání dinosaurů: před asi 66 miliony let

LIST PRO VYUČUJÍCÍ 2

Nevýhody – minulost

Informace se zjišťovaly a předávaly pomalejším a komplikovanějším způsobem.

Telefon neměl každý člověk, dokonce ani každá rodina.

Pro „rychlou“ zprávu se používal telegram.

Nikdo neměl počítač – psalo se na psacím stroji (komplikované opravování a přepisování).

Přivolání pomoci v nouzi bylo složitější.

Psaly se dopisy a pohledy (je to výhoda, nebo nevýhoda?).

Výhody – minulost

Více přímé komunikace z očí do očí.

Možnost nebýt dostupný, nebýt neustále na telefonu.

Víc času na hraní si venku.

Méně kontroly od dospělých.

Psaly se dopisy a pohledy (je to výhoda, nebo nevýhoda?).

Mnohem méně reklamy.

Nevýhody – současnost

Obrovské množství informací online, ve kterých je obtížné se vyznat.

Na internetu se rychle a snadno šíří i lži nebo pomluvy.

Na internetu je „všechno navždy“ včetně osobních informací o nás (tzv. digitální stopa).

Všichni čekají, že každý vždy zvedne mobil a má ho stále s sebou.

Zařízení se snadno ztrácí, rozbíjí a stojí dost peněz.

Lidé se nedívají na sebe, ale do mobilů (těch se také hodně dotýkají, možná více než lidí).

Výhody – současnost

Díky technologiím jsou možnosti téměř „nekonečné“: zabavit se, tvořit, hrát si, vzdělávat se, pracovat, platit, organizovat, vyjadřovat názor a diskutovat.

Snadné a rychlé vyhledání i šíření informací.

Snadné psaní a úpravy textu (včetně pravopisu).

Telefonování i s obrazem.

Okamžité přivolání pomoci.

Usnadnění života postiženým (technologie jim pomáhají).

OTÁZKY A ODPOVĚDI

1. Co je to internet?

Internet je **mezinárodní počítačová síť**, která umožňuje vzájemnou komunikaci počítačů a různých zařízení po celém světě. Název je složen ze slov inter (mezi) a net (síť). Původně se slovem Internet označovala jedna konkrétní síť, která propojovala vědecké počítače, ale později se název vžil jako označení celosvětové sítě.

2. Kdy, jak a proč internet vznikl?

Příběh internetu je spjat **s vývojem počítačů**. Dnes se to zdá neuvěřitelné, ale před desítkami let byly počítače obrovské stroje, které zabraly třeba celou jednu místnost. Měly za úkol počítat složité matematické problémy a jeden výpočet jim trval dny, týdny i měsíce. Aby se výpočty urychlily, počítače, které nebyly vytížené, počítaly jednu část problému, zatímco další jinou. I proto narůstala potřeba, aby spolu **jednotlivé počítače komunikovaly a předávaly si výsledky**. Tehdejší komunikace však byla velmi omezená – počítače musely být fyzicky propojené jeden s druhým. Proto se vývoj zaměřil na způsob **vzájemné komunikace více počítačů v tzv. síti**, kde by mohlo vzájemně komunikovat více počítačů. Na tomto úkolu pracovali američtí inženýři **Bob Kahn** a **Vint Cerf**, a proto jsou označováni jako otcové internetu.

ARPANET: zárodek internetu

Vývoj internetu ovlivnila i politická situace. V době studené války spolu soupeřily Spojené státy a Sovětský svaz. Chtěly uspět například při dobývání vesmíru a jedním z projevů jejich soutěže se stala i snaha získat technologickou převahu. Americká armáda si dala za cíl vytvořit takovou síť počítačů, která by byla provozuschopná i v případě, že by nepřítel vyřadil některou její část.

USA proto založily organizaci ARPA, jejímž cílem bylo podporovat výzkumné projekty, které povedou k převratným technologiím. První úspěch přišel v roce 1969, kdy vznikla síť ARPANET, která spojovala čtyři univerzity a přenášela mezi nimi informace. Byl to takový dnešní „malý internet“.

Brzy vědci vymysleli také **první e-mailový program** pro posílání zpráv mezi uživateli sítě. Jeho tvůrcem – a také autorem znaku @, který dnes známe jako zavináč – byl programátor **Tomlinson**. E-mailová komunikace se v rámci ARPANETu stala velmi populární.

Do sítě ARPANET se postupně přidávaly desítky dalších univerzit a institucí v USA a od roku 1973 i zahraniční instituce, mezi prvními jedna z univerzit v Londýně nebo norský seismologický ústav NORSAR.

Zánik ARPANETu a vznik nové sítě

V roce **1986** vzniká síť **NSFNET** provozovaná americkou nezávislou vládní agenturou pro podporu vědeckého výzkumu (NSF). Původní ARPANET později zanikl a nahradila ho samostatná síť MILNET. V té době však byly sítě stále ještě centrálně řízeny a určeny především pro univerzity a státní instituce. Veřejnost je stále ještě nemohla využívat.

Změna byla však jen otázkou času. Na přelomu 80. a 90. let vzniká ve švýcarské laboratoři CERN **první web**, který původně sloužil k výměně informací a dokumentů. Autory jsou **Tim Berners-Lee** a **Robert Cailliau**, který se později zasloužil o uvolnění této technologie webu z CERNu pro veřejnost v roce **1993**.

Struktura veřejného internetu:

Síťový uzel

a) **Propojovací bod** je zařízení, které vzájemně propojuje sítě
b) **Koncový bod** je zařízení, které je připojené k síti a zpracovává data (počítač, mobil, TV)

Jako **propojovací bod** si můžeme představit **modem** nebo **router**, který máte doma od svého poskytovatele internetu. Ten zajistí připojení vaší domácí počítačové sítě, kde máte propojená různá zařízení (počítač, notebook, mobil, chytrou TV, tiskárnu, kamery), k jeho síti. Ta je pak připojena přes další propojovací bod (router) k další větší síti nebo už přímo k páteřní síti, která je dále připojená k jiné páteřní síti v jiné zemi.

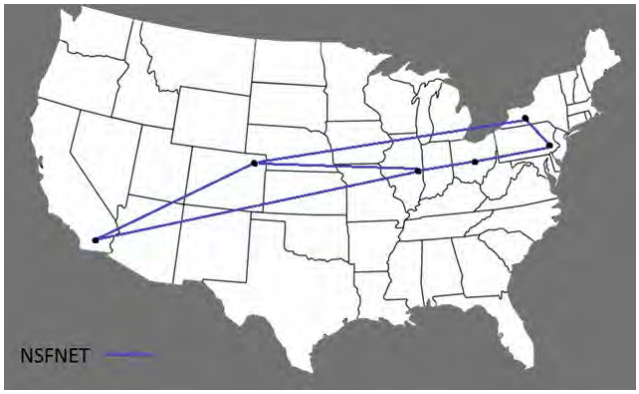
Páteřní síť umožňuje propojení nejdůležitějších síťových uzlů a vyznačuje se možností přenášet velké množství dat. Je to dáno zejména technologií, jakou je vybudována. V současnosti to jsou optické kabely, které umožňují přenášet data velkou rychlostí.

Strukturu sítě si můžeme představit jako krevní oběh. Srdce je velký router a spojuje nám dvě různé sítě, Malý oběh a Velký oběh. Síť Malý oběh vede do plic, kde se krev okysličí.

Síť Velký oběh zajišťuje přenos potřebných věcí do všech částí těla. Hlavní přenos vede tepnou největší a nejsilnější proud. K tepnám jsou připojeny menší cévky (poskytovatelé), které vedou blíže k příslušným orgánům, a k nim jsou připojeny kapiláry, které vedou do konkrétních tkání a tam vzniká výměna látek (teda informace a služby pro uživatele)

Podobně jako krevní oběh přenáší mnoho látek, nejenom kyslík, ale i různé živiny, a zajišťuje odvod odpadních látek v těle, poskytuje internet mnoho různých služeb.

Nejznámějšími službami jsou webové stránky a e-mail. Webové stránky umožňují zveřejňovat texty, obrázky, videa; e-mailová komunikace usnadňuje posílání zpráv a dokumentů mezi jednotlivými uživateli. Další službou jsou například různé konferenční programy, které umožňují pořádat videokonference mezi jednotlivými účastníky z různých koutů světa. Na pozadí je skryto také mnoho služeb, kde si jednotlivá zařízení sdílí svoje data. **Internet je označení pro obrovskou mezinárodní počítačovou síť a díky ní můžeme využívat mnoho na ni navázaných služeb.**



NFSNET v roce 1986
(zdroj: https://cs.wikipedia.org/wiki/NSFNET)

3. Jak vypadalo první připojování na internet?

V počátcích internetu byla většina firem a domácností připojená pomocí modemu tzv. **vytáčeným připojením** (dial-up). Modem byl zapojen do klasické telefonní linky, což znamenalo, že v jednom okamžiku bylo možné buď telefonovat, nebo být připojen k internetu, nikoliv ovšem obojí najednou. Později se objevila technologie ISDN (Integrated Services Digital Network), která tento nedostatek odstranila a zvýšila se také rychlost připojení, protože data už byla přenášena digitálně.

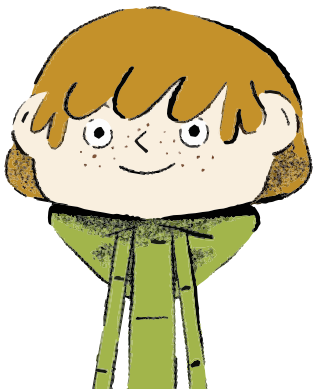
V současnosti se pro spojení pevnou linkou využívá **DSL technologie**. Firmy dnes využívají hlavně **optické kabely**, kde rychlost spojení není omezená vzdáleností.

V dnešní době se ve velké míře využívá **bezdrátové připojení – wifi –**, které je dostupné na mnoha veřejných místech a často je i zdarma.

Wifi může být **zabezpečená** nebo **nezabezpečená**. Na nezabezpečené síti rozhodně není dobré přihlašovat se do osobních účtů (e-mail, internetové bankovnictví apod.); u zabezpečené wifi pak záleží na typu zabezpečení – například doma by měla být dobře zabezpečená, aby do ní nikdo neproniknul, ale například ve fastfoodovém řetězci heslo stejně nezajišťuje vysokou bezpečnost, protože ho má možnost získat téměř každý.

Mnoho lidí dnes využívá k připojení k internetu **mobilní data**, která za poplatek poskytují operátoři. Díky tomu mohou být chytré mobilní telefony připojeny k internetu všude tam, kde je dostupný signál.

Jaké byly začátky internetu v Československu, resp. České republice?
První pokusy o připojení k internetu se v Československu odehrály v listopadu 1991, kdy začala fungovat linka z Českého vysokého učení technického (ČVUT) v Praze do internetového uzlu v rakouském Linci.



Oficiální připojení k internetu proběhlo 13. února 1992 a opět se tak stalo na půdě ČVUT. Postupem času, i když zpočátku pomalu, se k internetu začaly připojovat další instituce, firmy nebo domácnosti. Větší rozmach internetu nastal až po roce 2000.

V době, kdy internetové připojení nebylo ještě rozšířené, existovaly tzv. internetové kavárny, v nichž byly pro návštěvníky k dispozici počítače s připojením.

4. Co to znamená www?

Jedná se o zkratka slov World Wide Web **nebo také zkráceně** web. Označuje celosvětovou počítačovou síť, která má sloužit pro ukládání, prohlížení a odkazování dokumentů.

Autorem **webu** a s ním spojeného programovacího jazyka **HTML,** který umožňuje vytvářet webové stránky, je **Tim Berners-Lee**. Využil přitom myšlenku Vannevara Bushe o **hypertextu**, publikovanou již v roce 1945. Princip je založen na existenci **odkazů v textu**, které v případě kliknutí převedou uživatele na jinou část textu nebo na jiný článek, případně na úplně jiné stránky.

Pro přenos webových stránek mezi počítači vyvinul Tim Berners-Lee soubor pravidel nazvaný **HTTP** (hypertext transfer protocol), který známe i z webových adres (http://).

K prohlížení webových stránek využíváme **webové prohlížeče**, mezi nejčastěji používané patří Google Chrome, Internet Explorer, Mozilla Firefox nebo Safari, v České republice je známý Seznam.

5. Jak se vyvíjely vyhledávače a webové stránky?

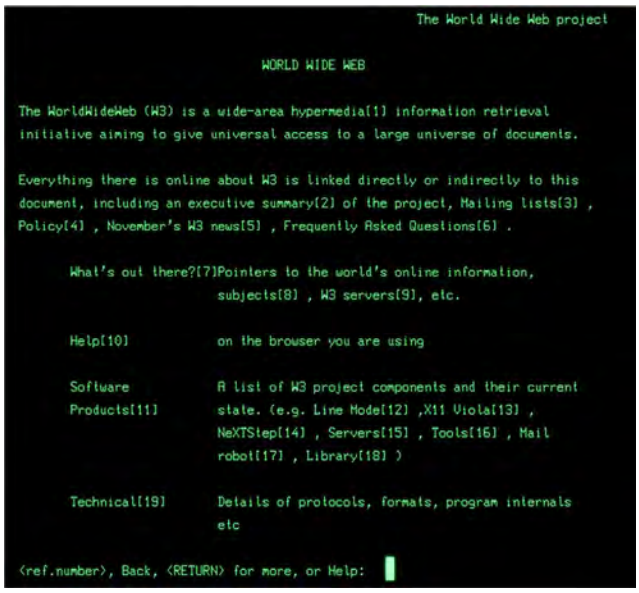
První **webová stránka** v prvním prohlížeči vypadala jako pouhý text.

S rozšiřováním obsahu internetu a vznikem nových stránek se zvyšovala potřeba **katalogizace** a **vyhledávání obsahu**. Existovaly katalogy stránek, kde bylo možné stránky ručně přidávat do různých kategorií (jako Instituce, Zábava, Kultura a umění). Ve světě byl známý server **Yahoo** vytvořený v roce 1994. V České republice fungoval mezi prvními od roku 1996 Seznam.cz.

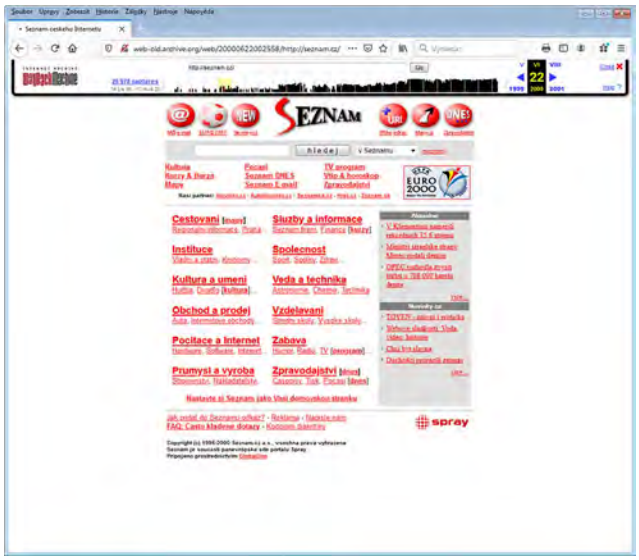
Protože ruční zadávání odkazů do katalogu bylo náročné, vznikly později specializované programy – tzv. fulltextové vyhledávače, které díky algoritmům prohledávaly „celý internet“ a uživatelům výrazně usnadnily orientaci na internetu. Mezi oblíbené vyhledávače patřil v minulosti portál **Altavista**. V České republice byl populární **Kompas**, který umožnil zadávat dotazy s českou diakritikou.

Nejznámějším vyhledávačem je dnes **Google**, který v roce 1998 založili studenti Stanfordovy univerzity Sergey Brin a Larry Page. Svůj fulltextový vyhledávač postupně zdokonalovali, až se stal synonymem vyhledávání. Průlomové bylo řazení odkazů podle hodnocení – PageRanku.

Složitý algoritmus hodnotil kvalitu stránek například i podle množství odkazů na ní.



Ukázka první webové stránky (zdroj: http://line-mode.cern.ch/www/hypertext/WWW/TheProject.html)



Takto vypadala stránka Seznam.cz v polovině roku 2000 (zdroj: http://web-old.archive.org/web/20000622002558/ http://seznam.cz/)

6. Co se od počátků internetu nejvíce změnilo?

Nejdůležitější změnou je zlepšování technologií pro přenos dat a s tím související **zrychlení** jejich toku. Dříve se webové stránky načítaly velmi pomalu, což změnily moderní technologie, a díky tomu může být dnes na webových stránkách i složitější grafika, videa atd. Výrazně se zvýšil také výkon samotných počítačů a objevila se i nová zařízení – chytré telefony (smartphony) a tablety.

Změnil se i způsob **vyhledávání na internetu**. Dnes je možné nalézt požadovanou stránku nebo informaci nejen pomocí textu, ale i podle obrázku.

K internetu lze připojit **chytrá zařízení** nejen v průmyslu, ale i v domácnosti – videokamery pro zabezpečení domácnosti nebo například kontrolu a nastavení vytápění domu. Ovládání zařízení na dálku pomocí internetu se nazývá **internet věcí** (Internet of Things – IoT).

Obrovskou změnou je také **široká dostupnost a možnost připojení**. Existuje jen málo míst, kde je internet nedostupný.

Masové rozšíření internetu má ale i své **negativní stránky** – skrze internet se šíří také dezinformace, využívají ho útočníci ke kyberútokům a řada lidí se na internetu stává závislými.

Odpovědi vypracoval:

Josef Džubák, IT specialista, hoax.cz

Podívejte se na lekci V digitálním světě: Výlet do historie na <jsns.cz/mv/vylet-do-historie>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.

POZNÁMKY

V digitálním světě

Digitální svět

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Mína, Filip a Kocour se ocitli v digitálním světě a diví se, že je prázdný. V tom je Surfař zachrání před vlnou čísel, která se na ně valí. Jakým jazykem „mluví" počítače, telefony, tablety a další elektronická zařízení? Říká se mu binární kód, což je soustava jedniček a nul, do kterých si digitální přístroje překládají příkazy a informace, jež jim zadáváme. Stačí, aby Mína sáhla pro jedinou číslici a přemístila ji v moři dat, která stojí za slovy či obrázkem na displeji, a vše je vzhůru nohama.

CÍLE LEKCE

1. uvědomit si rozdíl mezi reálným a digitálním světem
2. seznámit se s binárním kódem
3. začít se základy programování

DOPORUČENÝ VĚK

8+ LET

AKTIVITA: Binární kód

!!!

ANOTACE

Žáci si prostřednictvím aktivity uvědomí rozdíly mezi digitálním a reálným světem. Ve trojicích si v pracovních listech vyzkoušejí převádět slova do binárního jazyka, což jim pomůže pochopit práci počítače.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k učení, k řešení problémů, komunikativní, sociální a personální

CÍLE

Žáci:
- si uvědomí rozdíl mezi reálným a digitálním světem
- se seznámí s pojmem binární kód a naučí se do něj převádět abecedu

DÉLKA

45 min. (včetně projekce)

POMŮCKY

- PRACOVNÍ LIST pro každého žáka

POSTUP

1. Ptáme se žáků: *Co je to digitální svět? Co tvoří jeho opak?* (reálný svět)
2. Uvádíme jednoduché příklady z digitálního a reálného světa (kniha, SMS zpráva, babička, zlaté pohárky nasbírané ve hře). Děti určují (zvednutím jedné nebo obou rukou), jestli jde o reálný, nebo digitální svět.
3. Následuje **projekce dílu seriálu**.
   Poznámka: Snímek doporučujeme zhlédnout nejméně dvakrát.
4. Poté se žáků ptáme: *Z čeho bylo moře v digitálním světě? Jak v digitálním světě vznikal obrázek? Co se s obrázkem dělo?* Pokud mají žáci nejasnosti, vysvětlíme.
   (Surfař vezme děti na oceán složený z nul a jedniček. Na pláži pixely z nitě kódu „pletou" fotografie. Když jim děti do kódu „sáhnou", obrázek se změní.)
   Poznámka: Doporučujeme seznámit se s textem OTÁZKY A ODPOVĚDI k lekci.
5. Žákům rozdáme PRACOVNÍ LIST, aby si **vyzkoušeli kódování** – převedení textu na počítačem zpracovatelná data, tedy jedničky a nuly. Využívají k tomu převodovou tabulku a list pro kódování.
   Žáky rozdělíme do skupin po třech. Každý má ve skupině jinou funkci.
   Odesílatel si vymyslí krátké slovo na tři písmena a předá ho **počítači**, ten slovo převede do binárního kódu a předá ho **příjemci** – ten ho převede z binárního kódu opět do naší řeči.
6. Žáci ve skupině se postupně ve funkcích vystřídají.

REFLEXE AKTIVITY

Zjišťujeme, jestli bylo kódování a dekódování úspěšné a žákům se povedlo doručit příjemci původní slovo. Ptáme se i na to, co se jim nepodařilo. Pracujeme s chybou jako něčím v práci zcela běžným. Klademe otázku: *Co se stalo, když někdo přesně neopsal binární kód ke svému písmenu?* Dojdeme s žáky k tomu, že vzkaz byl zkreslený, dostali jiné nebo žádné písmeno. Můžeme znovu poukázat na seriál, kde se po odebrání nuly změnil nebo zdeformoval obrázek. Diskusi uzavřeme zopakováním, že počítače používají svůj vlastní digitální jazyk, který se skládá jen ze samých jedniček a nul.

ZKUŠENOSTI Z PRAXE

Žáci bez obtíží porovnali digitální a reálný svět. Vše hned pochopili a bezprostředně po projekci epizody začali komentovat, co viděli. Velmi je bavilo kódování a dekódování, většina žáků si po aktivitě ve volném čase dále zkoušela psát delší slova. Někteří si i odnesli tabulku s abecedou domů a zkoušeli kódovat pro sourozence a rodiče. Při prvním kódování se mnohokrát stalo, že se v tabulce spletli a vycházela jim jiná slova. Žáci se divili, že na internetu chyby moc nejsou, i když se lehce v nulách a jedničkách můžete ztratit. Doporučuji dětem ukázat i jiné možnosti šifrování, například Morseovu abecedu.
Markéta Břešťanová, *Základní škola Červený vrch, Praha*

PRACOVNÍ LIST

Převeďte slovo do binárního kódu:

Odesílatel si vymyslí krátké slovo na tři písmena a předá ho počítači, ten slovo převede do binárního kódu a předá ho příjemci – ten ho převede z binárního kódu opět do naší řeči.

PŘEVODOVÁ TABULKA

A	01000001	**I**	01001001	**Ř**	1100010110011000	**Ž**	1100010110111101
B	01000010	**J**	01101010	**S**	01010011	**Á**	1100001110000001
C	01000011	**K**	01001011	**Š**	1100010110100000	**É**	1100001110001001
Č	1100010010001100	**L**	01001100	**T**	01010100	**Ě**	1100010010011010
D	01000100	**M**	01001101	**Ť**	1100010110100100	**Í**	1100001110001101
Ď	1100010010001110	**N**	01001110	**U**	01010101	**Ý**	1100001110011101
E	01000101	**Ň**	1100010110000111	**V**	01010110	**Ó**	1100001110010011
F	01000110	**O**	01001111	**W**	01010111	**Ú**	1100001110011010
G	01000111	**P**	01010000	**X**	01011000	**Ů**	1100010110101110
H	01001000	**Q**	01010001	**Y**	01011001		
CH	0100001101001000	**R**	01010010	**Z**	01011010		

Poznámka: Pokud bychom psali malými písmeny, kód by byl odlišný. Zdroj: https://nickciske.com/tools/binary.php

LIST PRO KÓDOVÁNÍ

písmeno

_____

písmeno

_____

písmeno

_____

OTÁZKY A ODPOVĚDI

1. Co jsou to digitální technologie? Jak fungují?

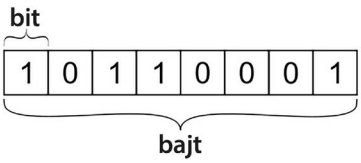
Digitální technologie jsou zařízení, která na rozdíl od analogových **používají k uchování informace binární podobu dat**. Jedná se například o počítač, tablet, mobilní telefon, digitální fotoaparát, ale i wifi, počítačové sítě, bluetooth, DVD nebo USB flash disk a další.

Všechny digitální technologie **využívají digitální záznam**, který se ukládá ve formě nul a jedniček. Tyto informace se pak většinou nezaznamenávají přímo, ale dochází k dalšímu kódování a komprimování, aby binární podoba analogického obrazu nebyla příliš velká. Pokud přenášíme například obraz, pak se nepřenáší obraz samotný, ale pouze číselný údaj o tom, jak má tento obraz vypadat. Jednotlivá čísla obsažená v přenášeném signálu nesou informaci o barvě, jasu, velikosti a umístění každého obrazového bodu (pixelu). Stejně tak se děje i v případě zvuku, textu či jiných dat.

Digitální technologie tedy nepracují v desítkové soustavě, ale v soustavě dvojkové neboli binární. To usnadňuje přenos a zvyšuje odolnost vůči chybám. Digitální data se dnešními moderními technologiemi přenášejí a uchovávají jednodušeji a efektivněji než data analogová.

2. Proč jsou v binárním kódování právě hodnoty 0 a 1?

Binární kódování **využívá principu jednoduchosti**, tedy pouze významu ano/ne, svítí/nesvítí, zapnuto/vypnuto. A tomu v binárním kódování odpovídají právě dvě hodnoty: 0 a 1. Tato základní jednotka se nazývá 1 bit (1 b) a z ní se tvoří větší bloky neboli bajty. 1 bajt (1 B) představuje 8 bitů (8 b), tedy osm po sobě jdoucích nul či jedniček.

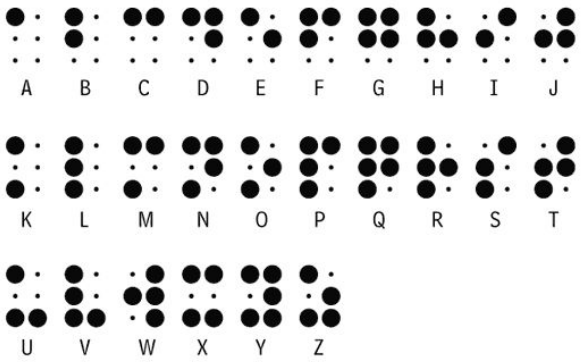


Jedním bajtem můžeme vyjádřit až 256 hodnot. I to je však velmi malá jednotka, a proto jsou používány její násobky, jako je kilo, mega, giga, tera atd. Binární kódování je univerzální metodou zpracování informací.

3. Kdo binární kódování vymyslel?

Binární kód poprvé představil v 17. století německý matematik a filozof **Gottfried Wilhelm Leibniz**. Snažil se najít systém, který by převáděl logické slovní prohlášení na čistě matematické. Vytvořil systém složený z řady nul a jedniček. Během svého života však Leibniz nenašel pro svůj systém využití.

V 19. století napsal britský matematik a filozof George Boole článek, v němž popisuje algebraický systém logiky založený na binárním přístupu, v tomto případě ano/ne a on/off přístupu. Používá tři základní operace: AND, OR a NOT. Tento systém však až ve 20. století uvedl do praxe student Massachusettského technologického institutu Claude Shannon. Shannon využil Booleovu metodu v praktických aplikacích, jako jsou počítače, elektrické obvody a další.



Na podobném principu jako binární kódování funguje i Braillovo písmo, které používají ke čtení a psaní nevidomí lidé. Tento systém se skládá z šesti pozic teček, přičemž v každém sloupci jsou tři tečky.

4. K čemu se binární kódování používá? Co je to programování?

Části našeho reálného světa, který je analogový, někdy potřebujeme **přeložit do digitální podoby** a právě k tomu používáme binární kódování. Například pro každé písmeno abecedy existuje jedinečný zápis v podobě nul a jedniček. K tomu, abychom naučili počítač **provádět různé úkony**, například přehrávat hudbu nebo zobrazovat webové stránky, slouží programování.

Počítačům a podobným zařízením je potřeba všechny příkazy zadat právě v binární podobě. Ale pro člověka je práce s nulami a jedničkami velice náročná a nepřehledná, proto používáme **programovací jazyky**. V programovacím jazyku zapíšeme, co má počítač dělat, a to lidsky čitelnými příkazy. Následně tyto čitelné příkazy pomocí speciálního nástroje přeložíme do strojového kódu v podobě nul a jedniček. A tento strojový kód už umí použít procesor počítače ke zpracování dat.

Programování probíhá v různých programovacích jazycích. Je to poměrně složitý proces, kdy je třeba **stanovit si cíl** a k němu dojít **pomocí správného algoritmu** (přesného návodu či postupu) a následně **zapsat zdrojový kód**. Vyžaduje to vynikající znalost daného programovacího jazyka, logické myšlení a smysl pro detail. Samotným programováním však proces nekončí, nedílnou součástí je i testování, ladění a následná údržba systému. Tomu všemu se souhrnně říká softwarové inženýrství.

Existuje nepřeberné množství programovacích jazyků. Mezi nejvíce používané se řadí Python, C/C++, PHP, Java a další.

Některé programovací jazyky jsou vhodné pro tvorbu mobilních aplikací, jiné zase na programování počítačových her, další pro tvorbu webových stránek a průmyslových úloh, například robotů výrobních linek.

5. Jak se můžu naučit programovat? Jak začít?

Programovat se mohou děti naučit poměrně snadno a rychle. Existuje k tomu celá škála programů či aplikací. Pro žáky na 1. stupni ZŠ je vhodný například **Scratch**. Je možné jej spustit přímo z webového prohlížeče. Menším dětem (ve věku 5 až 8 let) je určená aplikace **ScratchJr**, kterou si mohou na Google Play či App Store stáhnout přímo do mobilu nebo tabletu.

Tato hra naučí děti přemýšlet jako programátor. Mohou si vytvořit svůj vlastní příběh za použití různých postav a předmětů, zasadit je do rozličných situací. Postavy se pohybují a mluví přesně tak, jak si dítě určí zadáním jednoduchých příkazů (složením bloků s příkazy). Ovládání je intuitivní, ale přesto doporučujeme navštívit stránky ScratchEd, kde je k dispozici mnoho příkladů a materiálů pro učitele.

Pro zkušenější „programátory“ a jejich učitele je k dispozici například hra CodeCombat. Žáci se učí programovat formou ovládání hrdiny. Již nepřetahují bloky s příkazy jako ve Scratchi, ale píšou příkazy přímo na klávesnici. Tato hra seznámí hráče se základy skutečných programovacích či skriptovacích jazyků, jako jsou Python, JavaScript, CoffeeScript a další.

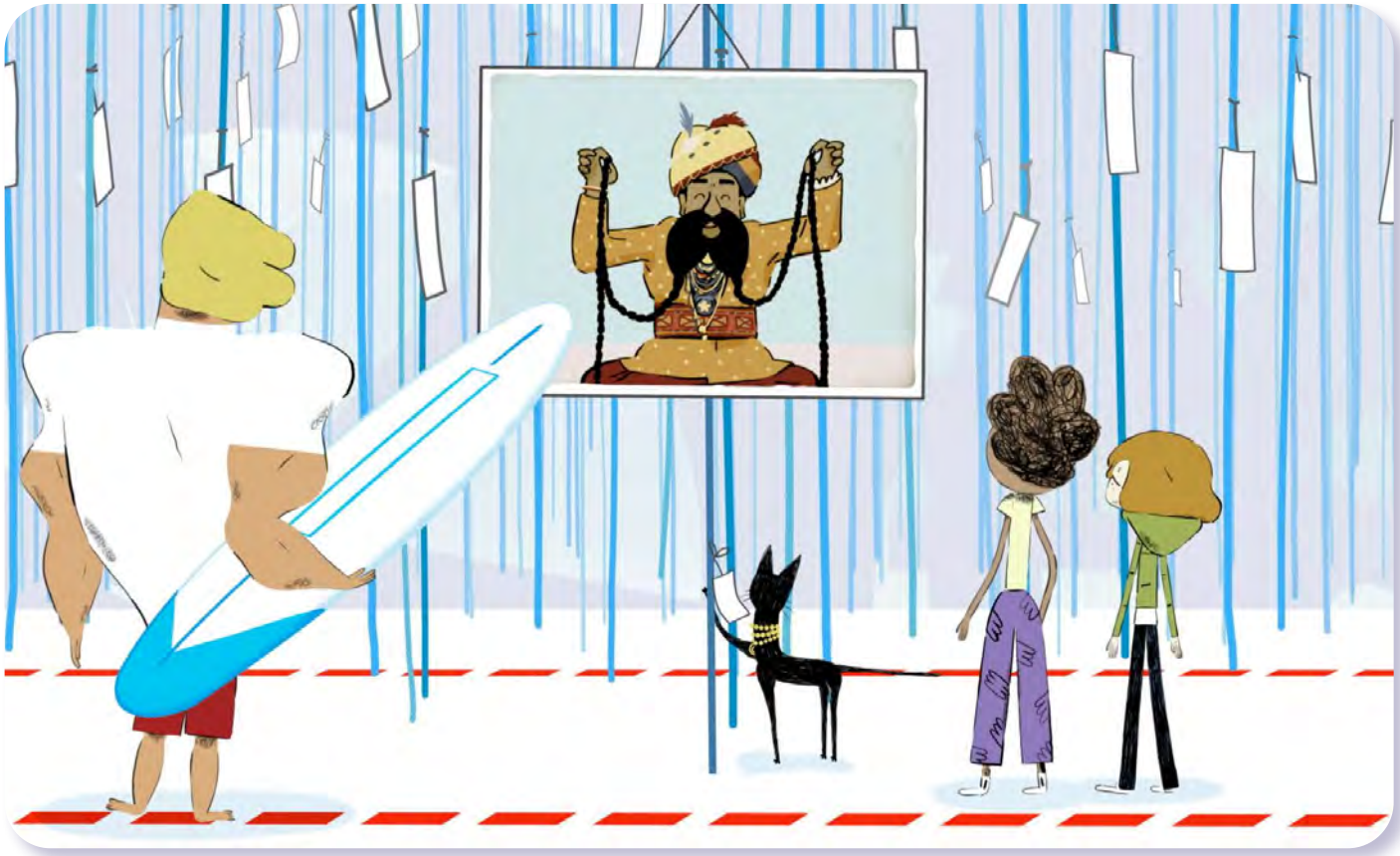
Za zmínku stojí i webové stránky Code.org, kde jsou k dispozici různé kurzy a aktivity rozdělené dle věkových kategorií, a to od 4 až do 18 let.

Odpovědi vypracovala:
Michala Radotínská, CZ.NIC

Podívejte se na lekci V digitálním světě: Digitální svět na <jsns.cz/mv/digitalni-svet>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.

POZNÁMKY

POZNÁMKY



V digitálním světě

Vyhledávače

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Hrdinové seriálu testují schopnosti internetových vyhledávačů a pokládají jim všetečné dotazy. Kostičky Ping a Pong jejich otázky upravují do vhodně zvolených klíčových slov, aby se dostali k přesnější odpovědi. Rychlé vyhledávání informací je jednou z hlavních funkcí internetu. Uživatelům v tom pomáhají vyhledávače, jako je Google či Seznam, které odpovědi „loví" na miliardách webových stránek pomocí tajného vzorce zvaného algoritmus. Ten pak také odpovědi vhodně uspořádá a Kocoura, který tvrdí, že má nejdelší fousky na světě, usvědčí z omylu.

CÍLE LEKCE

1. pochopit funkci internetových vyhledávačů
2. seznámit se s tím, jak vyhledávání ovlivnit
3. uvědomit si, že jsou o nás sbírána osobní data

DOPORUČENÝ VĚK

7+ LET

AKTIVITA: Vyhledávače !!!

ANOTACE

Žáci se blíže seznámí s nejznámějšími vyhledávači, propojují loga vyhledávačů a jejich názvy. Sami zkouší vyhledávat klíčová slova, čímž si vyzkouší, jak internetové vyhledávače fungují a jak je používat.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k učení, k řešení problémů, komunikativní, sociální a personální

CÍLE

Žáci:
- si uvědomí množství informací dostupných online
- se seznámí se základním nástrojem – vyhledávačem
- si uvědomí, jakými různými způsoby se dají vyhledávat informace

DÉLKA

45 min. (včetně projekce)

POMŮCKY

- PRACOVNÍ LIST do dvojic
- psací potřeby
- interaktivní tabule, přístup na internet pro žáky

POSTUP

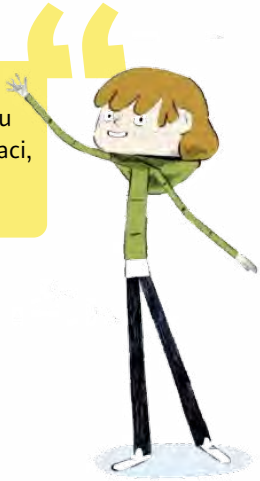
1. Na začátku hodiny se žáků zeptáme: *Když potřebujete něco zjistit, co uděláte?* (Zeptat se, zatelefonovat, podívat se na zprávy, vyhledat v knihovně, vyhledat na internetu.) Odpovědi zapíšeme na tabuli.
2. Následuje **projekce dílu seriálu**.
   Poznámka: Snímek doporučujeme zhlédnout nejméně dvakrát.
3. Krátce ověříme, zda žáci příběh pochopili. Mělo by zaznít, že vyhledávače nám díky klíčovým slovům pomáhají rychle nalézt informace tajnými postupy zvanými algoritmy. Ty pak Kocoura, který tvrdil, že má nejdelší fousky na světě, usvědčily z omylu.
4. Každé dvojici žáků rozdáme PRACOVNÍ LIST. Žáci mají za úkol **propojit logo a správný název vyhledávače**. Můžeme udělat anketu a zjistit, kdo ze žáků už vyhledávače umí aktivně používat.
5. Využijeme interaktivní tabuli, počítačovou místnost nebo vlastní zařízení a ukážeme žákům jeden či více vyhledávačů. Do adresního řádku zadáme klíčové slovo: název naší školy. Žákům pomůžeme, aby se na stránce zorientovali, ukážeme, kde ve výsledcích zobrazit videa nebo obrázky. Zadáme ještě několik klíčových slov, například název našeho města, slavné osoby apod.
6. Žákům zadáme, že mají samostatně vyhledat:
   a/ rekordy (největší ryba, nejrychlejší auto, nejstarší žena světa)
   b/ klíčová slova s nejednoznačným výsledkem (např. slovo „Petra“, což může znamenat ženské jméno i starověké skalní město v Jordánsku)
   c/ klíčová slova vhodná pro zobrazení obrázků (např. Eiffelova věž, nejvyšší hora světa, česká abeceda)
   d/ Stejná klíčová slova můžeme zadávat do různých vyhledávačů a srovnávat výsledky.

REFLEXE AKTIVITY

Ptáme se: *Jak vyhledáváme informace na internetu? Co jsou to klíčová slova? Proč se nějaký výsledek zobrazí jako první? Myslíte si, že všechny informace, které se objevily, jsou pravdivé? Znáte rčení „hledat jehlu v kupce sena“?* Zkusíme se žáky přijít na to, proč jsou vyhledávače důležité a proč je vůbec dobré vědět, co to je vyhledávač.

ZKUŠENOSTI Z PRAXE

Žáky velmi bavilo vyhledávání rekordů – nejdříve jsem jim zadávala já, co mají najít, a poté sami vymýšleli druhým, co mají hledat. Atmosféra byla „soutěživá“, všichni se snažili najít požadovanou informaci co nejdříve. Oceňuji, že přišli na to, že se nestačí podívat jen na první nalezenou informaci, ale musí si přečíst, i z jaké doby ta informace je, nebo že musí informace porovnat.
Jana Machovská, *ZŠ Nový Hrozenkov*



PRACOVNÍ LIST

Propojte správný název a logo vyhledávače:

YAHOO

DUCKDUCKGO

ATLAS.CZ

GOOGLE

SEZNAM.CZ

OTÁZKY A ODPOVĚDI

1. Co je to internetový vyhledávač?

Internetový vyhledávač je služba, která nám umožňuje **pracovat s internetem při vyhledávání informací** tak, jak to dnes běžně známe. Dříve si lidé museli pamatovat přesné adresy webových stránek, protože nebyl žádný nástroj, který by jim umožnil jednotlivé webové stránky postupně vyhledávat nebo procházet. Webových stránek však bylo stále více a tento způsob prohlížení internetu se velmi rychle stal nepoužitelným. Internetové vyhledávače byly tedy vytvořeny především proto, aby bylo vyhledávání na internetu efektivnější a pohodlnější. Jako uživatelé zadáváme do vyhledávače klíčová slova a jsou nám vráceny výsledky, které systém vyhledávače vyhodnotil jako nejvhodnější. Výsledkem vyhledávání však nemusí být jen webové stránky, může se jednat i o videa, obrázky nebo další informace.

2. Co jsou algoritmy?

Algoritmus je **návod, postup nebo posloupnost jednotlivých kroků, které umožní vyřešit zadanou úlohu**; platí tedy, že algoritmy mají nějaký výsledek. Nejčastěji se toto slovo vyskytuje ve spojitosti s programováním, ale už z principu můžeme jako algoritmus chápat celou řadu všedních věcí, které kolem sebe vidíme v běžném životě. Dobrým příkladem může být vaření dle receptu, které nás vede krok po kroku až k požadovanému výsledku. Základním stavebním kamenem algoritmů jsou **instrukce a příkazy**, které mají být naplněny v přesném pořadí, aby se dosáhlo výsledku.

3. Proč jsou algoritmy tajné?

Zveřejnění vyhledávacích algoritmů by znamenalo **odhalení obchodního tajemství** a současně je na internetu mnoho nebezpečných a závadných webů, které se na první místa ve výsledcích vyhledávání pokoušejí dostat pomocí nekalých praktik. Zveřejnění algoritmů by jim takové chování výrazně zjednodušilo a lidé by pak ve výsledcích vyhledávání viděli weby, které je nezajímají nebo které obsahují nerelevantní informace.

4. Jaké vyhledávače jsou v ČR nejrozšířenější?

Drtivou část (až 96 %) vyhledávání na českém internetu si mezi sebou dělí **Google a Seznam**. Ve zbylých procentech jsou zastoupené ostatní vyhledávače jako **Yahoo a Bing**. Procentní podíl Seznamu a Googlu je přibližně v poměru 25:75. Měřit to je však složité a proměnlivé, záleží například na tom, z jakých zařízení se uživatelé připojují a o jaký přístup k vyhledávání jde (viz níže).

5. Jak vyhledávače fungují a v čem se mezi sebou liší?

Existují dva základní přístupy vyhledávání informací na internetu a klasifikace webových stránek. Prvním z nich jsou **vyhledávače**, druhým jsou **předmětové katalogy**. Dnes mnohé vyhledávače už kombinují oba dva typy, nicméně i tak je dělení užitečné znát.

Vyhledávače fungují takto: **tzv. indexovací roboti** prochází obsah internetu, a pokud naleznou novou stránku nebo obsah, indexují ji (uloží) do své databáze (tzv. indexu). Takovou stránku automaticky označí **klíčovými slovy**, přiřadí jí určité charakteristiky, a tím později umožní tuto stránku vyhledat.

Pokud zadáme do vyhledávače patřičná klíčová slova, vyhledávač nám nabízí právě tyto weby, které robot objevil. Slabinou tohoto přístupu je, že vyhledávač tak eviduje i různé pochybné stránky, protože automatické mechanismy je nedokážou správně vyhodnotit. Tak funguje například Google.

Naopak předmětové katalogy jsou vytvářeny převážně **manuálně**. Obsah internetu je v tomto případě zpracovaný lidmi, nikoliv roboty. Výsledky předmětových katalogů jsou zpravidla mnohem užší než u vyhledávačů. Neobsahují tolik výsledků, výsledky jsou však lépe strukturované a řazené a jako uživatelé postupujeme různými kategoriemi. To oceníme nejvíce v momentě, kdy víme, co přesně hledáme. Propracovaný předmětový katalog má například Seznam (možná znáte jeho katalogový přehled Firmy.cz), který však zároveň má i funkci klasického vyhledávání.

6. Jak jsou výsledky vyhledávání řazeny? Vidíme všichni stejné výsledky?

Výsledky vyhledávání jsou řazeny **algoritmy** a každý vidíme jiné výsledky na stejná klíčová slova či vyhledávací dotazy. Stojí za tím vyhledávací **algoritmus, který se snaží výsledky vyhledávání přizpůsobit na míru tomu, kdo se ptá**.

Má to hned dva důvody. Na straně jedné je díky nim internet pro uživatele přívětivější, protože snáze najdeme, co potřebujeme. Na straně druhé jde o zisk. Velká část příjmů internetových společností plyne z reklamy, která je, stejně jako výsledky vyhledávání, personalizovaná. Jinými slovy „nabízená na míru“. Čím lépe se vyhledávači podaří nabídnout nám relevantní obsah, tím více času na internetu strávíme. Internetové společnosti tím také získají více prostoru pro **umístění reklamy**, která nás pravděpodobně zaujme.

7. Jak mohou provozovatelé stránek ovlivňovat, aby se jejich web zobrazil mezi prvními?

Existují **placené (SEM – search engine marketing) i neplacené (SEO – search engine optimization) metody**, kterými lze – z pohledu provozovatele webu – dosáhnout lepších výsledků ve vyhledávání. Placené metody jednoduše umožní posunout určité weby výše, protože někdo zaplatil za jejich inzerci. Jako uživatelé můžeme poznat, zda nějaký web za zobrazení platí, příspěvky bývají zobrazené jako **„ad“, „reklama“** či podobně. Formy placení však mohou být různé – existují i modely, kdy svůj web poskytneme jako reklamní prostor a za to se ocitneme výše ve výsledcích. Pokud chceme ovlivnit výsledky vyhledávání a dostat se na lepší místa, můžeme to do značné míry ovlivnit i sami – pomocí neplacené metody (SEO). Je důležité **dobře naplnit web informacemi**, které nevidí uživatel, ale vyhledávač ano. Jedná se například o **klíčová slova**, která jsou s obsahem našeho webu spojená. Vyhledávač díky těmto infor-

macím lépe ví, co od našeho webu vlastně může očekávat. Lépe si s naším webem rozumí, a tím pádem ho upřednostní. Pokud bychom však svůj web naplnili informacemi a klíčovými slovy, která jsou často vyhledávaná, ale s naším webem nemají nic společného, vyhledávač to časem odhalí a za tento podvod náš web naopak velmi upozadí.

8. Jaká osobní data o nás vyhledávače sbírají?

Problematika sběru dat se netýká jen vyhledávačů, ale i dalších služeb a aplikací, neboť jsou všechny různými způsoby propojené a umí spolu komunikovat. Jako příklad můžeme uvést sledování videa: když se jako přihlášení uživatelé na YouTube budeme dívat na video na svém notebooku a zastavíme ho, můžeme později pokračovat třeba z mobilního telefonu přímo tam, kde jsme přestali.

Vyhledávače jako takové mohou **například sledovat naši aktivitu, čas strávený na stránce nebo polohu**. Informace z e-mailu či kalendáře se mohou „propsat" až do našeho vyhledávání, pokud máme služby propojené. O tom, jak a jaká data se sbírají, rozhoduje řada věcí. Důležitým faktorem například je, zda jsme **přihlášení svým uživatelským účtem do služeb**. Google nabízí přehled našich přihlášených aktivit včetně časového záznamu: na která videa jsme se dívali, čemu jsme dali lajk nebo dislajk, co jsme komentovali, které stránky jsme navštívili, kde jsme byli a tak podobně. Vše je k vidění zde: https://myactivity.google.com/myactivity (připomínáme, že se to týká jen těch, kteří používají aplikace Googlu, např. Gmail apod.).

Často můžeme také vidět, že nás webová stránka informuje o tom, že pracuje s **cookies**. Cookies jsou **malé soubory, které umí například samy vyplnit kontaktní či objednávací formulář, který jsme už jednou vyplnili**. To však není záležitost vyhledávání ani vyhledávačů, ale webových prohlížečů.[1]

9. Lze sběr osobních dat vyhledávači nějak minimalizovat?

Pokud chceme snížit množství dat, která jsou o nás sbírána a zaznamenávána, můžeme například využít **funkce anonymního prohlížení**. Takové prohlížení nám ani zdaleka nezaručí stoprocentní anonymitu směrem do internetu, ale významně zredukuje množství dat, která o nás sbírá prohlížeč nebo služby.

Problematika sběru dat se však netýká jen vyhledávačů. Opět nezapomínejme na to, že služby či aplikace jsou dnes propojené různými způsoby a umí spolu komunikovat. Je tedy důležité dbát i na to, které aplikace si stahujeme, **jaká oprávnění od nás chtějí a co jim dovolujeme**. Google také ve svém pokročilém nastavení umožňuje **omezit či zakázat sběr určitých dat**. Musíme se pak ale smířit s tím, že výsledky vyhledávání nebudou tolik přesné, jak jsme většinou zvyklí. Existují také vyhledávače jako například www.duckduckgo.com, které se profilují tím, že žádná data o uživatelích nesbírají.

10. Jak zpřesnit výsledky vyhledávání?

Čím přesněji je položený dotaz, tím relevantnější odpověď lze vyhledávačem získat. Jednoslovná hesla nemusí vždy stačit, a tak je potřeba v dotazu specifikovat mnohem více podmínek a pravidel, které zužují portfolio odpovědí a filtrují pryč ty méně relevantní. Tyto složitější dotazy se ve vyhledávačích vytvářejí pomocí **správné dotazovací syntaxe (skladby) a operátorů („povelů", kterými vyhledávání upřesníme)**.

Takto můžeme zpřesnit dotaz přidáním dalších klíčových slov (operátor AND), výběrem některých z nich (operátor OR) nebo například vyloučením stránek dle určitých pravidel. Zároveň lze v dotazu omezit odpovědi jen na určitý typ souboru, umístění textu, umístění v konkrétní URL adrese, zda se klíčové slovo vyskytuje ve skrytých datech webu nebo zda se vyskytuje nějaký prvek v určitém rozsahu. Kromě syntaxe a operátorů se lze i přímo v nastavení vyhledávání omezit i na konkrétní jazyk či časové období.

11. Jaký je rozdíl mezi vyhledávačem a prohlížečem?

Vyhledávač je internetová služba k vyhledávání informací na internetu – webová stránka, do které zadáváme naše dotazy (www.google.com, www.seznam.cz, www.duckduckgo.com aj.). Abychom se ale na webové stránky vyhledávače vůbec dostali, potřebujeme mít ve svém počítači nainstalovaný prohlížeč (Chrome, Firefox, Safari aj.). **Prohlížeč je tedy program, díky němuž můžeme vyhledávat v libovolném vyhledávači.**

12. Co je to zabezpečená a nezabezpečená komunikace na internetu?

Internetovou komunikací rozumíme přenášení jakýchkoliv informací na internetu. Zabezpečená komunikace pak znamená, že informace, které na web odešleme nebo jeho prostřednictvím získáme, jsou **chráněné a soukromé**. Proto je před zadáváním citlivých informací (jako je zadávání údajů z platební karty) důležité zkontrolovat, že prohlížeč s webem navázal soukromé spojení – například tak, že u adresního řádku vidíme symbol zámku.

Je-li komunikace zabezpečená, můžeme si také ověřit identitu druhé strany, což zvyšuje její důvěryhodnost.

Dnešní **prohlížeče standardně na zabezpečení webu upozorňují**, ale i přesto je důležité být při sdílení soukromých informací vždy opatrný a zkontrolovat, zda jsme opravdu na webu, který chceme navštívit.

13. Jak poznám zabezpečenou a nezabezpečenou komunikaci?

Prohlížeče nás informují, jestli je komunikace zabezpečená, nebo nezabezpečená pomocí jednoduché **ikonky v adresním řádku prohlížeče**. V různých prohlížečích mohou vypadat odlišně, nicméně zabezpečené připojení je zpravidla

1 *Více o cookies se dozvíte v aktivitě na str. 56.*

znázorněné ikonkou **zamčeného zámku.** Více informací o způsobu používané komunikace se můžeme dozvědět po rozkliknutí zmíněných ikonek.

Zabezpečenou komunikaci také znázorňuje prefix https:// (pozor, ne http://) před adresou stránky. Avšak prohlížeče někdy tento prefix skrývají.

Odpovědi vypracovali:
David Kudrna, Národní úřad pro kybernetickou a informační bezpečnost (otázky 1–10)
Marek Perichta, CESNET, IT specialista (otázky 11–13)

Navštivte lekci V digitálním světě: Vyhledávače na <jsns.cz/mv/vyhledavace>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.

POZNÁMKY

V digitálním světě

Viry

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

„Nemůžeš otevírat dárky od cizích lidí!“ volá Mína, ale Kocour už klikl na podezřelý e-mail a rodinný počítač napadne vir. Počítačové viry jsou nežádoucí programy, které nás mohou připravit o hesla, kontakty či zcela ovládnout náš osobní počítač. Právě za tímto účelem šíří počítačoví piráti viry ve formě e-mailů s lákavým předmětem či šikovně pojmenovaných souborů ke stažení. Naštěstí jsou tu antivirové programy, které umí viry vypátrat a zničit.

CÍLE LEKCE

1. naučit se, proč a jakým způsobem viry napadají počítače
2. osvojit si postupy, jak se počítačovým virům bránit
3. uvědomit si pravidla pro pohyb v online světě

DOPORUČENÝ VĚK
10+ LET

AKTIVITA: Viry

!!!

ANOTACE

Žáci se prostřednictvím příkladů ze života svých vrstevníků seznámí s fenoménem počítačových virů. Dozví se, jak fungují a jak ohrožují počítače, tablety a mobily a naše data v nich. Také zjistí, jak zařízení před viry chránit a jak se na internetu chovat obezřetně.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie, člověk a svět práce

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k učení, k řešení problémů, komunikativní, sociální a personální, občanské, pracovní

CÍLE

Žáci:
- pochopí, že i počítače mohou „onemocnět“
- se naučí, proč a jakým způsobem viry napadají počítače
- si osvojí postupy, jak se počítačovým virům bránit

DÉLKA

45 min. (včetně projekce)

POMŮCKY

- PRACOVNÍ LIST 1 do skupin
- LIST PRO VYUČUJÍCÍ
- PRACOVNÍ LIST 2 pro doplňkovou aktivitu

POSTUP

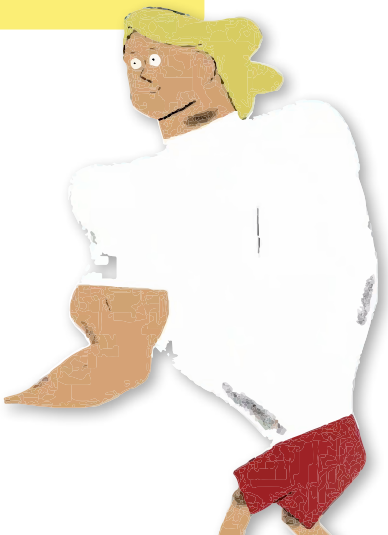
1. Zeptáme se žáků, **zda znají příběh z řeckých bájí o trojském koni**. Příběh krátce shrneme a zdůrazníme jeho hlavní myšlenku – nepřítel přichází skrytý.
   Poznámka: Doporučujeme prostudovat informační materiál OTÁZKY A ODPOVĚDI k lekci.
2. Následuje **projekce epizody seriálu**.
3. Ověříme si porozumění obsahu epizody. Ptáme se:
   Co se stalo chlapci v epizodě seriálu? Hrozilo dětem nebezpečí? Jak se situace vyřešila?
   Poznámka: Snímek doporučujeme zhlédnout nejméně dvakrát.
4. Žáky rozdělíme do skupin. Do každé skupiny rozdáme jeden PRACOVNÍ LIST. Žáci **společně posuzují a komentují modelové situace**. Vyčleníme dostatečný čas pro samostatnou práci.

REFLEXE AKTIVITY

V reflexi postupně uvádíme příklady situací z pracovního listu, se kterými se žáci mohou setkat online. **Společně diskutujeme, v čem mohou být uvedené situace problematické.**
Poznámka: Vysvětlující komentáře k situacím z pracovního listu najdete v LISTU PRO VYUČUJÍCÍ.
V diskusi s žáky se můžeme také ptát:
Setkali jste se vy nebo rodina s počítačovými viry? Pokud ano, jak jste postupovali? Jak se můžeme počítačovým virům bránit? Znáte nějaké antivirové programy?
Co bylo pro vás nové? Změníte v něčem svoje chování nebo zvyky při používání mobilu?
Poznámka: Můžete využít také DOPLŇKOVOU AKTIVITU a PRACOVNÍ LIST 2.

ZKUŠENOSTI Z PRAXE

Aktivita byla pro žáky zajímavá i srozumitelná. V reflexi jedním slovem se často objevovaly termíny spojené s koronavirem, což je ovlivněno dnešní dobou. Situace v pracovním listu byly pro žáky srozumitelné, ve skupinkách živě diskutovali. Poměrně nové byly pro žáky termíny v druhém pracovním listu, informace je zajímaly.
Andrea Tláskalová, *ZŠ Zbiroh*



PRACOVNÍ LIST 1

Ve skupině se zamyslete a zapište, V ČEM PŘESNĚ MOHOU BÝT POPSANÉ SITUACE PROBLEMATICKÉ. Přemýšlejte, jak by se při používání mobilu měly děti z příběhů zachovat a proč.

1 Matěj se vrátil ze školy, je doma sám a hraje hru na mobilu. Klikne na lákavou reklamu, která tvrdí:

„Neutrácej zbytečně za placené aplikace, stáhni si u nás zdarma toto skvělé herní rozšíření!“ Matěj aplikaci instaluje.

2 Jana včera pořádně zmokla, a tak si teď stahuje aplikaci Počasí. Objeví se hláška:

„Aplikace Počasí úspěšně stažená! Vyžaduje přístup ke kontaktům, fotoaparátu, do galerie a přístup k poloze. Klikni Ano/Ne.“

3 Petra a Lucie byly na hudebce a mají ještě čas, než jim pojede autobus. Na lavičce se připojí na wifi blízké kavárny a prohlížejí si oblíbený e-shop. Ten má právě neodolatelný výprodej. **Lucie si objedná a zaplatí několik kousků oblečení.**

4 Jáchymovi pípla SMS od operátora:

„Dobrý den, ověřujeme platnost vašich údajů. Jméno, adresu a rodného číslo pošlete zpět nebo si je zkontrolujte na: https://op23kasr.login.info/ **Váš operátor.“** Jáchym klikne na uvedený odkaz a vyplní údaje.

5 Markéta si na sociální síti všimla, že její kamarádka právě lajkovala příspěvek. ***„Rozdáváme iPhony! Jak na to?“*** Rozklikla jej a čte:

1. Prohlédni si ZDE všechny fotky – máme hodně barev!
2. Napiš do komentářů, jakou barvu chceš.
3. Lajkuj a sdílej.
4. Čekej na výherní zprávu.

Stejně jako kamarádka i Markéta všechno prokliká a sdílí dál.

DOPLŇKOVÁ AKTIVITA – PRACOVNÍ LIST 2

Chcete znát pojmy, které používají „ajťáci"? Přiřaďte pojmům správné vysvětlení.

1	**TROJSKÝ KŮŇ**
2	**ANTIVIRUS**
3	**MALWARE** [čti malvér]
4	**ADWARE** [čti advér]
5	**RANSOMWARE** [čti ranzomvér]

A	Program, který zaplaví počítač nebo mobil reklamou a vyskakovacími okny.
B	Škodlivý program, který zašifruje a zablokuje počítač. Za obnovení přístupu potom vyžaduje zaplatit výkupné.
C	Jeho úkolem je chránit počítač nebo mobil. Odhaluje a maže škodlivý obsah.
D	Souhrnné pojmenování škodlivých programů, které mají za úkol umožnit útočníkovi (pirátovi) tajný přístup do počítače nebo mobilu.
E	Typ škodlivého kódu, který se často ukrývá v bezplatných aplikacích, hrách i filmech. Jeho cílem je ovládat cizí počítač, krást nebo mazat data, získat hesla a jinak škodit.

1	
2	
3	
4	
5	

DOPLŇKOVÁ AKTIVITA

Poznámka: Správné řešení najdete v LISTU PRO VYUČUJÍCÍ.

REFLEXE AKTIVITY

Společně shrneme **nejdůležitější pravidla pro ochranu zařízení s přístupem na internet**. Pravidla ideálně formulují sami žáci, můžeme je navést otázkami (v závorce):

1. **Vždy mít aktivní antivirový program.** *(Máte k dispozici programy na ochranu mobilů a počítačů před viry?)*
2. **Nikomu v online (ani offline) světě nesdělovat osobní či jinak citlivé (přihlašovací) údaje.** *(Sdělíte komukoliv adresu bydliště?)*
3. **Používat silné heslo, nepoužívat univerzální hesla.** *(Je v pořádku heslo např. 1234?)*
4. **Neplatit za neověřené zboží či služby.** *(Nakupujete na jakémkoliv e-shopu?)*
5. **Neklikat na nedůvěryhodné odkazy.** *(Jaký je problém s adresou ceskatelevize.com? Stránku vyhledejte.)*
6. **Nestahovat a neinstalovat neověřené aplikace z neznámých zdrojů.** *(Stáhli byste si aplikaci ze zmíněné stránky ceskatelevize.com?)*
   Poznámka: Pravidla jsou převzata z webové stránky projektu E-Bezpečí (www.e-bezpeci.cz).

POZNÁMKY

LIST PRO VYUČUJÍCÍ

Komentáře k situacím z PRACOVNÍHO LISTU 1

1	Nenecháme se zlákat nabídkou aplikace zadarmo, pokud se za ní běžně musí platit. Hrozí totiž, že obsahuje nějaký typ škodlivého viru. Aplikace vždy stahujeme jenom z oficiálních stránek, jako je Google Play nebo App Store.
2	Většina aplikací vyžaduje přístup k datům v našem mobilu. Vždy je ale třeba zvážit, k jakým datům jí přístup povolíme. Například aplikace na úpravu fotek přístup do galerie potřebuje, ale aplikace Počasí ne (nepotřebuje ho ani k fotoaparátu ani ke kontaktům).
3	Nikdy nenakupujeme ani nikam nezadáváme žádné citlivé údaje, jsme-li připojeni k jakékoliv veřejné wifi (i když je zabezpečená heslem). Skrze veřejnou wifi může někdo cizí jednoduše získat všechny naše informace. Ideálně se do veřejných sítí vůbec nepřipojujeme.
4	Operátor (ani nikdo jiný) od nás nikdy takovým způsobem kontrolu údajů nevyžaduje, takže víme, že jde o podvod. Naše osobní údaje tímto způsobem rozhodně nesdělujeme, na takovou zprávu nereagujeme a hlavně neklikáme na odkaz, jelikož může být závadný.
5	Cokoliv nám někdo nabízí zadarmo je velmi podezřelé. Na odkaz neklikáme, protože hrozí, že si stáhneme nevyžádaný malware.

PRACOVNÍ LIST 2

SPRÁVNÉ ŘEŠENÍ: 1E, 2C, 3D, 4A, 5B

Poznámka:
adware od anglického *advertisement* = reklama
malware od anglického *malicious* = zlomyslný

OTÁZKY A ODPOVĚDI

1. Co jsou počítačové viry?

Počítačový vir je program (nebo část kódu), **který se spustí v našem počítači po navštívení infikované webové stránky, otevření přílohy podezřelého e-mailu**, instalaci softwaru či aplikace do mobilu.

Viry na nás mohou číhat kdekoliv na internetu, bohužel i tam, kde je vůbec nečekáme. O přítomnosti viru v počítači, mobilu či tabletu často **ani nemusíme vědět**. Může se sám spustit až po nějaké době, například v předem určený den nebo po nakažení specifického počtu přístrojů. Dále nás může **nevědomky špehovat a odesílat informace** o tom, co právě děláme.

Viry jsou buď **cíleně ničivé,** nebo **„jen" obtěžující**, tedy relativně neškodné. Ty méně zákeřné nám například zpomalí chod počítače. Některé viry ale způsobují nevratné poškození vytipovaných souborů či jejich smazání. Jiné se zase snaží převzít kontrolu nad napadeným systémem a odesílají naše osobní data útočníkům (autorům virů).

Mezi počítačovým virem a virem, který útočí na lidi, je velká podobnost, a to jak v zákeřnosti, s jakou působí na svého hostitele, tak v potřebě expandovat dále. Oba druhy virů mají za úkol znepříjemňovat nám život a infikovat co nejvíce cílů. Proti oběma virům se však lze i účinně chránit.

2. Kdy se objevil první virus a proč?

Historie počítačových virů sahá do 80. let 20. století. V roce 1983 vytvořil **dr. Frederik Cohen** samomnožící program, který označil jako virus. Jednalo se v podstatě jen o neškodný kód. O tři roky později **naprogramovali bratři Alviové virus s názvem Brain** neboli mozek, a to za účelem ochrany proti šíření softwaru, který vyvinuli v rámci své firmy Brain Computer Services. Šlo o experiment, jenž měl vystrašit vlastníky nelegálně kopírovaných disket s jejich programem, a zamezit tak dalšímu vzniku pirátských kopií. Vir se však nečekaně rozšířil mimo záměr svých autorů až do USA a Evropy. Aniž by to tušili, podařilo se jim odstartovat éru počítačových virů, které se od té doby dále rozvíjely a nabývaly různých podob. Tvůrci virů si někdy dokonce mezi sebou předávají know-how a techniky, které jim umožňují viry zdokonalovat a schovávat před antivirovými programy. Současné viry jsou velice propracované a dokážou napáchat nemalé škody.

3. Jaké existují základní druhy virů?

Ačkoliv se v českém názvosloví ustálil výraz „počítačový virus", je to ve skutečnosti jen **podkategorie skupiny označované jako škodlivý software neboli malware**. **Malware se tedy dělí na viry, červy, trojské koně, spyware, ransomware, adware a další.**

Vir jako takový se dnes už prakticky nevyskytuje. Sám o sobě nemůže existovat a přenáší se na základě infekcí jiných počítačových programů. Aktivuje se až při spuštění infikovaného instalačního souboru či běžně používaných programů (např. prohlížeče pdf souborů).

Červ je proti tomu samostatně fungující program, který se sám množí a šíří prostřednictvím sítě nebo přenosných médií. Jeho záměrem je nakazit co největší množství počítačů a snížit jejich výkon.

Trojský kůň se zase snaží přesvědčit uživatele, aby spustil program, který útočníkovi umožní vzdálený přístup do počítače. Na první pohled se chová jako zcela normální a užitečný program, avšak ve skutečnosti tajně provádí škodlivé operace.

4. Jak se vir do počítače nejčastěji dostane?

Vir si do počítače nejčastěji stáhneme právě my sami, a to vlastní aktivitou. Nejnebezpečnější je **návštěva webových stránek, které nabízí stažení filmů či užitečného softwaru zdarma**. U podobných nabídek bychom měli maximálně zpozornět a nenechat se nachytat na to, že nám někdo nabídne zdarma ten nejnovější film nebo software, který u výrobce seženeme za nemalé peníze. Například soubory, které obsahují příponu .exe, není radno stahovat, natož otevírat.

Dalším způsobem, jak si zaneseme do počítače či jiného zařízení vir, je **stažení a otevření přílohy z nevyžádaného e-mailu**. Stačí si jen osvojit základní pravidlo, že e-maily od neznámých lidí, často psané zvláštní češtinou, budeme rovnou mazat. Případně je můžeme označit jako spam, aby nám příště „padaly" rovnou do spamového koše.

Vir ale umí podvrhnout i adresu odesílatele. Pokud nám tedy přijde **e-mail ze známé adresy, ale s podivným obsahem,** raději u odesílatele ověřme, zda jej skutečně poslal on sám. Některé zprávy se zas **mohou tvářit**, že jsou **rozesílané renomovanou společností** (např. bankou), která nás chce pouze upozornit na novou aktualizaci softwaru atp. Opět je dobré použít zdravý selský rozum a zamyslet se nad tím, zda by nás banka informovala právě touto cestou.

5. Jak eliminovat riziko, že bude můj počítač nakažen virem?

Riziko nakažení počítače či jiného zařízení virem můžeme snížit dodržováním určitých **bezpečnostních pravidel**. Jedním z nich je, že **nebudeme otevírat přílohy nevyžádaných e-mailů a zprávy od neznámých, podezřelých kontaktů**.

Další zásadou je **stahovat aplikace do mobilu pouze z oficiálních tržišť,** jako je Google Play či App Store, a **nenavštěvovat webové stránky s nelegálními kopiemi** filmů, hudby nebo pirátského softwaru. Dále bychom **neměli vkládat do počítače USB** klíčenky, u kterých neznáme původ a jejich vlastníka. I ty totiž mohou obsahovat zákeřný vir, jenž má za úkol poškodit naše zařízení. V neposlední řadě nás proti nákaze může ochránit **pravidelná aktualizace**

operačního systému a všech programů, které používáme, a to z originálních zdrojů.

6. Jak technicky zabezpečit svůj počítač proti virům?

Jakékoliv zařízení, pomocí něhož se připojujeme k internetu, bychom měli opatřit účinným **antivirem**, který slouží k ochraně před viry a dalším malwarem. Antivirové programy škodlivé kódy detekují na základě svých databází a způsobu chování programů nainstalovaných v zařízení. Umí eliminovat jejich činnost a úplně je odstranit ze zařízení. Musíme je však pravidelně **aktualizovat**, aby nezastaraly. Bez aktualizace nedává používání antivirového programu smysl, jelikož podle statistik **denně vznikne několik desítek tisíc nových virů** nebo jiného škodlivého softwaru, na které musí bezpečnostní experti antivirových společností pohotově reagovat.

Každým rokem se počet odhalených unikátních škodlivých kódů rapidně zvyšuje, například v roce 2019 se jednalo o 24,5 milionu škodlivých objektů.

Na trhu je k dispozici nepřeberné množství antivirových programů jak pro počítače, tak pro mobilní zařízení. Mezi nejznámější patří Avast, ESET NOD32 Antivirus, Kaspersky Antivirus a další. **Nikdy ale neinstalujeme dva či více antivirových programů do jednoho zařízení.** Budou si navzájem vadit a ani jeden z nich nebude zcela plnit svou bezpečnostní funkci. V případě změny antiviru musíme nejprve ten původní odinstalovat.

7. Jaké škody mohou viry napáchat?

Některé viry **nepáchají žádné škody, pouze se rozmnožují,** ale vědomě nikoho neohrožují a nijak nezasahují do systému. Mnohé viry mají pouze **obtěžující charakter**. Nijak tedy nepoškozují systém, ale aktivují se nám na obrazovce počítače či displeji telefonu například v podobě nesmyslných hlášení. Tím **nejzákeřnějším typem však jsou destrukční viry,** které již mají za úkol poškodit či zničit data a nakonec třeba i samy sebe.

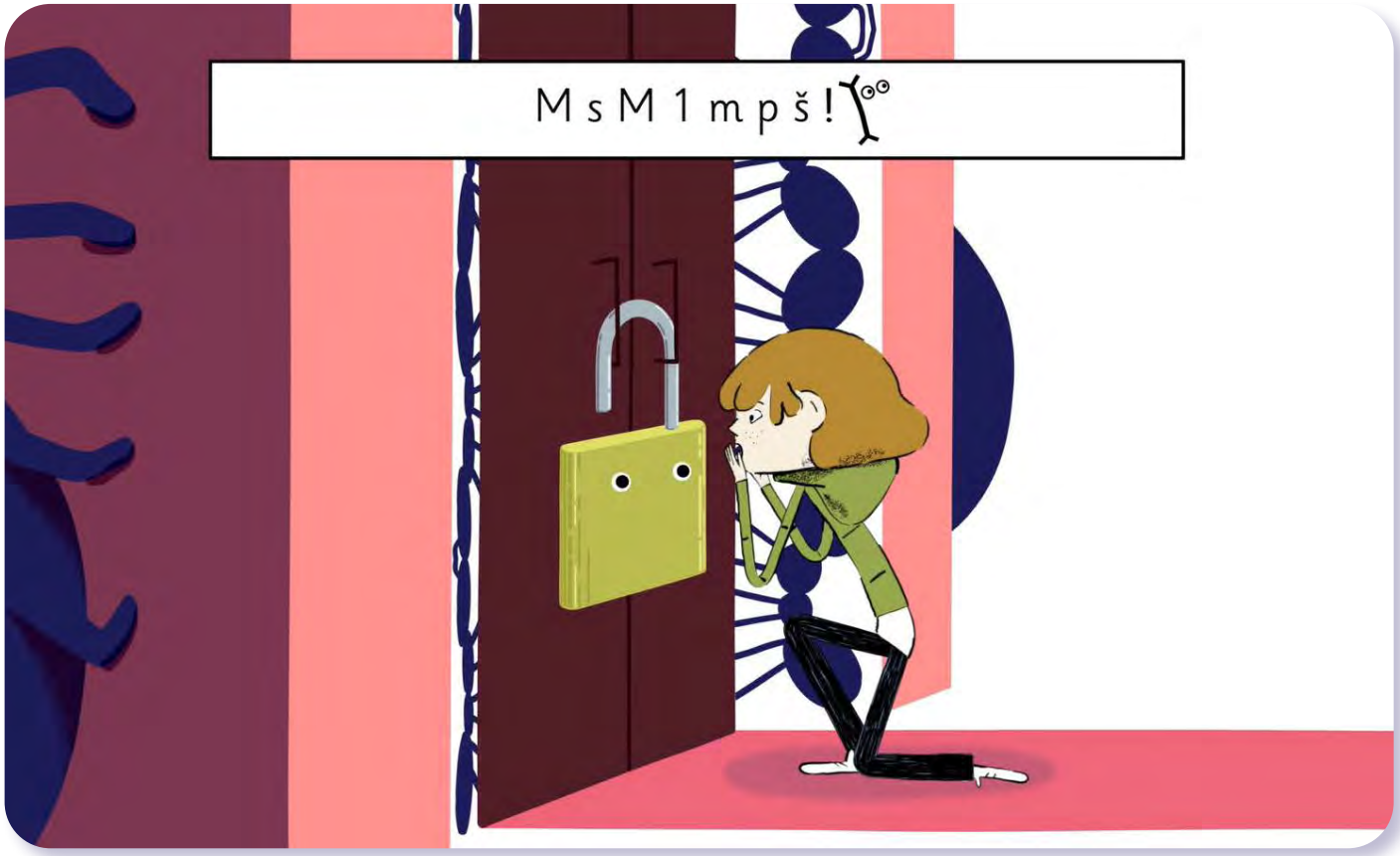
Viry mohou napáchat různě velké škody od **zpomalení zařízení, poškození souborů v počítači či hardwaru až po rozsáhlé škody na počítačových systémech**. Na konci roku 2019 se podařilo ruskému viru Ryuk proniknout do počítačového systému v benešovské nemocnici, kterou jeho obnovení stálo několik desítek milionů korun. Tento druh viru, resp. malwaru se nazývá ransomware. Nejprve důkladně prozkoumá všechna data, poté vše důkladně zanalyzuje a nakonec počítač zašifruje. Za klíč k zašifrovaným datům pak tvůrci viru požadují výkupné.

8. Co dělat, když mám podezření, že je v mém počítači vir?

V případě podezření na zavirovaný počítač či mobil doporučujeme **zkontrolovat platnost antivirového programu a poté spustit aktualizaci softwaru** a **následně prověřit aktuálnost virové databáze**. V případě, že je náš antivir aktuální, ověříme, zda **operační systém v počítači či mobilním zařízení není zastaralý**. Pokud zjistíme, že ano, opět **spustíme instalaci aktuální verze** či nejnovější bezpečnostní záplaty neboli *patche*. Po dokončení obou těchto úkonů následně **spustíme hloubkovou kontrolu zařízení antivirovým programem nad celým systémem**. V případě nalezení škodlivého softwaru začne program infikované objekty v zařízení „léčit“. Po úspěšné „léčbě“ nám program ukáže shodné počty infikovaných a vyléčených souborů. V opačném případě však raději bezodkladně **informujeme technickou podporu** našeho antivirového programu a zašleme tam vytvořený protokol z kontroly zařízení. Pracovníci technické podpory nám pomohou situaci co nejlépe vyřešit.

Odpovědi vypracovala:
Michala Radotínská, CZ.NIC

Podívejte se na lekci V digitálním světě: Viry na <jsns.cz/mv/viry>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.



V digitálním světě

Hesla

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Filipovi se nedaří přihlásit do účtu a Kocour mu prozradí, že v tom má prsty Mína. Změnila mu heslo, protože bylo snadno uhodnutelné. Hesla chrání to nejcennější, co v prostoru internetu máme. Pokud zvolíme slabé heslo, piráti se mohou dostat do našich e-mailových schránek a k dalším citlivým informacím a dokumentům. Další epizoda seriálu popisuje, jak vymyslet silné heslo, a doporučuje ho s nikým nesdílet.

CÍLE LEKCE

1. zamyslet se nad tím, jakou hodnotu má naše soukromí
2. naučit se, jak vytvořit silné heslo
3. zjistit, jaká hesla nikdy nepoužívat

DOPORUČENÝ VĚK
8+ LET

AKTIVITA: Hesla

!!!

ANOTACE

Žáci se prostřednictvím aktivity zamyslí nad důležitostí ochrany cenností a osobních údajů – jak v reálném, tak i virtuálním světě. V úvodu aktivity žáci hádají, co cenného nebo tajného se skrývá v pokladničce či kufru a jakým jedinečným klíčem se lze dostat dovnitř. Žáci si dále vyzkouší vytvořit silné heslo.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k učení, k řešení problémů, komunikativní, sociální a personální

CÍLE

Žáci:
- se zamyslí nad hodnotou soukromí a cenných předmětů nebo informací
- se naučí, jak vytvořit silné heslo
- se dozví, jaká hesla určitě nepoužívat

DÉLKA

60 min. (včetně projekce)

POMŮCKY

- PRACOVNÍ LIST pro každého žáka
- pokladnička se zámkem na klíč (příp. kufr s mechanickým nebo číselným zámkem)
- obsah pokladničky (např. peníze, šperk, fotografie, dopis apod.)
- tabule nebo flipchart

POSTUP

1. Do pokladničky se zámkem na klíč (příp. do kufru se zámkem, pokud pokladničku nemáme k dispozici) **schováme drobné předměty**, například peníze, prstýnek, fotografie nebo pohled. Necháme žáky hádat, **co a proč v pokladničce je**. Nápady zapisujeme na tabuli/flipchart.

2. Zeptáme se žáků: *Jak se dostaneme do pokladničky?* Připomeneme si, že klíče mohou být různé a je nutné mít ten správný. Pokladničku otevřeme a objasníme si, **proč jsou schované věci cenné**, krátce diskutujeme o tom, co si chráníme a proč. V diskusi žáci zřejmě zmíní i nutnost ochrany telefonu a jeho obsahu.

3. Následuje **projekce epizody seriálu**.

4. Ověříme porozumění obsahu dílu. Můžeme se ptát: *Co provedla Mína Filipovi? Jak se Filip cítil? Jak problém s heslem vyřešili?*
   Poznámka: Snímek doporučujeme zhlédnout nejméně dvakrát.

5. Každému žákovi **rozdáme PRACOVNÍ LIST**.
   a/ Navážeme na piráta z příběhu a společně se v pracovním listu podíváme na uvedené příklady **slabých hesel, která nikdy nepoužíváme**.
   b/ Připomeneme si, jaké silné heslo vytvořil Filip na konci příběhu:
   Moje sestra Mína 1 mně pěkně štve! → **MsM1mpš!**
   c/ Vysvětlíme žákům i další **doporučený postup tvorby silného hesla:**
   Použijeme několik slov, sousloví nebo i celou větu.
   Použijeme také vždy velké písmeno, číslici a znak (teda např. tečku, otazník).
   Dohromady má heslo alespoň 10 znaků.
   Příklady: Hrajufotbal!87 *nebo* hrajuFotbal87! *nebo* !Hraju8Fotbal7
   Nejradsinasvetetancim§ 26 *nebo* nejradsinasvete-Tancim§ 26 *nebo* 26Nejradsinasveteš§Tancim

6. Žáci samostatně **vytvoří dvě silná hesla** a zapíšou je do druhé části pracovního listu. Necháme jim na vymyšlení hesel dostatek času, mohou konzultovat se spolužáky nebo s učitelem.
   a/ Připomeneme, že heslo má být **silné, ale také praktické** – musí se snadno a ne příliš zdlouhavě psát na klávesnici.
   Poznámka: Postup, kde použijeme větu nebo sousloví, díl seriálu nezmiňuje, dnes se ale jedná o způsob, který experti nejčastěji doporučují. V epizodě seriálu se doporučuje délka hesla 8 znaků, dnes už je standardem spíše 10 a více znaků.

7. Doporučujeme seznámit se také s textem OTÁZKY A ODPOVĚDI, který přináší podrobnější odborný vhled do tématu.

REFLEXE AKTIVITY

Dobrovolníci zapíšou svoje heslo na tabuli, společně kontrolujeme, jestli splňuje všechny náležitosti:
- alespoň 10 (nebo víc) znaků
- velké písmeno, číslice, znak

Zdůrazníme, že v hodině vytvořená a zveřejněná hesla by žáci neměli ve skutečnosti používat a musí si vymyslet nové, které budou znát jen oni.
V reflexi se zaměříme na důvody ochrany našich cenností a soukromých nebo i důvěrných informací (můžeme zmínit i evropské nařízení o ochraně dat známé pod zkratkou GDPR). Společně promyslíme, u jakých online služeb mohou žáci heslo potřebovat, například při přihlášení do e-mailové schránky, do virtuální učebny nebo do různých aplikací. Žákům můžeme doporučit, aby heslo nikdy nesvěřovali kamarádům.

ZKUŠENOSTI Z PRAXE

V době distanční výuky jsem pracovala s mojí 4. třídou v MS Teams, kde si žáci museli nastavit vlastní heslo. Díky tomu jsem mluvila o tom, jak silné heslo vypadá. Bohužel během 45 minut nebyla většina žáků schopna si heslo vymyslet a spousta z nich prostě okopírovala to mé, které jsem jim ukázala jako příklad.
Ukázal se také jako problém si ta hesla zapamatovat nebo je napsat správně na klávesnici.
V dnešní době děti v tomto věku jedou hlavně na mobilu a tam mají ta hesla uložená, takže si je „nemusí pamatovat".
Myslím, že by tedy bylo fajn tuto aktivitu provést na začátku výuky ICT, kdy se žáci například učí, jak se dostat do Bakalářů nebo do e-mailu. A propojit tak teorii s praxí.
Jana Machovská, *ZŠ Liptál*

POZNÁMKY

PRACOVNÍ LIST

1. Přečtěte si příklady hesel, která nikdy nepoužíváme:

123456

abc123

heslo

password

123123

milujite

Nepoužíváme také: svoje jméno, datum narození ani adresu

2. Vytvořte si silné heslo. Použijte:

alespoň 10 znaků

velké písmeno

speciální znak, jako například tečku, otazník, hvězdičku

.....

.....

OTÁZKY A ODPOVĚDI

1. Proč potřebujeme v prostředí internetu hesla?

Internet je z principu otevřený a nabízí nám řadu služeb, ke kterým máme všichni rychlý přístup. V takovém prostředí je potřeba se jednoznačně identifikovat, jinak by vznikl zmatek. Služby jsou často navázány přímo k naší osobě – například e-maily, sociální sítě nebo internetové bankovnictví. **Abychom mohli v prostředí internetu ověřit a prokázat, že jsme to opravdu my, potřebujeme k tomu znalost hesla.** Způsobů ověřování existuje více, zadávání hesla je ale velmi praktické, jednoduché, a proto hojně využívané.

2. Jak vytvořit bezpečné heslo?

Mnozí si myslí, že bezpečné heslo musí být ve výsledku špatně zapamatovatelný shluk znaků typu x19ortWc0. To není tak docela pravda. **Bezpečné heslo může být naopak pro nás velmi dobře zapamatovatelné.**

Doposud doporučované požadavky na bezpečné heslo (velká a malá písmena, čísla, speciální znaky) se opouštějí a čím dál častěji bývají **doporučovány fráze**. Co to znamená? **Použijeme řadu slov nebo větu**. Příklad: 2ZeleníKoněŽraliTrávu, 4ZTankuAPes.

Můžeme si najít i své pravidlo, které aplikujeme. Třeba vzít kousek naší oblíbené písničky, a tu použít jako pomůcku k zapamatování našeho hesla. Příklad: Stokrát chválím čas = 100xChválímČas.

Dobrým ochranným prvkem může být také použití **hrubky** nebo **faktografické chyby**. Příklady, které zde uvádíme, jsou pro počítač jenom nesmyslným řetězcem znaků. My v něm však smysl vidíme, proto je to pro nás přívětivější.

Doporučujeme také využít **dvoufázové ověřování**. Jedná se o proces, který zahrnuje dva nezávislé způsoby, jak ověřit totožnost uživatele při přihlašování – například vedle hesla musíme zadat ještě kód, který nám přijde prostřednictvím sms. Je to zvýšená ochrana našeho účtu a „záchranná brzda“ v případě, kdyby se k našim přihlašovacím údajům dostal někdo nepovolaný.

Poznámka: Postoje a doporučení, jak vytvořit heslo, se vyvíjí. Seriál *V digitálním světě* určený pro malé děti je v něčem zjednodušující, proto je některé uvedené rady dobré doplnit. V epizodě *Hesla* je zmíněno, že silné heslo má být složeno ze šesti znaků, což ale není zcela pravda. Takové heslo je totiž **snadno prolomitelné** a dnes se doporučuje heslo delší (viz výše).

V epizodě je dále uvedena rada „pro jistotu si heslo někam zapište“. Je důležité přemýšlet o tom, **kam a jakým způsobem si heslo napsat**.

V seriálu zazní také zmínka o sdělení hesla rodičům. To nemusí být nutně špatné řešení, ale opět je třeba zvážit okolnosti.

3. Potřebuji různá hesla pro různé stránky nebo aplikace?

Ano. Měli bychom skutečně **využívat různá hesla**. Je ale důležitý selský rozum. Můžeme mít například balík hesel, **která mají část stejnou, ale část vždy obměněnou**. Takový balík hesel pro méně důležité služby může být například 93-03VáclavHavel, 03-13VáclavKlaus atp. Platí, že bychom měli mít **tak silné heslo, jak důležitá je pro nás služba, kterou má chránit**. Z toho plyne, že pro internetové bankovnictví nebo pro e-mail bychom měli mít pečlivě a bezpečně zvolené heslo.

4. Co bychom rozhodně neměli při používání hesel dělat?

Nepsat hesla na papírky, protože ten se může dostat do nepovolaných rukou. **Nepsat si hesla ani do počítače**, například do excelového souboru (a už vůbec takový soubor nepojmenovávat „Hesla“). **Hesla nikomu neříkat** (až na naprosté výjimky) – můžeme se pohádat a heslo může být pak v konfliktu zneužito. Neměli bychom ani využívat možnosti „zapamatovat si heslo“, které nám nabízí internetový prohlížeč – **zde uložená hesla je možné odcizit**, pokud máme počítač nebo mobilní telefon nakažený nějakým virem, o kterém nemusíme ani vědět.

Naopak nám může velmi pomoci přihlašovat se do citlivých a pro nás důležitých služeb přes anonymní režim prohlížeče. Ideálně bychom neměli mít otevřenou žádnou jinou záložku vedle okna, kam se přihlašujeme. Existují i praktiky, jak mohou útočníci mezi těmito záložkami přeskakovat.

5. Lze doporučit aplikace na správu hesel?

Existují aplikace, kterým se říká **správce hesel**. Ty nám heslo v případě potřeby **vygenerují, poskytnou, uloží** a nemusíme si ho pamatovat. Stačí, že se umíme do tohoto správce přihlásit a hned máme přístup k našim dalším heslům. Je třeba volit si do tohoto správce **opravdu enormně silné heslo**. **Nedá se také doporučit dávat do něj všechna hesla** – třeba internetové bankovnictví sem nepatří. Obecně je dobré **preferovat** takové **nástroje**, které mají tzv. **otevřený kód** (open-source). To jsou obvykle komunitně a celosvětově vyvíjené nástroje, které mají svůj kód (způsob, jakým fungují) zveřejněný a kdokoliv se na něj může podívat. To znamená, že pokud by s takovým nástrojem byl spojený bezpečnostní problém, rychle se odhalí a bude se o něm vědět. Takový nástroj založený na open-source principu je například KeePass. Ten je zajímavý i v tom, že Evropská unie pravidelně provádí audit jeho kódu.

Další zajímavou možností je **MojeID**, které spravuje sdružení CZ.NIC. Na MojeID si **vytvoříme svou identitu, projdeme ověřovacím kolečkem a následně získáme z jednoho místa přístup do řady služeb, které využíváme** – zpravodajství, stránky města, stránky knihovny, e-shopy atp. Nepřihlašujeme se na jednotlivé stránky, ale přihlásíme se do MojeID, které nás pak pustí dále. Rozdíl oproti správcům hesel je tedy ten, že se nepřihlašujeme do každé služby zvlášť. Nevýhodou zase je, že se přes toto řešení nemůžeme

přihlásit všude, ale jen do služeb, které MojeID podporují. MojeID je zdarma.

6. Jak někdo může zjistit moje heslo?

Nejčastěji se naše heslo dostane do nepovolaných rukou kvůli naší **uživatelské nedbalosti**. Nebezpečné jsou papírky s hesly nalepenými na monitoru a podobné pomůcky. Může se také stát, že se při přihlašování přehlédneme a vyplníme své heslo do kolonky „uživatelské jméno“, ve stejném zařízení se pak může zobrazovat i dalším uživatelům. Výjimkou nejsou ani případy, kdy uživatel heslo sám a dobrovolně sdělí jinému člověku (kamarádovi, přítelkyni nebo například člověku, který se pod záminkou snaží heslo vylákat).

Může také dojít k **úniku na straně služeb**, které využíváme. Existují případy, kdy velké balíky přihlašovacích údajů uniknou na internet, kde pak kolují. Téměř nikdy neuniknou na internet hesla v člověku čitelné podobě, ale i s těmito strojově čitelnými daty se dá různými způsoby pracovat a naše heslo z nich získat.

Existují i způsoby, jak se k našemu heslu dostat na základě **výpočtů a matematických operací**. To je například tzv. slovníkový útok, který se snaží naše heslo odhadnout na základě databází slov, která lidé pro tvorbu hesel často používají.

Rozsáhlou praktikou jsou **podvodné e-maily**, které se tváří například jako z banky, ale v momentě, kdy se do takové stránky přihlásíme, dobrovolně odevzdáme své přihlašovací údaje.

Existují i podvodné praktiky, kde se **pracuje s různými chytáky** v odkazu, kam máme přejít. Ty atakují především nepozornost uživatele. Stačí, když útočník zamění písmeno „m“ za „rn“, „malé „l“ (el) za velké „I“ (i) a další maličkosti.

7. Jak dlouho trvá jednotlivá hesla prolomit?

To záleží na **síle našeho hesla a na výpočetním výkonu útočníka**. Jednoduchá a slabá hesla typu 123456 se běžně prolomí v řádu milisekund. Taková hesla bychom však v dnešní době neměli mít možnost nastavit snad nikde. **Automatizované nástroje se snaží hlídat běžné uživatele, aby měli ve svých heslech právě velká a malá písmena, čísla, speciální znaky, a to vše v požadované délce.** Je ale přirozené, že velké písmeno si lidé dávají na začátek svého heslo a čísla na jeho konec. To jsou předpoklady, které umí útočníci využít, pracují s nimi a to jim postup zjednodušuje.

8. Co dělat, když zjistím, že se někdo nabourал do mého účtu?

Zde záleží na tom, **kdo, kam a jak se nabourал**. Pokud se jedná například o **internetové bankovnictví**, pak nejdříve kontaktujeme banku z důvodu zablokování přístupu ke kartám a účtu. **Banka** nás také bude informovat, jak postupovat dále.

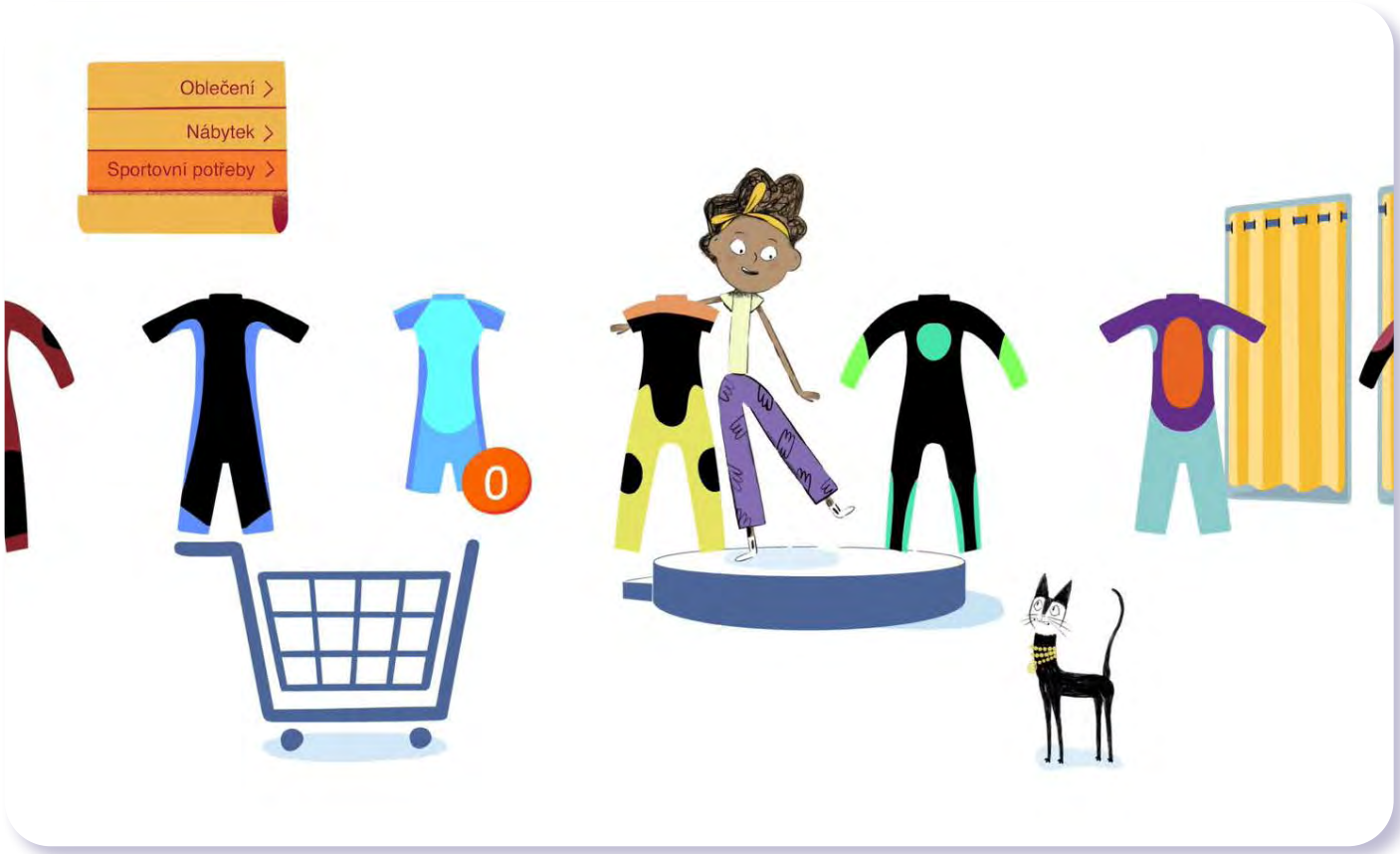
Dojde-li k **nabourání účtu**, který souvisí s výkonem našich **pracovních povinností** (např. pracovní e-mail nebo interní systém zaměstnavatele), rozhodně bychom o této skutečnosti měli informovat **IT oddělení zaměstnavatele**. Pokud se jedná o **účet**, na kterém mohou být **citlivé informace** (např. adresa, rodné číslo, smlouvy apod.), které by někdo mohl zneužít, pak je namístě kontaktovat také **Policii ČR**.

Co se týče **poskytovatelů e-mailových služeb**, ti se nás dnes snaží varovat či informovat o tom, že se někdo snažil přihlásit do našeho e-mailu z místa, kde se běžně nepohybujeme. Existují také podvodné praktiky, kdy nám přijde e-mail z naší vlastní adresy, kde se píše, že má útočník přístup do našeho účtu a zneužije ho, pokud nezaplatíme požadovanou částku. **Nejlepší je těmto věcem předcházet pravidelným a pečlivým zálohováním našeho obsahu na účtech**. To znamená, že si čas od času nahrajeme své soubory nebo údaje i na další místo.

Odpovědi vypracoval:

David Kudrna, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Podívejte se na lekci V digitálním světě: Hesla na <jsns.cz/mv/hesla>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.



V digitálním světě

Cookies

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Kocour a Mína brouzdají svými oblíbenými stránkami. Když z e-shopu odejdou, pronásledují je otravné reklamní e-maily. Vyměnit svoji e-mailovou adresu za přístup k obsahu některých webových stránek je zdánlivě nízká cena. Když se ale naše soukromá schránka začne plnit propagačními e-maily, možná si to příště rozmyslíme. O tom, jaká reklama se nám na internetu zobrazí nebo nám přistane v e-mailu, rozhodují neviditelní „špioni" v našem počítači, kterým se říká cookies. Seriálová epizoda radí, jak se těmto sběratelům citlivých údajů bránit.

CÍLE LEKCE

1. uvědomit si, že jsou o nás všech při užívání internetu sbírána data
2. pochopit, že existuje personalizovaná reklama
3. poučit se, jak se vyhnout nevyžádaným reklamám

DOPORUČENÝ VĚK
8+ LET

AKTIVITA: Cookies – špioni na internetu !!!

ANOTACE

Žáci se na začátku aktivity zamýšlejí nad funkcí cookies – špionů na internetu. Poté diskutují o pozitivech a negativech reklamy. Vytvoří si vlastní vtipnou e-mailovou adresu pouze na reklamy a osvojí si, jak jinak se nevyžádaným reklamám vyhnout.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k řešení problémů, komunikativní, sociální a personální, občanské

CÍLE

Žáci:
- se zamýšlí nad pozitivy a negativy reklamy
- se učí, jak se vyhnout nevyžádaným reklamám
- si uvědomí, že jsou o nás při užívání internetu sbírána data

DÉLKA

45 min. (včetně projekce)

POMŮCKY

- tabule nebo flipchart
- papíry, psací potřeby

POSTUP

1. Ptáme se žáků: *Kdo je to špion? Koho sleduje? Proč? Myslíte, že vás může sledovat nějaký špion na internetu?* Necháme zaznít všechny reakce žáků.
2. Následuje **projekce dílu seriálu**.
   Poznámka: Snímek doporučujeme zhlédnout nejméně dvakrát.
3. Krátce ověříme, zda žáci pochopili příběh. (Mína si v e-shopu vybírá kombinézu na surfování, ze stránky jí začnou pronásledovat cookies, které sbírají osobní údaje a informace o prohlížení. Je třeba smazat historii prohlížení, blokovat cookies a vytvořit novou adresu pro reklamy.)
4. Ptáme se: *Už se vám někdy stalo něco podobného jako Míně? Co si myslíte o reklamách?* Vyzveme žáky, aby **vyjmenovali negativa a pozitiva reklamy** (co se jim na reklamách líbí a co jim vadí). Návrhy žáků zapisujeme na tabuli.
5. Vyzveme žáky, ať **vysvětlí, co je to e-mail** a zda s ním mají zkušenosti. Kocour si v seriálu vytvořil nový e-mail, kam mu budou chodit jenom nevyžádané reklamy. Žáci dostanou za úkol vymyslet vlastní variantu vtipné e-mailové adresy, která by jim mohla sloužit právě pro nevyžádané reklamy.
6. Žáci své smyšlené vtipné **e-mailové adresy přečtou**.

REFLEXE AKTIVITY

Vyzveme žáky, ať zkusí **zopakovat pravidla**, která dodržovat, abychom se špionům a nevyžádaným reklamám online vyhnuli.
Příklad pravidel:
- Smazat historii prohlížení.
- Využít anonymní režim prohlížeče.
- Vytvořit si zvláštní e-mailovou adresu, na kterou nám budou chodit jen reklamy.

Poznámka: Doporučujeme využít OTÁZKY A ODPOVĚDI k lekci.

ZKUŠENOSTI Z PRAXE

Pro většinu žáků to bylo první seznámení s daným problémem. Jsem ráda, že se o tom dozvěděli a časem se budou moci zařídit. Během týdne mi několik žáků řeklo, že zkoušeli s rodiči smazat historii prohlížení a nastavit prohlížeč tak, aby nic nestahoval.
Kateřina Fučíková, *MŠ a ZŠ Prosetín*

OTÁZKY A ODPOVĚDI

1. Co jsou cookies a jak fungují?

Cookies jsou malé datové soubory vytvořené webovou stránkou, které se přes prohlížeč ukládají do počítače či mobilního telefonu uživatele. **Zaznamenávají informace o chování uživatele** (resp. jeho zařízení) na webu a slouží k jeho pozdější identifikaci při opětovné návštěvě. Díky cookies si webová stránka pamatuje například přihlašovací a kontaktní údaje, položky v košíku nebo jazykové nastavení a při pozdější návštěvě tak není nutné vše znovu vyplňovat/nastavovat.

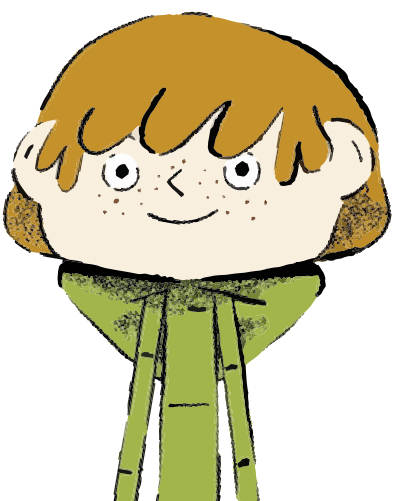
Cookies jsou rovněž **využívány k cílení reklamy**. Využívají je provozovatelé webových stránek, neboť díky nim mohou identifikovat cílovou skupinu, které své služby chtějí nabízet. Pokud ji dobře znají, mohou jí zobrazovat nabídky, jež přesně odpovídají jejím zájmům a potřebám, což zvyšuje šanci, že si daný uživatel produkt koupí a provozovateli webu tak přinese zisk.

2. Jaké výhody a nevýhody uživatelům cookies přinášejí?

Cookies a další personalizovaná komunikace nám **dokážou zobrazit relevantnější obsah odpovídající našim zájmům a potřebám**. Usnadňují také výběr zboží, zásadně zlepšují uživatelské pohodlí při používání internetového prohlížeče nebo orientaci na webové stránce. Tato tzv. personalizace je nicméně možná jen za cenu určité **ztráty soukromí**. Někteří odborníci v souvislosti s přizpůsobováním obsahu konkrétním skupinám uživatelů či jednotlivců upozorňují také na **rizika spojená s omezováním svobodné volby**. Konkrétně v případě sociálních sítí se pak kvůli algoritmům sociálních sítí, které nám vybírají jen určitý obsah, uzavíráme do informačních a sociálních bublin.

3. Jak lze sběr cookies omezit? Jaké to pak má praktické dopady?

V prohlížeči (např. Google Chrome, Internet Explorer, Mozilla Firefox, Safari apod.) si můžeme **ukládání cookies zablokovat**, čímž však přijdeme o všechny výhody s nimi spojené. Někteří uživatelé si cookies ze svého počítače pravidelně vymazávají. Zobrazování personalizované reklamy je možné upravit také v nastavení svého účtu na Google či Facebooku. Další možností je využívat v prohlížeči tzv. anonymní režim, v němž se neukládá historie prohlížení, soubory cookies, data webů ani informace zadané do formulářů.



Prohlížeče rovněž nabízejí možnost zablokovat reklamy od konkrétního inzerenta, případně si instalovat blokovací rozšíření prohlížeče umožňující plošný zákaz zobrazování reklam. Rostoucí fenomén blokování reklam má však negativní dopad na vydavatele obsahu (např. zpravodajské weby apod.), jejichž příjmy plynou mnohdy pouze z inzerce. Zájmem všech účastníků reklamního procesu (inzerent, agentura, médium) je proto **zobrazovat uživatelům pouze relevantní reklamu**, která je nebude obtěžovat a motivovat k používání blokátorů.

Existují různá rozšíření do prohlížečů, která se snaží cookies eliminovat. Je to například **Remove Cookies for Site**, tlačítko s obrázkem sušenky – pokud na ně kliknete, odstraníte cookies soubory, které jsou svázány s právě navštíveným webem; Edit This Cookie, který umožňuje cookies soubory analyzovat, upravovat, selektivně promazávat nebo do nich vpisovat nové informace, nebo Click & Clean, který si poradí i s mazáním historie stažených souborů a cookies umí odstranit.

4. Co se stane, když smažu historii prohlížení? Pomůže to?

Smazáním historie z prohlížeče lze vedle historie procházení odstranit také cookies a jiná data webů. Smazání je možné buď kompletní, nebo za určité časové období. Tím **dojde k jednorázovému odstranění cookies z počítače.** Při dalším spuštění se cookies začnou opět ukládat.

5. Jak funguje anonymní prohlížení? Omezím jeho používáním sběr osobních dat?

Anonymní prohlížení umožňuje **procházet internet bez ukládání informací** o navštívených stránkách a dalším chování uživatele. V anonymním režimu si prohlížeč neukládá historii prohlížení, soubory cookie, data webů ani informace zadané do formulářů. V praxi se nám tak například nepředvyplňují formuláře, URL adresy, přihlašovací jména/hesla apod. Prohlížeč si vedle historie prohlížení nepamatuje ani seznam stažených souborů, byť samotné stažené soubory a vytvořené záložky jsou zachovány. Cookies se v anonymním režimu ukládají jen dočasně (odděleně) a při zavření okna prohlížeče jsou z počítače vymazány.

6. Jaký má sběr dat o uživatelích zákonné rámce?

Provozovatelé webových stránek by měli uživatele informovat, že jejich web cookies ukládá, a **mají povinnost získat od něj k využívání cookies souhlas**. Za ten se nicméně považuje i samotné nastavení prohlížeče, ve kterém uživatel ukládání cookies nezablokoval. Zákon dává spotřebitelům také právo na **přístup k jejich údajům**. Každá firma by měla uživateli na vyžádání sdělit, které údaje o něm zpracovává, za jakým účelem a komu dalšímu je poskytuje.

Obecné nařízení o ochraně osobních údajů (GDPR) specifikuje také právo „být zapomenut“, tzn. požádat o vymazání všech údajů, které o něm společnost shromáždila. To by měly společnosti také dodržet v případě, kdy spotřebitel svůj souhlas se zpracováním osobních údajů odvolá.

7. Došlo k nějakému velkému zneužití cookies?

Velké kauzy zneužití či úniku osobních dat se týkají většinou jiného typu osobních dat, než jsou cookies. Jedná se například o osobní údaje uživatelů sociálních sítí, kontaktní údaje z firemních zákaznických databází apod.

Odpovědi vypracoval:

Michal Kříž, PR a marketingový konzultant

Podívejte se na lekci V digitálním světě: Cookies na <jsns.cz/mv/cookies>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.

POZNÁMKY

V digitálním světě

Online hry

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Filip je odhodlaný ve své oblíbené hře Mravenčáci získat co nejvíc bodů. Kdyby si tak mohl přikoupit ty Sedmimílové boty! Stojí jen pár stovek zlatých dukátů… Na internetu je mnoho her, které je možné hrát online a zdarma. Past některých z nich spočívá v tzv. integrovaných nákupech, tedy nabídkách nákupu herních bonusů. Tady hra končí. „Zlaté cihličky" totiž stojí reálné peníze, jež odcházejí z naší platební karty.

CÍLE LEKCE

1. uvědomit si rizika spojená s užíváním internetu
2. pochopit, že na internetu se platí herními měnami i reálnými penězi
3. rozeznat pozitiva a negativa hraní her

DOPORUČENÝ VĚK
8+ LET

AKTIVITA: Online hry

!!!

ANOTACE

Aktivita vede žáky k tomu, aby si uvědomili, co je na hraní online (video)her zábavné a poučné a co může být naopak problematické. Žáci formou písemného úkolu reflektují svoje oblíbené hry. Uvědomí si, že v hrách na internetu se utrácí nejen herní, ale i reálné peníze.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k řešení problémů, komunikativní, sociální a personální, občanské

CÍLE

Žáci:
- si uvědomí, že na internetu se platí jak herními měnami, tak reálnými penězi
- si uvědomí pozitiva i negativa hraní videoher
- se učí aspektům bezpečného chování na internetu

DÉLKA

45 min. (včetně projekce)

POMŮCKY

- PRACOVNÍ LIST pro každého žáka
- psací potřeby

POSTUP

1. Na začátku aktivity položíme žákům otázky: *Nakupuje vaše rodina na internetu? Jak se na internetu platí? Odkud se berou peníze na platební kartě?*
2. Následuje **projekce epizody seriálu**.
   Poznámka: Snímek doporučujeme zhlédnout nejméně dvakrát.
3. Ověříme porozumění obsahu dílu seriálu. Ptáme se: *Co se stalo Filipovi? Jak bylo možné, aby ve hře utratil skutečné peníze?*
4. Po projekci rozdáme žákům PRACOVNÍ LIST. Žáci pracují samostatně a zapisují odpovědi na otázky. Odpovědi společně sdílíme.
5. S celou třídou se společně **zamyslíme nad plusy a minusy hraní her**. Zapisujeme na tabuli nebo flipchart. Mezi plusy můžeme uvést, co je na videohrách poučné nebo zábavné, k minusům, co může být u hraní videoher problém (např. nadměrné utrácení nebo nevědomá platba, příliš časté a příliš dlouhé hraní, hry s nevhodným obsahem určené spíš dospělým než dětem...).

REFLEXE AKTIVITY

Provedeme důkladnou reflexi formou diskuse. **Sdílíme zkušenosti žáků s hraním videoher.** Klademe důraz i na finanční stránku. Ptáme se například: *Dovolí vám rodiče nákupy v hrách? Za co konkrétně? Stalo se vám někdy, že jste peníze utratili bez dovolení? Je těžké odolat nákupům v hrách?*
V diskusi zdůrazníme, že s finančními prostředky je potřeba nakládat rozvážně a rozlišovat herní měnu a reálné peníze.
Lekci doporučujeme ukončit pozitivně, například oceněním množství poznatků, které žáci o hrách mají, nebo oceněním kreativity a spolupráce při hraní.
Doporučujeme využít OTÁZKY A ODPOVĚDI k lekci.

PRACOVNÍ LIST

Stručně odpovězte na otázky:

1. Jaké jsou vaše oblíbené hry na počítači, telefonu nebo tabletu?

.....

2. Co vás na vašich oblíbených hrách baví?

.....

3. Hrajete sami nebo i online s kamarády?

.....

4. Dá se ve hrách, které vás zajímají, platit i skutečnými penězi?

.....

5. Dá se ve hrách, které vás zajímají, získat herní měna za úspěchy ve hře?
Tedy například diamanty, zlaté cihly, tokeny, gemy, coiny, robůxy apod.?

.....

6. Co byste si ve hře nejvíc přáli? Dá se to získat hraním, nebo jenom koupit za skutečné peníze?

.....

OTÁZKY A ODPOVĚDI

1. Jaké existují základní druhy počítačových her?

Videohry se dají rozdělit podle různých kritérií – nejčastěji se ale rozdělují **podle žánrů**. Těch uvádí jen taková Wikipedie více než dvacet. Patří sem kategorie jako **akční hry, logické, strategické, závodní, simulace, adventury, role playing (hry na hrdiny), sportovní hry nebo „střílečky“**. Velkou samostatnou skupinu v rámci jednotlivých žánrů tvoří i **hry pro více hráčů,** které spadají do různých žánrů.

Klasifikovat videohry můžeme ale také **dle použití** – nejčastěji rozeznáváme hry **komerční, s cílem zabavit**; a **videohry edukační, s cílem něco naučit**.

Třetím dělením je dělení her na hry tzv. **casual**, což jsou hry snadno přístupné pro hráče (jednoduché hry), a tzv. **hardcore** (náročnější hry, které vyžadují předešlé zkušenosti s hraním her). V dnešní době je obrovské množství právě zmíněných casual her, které má téměř každý z nás ve svém telefonu. A najdou se hry prakticky pro každého – od tříletých dětí až po hry pro seniory, pro muže i ženy, pro ty, kteří chtějí při nich pouze „vypnout“, až po supernáročné simulace, které by někomu mohly připadat spíš jako práce.

2. Jaká je historie hraní her? Jak se hraní proměnilo v čase?

Videohry byly na úplném začátku pouze intelektuální kratochvílí vědců, kteří pracovali s prvními počítači. Do povědomí široké veřejnosti se ale dostaly až v **70. a 80. letech minulého století**, kdy se objevily **první osobní počítače, herní konzole a arkádové automaty**. Základními milníky v herní historii byly hlavně technologické novinky – osobní počítače, konzoly, **handheldy, 3D zobrazování a 3D hry, internet a online hraní následované revolucí v mobilních telefonech, smartphonech** až po virtuální a rozšířenou realitu. Hry se postupně vyvíjely a zvyšovaly svou komplexnost, začaly je vyvíjet profesionální týmy a dnes jsou integrální součástí našeho světa. S rozvojem komplexity vznikaly i nové žánry, výrazně se rozšířilo i publikum, na které se jejich tvůrci zaměřovali.

Postupně se **měnily i modely prodeje** – z **fyzických nosičů** se přesunuly k **digitální distribuci**, přímý prodej her nahradily **„free to play“** hry, které se snaží vydělat na dokupování dodatečného obsahu, reklamě a předplatném.

V neposlední řadě je třeba zmínit **e-sporty**, které v dnešní době vyprodávají virtuální haly. V tomto byznysu se dnes točí ohromné peníze.

3. Proč je gaming pro děti (ale i dospělé) atraktivní?

Gaming má proti jiným volnočasovým aktivitám řadu atraktivních rysů. Především je to **dostupnost**. Pro pěstování většiny koníčků potřebujete jednak vstupní vybavení (např. kolo a helmu pro cyklistiku, boty, oblečení apod. pro fotbal), jednak určité další podmínky pro provozování (počasí, místo, společnost jiných lidí v případě kolektivních sportů, peníze v případě organizovaných kroužků apod.). V případě gamingu si často vystačíte se vstupní investicí do vybavení (počítač/konzole, periferie, hry) a pak už se můžete činnosti věnovat kdykoliv z pohodlí domova. Dalo by se říct, že je v tomhle gaming podobný třeba sledování televize nebo čtení. Gaming ale na rozdíl od nich nabízí **větší interaktivitu a imerzivitu** (míru ponoření hráče do virtuálního světa hry). Navíc s rychlým rozvojem e-sportů (progamingu) nabízí hraní her i **soutěžní** (profesionální) **kariéru s možností vysokého výdělku**, čímž se přibližuje prestižním sportům typu hokej, fotbal nebo tenis, ale s nižším vstupním prahem (je snazší začít trénovat League of Legends než hokej).

4. Jaké hry mezi dětmi ve věku 8–11 let nejvíc „frčí“?

To je velmi individuální. Jedná se o období, kdy děti přestávají bavit „dětské“ hry a stále více se dožadují titulů určených pro starší cílové skupiny. Jejich paleta je velmi pestrá a zahrnuje i příklady, které pro tuto věkovou kategorii nejsou vhodné.

Mezi nejpopulárnější se již léta stabilně řadí **Minecraft,** ale také „automobilový fotbal“ **Rocket League**. Z novějších jsou to hry, jako je adventura **The Legend of Zelda: Breath of the Wild** nebo „skákačka“ **Super Mario Odyssey**. Kromě toho se velké popularitě těší i Minecraftem silně inspirovaný **Roblox**.

Nutno říci, že existuje spoustu her, které děti velice často hrají, přestože této věkové kategorii nejsou určeny.

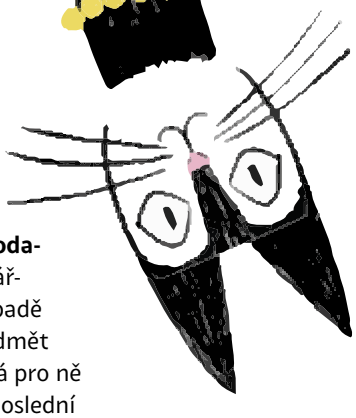
5. Jaké hry jsou naopak pro děti tohoto věku nevhodné?

Existuje velká kategorie her, které jsou dětmi masivně hrané, **ale pro tuto věkovou kategorii nejsou vhodné: online střílečky jako Counter Strike: Global Offensive** nebo **Overwatch**, jakož i několik stříleček ze série **Call of Duty**. V posledních letech nabraly největší popularitu hry z nového žánru zvaného „**battle royale**“, jsou to online hry, které kombinují střílečku a hru na přežití (něco jako Hunger Games). V tomto žánru se těší obrovské popularitě hry **Fortnite** nebo **PlayerUnknown's Battlegrounds (PUBG)**. Je třeba dodat, že jsou úplným mainstreamem mezi dětmi a dospívajícími, přestože této věkové kategorii nejsou určeny a jejich rodiče by měli zvážit, zda nezasáhnout.

Pro první orientaci z hlediska obsahu hry je dobrou pomůckou **PEGI (Pan European Game Information),** systém platný ve 30 evropských zemích, který **informuje uživatele o vhodnosti daného titulu pro různé věkové skupiny** (3, 7, 12, 16, 18). Poskytuje i další informace – zda se ve hře mluví sprostě, zda se tam objevují drogy, sex nebo násilí atd. Je dobré taky **zvážit** časovou náročnost dané hry, protože některé vyžadují pro plný požitek více času než jiné (typicky velmi komplexní hry, např. MMORPG). V případě, že dítě hraje hry, které vyžadují více času, než má k dispozici, mohou se projevit **negativní důsledky, jako je zanedbávání spánku, školních povinností, jiných aktivit** apod.

6. Jaké hry jsou vhodné pro děti ve věku 8–11 let?

To je velmi individuální a liší se to od dítěte k dítěti. Hra by měla být pro dítě **přiměřeně náročná – to znamená ani**



příliš snadná, ani příliš obtížná. V prvním případě by se dítě nemuselo ani snažit a hra by jej nudila, pak by byla jen „ubíjením času“. V druhém případě by dítě zažívalo spíše neúspěch a frustraci, případně stres. **Nejjistější metoda je, aby se rodič se hrou sám seznámil – může přečíst recenze, zhlédnout na YouTube ukázky z průběhu hry, může si hru zkusit sám zahrát.** Taky je vhodné **chvíli sledovat dítě při hře**. Podle toho pak rodič dokáže docela dobře posoudit, zda hra je, či není vhodná pro jeho dítě.

7. Jak se projevuje závislost na hraní her?

Závislost na hraní her je samostatným, jasně definovaným onemocněním teprve krátce. Dříve hráči, kteří kvůli svým problémům s hraním vyhledali odbornou pomoc psychologa, psychiatra či adiktologa, spadali nejčastěji pod škatulku patologického hráčství (gamblingu). Diagnostická kritéria pro poruchu z hraní (online) her – (Internet) Gaming Disorder – byla odvozena od jiných typů závislostí. **V současném diagnostickém a statistickém manuálu duševních poruch (DSM-5) je uvedeno devět příznaků:**

- hra se stává **nejvýznamnější činností**, na kterou hráč nemůže často přestat myslet (preoccupation),
- hráč je často **podrážděný, neklidný nebo smutný**, když nemůže hrát tolik, co obvykle (withdrawal),
- hráč má potřebu **„větších herních dávek“** pro dosažení pocitu, „že si zahrál“ (tolerance),
- hráč **nedokáže redukovat herní čas** (loss of control),
- hráč **omezuje své ostatní aktivity** (giving up other activities),
- hráč hraje i **navzdory negativním dopadům**, například zhoršeným školní výsledkům, konfliktům s blízkými (continuation),
- hráč se často **snaží před blízkými zastírat**, kolik času hraním strávil (deception),
- hráč často používá hraní ke **zbavení negativních pocitů** (escape),
- hráč je ochoten **ohrozit své vztahy nebo školní/pracovní výsledky** kvůli hraní (negative consequences).

Pozitivní diagnóza vyžaduje, aby hráč splňoval alespoň **pět z těchto kritérií.** Zajímavé je, že **vysoký herní čas**, který často znepokojuje rodiče, sám o sobě **příznakem závislosti není**. Čekali bychom, že dítě/dospívající, který tráví hraním třeba víc než 20 hodin týdně, už určitě musí být závislý. Odborníci ale upozorňují, že nadměrné hraní se nerovná problematické hraní (závislost). Záleží vždy na tom, zda vysoké herní časy poškozují jiné aspekty života hráče a zda hráč je či není schopen hraní omezit ve chvíli, kdy se změní jeho životní podmínky (např. začne studovat, pracovat, stane se rodičem apod.).

8. Jak se snaží tvůrci her vydělávat? Jakými způsoby lákají z hráčů peníze?

Tradiční model vydělávání na videohrách byl jednoduchý – výrobce **hru uvedl na trh a nastavil cenu**. Pak se pokusil prodat co největší počet kopií. Toto se ale v posledních 15 letech výrazně změnilo, velmi mnoho her využívá tzv. **freemium model, tj. hra je volně dostupná** (tzv. free to play), **ale uživatel nakupuje dodatečný obsah** přímo v ní. Vývojářská studia musí v takovém případě přesvědčit hráče o tom, že předmět nebo balíček, který si koupí, má pro ně přidanou hodnotu. Bohužel v poslední době se to děje ne zrovna šťastným způsobem, protože mnoho vydavatelů přistoupilo k prodeji tzv. loot boxů – balíčků s různým náhodným obsahem. Tento prvek je převzat z kasin a gamblingu a vrhá špatné světlo na celý videoherní svět (protože u hráčů, kteří mají predispozici k závislostnímu chování, bývá takový obsah často jeho spouštěčem).

Mnozí vývojáři začali tyto **modely kombinovat – hru lze zakoupit, přesto si v ní můžete ještě kupovat obsah**. Podobně jsou na tom i tzv. **DLC – downloadable content – rozšíření,** která častokrát stojí ve finále více než hra samotná. Herní studia se takto snaží co nejvíce vydělat na každém vydaném titulu a obsahu, který do nich přidávají. Proto v dnešní době nemluvíme o hrách jako produktu, ale spíše jako službě, kterou studia poskytují a za kterou uživatelé pravidelně platí. V neposlední řadě stále více vývojářů přidává do her **reklamy**, pomocí kterých se snaží vydělat i na „neplatičích“ (hráči, kteří ve free to play nenakupují dodatečný obsah). Nejnovějším hitem je takzvaný **battle pass / subscription**, kde mají hráči za pravidelný menší (obvykle měsíční) **poplatek nějakou výhodu** ve hře oproti ostatním.

9. Jak přesně loot boxy fungují?

Loot boxy spadají do souhrnného označení mikrotransakcí. **Mikrotransakce** je označení finanční transakce s malými (v současné době již i většími) obnosy v hrách. Termín se používá zejména pro platby na internetu a hranice „menšího obnosu“ je vnímána různě.

Loot boxy obsahují **náhodný digitální obsah**, který **může, ale i nemusí** dodávat herním postavám různé výhody. Tyto balíčky je možné získávat jako odměnu za hraní, ale též je možné si je **koupit za skutečné peníze**. V současné době je známá především druhá varianta, a to zejména s rozmachem tzv. free to play her neboli her zdarma. Získaný digitální obsah umožňuje hráči získat nové vybavení do hry (např. oblečení, výstroj, výzbroj), schopnosti (např. větší síla ve hře), popřípadě umožňuje zjednodušit samotný průchod hrou (pay-to-win).

Loot boxy se velmi často objevují i v mobilních hrách a aplikacích, kde v převážné míře cílí právě na malé děti.

10. V čem spočívají úskalí loot boxů?

Loot boxy skýtají mnohá rizika a nástrahy. Tou nejvíce rizikovou částí je fakt, že **mají velmi blízko ke gamblingu** – kupujeme tzv. „zajíce v pytli“. Loot box je založen na tom, že vidíme opravdu jenom tu pomyslnou krabici, která uvnitř **ukrývá něco, co asi chceme**. Hráč za ní zaplatí, virtuálně otevře a doufá, že uvnitř bude něco, co by chtěl. To se ale velmi často nestane. Následně kupuje další a další, dokud se mu nepodaří získat něco, co chce. Ale to již v té době mohl utratit tisíce.

S loot boxy se také pojí pojem **tzv. kompulzivní smyčka**. Jedná se o **chemickou reakci a situaci, která nastává v mozku každého hráče při produkci dopaminu, který pomáhá regulovat emocionální reakce a navozuje zejména pocit štěstí**. Otevírání loot boxu je často doprovázeno příjemným zvukem, u konzolí vibruje ovladač, na obrazovce ve videohře „vybuchují" a létají konfety a vše okolo hráči připomíná, že se stalo něco pozitivního, něco, v čem by měl dále pokračovat. Ovšem za cenu neustálých dalších plateb a finančních transakcí.

S kompulzivní smyčkou se pojí i případná možnost vzniku závislosti na dané videohře i na otevírání jednotlivých beden – balíčků. Některé hry v dnešní době obsahují mikrotransakce a loot boxy ve formě videoherních automatů, tudíž je riziko vzniku závislosti či gamblingu o to větší. Též lze ve vybraných videohrách i s předměty, které jsme z loot boxu získali, dále obchodovat.

V současné době lze pořídit i tzv. **Paysafecards** („karty k bezpečné platbě"), které jsou určené právě pro online nákupy a do obliby se dostaly i díky zásluze free to play her.

Paysafecard je **druh předplaceného kuponu** s číselným kódem (princip mobilního kreditu). S jeho pomocí lze platit v mobilních aplikacích, hrách či službách kdekoliv na internetu. Výhodu této služby je možné spatřit v anonymizaci jednotlivých údajů, resp. k možnosti nezadávat číslo kreditní karty do videohry, jež je jinak obvykle nutná ke koupi videoherního předmětu (např. již zmiňovaný loot box). Též lze stav svého účtu sledovat ze speciální mobilní aplikace, tudíž mohou mít například rodiče přehled nad nákupy svého dítěte, které Paysafecard k nákupu v aplikacích a hrách používá.

Stává se ale i to, že karta je dítětem zakoupena a používána za zády rodiče, a v tom případě ještě zvyšuje riziko nepřiměřených nákupů.

11. Některé státy loot boxy zakazují. Které a proč?

Loot boxy jsou v posledních pár letech aktuální téma i na politické úrovni. V roce 2019 se Dánsko a Finsko věnovaly průzkumu, zda by se na hraní vybraných videoher neměl vztahovat loterijní zákon. **Belgie dokonce zašla tak daleko, že nechala zcela loot boxy z her, ve kterých se vyskytují, odstranit.** Herní vývojáři tak byli nuceni nejpozději do 30 dnů odstranit veškeré mikrotransakční prvky. V případě nesplnění jim dokonce hrozil trest odnětí svobody až do maximální výše 5 let a v případě ohrožení dítěte, kdy by se prokázalo, že danou věc kupovala osoba pod stanovenou zákonnou hranicí jejího nákupu, se trest mohl zdvojnásobit.

Též Nizozemský úřad pro hry a hazard v roce 2018 rozhodl, že loot boxy v některých hrách vykazují známky hazardu, načež byly zrušeny a zakázány.

V současné době (2020) se problematikou loot boxů zabývá i Francie a Anglie.

12. Jaká je situace v ČR?

V rámci České republiky a jejího postoje k problematice loot boxů v současné době **žádný dokument vypracovaný není**. Je zde snaha, aby se zákaz (alespoň částečný) loot boxů ve videohrách opíral o zákon č. 186/2016 Sb., o hazardních hrách. Jde o to, že v případě, že by loot box spadal pod tento výše uvedený zákon, herní společnosti by musely získat licenci od Ministerstva financí. Umisťování nejen loot boxů, ale všech hazardních prvků do videohry by následně bylo mnohem složitější, ne-li nemožné. Česká republika je v současné době v pracovní skupině Evropského fóra regulátorů hazardních her (zkr. GREF), které se zaměřuje primárně přímo na problematiku hazardních prvků ve videohrách. Mj. se zde řeší i stále větší propojenost a provázanost mezi hazardními a klasickými hrami. Tedy ano, Česká Republika je velmi zainteresovaná v této problematice a do budoucna můžeme očekávat, že se v tomto směru vybrané změny jistě uskuteční.

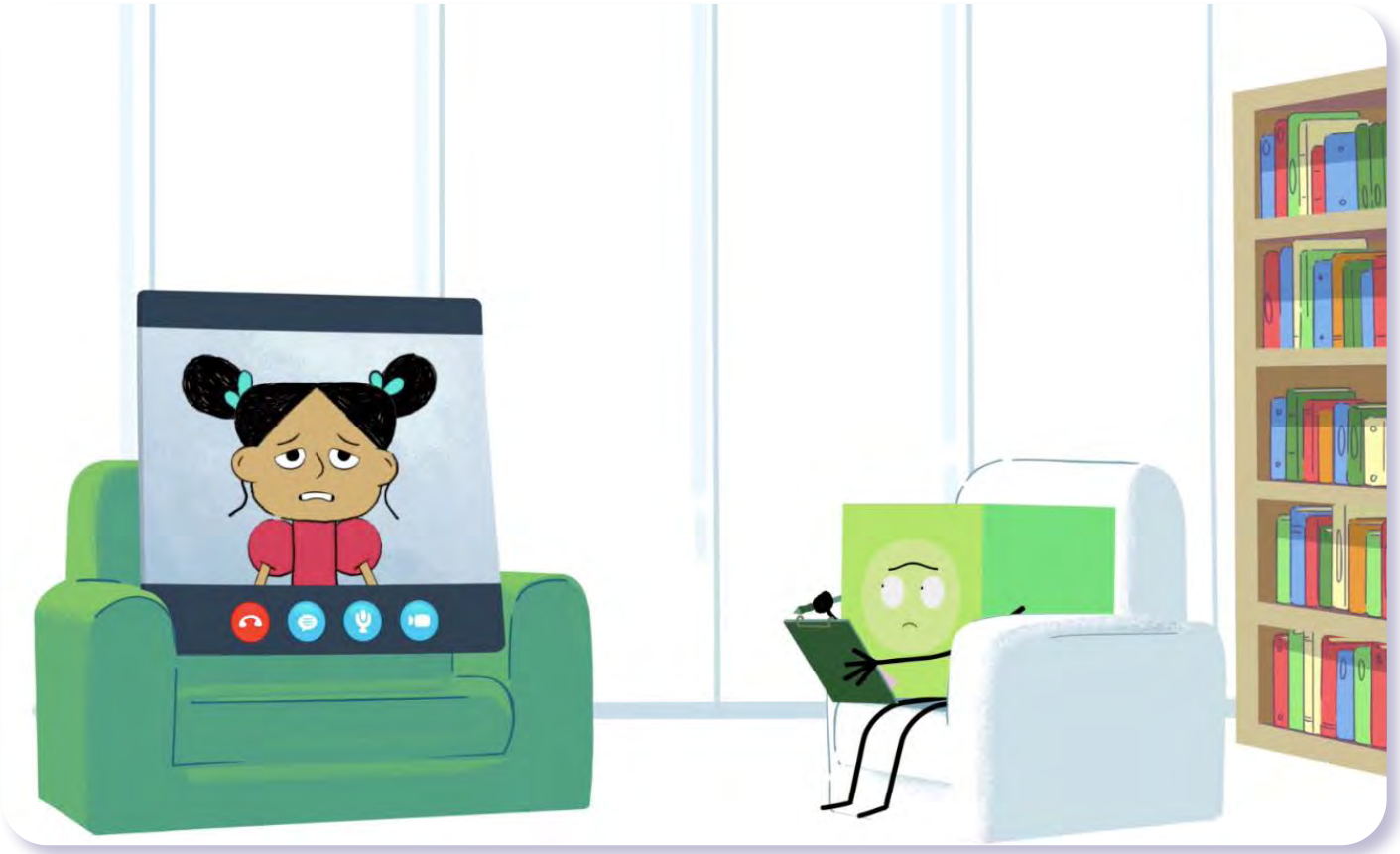
13. Jak mohou děti samy monitorovat svůj pohyb na internetu a kontrolovat, kolik času jsou online?

U uživatelů iOS se stačí obrátit na nativní aplikaci **Screen Time**, která monitoruje čas, jež na jednotlivých aplikacích trávíme, počet odemknutí telefonu za den apod. V novějších verzích lze velice dobře nastavit rodičovská omezení. Pro **Android** existuje velké množství podobných aplikací s takovými funkcemi, například **YourHour** nebo **Moment**. S aplikacemi typu **Freedom** lze pak tvořit offline zóny například na učení tak, že si skrze ně nastaví požadovaný časový limit na soustředěnou práci, během nějž jsou všechna vaše zařízení blokována.

Odpovědi vypracovali:

Kateřina Lukavská, Katedra psychologie PaedF UK, Klinika adiktologie 1. LF UK (otázky 3, 5–7)
Michal Božík, psycholog a výzkumník v oblasti videoher, zakladatel portálu VÍčatá.sk (otázky 1, 2, 4, 8, 13)
Jiří Vimr, krajský protidrogový koordinátor, Krajský úřad Karlovarského kraje, oddělení bezpečnosti a prevence (otázky 9–12)

Podívejte se na lekci V digitálním světě: Online hry na <jsns.cz/mv/online-hry>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.



V digitálním světě

Závislost na internetu

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

„Od chvíle, co jsem s Filipem objevila Mravenčáky, musím pořád hrát," svěřuje se zkroušeně sestřenka Nita terapeutovi na speciální klinice pro léčbu závislostí. Svodům virtuálního světa, který je nám k dispozici 24 hodin denně, je občas těžké odolat. Závislost na online hrách je stejně vážná jako kterákoliv jiná a v momentě, kdy zjistíme, že hraní negativně zasahuje do našeho života, je na čase problém řešit.

CÍLE LEKCE

1. zamyslet se nad vlivem digitálních technologií v našich životech
2. pochopit, co vede k závislosti na internetu
3. uvědomit si důležitost reálných mezilidských vztahů

DOPORUČENÝ VĚK

9+ LET

AKTIVITA: Závislost !!!

ANOTACE

Žáci v průzkumu zjistí množství času, který tráví online zábavou, a porovnávají svoje zvyklosti a nastavení hranic z rodin. Prostřednictvím aktivity a reflexe si uvědomí, že je potřeba hledat rovnováhu mezi realitou a pobytem ve virtuálním světě. Dozví se, že v krajním případě může nadměrné hraní vést až k závislosti.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie, člověk a svět práce

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k učení, k řešení problémů, komunikativní, sociální a personální, pracovní

CÍLE

Žáci:
- se zamyslí nad přítomností digitálních technologií ve svých životech
- pochopí, že každodenní a dlouhodobý pobyt na internetu může vést až k závislosti
- zjistí, že zájem o technologie může být ve třídě různý

DÉLKA

45 min. (včetně projekce)

POMŮCKY

- tabule nebo flipchart
- lepicí papírky
- PRACOVNÍ LIST pro doplňkovou aktivitu

POSTUP

1. Na začátku hodiny se žáků zeptáme: *Napadá vás příklad něčeho, co lidé běžně používají, ale může jim to zároveň i škodit? Co nám život ulehčuje nebo zpříjemňuje, ale může se obrátit i proti nám?* Můžeme zmínit příklady jako třeba oheň, vodu, strach, slunce, klimatizaci…
2. Následuje **projekce epizody seriálu**.
3. Ověříme porozumění obsahu dílu. Můžeme se ptát: *Proč měli Mína a Kocour strach o Filipa? Kde potkaly Nitu? Stalo se jí něco?* **Díl seriálu dle potřeby zhlédneme víckrát.**
   Poznámka: Doporučujeme také využít materiál OTÁZKY A ODPOVĚDI, který obsahuje informace k tématu vypracované odborníky. V dokumentu **najdete i znaky závislosti, jak je definují psychologové**.
4. Ve třídě provedeme **malý průzkum**. Všichni žáci si do ruky **vezmou tužku**.
   Vyzveme je, aby se:
   - k oknu postavili ti, co mobily nebo jiné technologie nepoužívají vůbec
   - doprostřed třídy ti, co si myslí, že je používají málo,
   - na jiné místo ti, co tak akorát
   - a na poslední domluvené místo ti, co si myslí, že hodně

   Žákům stojícím ve skupinkách rozdáme lepicí papírky. Ptáme se: *Kolik minut nebo hodin denně vám rodiče dovolí hrát hry nebo se dívat na videa na telefonu nebo jiném zařízení?* Každý žák na papírek napíše svoji odpověď – časový údaj v minutách nebo hodinách.
   Na tabuli zakreslíme čtyři kruhy s nápisy: VŮBEC, MÁLO, TAK AKORÁT, HODNĚ. Žáci papírky nalepí do příslušného kruhu. Žáky necháme prohlédnout si všechny odpovědi.

REFLEXE AKTIVITY

Společně se zamýšlíme nad tím, co se v odpovědích objevilo – je pravděpodobné, že se stejné časy vyskytnou v různých skupinách a že žáci vnímají časové omezení odlišně. Necháme je uvádět argumenty a dáme prostor i těm, které hraní her a pobyt v online světě nezajímá. Můžeme navázat na evokaci z úvodu hodiny, ptáme se: *Jak rozumíte větě – internet je dobrý sluha, ale špatný pán? Můžou nás technologie o něco připravit, něco nám vzít? Používáte také aplikace nebo hry, které jsou zaměřené na tvořivost nebo něčemu učí?*

V reflexi by mělo zaznít, že technologie mají sloužit nám a ne naopak. Měli bychom upozornit na důležitost skutečných (nikoliv jen virtuálních) mezilidských vztahů v našich životech a na to, že technologiím je důležité věnovat jen přiměřeně času.
Poznámka: Lekce si klade za cíl sebereflexi žáků a zamyšlení se nad rovnováhou reality a virtuality v jejich životech. **Cílem aktivity není obeznamovat žáky se znaky závislosti** na technologiích, které jsou podrobněji popsané v materiálu pro vyučující Otázky a odpovědi. Pokud byste nabyli dojmu, že je u některého z žáků potřeba diagnosticky zasáhnout, obraťte se na školního psychologa nebo metodika prevence.

DOPLŇKOVÁ AKTIVITA

Žáci se rozdělí do dvojic, do každé rozdáme PRACOVNÍ LIST s otázkami. Vzájemně si pokládají otázky z pracovního listu a zjišťují o spolužákovi/spolužačce:

- Co opravdu rád/a děláš?
- Co si myslíš, že ti jde?
- U čeho nebo kdy se cítíš dobře?

Pokud je to vhodné, spolužáci si mohou aktivitu navzájem pantomimicky předvést.

POZNÁMKY

PRACOVNÍ LIST

Zjistěte něco nového o svém spolužákovi a zeptejte se na následující otázky:

Co opravdu rád/a děláš?

(kromě trávení času na telefonu, na internetu nebo hraní her na počítači)

Co si myslíš, že ti jde?

(kromě trávení času na telefonu, na internetu nebo hraní her na počítači)

U čeho nebo kdy se cítíš dobře?

(kromě trávení času na telefonu, na internetu nebo hraní her na počítači)

OTÁZKY A ODPOVĚDI

1. Jaké existují základní druhy počítačových her?

Videohry se dají rozdělit podle různých kritérií – nejčastěji se ale rozdělují podle žánrů. Patří sem kategorie jako **akční hry, logické, strategické, závodní, simulace, adventury, role playing (hry na hrdiny), sportovní hry nebo „střílečky“**. Velkou samostatnou skupinu v rámci jednotlivých žánrů tvoří i **hry pro více hráčů**.

Klasifikovat videohry můžeme ale také dle použití – nejčastěji rozeznáváme hry **komerční, s cílem zabavit**; a **videohry edukační, s cílem něco naučit**.

Třetí je dělení her na hry tzv. **casual**, což jsou hry snadno přístupné pro hráče (jednoduché hry), a tzv. **hardcore** (náročnější hry, které vyžadují předešlé zkušenosti s hraním her). Existují hry prakticky pro každého – od tříletých dětí až po hry pro seniory, pro muže i ženy, pro ty, kteří chtějí u her relaxovat, i pro ty, kteří mají rádi supernáročné simulace.

2. Jaká je historie hraní her? Jak se hraní proměnilo v čase?

Videohry byly na úplném začátku pouze kratochvílí vědců, kteří pracovali s prvními počítači. Do povědomí široké veřejnosti se ale dostaly až v **70. a 80. letech minulého století**, kdy se objevily **první osobní počítače, herní konzole** a tzv. arkádové automaty.

Rozvoj her ovlivnily hlavně technologické novinky – **osobní počítače, konzoly, handheldy** (přenosná herní zařízení)**, 3D zobrazování a 3D hry, internet a online hraní**. Důležitý byl rozmach chytrých telefonů a v poslední době zaznamenává boom virtuální a rozšířená realita.

Hry se postupně vyvíjely a zvyšovaly svou komplexnost. Dnes se jejich vývojem zabývají profesionální týmy. S rozvojem komplexity vznikaly i nové žánry, výrazně se rozšířilo i publikum, na které se jejich tvůrci zaměřovali.

Postupně se **měnily i modely prodeje** – z **fyzických nosičů** se přesunuly k **digitální distribuci**, přímý prodej her nahradily **„free to play“** hry, které se snaží vydělat na dokupování dodatečného obsahu, reklamě a předplatném. V neposlední řadě je třeba zmínit **e-sporty** (soutěžní hraní počítačových her), které v dnešní době vyprodávají virtuální haly. V tomto byznysu se tak v současnosti točí i velké peníze.

3. Proč je gaming pro děti (ale i dospělé) atraktivní?

Gaming je pro děti relativně dostupný, a tím i atraktivní. Postačí k němu vstupní investice do vybavení (počítač či herní konzole, hry) a poté už se může uživatel věnovat hraní z pohodlí domova. Nemusí nikam chodit nebo být závislý na počasí jako v případě některých jiných koníčků. Gaming nabízí **interaktivitu a imerzivitu** (míru ponoření hráče do virtuálního světa hry). Navíc s rychlým rozvojem e-sportů (progamingu) nabízí hraní her i **soutěžní** (profesionální) **kariéru s možností vysokého výdělku**, čímž se přibližuje sportům typu hokej, fotbal nebo tenis, ale s nižším vstupním prahem (je snazší začít trénovat hru League of Legends než hokej).

4. Jaké hry jsou nejvíc oblíbené mezi dětmi ve věku 8–11 let?

Jedná se o období, kdy děti přestávají bavit „dětské“ hry a stále více se dožadují titulů určených pro starší cílové skupiny. Jejich paleta je velmi pestrá a zahrnuje i příklady, které pro tuto věkovou kategorii nejsou vhodné.

Mezi nejpopulárnější se již léta stabilně řadí **Minecraft,** ale také „automobilový fotbal“ **Rocket League**. Z novějších jsou to hry, jako je adventura **The Legend of Zelda: Breath of the Wild** nebo „skákačka“ **Super Mario Odyssey**. Kromě toho se velké popularitě těší i Minecraftem silně inspirovaný **Roblox**.

Nutno říci, že existuje spoustu her, které děti velice často hrají, přestože této věkové kategorii nejsou určeny.

5. Jaké hry jsou naopak pro děti tohoto věku nevhodné?

Existuje velká kategorie her, které jsou dětmi masivně hrané, **ale pro tuto věkovou kategorii nejsou vhodné: online střílečky** jako **Counter Strike: Global Offensive** nebo **Overwatch**, jakož i několik střílečeк ze série **Call of Duty**.
V posledních letech nabraly největší popularitu hry z nového žánru zvaného „**battle royale**“, což jsou online hry, které kombinují střílečku a hru na přežití. V tomto žánru se těší obrovské popularitě hry **Fortnite** nebo **PlayerUnknown's Battlegrounds (PUBG)**. Je třeba dodat, že jsou úplným mainstreamem mezi dětmi a mladými, přestože této věkové kategorii nejsou určeny a jejich rodiče by měli zvážit, zda nezasáhnout.

Pro první orientaci z hlediska obsahu hry je dobrou pomůckou **PEGI (Pan European Game Information)**, systém platný ve 30 evropských zemích, který **informuje uživatele o vhodnosti daného titulu pro různé věkové skupiny** (3, 7, 12, 16, 18 let). Poskytuje i další informace – zda se ve hře mluví sprostě, zda se tam objevují drogy, sex nebo násilí atd. Je dobré taky **zvážit časovou náročnost** dané hry, protože některé vyžadují více času než jiné (typicky velmi komplexní hry, např. MMORPG). V případě, že dítě hraje hry, které vyžadují více času, než má k dispozici, mohou se projevit **negativní důsledky, jako je zanedbávání spánku, školních povinností, jiných aktivit** apod.

6. Jaké hry jsou vhodné pro děti ve věku 8–11 let?

Hra by měla být pro dítě **přiměřeně náročná** – to znamená ani příliš snadná, ani příliš obtížná. V prvním případě by se dítě nemuselo ani snažit a hra by jej nudila, ve druhém případě by dítě zažívalo spíše neúspěch a frustraci, případně stres.

Nejjistější metoda je, aby se rodič se hrou sám seznámil – může si přečíst recenze, zhlédnout na YouTube ukázky z průběhu hry, může si hru zkusit sám zahrát. Ideální je také **chvíli sledovat dítě při hře**. Podle toho pak rodič do-

káže docela dobře posoudit, zda hra je, či není vhodná pro jeho dítě. Konkrétní tipy na vhodné hry (i když pro mladší děti, 2–8 let) najdete na stránce http://hrajemesichytre.cz.

7. Jaký dopad mají na děti násilné/agresivní hry?

V současné době v odborné komunitě **neexistuje konsenzus ohledně vlivu agresivních her**. Některé výzkumy ukazují, že (experimentálně navozené) hraní agresivní hry může přinejmenším krátkodobě zvýšit agresivní projevy jedince. Jiní výzkumníci však upozorňují, **že výsledky takových experimentů je třeba brát s rezervou**, protože **nedokážou** plně **rozlišovat mezi agresivními a kompetitivními aspekty her** (a jejich vlivem na celkovou úroveň bdělosti – nabuzení organismu) a zároveň se takové experimenty odehrávají v nepřirozených laboratorních podmínkách. Výzkumy v přirozených podmínkách ale zase **nedokážou odlišit samotný efekt agresivních her od osobnostních rysů jedince** (např. snížená empatie, nižší citlivost vůči násilí, agresivita), které mohly být přítomny bez ohledu na hraní a mohou se projevit třeba právě zvýšeným zájmem o agresivní hry.

8. Jaké může mít obecně hraní her přínosy a jaká úskalí?

Některé hry rozvíjejí myšlení a postřeh hráčů, mnohé jsou zaměřené i na logické a strategické uvažování. Hra je pro uživatele často zdrojem pozitivních prožitků, jako je pocit úspěchu, radosti, odpočinku, uklidnění.

Moderní digitální hry jsou chytře navržené, aby vycházely vstříc psychickým potřebám uživatelů (dosažení úspěchu, proměnlivost podnětů apod.), což je spojené s rizikem, že hráč bude k uspokojení svých potřeb používat výhradně hru a bude jejím prostřednictvím **unikat z reality**. To může vést až k rozvoji závislosti na hraní, což je stav spojený s řadou negativních dopadů (např. zhoršený spánek a další fyzické potíže, úzkost, deprese, špatná paměť, sebevražedné tendence, narušené vztahy s blízkými, snížená výkonnost ve škole/v práci).

9. Jak se projevuje závislost na hraní her?

Závislost na hraní her je klasifikovaná jako samostatné onemocnění teprve krátce. Dříve bývali hráči počítačových her, kteří kvůli svým problémům s hraním vyhledali odbornou pomoc psychologa, psychiatra či adiktologa, zařazováni do kategorie patologického hráčství (gamblingu). Diagnostická kritéria pro poruchu z hraní (online) her – (Internet) Gaming Disorder – byla odvozena od jiných typů závislostí. V současném diagnostickém a statistickém manuálu duševních poruch (DSM-5) je uvedeno **devět příznaků**:

1. hra se stává **nejvýznamnější činností**, na kterou hráč nemůže často přestat myslet
2. hráč je často **podrážděný, neklidný nebo smutný**, když nemůže hrát tolik, co obvykle
3. hráč má potřebu **„větších herních dávek“** pro dosažení pocitu, „že si zahrál“
4. hráč **nedokáže redukovat herní čas**
5. hráč **omezuje své ostatní aktivity**
6. hráč hraje i **navzdory negativním dopadům**, například zhoršeným školním výsledkům, konfliktům s blízkými
7. hráč se často **snaží před blízkými zastírat**, kolik času hraním strávil
8. hráč často používá hraní ke **zbavení negativních pocitů**
9. hráč je ochoten **ohrozit své vztahy nebo školní/pracovní výsledky** kvůli hraní

Pozitivní diagnóza vyžaduje, aby hráč splňoval alespoň **pět z těchto kritérií**. Zajímavé je, že **dlouhá doba samotného hraní**, která často znepokojuje rodiče, sama o sobě **příznakem závislosti není**, ač bychom čekali, že dítě/dospívající, který tráví hraním třeba víc než 20 hodin týdně, určitě musí být závislý. Odborníci ale upozorňují, že nadměrné hraní se nerovná problematické hraní (závislost). Záleží vždy na tom, zda vysoké herní časy poškozují jiné aspekty života hráče a zda hráč je či není schopen hraní omezit ve chvíli, kdy se změní jeho životní podmínky (např. začne studovat, pracovat, stane se rodičem apod.).

10. Do jaké míry je vhodné limitovat dětem čas, který mohou trávit hraním?

Záleží na věku dítěte a na jeho vlastních schopnostech regulace. **Je dobré nastavit jasná pravidla,** kdy a jak (moc) může dítě/dospívající hrát, a dohlížet na jejich dodržování. Na druhou stranu je nutné u dospívajících **posilovat jejich vlastní schopnost seberegulace** a je otázka, zda rodičovská kontrola v tomto více pomáhá, či škodí. V každém případě je při nastavování pravidel dobré zohlednit typ hry a kolik času (a jak rozložený) konkrétní hra vyžaduje. Některé velmi komplexní hry (typicky MMORPG) mohou vyžadovat i značně vysoké herní časy (až 40 hodin týdně).

11. Jak se snaží tvůrci her vydělávat? Jakými způsoby lákají z hráčů peníze?

Tradiční model vydělávání na videohrách byl jednoduchý – výrobce **hru uvedl na trh a nastavil cenu**. Pak se pokusil prodat co největší počet kopií. Toto se ale v posledních 15 letech výrazně změnilo, velmi mnoho her využívá tzv. **freemium model, tj. hra je volně dostupná** (tzv. free to play), **ale uživatel nakupuje dodatečný obsah** přímo v ní. Vývojářská studia musí v takovém případě přesvědčit hráče o tom, že předmět nebo balíček, který si koupí, má pro ně přidanou hodnotu. Bohužel v poslední době se to děje ne zrovna šťastným způsobem, protože mnoho vydavatelů přistoupilo k prodeji tzv. loot boxů – balíčků s různým náhodným obsahem. Tento prvek je převzat z kasin a gamb-

lingu a u hráčů, kteří mají predispozici k závislostnímu chování, bývá takový obsah často jeho spouštěčem.

Mnozí vývojáři začali tyto **modely kombinovat – hru lze zakoupit, přesto si v ní můžete ještě kupovat obsah**. Podobně jsou na tom i tzv. **DLC – downloadable content – rozšíření**, která častokrát stojí více než hra samotná. Herní studia se takto snaží co nejvíce vydělat na každém vydaném titulu a obsahu, který do nich přidávají. Proto v dnešní době nemluvíme o hrách jako produktu, ale spíše jako službě, kterou studia poskytují a za kterou uživatelé pravidelně platí. V neposlední řadě stále více vývojářů přidává do her **reklamy**, pomocí kterých se snaží vydělat i na „neplatičích" (hráči, kteří ve free to play nenakupují dodatečný obsah). Nejnovějším trendem je takzvaný **battle pass / subscription**, kde mají hráči za pravidelný menší (obvykle měsíční) **poplatek nějakou výhodu** ve hře oproti ostatním.

12. Jak předejít jako rodič tomu, aby mé dítě utrácelo skutečné peníze?

Herní svět současnosti není jen hrou samotnou, ale i sociálním prostorem dítěte. Mnoho her, zejména těch, které jsou free to play, nabízí zkratky, jak si sociální potřeby naplnit. Rodič by se měl řídit několika základními pravidly. To první je absolutně nejdůležitější – **nedávejte dětem přístup k vaší kreditní kartě**. Nastavte si rodinný účet v Apple Store, Google Play, na Steamu nebo ve vaší herní konzoli. S rodinným účtem budou moci děti požadovat nákupy, ale vy je budete muset vždy nejprve potvrdit. Druhé dobré pravidlo je **oddálit nákup** – mnoho her využívá toho, že vývojáři přesně vědí, kdy je hráč nejzranitelnější a nejnáchylnější realizovat nákup. Pokud pomocí rodinného účtu a autorizace oddálíme nákup, často se nerealizuje vůbec. Dítě ztratí zájem nebo mu rodič vysvětlí, že danou věc nepotřebuje.

V neposlední řadě je velmi důležité **nastavit si pravidla, jak přistupovat k tzv. loot boxům**. Je třeba vysvětlit dětem, že hazardem se hry nevyhrávají, že si mohou koupit 1 loot box, ale koupit jich 100 najednou je hazard. Stejně ve většině her mohou hráči získat loot boxy i postupným hraním, jen to trvá déle.

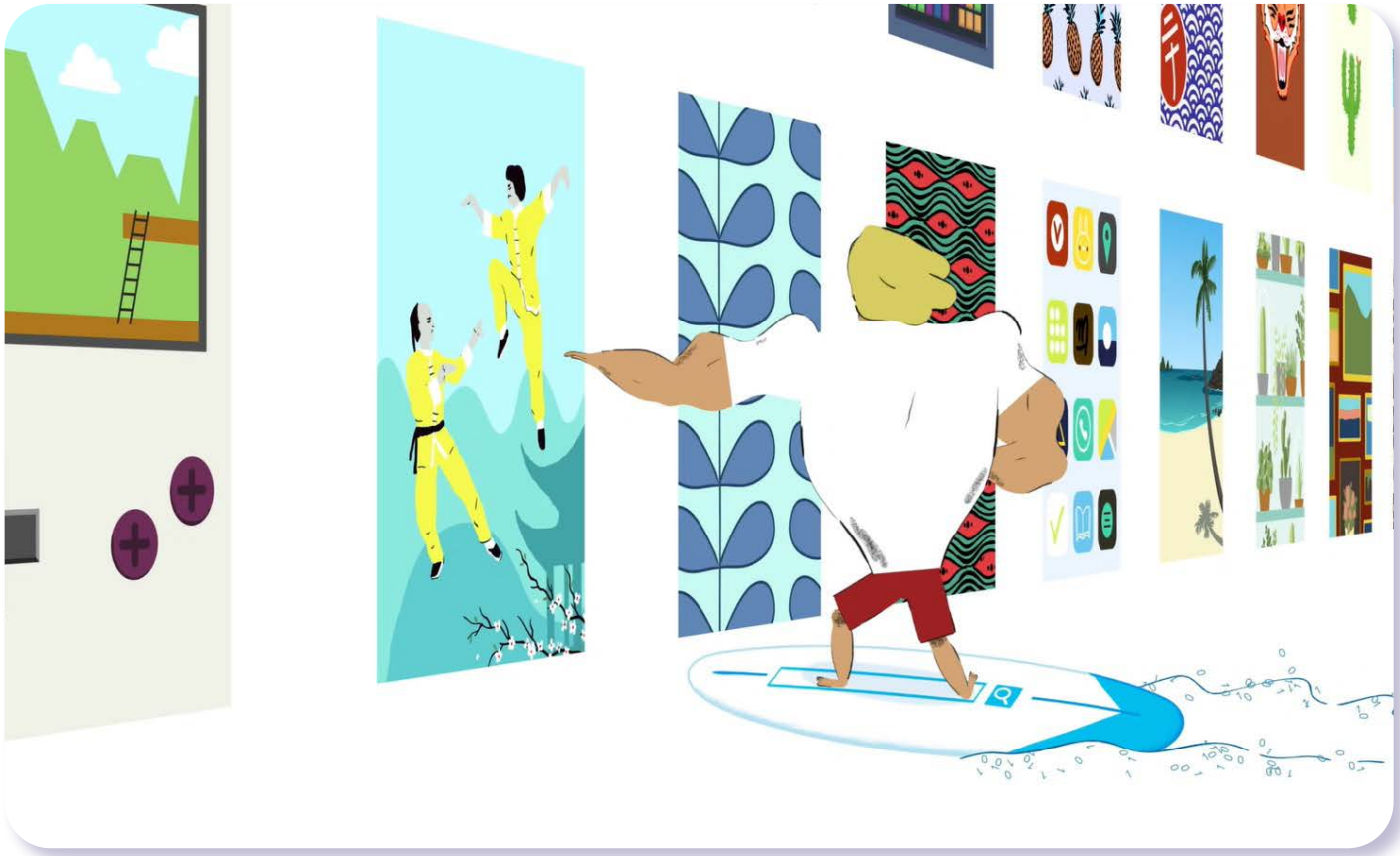
Pokud máte prostor, **posaďte se k dítěti a alespoň chvíli pozorujte, jak hraje**, můžete s dítětem při hře komunikovat a pochopit, co se mu „odehrává v hlavě". Lépe ho takto pochopíte a je velká šance, že zájem o to, co dítě hraje, zlepší i váš vzájemný vztah.

Odpovědi vypracovali:

Kateřina Lukavská, Katedra psychologie Pedagogické fakulty UK, Klinika adiktologie 1. LF UK (otázky 3, 5–11)
Michal Božík, psycholog a výzkumník v oblasti videoher, zakladatel portálu Vĺčatá.sk (otázky 1, 2, 4, 12, 13)

Podívejte se na lekci V digitálním světě: Závislost na internetu na <jsns.cz/mv/zavislost-na-internetu>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.

POZNÁMKY



V digitálním světě

Rodičovská kontrola

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Filip s Mínou a Kocourem brouzdají internetem, až narazí na stopku. Prohlížeč zakázal Filipovi vstoupit na lákavě vypadající web. Při surfování na internetu je snadné nechat se unést a vlákat na nejrůznější stránky, které se nám samy nabízejí. Zdaleka ne všechno na webu je ale vhodné pro dětské oči. Programům, které hlídají, aby se děti nedostaly na místa, jež by je mohla vyděsit nebo šokovat, se říká rodičovská kontrola. Rodiče díky nim mohou filtrovat, co děti smějí navštěvovat, nebo omezovat dobu, po kterou mohou být online.

CÍLE LEKCE

1. uvědomit si rizika používání internetu dětmi a dospívajícími
2. určit si pravidla používání internetu
3. informovat se, v jakých případech by měli nejen rodiče děti na internetu chránit

DOPORUČENÝ VĚK
7+ LET

AKTIVITA: Rodičovská kontrola !!!

ANOTACE

Na základě aktivity si žáci uvědomí, že ne všechno na internetu je vhodné pro děti a že dospělí je mohou před nevhodným obsahem chránit. Žáci se zaměří na svoje emocionální prožívání a určují, na které emoce by „dali zámek“ oni sami nebo jejich rodiče.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k řešení problémů, komunikativní, sociální a personální, občanské

CÍLE

Žáci:
- si uvědomí, že ne všechno na internetu je vhodné pro děti
- se zamyslí nad tím, v jakých případech chtějí rodiče děti na internetu chránit
- si uvědomí své prožívání emocí

DÉLKA

45 min. (včetně projekce)

POMŮCKY

- PRACOVNÍ LIST pro každého žáka
- LIST PRO VYUČUJÍCÍ

POSTUP

1. Postavíme se s žáky do kruhu. **Čteme příklady emocí** z tabulky v PRACOVNÍM LISTĚ. Krok směrem do středu udělá ten, komu je uvedený prožitek příjemný. Krok vzad, pokud je prožitek nepříjemný.
2. Následuje **projekce epizody seriálu**.
   Poznámka: Snímek doporučujeme zhlédnout nejméně dvakrát.
3. Ověříme, zda žáci epizodě porozuměli. Ptáme se: *Proč se Mína a Filip na nějakou stránku na internetu nedostali? Jaká to mohla být stránka?*
4. Po projekci rozdáme každému žákovi PRACOVNÍ LIST. Žáci plní úkoly z pracovního listu. V tabulce **označí, které emoce by je podle nich jejich rodiče nechtěli nechat prožít v online světě**. Tyto emoce označí zámkem. Poté mají napsat, při jaké činnosti je můžou zažít. (Např. videohra se zbraněmi a střílením, film pro dospělé, hraní her v pozdních hodinách…)
   Poznámka: Může nastat situace, že žáci zmíní i pornografický obsah. Předem zvažte, jak na situaci zareagujete. Téma pornografie doporučujeme se žáky citlivě otevřít. Doporučení, jak je k tématu možné přistoupit, je podrobněji zpracované v materiálu LIST PRO VYUČUJÍCÍ.

REFLEXE AKTIVITY

V reflexi se zaměříme na **diskusi o nevhodném obsahu**. Navážeme na příklady, které žáci uvedli v pracovním listu. Ptáme se, kam nakreslili zámek a proč. Diskusi můžeme rozvést otázkami: *Viděli jste něco, co vám nahnalo strach? Měli jste někdy děsivé sny po zhlédnutí filmu? Na co se nechcete dívat bez ohledu na zákazy?*
Společně formulujeme, jaký obsah není vhodný pro děti: násilí, krev, agresivita (a také pornografie).
Na závěr doporučujeme reflexi ukončit pozitivně: Na tabuli/flipchart nakreslíme smajlíka. Formou brainstormingu zapisujeme, kdy při sledování televize nebo aktivitách na internetu prožíváme pozitivní emoce (humorné video, hezká pohádka, úspěch ve hře apod.).

ZKUŠENOSTI Z PRAXE

Bylo by přínosné, kdyby této aktivitě předcházela třídní schůzka s rodiči, kde bychom jim plánovanou lekci a její smysl vysvětlili. Rodičům můžeme také předat informace o rodičovském zámku.
Andrea Tláskalová, *ZŠ Zbiroh*

PRACOVNÍ LIST

**Představte si, že vám rodiče dovolí být online.
Jaké prožitky/emoce z tabulky by podle vás nechtěli, abyste zažili?**

Označte tyto emoce zámkem. Dopište, při jaké činnosti je můžete zažít. (Např. hra se zbraněmi a střílením, film pro dospělé apod.)

„CÍTÍM SE…"

ŠŤASTNĚ	ROZZLOBENĚ
SMUTNĚ	PŘEKVAPENĚ
HRDĚ	NADŠENĚ
KLIDNĚ	USTARANĚ
VYDĚŠENĚ	ZNECHUCENĚ
POBAVENĚ	ZMATENĚ
UNAVENĚ	OSAMĚLE
VYSTRAŠENĚ	NERVÓZNĚ
ZNUDĚNĚ	VESELE
ZKLAMANĚ	NEJISTĚ

LIST PRO VYUČUJÍCÍ: JAK MLUVIT S DĚTMI O PORNOGRAFII

Kromě násilí a agresivity je pornografie dalším obsahem, ke kterému se na internetu snadno dostane kdokoliv. Učitelé spolu s rodiči mají možnost působit v tomto směru preventivně nebo uvést náhodnou zkušenost dětí s tímto obsahem do vhodného kontextu.

Pro rodiče

Rodiče najdou metodickou podporu k tématu, jak mluvit s dětmi o pornografii, na webu hrajemesichytre.cz.

„Dnešní děti jsou vystaveny pornografickému obsahu již ve velice útlém věku, světová i česká čísla mluví o 8. až 11. roce života. Podle naší zkušenosti k tomu může dojít ještě mnohem dříve. Stále častěji se setkáváme s příběhy velice malých dětí, které na pornografický obsah narazily, sdílely ho s vrstevníky a případně s nimi zkoušely, co na obrazovce viděly. Poslední příběh se týkal dětí ve věku čtyři a půl a pět let. To nás definitivně přimělo k tomu, abychom připravili nástroje pro rodiče, jak mluvit o pornografii s těmi úplně nejmenšími.

Že se vám to stále zdá brzy? Bohužel není. Nevhodný obsah se ukrývá ve vyskakovacích oknech křížem krážem internetem, ale i pod linky v komentářích u dětských a pohádkových YouTube videí.

Mnoho rodičů se v první řadě pídí po možnostech blokování přístupu k takovému obsahu. Otázkou však není, jak před ním děti uchránit, ale spíše kde, kdy a jak moc (ne)připraveny na něj narazí. Ať bude váš software rodičovské kontroly sebevíc dokonalý, nemáte vyhráno. Děti se k pornu dostanou skrze telefony kamarádů nebo na počítačích, které nejsou tak dobře chráněné. Překvapivým, ale častým místem jsou telefony, počítače a tablety u prarodičů…

Podle zahraničních, ale i českých statistik v deseti letech již celá čtvrtina dětí pornografii viděla. V tomto věku je málokteré dítě na takové obrázky připraveno, některé si mohou dále nést traumatizující pocity. Stejně tak si budují pokřivený obrázek toho, jak sexuální život vypadá. Buďte tedy připraveni a začněte o pornografii mluvit co nejdříve.“

Michaela Slussareff, Studia nových médií, Filozofická fakulta Univerzity Karlovy; zakladatelka Slow Tech Institute

TIP: Ze stránek hrajemesichytre.cz je možné použít scénáře rozhovorů o pornografii dle věku a upravit je podle individuálních potřeb rodiny a dítěte.

Scénáře naleznete v následujícím článku na odkaze „Porno-konverzace. Aneb kdy a jak mluvit o pornografii s dětmi různého věku“ https://hrajemesichytre.cz/2019/06/15/porno-konverzace-scenare-jak-mluvit-o-pornografii-s-detmi-ruzneho-veku/.

Pro školy

Slow Tech Institute nabízí semináře pro základní školy o virtuálním světě a jeho rizicích, včetně tématu pornografie: http://slowtechinstitute.org/practice/pro-skoly/.

OTÁZKY A ODPOVĚDI

1. Jaká jsou rizika spojená s aktivitami dětí a dospívajících na internetu?

Odborníci upozorňují na několik typů rizik spojených s aktivitami dětí či dospívajících. Děti se mohou dostat **k nevhodnému obsahu** (např. sexuálnímu nebo násilnému), **setkat se s kyberšikanou, zažít reklamní či dezinformační manipulaci** anebo z nich někdo může **vylákat citlivý obsah** (fotografie apod.).

V některých závažných případech může i kvůli internetu dojít u dětí k těžkému traumatu s vlivem na jejich další život.

Významným zdrojem těchto hrozeb jsou tzv. **predátoři**, kteří cíleně vyhledávají a zneužívají nezkušené uživatele, zejména děti a dospívající. V poslední době se problematice začíná věnovat více pozornosti díky některým projektům, třeba dokumentu Víta Klusáka a Barbory Chalupové *V síti*.

Jiným druhem rizika je **nadměrné užívání internetu**, nebo dokonce **závislost na internetu**. Do seznamu duševních poruch byla sice zatím zařazena pouze závislost na hraní online her, ale i jiné formy užívání internetu (např. používání sociálních sítí, youtubing) jsou intenzivně zkoumané a zdá se, že mohou významně zhoršovat kvalitu života a způsobovat různé fyzické i psychické problémy.

2. Co znamenají pojmy kybergrooming a sexting?

Kybergrooming je chování uživatelů internetu, jehož cílem je pomocí internetových komunikačních prostředků a jiných technologií **vyvolat v dospělém/dítěti pocit důvěry a prostřednictvím falešné identity ho zneužít nebo vylákat na schůzku**. Za kybergrooming může být také považováno zneužití dětí a mladistvých k **jinému účelu – například k terorismu** (dítě je zmanipulováno a stává se ve jménu víry teroristou).

Sexting je zasílání textových zpráv, fotografií nebo videí se sexuálním obsahem.

3. V čem spočívá riziko sdílení intimních fotek?

Sdílení intimních fotografií nebo videí je vždy rizikové. Po odeslání zpráv s citlivým materiálem (zejména pak obrazovým) uživatel **ztrácí nad jeho šířením kontrolu**. Neplatí přitom, že stačí později materiál smazat – cokoliv, co umístíme na internet, tam je svým způsobem „navždy“. Druhá strana si může udělat například fotografii obrazovky počítače či mobilu, a tím nevhodný materiál zachovat. Materiál může být **kdykoliv zneužit, využit k vydírání, kyberšikaně** apod.

Provozování sextingu s nezletilými je považováno za obzvlášť závažné a je mnohdy posuzováno jako **šíření dětské pornografie, ohrožování mravní výchovy** apod. O tento typ obsahu s intimní tematikou je na internetu obrovský zájem a je velice často vyhledáván. Tyto materiály se mnohdy **šíří virálně** a během několika málo hodin mohou být na desítkách stránek po celém světě.

Jde téměř vždy o materiály, o jejichž pořízení oběti věděly nebo se přímo na jejich pořízení podílely. Před pořízením „pikantních“ fotografií nebo videí je proto třeba si položit tři otázky: *Máte opravdu naprostou důvěru v toho, kdo fotku pořídí nebo k ní má přístup, že podobné snímky nikdy nezneužije? Budete mít stejný pocit důvěry i za několik let? Nejde o fotografie, které by vám mohly někdy v budoucnu ublížit?*

4. Když chci jako rodič své dítě před riziky internetu chránit, jaké mám možnosti?

Relativně nejjednodušší je situace v případě nevhodného a nepřiměřeného obsahu, kdy lze využít různá technická řešení „**rodičovské kontroly**“ (např. zapnete v prohlížeči filtr, který by měl zabránit zobrazení sexuálního nebo násilného obsahu). Na technická řešení však nelze zcela spoléhat, protože nefungují vždy stoprocentně. Navíc dokážou „vyřešit“ jen jeden typ rizik (náhodné vystavení nepřiměřenému obsahu).

Lepší variantou je **učit děti už ve chvíli, kdy začínají samy internet používat, jak internet funguje, vysvětlit zásady jeho bezpečného používání, mluvit s nimi o hlavních rizicích**. Odborně se toto rodičovské vzdělávání vlastních dětí v užívání internetu nazývá „**internet parenting**“ nebo obecněji „**media parenting**“. Rodiče, kteří sami vyrůstali bez internetu, ale na tento úkol často nejsou připraveni.

5. Ke kterým tématům je možné a vhodné dětem zcela omezit na internetu přístup? A jak?

Obecně by dítě nemělo vidět **obsah, na který není připraveno, nerozumí mu, nedokáže jej kriticky zhodnotit a který by jej mohl traumatizovat nebo nějak negativně ovlivnit jeho vývoj** (sex, násilí, ale taky „návody“ na různé více či méně rizikové formy chování – např. experimentování s návykovými látkami, s vlastním tělem apod.).

Je velmi těžké posoudit, který obsah je pro dítě rizikový, protože to závisí nejen na věku, ale na řadě dalších faktorů, jako je kognitivní zralost, emoční stabilita apod. Opět platí, že ideálním řešením je **prevence ze strany rodiče**, který dítě nejlépe zná a který s ním může dohodnout určitá pravidla, jaké stránky navštěvovat a jaké ne. Taky při uplatnění technické „rodičovské kontroly“ (filtrace obsahu) je vhodné **spolupracovat s dítětem, aby rozumělo tomu, že nastavená omezení mají sloužit v jeho prospěch**.

Jednoduché blokování vybraných stránek na počítači lze nastavit ve Windows skrze Start – Ovládací panely – Rodičovská kontrola. Vyberte účet, pro který chcete nastavit

rodičovskou kontrolu – nastavení systému Windows – Webový filtr – a vložte link stránky, kterou chcete blokovat, například Youtube.com. Pak klikněte na „blokovat“.

Podobně lze omezovat obsah skrze službu **Google Family Link**. Jde o službu, ve které si můžete nastavit všechna vaše rodinná zařízení, nejrůznější omezení (od blokování obsahu až k časovým zámkům) a můžete sledovat na těchto zařízeních aktivitu.

Na iPadu nebo iPhonu pak podobný princip najdete v Nastavení – Obecné – Omezení. Příkladem komplexnějšího řešení je také třeba **Family Media Plan** navržený Americkou pediatrickou asociací.

6. Mohu jako rodič sledovat, co mé dítě na internetu dělá? Jak?

I když patříte mezi poučené rodiče, co se svými dětmi mluvili o časových limitech u obrazovek a zodpovědném chování online, je stále těžké zajistit bezpečí, když s nimi nejste online. Rodičovská kontrola vás může podpořit v úsilí udržet internet vašich dětí v bezpečných hranicích. Nejefektivnější je **rodičovská kontrola, když je používána v otevřené komunikaci s vašimi dětmi, ne jako metoda tajné špionáže**.

Některé rodiny potřebují jednoduché a bezplatné nastavení prohlížeče k filtrování nevhodného obsahu, jiné potřebují pomoc s omezením času na obrazovce. Někteří rodiče chtějí kompletně kontrolovat všechna zařízení svých dětí.

Pro správu všech zařízení v rodinné síti, omezení času u obrazovek, filtrování obsahu či automatické vypínání wifi jsou dispozici hardwarová i softwarová řešení, například OpenDNS, Circle Home Plus, Norton Family Premier, Kaspersky Safe Kids. Pro blokování obsahu a kontrolu využijete in ESET Parental Control, McAfee LiveSafe, pro mobilní zařízení aplikaci Kidslox.

7. Nakolik bych měl jako rodič omezovat čas, který dítě tráví na internetu? Jak nastavit pravidla?

To záleží na několika faktorech, jedním z nich je samozřejmě **věk** – ty nejmenší děti a předškoláci si těžko budou sami hlídat čas, který na internetu stráví. Zde je vhodné **nastavit pevné hranice**, vyžadovat jejich plnění, kontrolovat, ale zároveň i aktivně vybírat vhodný a vzdělávací obsah v médiích, který bude děti zajímat a rozvíjet.

Přísné kontrolování se však příliš nevyplatí u starších dětí, tam může spíše narušovat vzájemnou důvěru. **Se staršími dětmi nastavujte hranice společně, diskutujte o nich a zajímejte se o to, co sledují. Tak se velice nenásilně dozvíte, zda jim něco nehrozí, zda se v online světě nepouštějí do nebezpečných zákoutí.**

Další důležitou proměnnou jsou **seberegulační schopnosti dítěte**. Některé děti dobře zvládají po časovém limitu od hry v klidu odejít, pro jiné je zase ono přepnutí do reality spouštěčem silných emocí a stresu. Děti se musí seberegulaci učit a jejich mozek je stále ve vývoji, přičemž právě centra kontroly a seberegulace dozrávají až v pozdějším školním věku. Zde je vhodné **nastavit pravidla a styl komunikace optimálně tak, aby nedocházelo k vyhroceným situacím**.

V každém případě je velice vhodné používat software rodičovské kontroly.

8. Kde by měla být hranice mezi důvěrou a kontrolou? Do jakého věku děti na internetu kontrolovat?

To je opět dost individuální. Představme si to jako **cestu k řidičskému průkazu**. Asi svému dospívajícímu dítěti hned nesvěříte klíčky a nenecháte ho bez přípravy řídit vaše auto. Nejdříve se toho bude muset v autoškole spoustu naučit o značkách, pravidlech a možných nebezpečích. Teprve pak může začít řídit, ale se zkušeným lektorem, který má připravenou nohu na druhé brzdě. Až po dlouhé době dostane řidičský průkaz a po ještě delší době ho budete s klidem na silnici pouštět i vy sami. Stejným způsobem přistupujte i k online světu. **Cíleně s dětmi mluvte o nebezpečích, ale i o možnostech využít internet k učení či ke kvalitní zájmové činnosti. Používejte rodičovský software a kontrolujte online život dítěte do doby, než bude opravdu schopné pohybovat se na internetu bezpečně.**

9. Jak s dětmi mluvit o nevhodném obsahu na internetu?

Pokud jde o užívání návykových látek, agresivní chování a reklamní obsah v médiích, je vhodné tato témata otevírat přiměřeně věku a diskutovat o nich hned od začátku. **Obzvlášť naléhavý je tento požadavek u pornografického obsahu. Dnešní děti jsou mu vystaveny již ve velice útlém věku,** světová i česká čísla mluví o věku 8 až 11 let. Nezáleží na tom, jak dobře máte zabezpečena všechna mobilní a nemobilní zařízení připojená k domácímu internetu, většina dětí se s tímto obsahem setká na mobilech spolužáků a kromě toho, že takový obsah není pro ně vhodný sám o sobě, si některé děti z tohoto prvního setkání mohou dále nést traumatizující pocity.

Pokud jste v internetové historii odhalili některé překvapivé pornografické weby, držte se následujících pravidel:

- Zůstaňte v klidu.
- Otevřete s dětmi na toto téma konverzaci.
- Nemoralizujte, ale normalizujte; sdílejte pochopení, dejte dítěti najevo, že zvědavost je v jeho věku naprosto přirozená.
- Poskytněte dítěti fungující nástroje, jak s nevhodným obsahem, na který náhodně narazí, naložit.
- Nezůstávejte u jedné konverzace. S věkem se vše mění, důležité věci je třeba opakovat a zdůrazňovat neustále.

10. Jak mohou děti samy monitorovat svůj pohyb na internetu a kontrolovat, kolik času jsou online?

U uživatelů zařízení Apple se stačí obrátit na aplikaci **Screen Time**, která monitoruje čas, jež na jednotlivých aplikacích trávíme, počet odemknutí telefonu za den apod. V novějších verzích lze velice dobře nastavit rodičovská

omezení. Pro **Android** existuje velké množství podobných aplikací s takovými funkcemi, například **YourHour** nebo **Moment**. S aplikacemi typu **Freedom** lze pak tvořit offline zóny například na učení tak, že se skrze ně nastaví požadovaný časový limit na soustředěnou práci, během nějž jsou všechna vaše zařízení blokována.

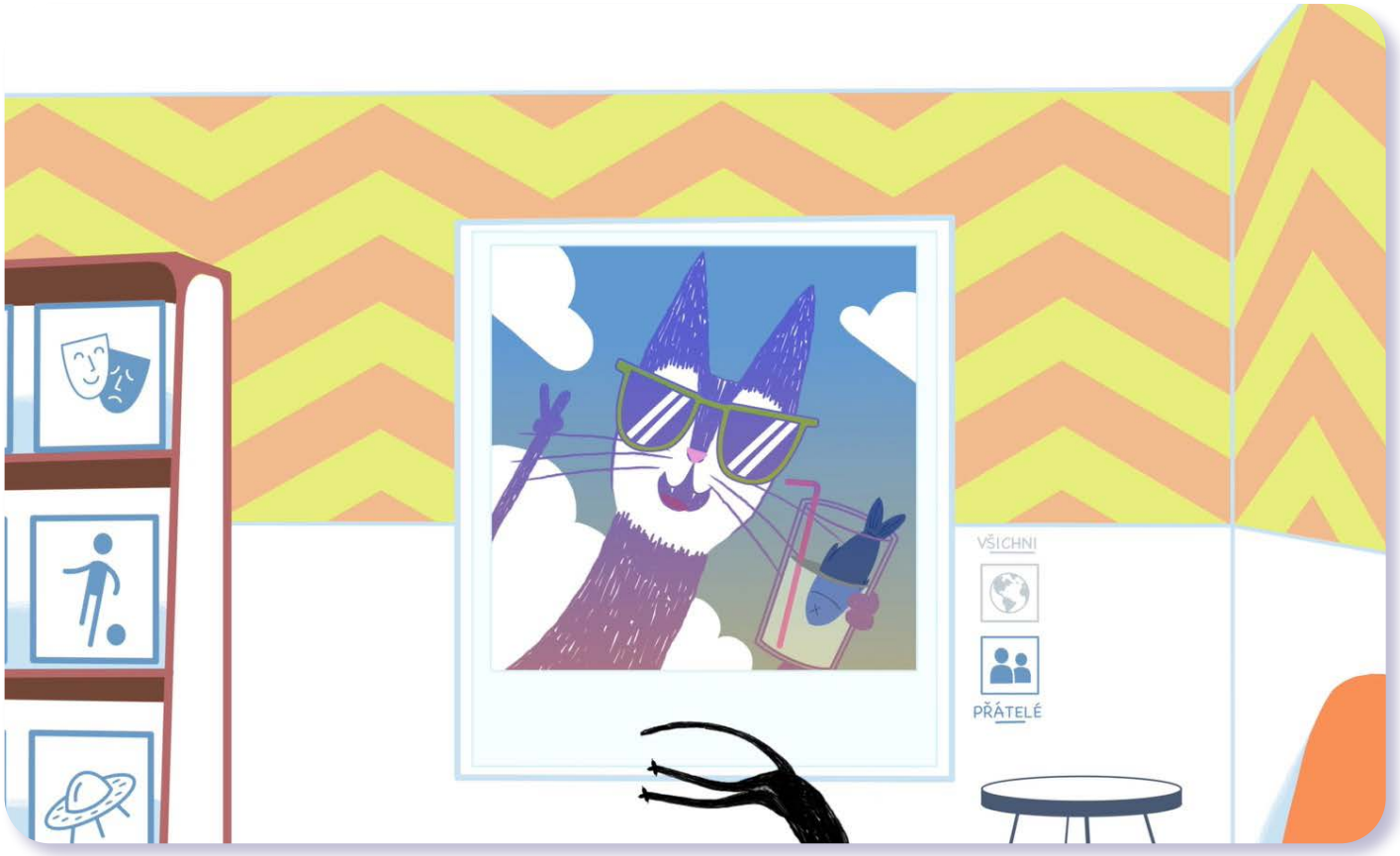
Odpovědi vypracovali:

Kateřina Lukavská, Katedra psychologie Pedagogické fakulty Univerzity Karlovy, Klinika adiktologie 1. lékařské fakulty UK (otázky 1, 4, 5)
Michaela Slussareff, Studia nových médií, Filozofická fakulta Univerzity Karlovy; zakladatelka Slow Tech Institute (otázky 6–10)
Martin Kožíšek, expert na kybernetickou bezpečnost, CZ.NIC (otázky 1–3)

Podívejte se na lekci V digitálním světě: Rodičovská kontrola na <jsns.cz/mv/rodicovska-kontrola>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.

POZNÁMKY

POZNÁMKY



V digitálním světě

Sociální sítě

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Seriáloví sourozenci zakládají rodinný profil na sociální síti. Než se stačí rozkoukat, Kocour nasdílí veřejně své podařené selfíčko a na profilu se strhne lavina reakcí. Díky sociálním sítím, jako jsou Facebook, Instagram nebo TikTok, můžeme být v kontaktu s přáteli. Stejně tak nám tyto platformy umožňují propojit se s novými lidmi a sledovat veřejně známé osobnosti. Na místě je však obezřetnost. Dříve než cokoliv zveřejníme, je potřeba zamyslet se nad nastavením soukromí příspěvku.

CÍLE LEKCE

1. uvědomit si rizika sociálních sítí
2. naučit se regulovat soukromí na sociálních sítích
3. zamyslet se nad specifiky sítí oblíbených mezi dětmi a mladými

DOPORUČENÝ VĚK
8+ LET

AKTIVITA: Sociální sítě !!!

ANOTACE

Prostřednictvím aktivity s popisem fotografií se žáci učí rozlišovat, jaký obsah je nebo není vhodný pro veřejné sdílení na sociálních sítích. Zvažují rizika zveřejňování citlivých informací a postupně se zamýšlí nad výhodami a nevýhodami sociálních sítí.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k řešení problémů, komunikativní, sociální a personální

CÍLE

Žáci:
- pochopí rozdíl mezi soukromým a veřejným sdílením
- se zamýšlí nad pozitivy a negativy sociálních sítí
- si uvědomí, že je třeba být na sociálních sítích ostražitý

DÉLKA

45 min. (včetně projekce)

POMŮCKY

- tabule nebo flipchart
- nápisy: „sdílet veřejně“ a „sdílet s rodinou a přáteli“

POSTUP

1. Vybídneme žáky, aby **vyjmenovali sociální sítě, které znají**. Zapisujeme je na tabuli. (Případně jim trochu napovíme, zda slyšeli o Facebooku, YouTube, Twitteru apod.) Žáci sdílí své/rodinné zkušenosti se sociálními sítěmi.
2. Následuje **projekce epizody seriálu**.
   Poznámka: Snímek doporučujeme zhlédnout nejméně dvakrát.
3. Ověříme, že žáci pochopili pointu. (Na sociálních sítích je problematické sdílet cokoliv veřejně.)
4. Žáky vyzveme, aby se postavili doprostřed třídy. Nalevo na tabuli nalepíme nápis **„sdílet veřejně“**, napravo **„sdílet s rodinou a přáteli“**.
5. Vysvětlíme jim, že jim postupně představíme několik typů fotografií. Ať následně rozhodnou, zda by dle popisu snímek sdíleli veřejně (přemístí se doleva), nebo pouze mezi rodinu a přátele (přemístí se doprava).
6. Postupně čteme ze seznamu (viz níže). Po každé vyjmenované fotografii necháme **každého žáka, aby se přemístil na ose nalevo či napravo**. Několik jich vždy vysvětlí, proč se tak rozhodli postavit. Osu rozhodování můžeme odstupňovat. Pokud je žák například více přesvědčen o sdílení veřejně, posune se více doleva, pokud trochu váhá, stoupne si více ke středu.

Seznam fotografií:
- Fotografie mé rodiny před naším domem, kde je vidět název ulice i číslo popisné.
- Fotografie mé rodiny před naším domem.
- Fotografie mě a mých kamarádů zabalených v ručnících na koupališti.
- Fotografie mě a mých kamarádů v plavkách na koupališti.
- Záběr na tachometr, kde je vidět, že jedeme s rodinou autem přes 180 km/h.
- Fotografie mě a mé rodiny v autě.
- Fotografie spolužačky, na které se vzteká, je celá rudá a nesluší jí to.
- Fotografie mé kamarádky a mě, jak děláme vylomeniny.
- Fotografie mé kamarádky, jak legračně tančí, aniž bych se jí zeptal/a, zda můžu snímek publikovat.
- Fotografie mě a mých spolužáků před naší školou.

REFLEXE AKTIVITY

Probereme s žáky typy fotografií, o kterých se ve hře mluvilo. Ptáme se jich: *Proč je rozdíl mezi fotografiemi určenými pro rodinu/přátele a pro širší veřejnost? Jaké fotografie je tedy dobré nesdílet veřejně? Jaké hrozí nebezpečí? Jak se s našimi fotografiemi zachází na sociálních sítích?*

V diskusi by mělo zaznít, že za problematické lze považovat obnažené fotografie nebo ty, které obsahují citlivé informace.
Poznámka: Doporučujeme využít OTÁZKY A ODPOVĚDI k lekci.

ZKUŠENOSTI Z PRAXE

Téma sociální sítě bylo pro žáky zajímavé, bavilo je video i aktivity. Aktivitu jsme dělali dvojím způsobem: nejprve jsme rozdělili koberec ve třídě na dvě části a do každé dali jednoduchý nápis VEŘEJNĚ a RODINA A PŘÁTELÉ, četla jsem seznam fotek a žáci se měli postavit do té části koberce, jak cítili, kam fotka patří, roli hrála i vzdálenost od hranice obou oblastí.
Kateřina Fučíková, *MŠ a ZŠ Prosetín*

POZNÁMKY

OTÁZKY A ODPOVĚDI

1. Co jsou sociální sítě a jaký je jejich účel?

Sociální sítě jsou internetové služby určené k **vzájemnému propojování** uživatelů internetu, především pak k **udržování** a **navazování** různých druhů **kontaktů** – a to napříč celým světem. Sociální sítě umožňují vytvářet **uživatelské profily** a jejich prostřednictvím se na internetu prezentovat, **sdílet různé druhy informací**, včetně fotografií a videí, komentovat a hodnotit příspěvky ostatních uživatelů, chatovat s nimi, vytvářet nová virtuální přátelství apod. Mezi nejznámější sociální sítě patří **Facebook**, **Instagram** či **Twitter**, k sociálním sítím ale řadíme například i server **YouTube** zaměřený na videa.

2. Jak sociální sítě vznikaly a jak se vyvíjí?

Za první sociální síť, tak jak ji dnes chápeme, lze považovat stránku SixDegrees (1997), která uživatelům umožňovala pomocí profilů navazovat vztahy s ostatními. Následně vznikaly stránky jako Friendster, LinkedIn nebo MySpace.

Největší boom sociálních sítí přišel se vznikem Facebooku (2004), jehož zakladatel Mark Zuckerberg je nyní majitelem i dalších populárních sociálních sítí – **Instagramu, Messengeru** a **WhatsAppu**. Nelze opomenout ani vznik **YouTube** (2005) a **Twitteru** (2006). V současnosti roste popularita čínské sociální sítě **TikTok** (2018), která dříve existovala pod názvem Musical.ly.

Mezi populární české sociální sítě patřil například portál **Spolužáci.cz** sloužící ke kontaktu a výměně informací mezi spolužáky daných tříd, **Libimseti.cz** fungující jako internetová seznamka a **Lide.cz**, kde si uživatelé mohli vytvářet vlastní profily, chatovat a seznamovat se a mohli sdílet fotografie a videa. Avšak poté, co byla v roce 2008 spuštěna česká verze Facebooku, zájem o české sociální sítě začal upadat.

3. Které sociální sítě jsou nejoblíbenější mezi dětmi ve věku 8–11 let? Jaká jsou jejich specifika?

Mezi nejoblíbenější sociální sítě u dětí ve věku 8–11 let patří **YouTube, TikTok a Instagram**. Později si děti mohou oblíbit také **Facebook**, **Snapchat** a další služby.

YouTube je největší internetová platforma pro sdílení videí, kterou využívá více než 2 miliardy lidí denně. Každou minutu na tuto platformu uživatelé nahrají okolo 300 hodin nových videí nejrůznějšího obsahu – hudební klipy, vlogy (videoblogy), trailery k filmům či samotné filmy, vzdělávací nebo zábavná videa apod.

Mezi dětmi jsou velmi oblíbená právě **vtipná videa** (tzv. pranky, žertíky), **výzvy** (tzv. challenge), **unboxing videa** (rozbalování věcí) nebo videa typu **let's play** (herní videa), kde mohou sledovat, jak někdo jiný hraje určitou počítačovou hru. Děti mají také v oblibě videa od **youtuberů**, což jsou tvůrci videí s nejrůznější tematikou, kteří si kolem sebe budují základnu sledujících, a pro děti se tak stávají idoly a novodobými celebritami.

V posledních letech je u menších dětí stále oblíbenější sociální síť **TikTok**, která je postavena na vzájemném sdílení **patnáctivteřinových videí, často hudebních videoklipů**. Ty lze velmi snadno vytvářet a sdílet, k dispozici je také celá řada předpřipravených filtrů, díky kterým působí videa kvalitněji. TikTok je populární především u dětí do 13 let věku, starší uživatelé se již orientují na jiné sociální sítě a služby. TikTok využívá více než miliarda uživatelů (stav k létu 2020).

Další oblíbenou službou je **Instagram**, který je zaměřen především na vizuální obsah – na zveřejňování a sdílení zajímavých fotografií, případně videí.

4. Je dobré o sobě zveřejňovat hodně informací? Ověřují sociální sítě jejich pravdivost?

Obecně platí: **čím míň informací o sobě budeme zveřejňovat, tím lépe**. Budeme pak mít větší jistotu, že tyto informace nemůže někdo zneužít. Existuje celá řada příkladů, kdy byla zveřejněná informace zneužita ke kyberšikaně. Příkladem může být sdílení naší **vtipné fotografie**, kterou chceme pobavit svoje přátele, ale tato fotografie se poté začne šířit internetem a ostatní nás kvůli ní mohou urážet a posmívat se nám.

Sociální sítě informace uvedené v profilech v zásadě **neověřují**, což znamená, že je poměrně snadné vytvořit falešný profil a v něm uvádět nepravdivé údaje. Zároveň ale někdy provozovatelé sítí reagují na podněty uživatelů. Jestliže více lidí účet označí jako falešný, prověřují to a mohou ho zablokovat.

Jak můžeme odhalit, že je nějaký profil falešný? Jedním z prvních kroků může být ověření věrohodnosti profilové fotky pomocí služby Google obrázky. Pokud zjistíme, že se někdo vydává za chlapce z České republiky, ale jeho profil je tvořen fotografiemi staženými od zahraničních blogerů, je to s velkou pravděpodobností falešný profil.

5. Jak mohou děti obcházet věková pravidla pro založení sociálních sítí? Jak tomu mohou rodiče nebo učitelé zamezit?

V tuto chvíli je to velmi snadné, žádná populární sociální síť **neobsahuje mechanismy, které by umožnily ověřit skutečný věk registrovaných uživatelů**, dítěti tedy stačí pouze uvést nepravdivé datum narození a na sociální síť se dostane. Sociální sítě tak často používají děti, které minimální věkovou hranici ve skutečnosti nesplňují.

Rodičům a učitelům se často nedaří v tom dětem zabránit. Děti si profil na sociální síti mohou založit například přes kamarádův počítač, počítač v knihovně, koupit si mobil apod. Něco zakazovat tedy není řešení.

Dítěti může účet na síti založit rodič. Heslo k tomuto účtu bude mít také rodič, který zároveň může sledovat, co dítě dělá, s kým si píše, co sleduje, a bude o tom s dítětem komunikovat. Až bude mít rodič jistotu, že dítě je dostatečně

zralé na to, aby mohlo sociální sítě používat bez kontroly, může mu dát větší svobodu.

6. Kdo s kým se na sociálních sítích propojuje? Existují nějaká rizika?

Na sociálních sítích se propojují uživatelé internetu, aby spolu mohli **komunikovat**. Lidé se mohou propojit na základě přátelského či příbuzenského vztahu, společného zájmu, pohledu na svět apod.

Propojit se můžeme v podstatě **s jakýmkoliv uživatelem** dané sociální sítě, **aniž bychom ho znali nebo osobně potkali**. V případě, že s námi naváže kontakt **neznámý člověk**, měli bychom být velmi **obezřetní** a ověřit si, zda se nejedná o falešný účet. Internetoví predátoři si mohou vytvářet falešné profily s fotkami a údaji našich přátel, aby působili věrohodněji. Pomůže, když si ve svém účtu vypneme **viditelnost** našich přátel pro ostatní uživatele dané sociální sítě. Měli bychom myslet na to, že **nikdy nemáme jistotu, kdo sedí na druhé straně**.

Důležité také je hlídat, kdo nás sleduje. Svůj účet si nastavme tak, aby **nebyl veřejný** a mohli jsme sami schvalovat, kdo nás může a nemůže sledovat.

7. Jaké obsahy na sociálních sítích vidíme?

Sociální sítě zobrazují svým uživatelům tzv. **personalizovaný obsah**, který je vytvořen pomocí speciálních algoritmů. To znamená, že každý z nás vidí jiné informace, které se mu zobrazují podle jeho zájmů a zálib, a to na základě toho, jak se na sociální síti **chováme – co sledujeme, co lajkujeme, co komentujeme**.

Sociální sítě tak přispívají k rozdělování lidí do tzv. **sociálních bublin**. Ty sdružují názorově podobné uživatele a sítě jim nabízejí podobný typ obsahu. Rizikové může být, že v těchto sociálních bublinách nejsme konfrontováni s odlišnými názory, a proto můžeme podléhat iluzi, že náš názor je ten jediný správný, a snižuje se tak naše tolerance vůči čemukoliv odlišnému a neznámému. Algoritmy se zároveň snaží svým uživatelům nabízet natolik atraktivní obsah, aby trávili na dané sociální síti co nejvíce času.

To vše má svůj důvod: čím více času v prostředí sociální sítě trávíme, tím přesněji dokáže sociální síť zacílit podle našeho profilu reklamní sdělení, která nám poté zobrazuje. Reklama je pro sociální síť základním zdrojem příjmu.

8. Jak si na sociálních sítích regulovat soukromí?

Drtivá většina sociálních sítí umožňuje nastavit, který obsah bude pro ostatní uživatele **veřejný** a který **uvidí pouze přátelé**. Zároveň je však **u většiny sociálních sítí výchozí nastavení veřejné a je třeba je změnit na soukromé**.

Většina sociálních sítí obsahuje položku **Nastavení**, ve které je možné nastavit **Soukromí** – tedy **kdo** uvidí naše budoucí příspěvky (přátelé, všichni…), jak nás budou moci lidé najít a kontaktovat (kdo nám může poslat žádosti o přátelství), kdo všechno uvidí seznam našich přátel (jenom já, ostatní přátele, přátele přátel, všichni…), kdo nás bude moci na sociální síti vyhledat pomocí e-mailové adresy či telefonního čísla, zda bude náš profil propojen s běžnými vyhledávači, zda budeme kontrolovat příspěvky, na kterých nás někdo jiný označí, apod.

Důležité je také **zabezpečení přihlašování do sociální sítě** – ať už prostřednictvím webových stránek, nebo pomocí konkrétních aplikací pro mobilní telefony či tablety. Pozor – u sociální sítě Facebook je třeba myslet i na zabezpečení komunikačního nástroje Messenger, který lze používat i bez nutnosti mít účet na samotné sociální síti – Messenger má vlastní bezpečnostní nastavení.

Pokud máte podezření, že se do sociální sítě někdo neznámý přihlašuje prostřednictvím vašeho účtu a pravděpodobně zná vaše heslo, podívejte se na **výpis uživatelů/zařízení**, která jsou k vašemu účtu přihlášena.

Na stránkách projektu E-Bezpečí najdete konkrétní návody, jak si zabezpečit své soukromí v prostředí jednotlivých sociálních sítí.

- Facebook
- Instagram
- TikTok
- Snapchat

9. Jaký obsah bychom neměli na sociálních sítích sdílet a proč?

Na sociálních sítích bychom **neměli sdílet osobní a citlivé informace**, jako je náš **věk, místo bydliště, kam chodíme do školy, kde pracují naši rodiče, telefonní čísla, hesla** apod. Tyto informace mohou velmi snadno zneužít internetoví predátoři. Když například zveřejníme místo svého bydliště, může predátor začít vyhrožovat, že ublíží nám a naší rodině, pokud neuděláme, co po nás chce.

Neměli bychom sdílet ani naše **intimní fotografie či videa**. Pokud se k tomuto materiálu někdo dostane, získává nad námi moc a může nás začít šikanovat nebo vydírat. Rodiče by zase měli myslet na to, že fotografie jejich dětí (např. nahé fotky v bazénku) mohou být zneužity a šířeny predátory jako dětská pornografie.

Na sociální sítě nepatří informace o **naší domácnosti, o jejím vybavení nebo kdy odjíždíme na dovolenou**. Tyto informace jsou pozvánkou pro zloděje, kteří mohou vykrást náš dům či byt zrovna ve chvíli, kdy nejsme doma.

Rozhodně bychom neměli sdílet **nevhodné fotografie** (ať už svoje, nebo druhých osob). Jedná se o fotografie, které nás zachycují při nelegálním chování (např. pití alkoholu, pokud nám ještě nebylo 18 let, užívání drog, porušování rychlosti při jízdě autem apod.), nebo fotografie zachycující nás v situaci, za kterou bychom se mohli stydět (např. opilost, obnažování).

Hlídat bychom si měli také **tzv. geolokační informace**, jinak každý může vědět, kde se zrovna nacházíme.

10. Co dělat, když někdo sdílí fotky se mnou a já nechci, aby byly veřejné?

V případě, že byly fotky už zveřejněny, toho moc nezmůžeme. Můžeme **požádat osobu**, která fotky sdílela, aby je smazala. Avšak nemáme žádnou jistotu, že si fotografie někdo nestáhl a neuložil. Danou osobu můžeme upozornit, že si pro příště nepřejeme, aby fotografie sdílela bez našeho souhlasu.

Pokud bychom chtěli pouze to, aby byla fotka soukromá, a ne veřejná, můžeme u ní upravit, kdo všechno ji smí vidět (např. jen já nebo moji přátelé). Kdyby se nám nelíbila fotografie, na které nás někdo označil, můžeme označení odebrat nebo danou fotografii nahlásit.

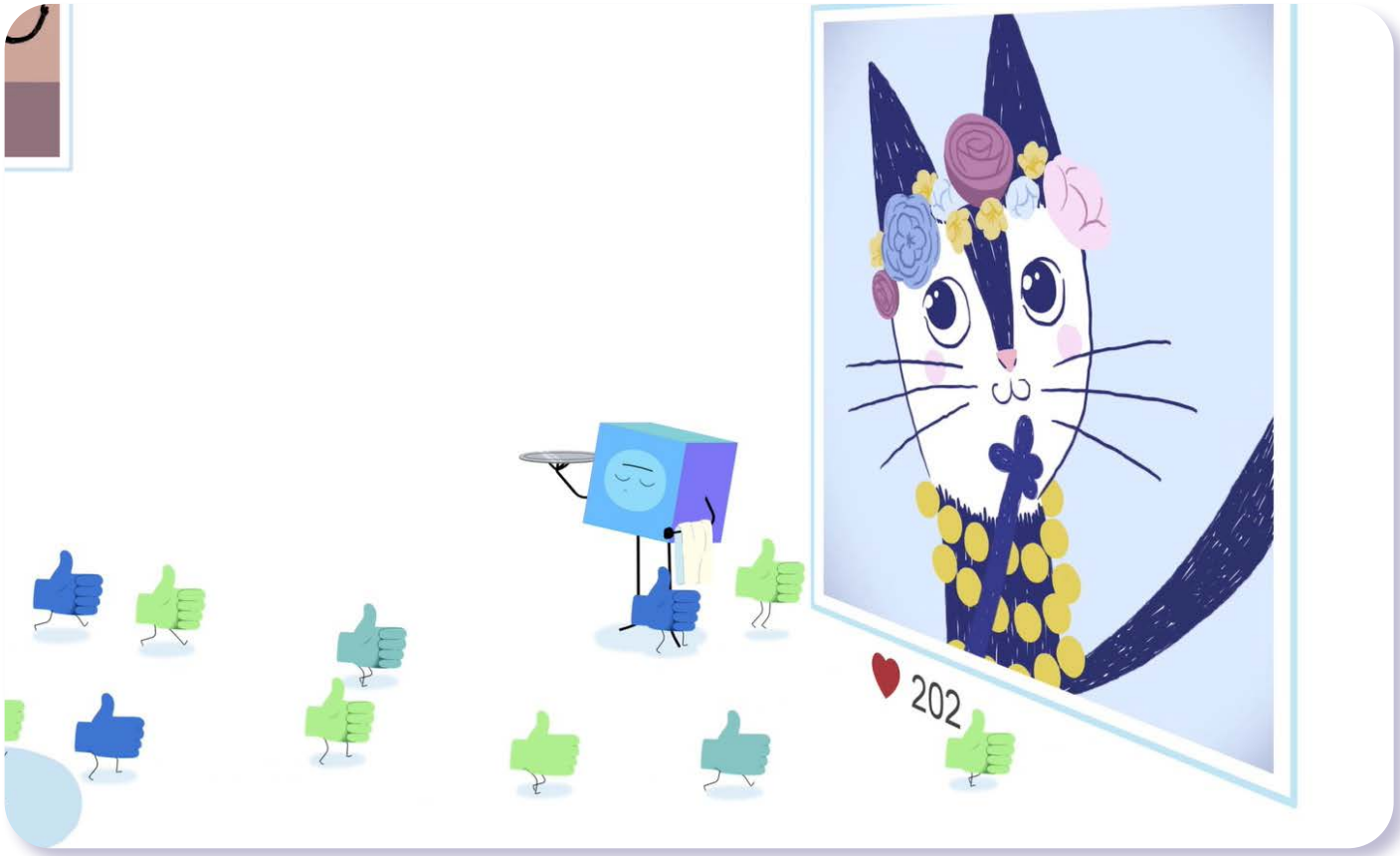
Další možností je **závadný obsah na dané sociální síti nahlásit**. Tuto možnost dnes nabízejí v podstatě všechny sociální sítě. Pokud se pak jedná o vyloženě závadné materiály (dětská pornografie), případně nám někdo prostřednictvím těchto materiálů vyhrožuje nebo nás vydírá, **můžeme se také obrátit na Policii ČR**.

Odpovědi vypracovali:

Klára Mikulcová, Kamil Kopecký,
E-Bezpečí, Univerzita Palackého v Olomouci

Podívejte se na lekci V digitálním světě: Sociální sítě na <jsns.cz/mv/socialni-site>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.

POZNÁMKY



V digitálním světě

Lajky na internetu

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Kocour a Filip mezi sebou soutěží, kdo na sociální síti získá víc lajků. Bude to Kocourovo nové „selfíčko“, nebo Filipovo roztomilé štěňátko? S lajky jako by se na internetu roztrhl pytel. Čím víc jich nějaká fotka nebo příspěvek má, tím spíš si myslíme, že se ostatním líbí. Jakou váhu jim ale ve skutečnosti přičítat? A opravdu platí, že každý, kdo něco lajkuje, tím touží vyjádřit, že se mu příspěvek líbí?

CÍLE LEKCE

1. dozvědět se o tom, jak a proč lajky fungují
2. uvědomit si, že lajky nejsou odrazem naší offline reality
3. přemýšlet nad tím, že by počtům lajků neměl být přikládán příliš velký význam

DOPORUČENÝ VĚK
8+ LET

AKTIVITA: „Líbí“ !!!

ANOTACE

Žáci se zamýšlí nad tím, co jim dělá radost a na čem jim záleží. Ve skupině pracují s fotografiemi, udělují lajky a pokouší se vystihnout, co se jim na nich líbí. Aktivita vede žáky k tomu, aby si uvědomili, že podporovat a oceňovat něco v reálném životě je náročnější než „dávat lajky“ na internetu.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k řešení problémů, komunikativní, sociální a personální, občanské

CÍLE

Žáci:
- zjistí, že podporovat něco v reálném životě je těžší a hodnotnější než dávat lajky
- si uvědomí, že lajky nejsou odrazem naší offline reality
- přemýšlí nad tím, že by počtům lajků neměli přikládat příliš velký význam

DÉLKA

60 min. (včetně projekce)

POMŮCKY

- PRACOVNÍ LIST do každé skupiny
- lepicí papírky, nůžky, psací potřeby
- tabule nebo flipchart

POSTUP

1. Na tabuli napíšeme: ***„Radost mi dělá…“*** a ***„Záleží mi na…“***. Každému žákovi rozdáme čtyři lepicí papírky a vyzveme všechny, aby napsali na každý papírek jedno slovo, které vyjadřuje, co jim dělá radost a na čem jim záleží, a papírky pak nalepili pod nápisy na flipchart/tabuli. Vznikne plakát, který necháme viset ve třídě. V závěru lekce se k němu vrátíme.
2. Rozdělíme žáky do skupin po čtyřech a rozdáme jim PRACOVNÍ LIST (jeden do skupiny).
3. Ukážeme jim obrázek lajku (v PRACOVNÍM LISTU). Ptáme se jich, co to je, a pokud je to potřeba, společně si pojem a jeho funkci vysvětlíme (to se týká zejména první nebo druhé třídy ZŠ).
   Poznámka: Doporučujeme využít OTÁZKY A ODPOVĚDI k lekci.
4. Poté žáky vyzveme, aby vystřihli ikonky lajků a vybrali fotografie, které se líbí všem ve skupině, a dali jim lajk. Žáci se následně zajdou podívat, které obrázky se líbily ostatním skupinám. Požádáme žáky, aby obrázky ponechali na lavici, protože s nimi budeme ještě pracovat.
5. Následuje **projekce epizody seriálu**.
   Poznámka: Snímek doporučujeme zhlédnout nejméně dvakrát.
6. Krátce ověříme, jestli žáci pochopili příběh dílu, a provedeme reflexi emocí (Kocour a poté i Filip zveřejnili novou fotografii a začaly jim přibývat lajky. *Kdo nakonec posbíral lajků nejvíc? Jak se cítil Kocour? Které z postaviček jste fandili a proč?*).
7. Vrátíme se k fotografiím, kterým žáci předtím dali lajk. Rozdáme každé skupině lepicí papírky. Vyzveme žáky, aby ke všem fotografiím, kterým předtím přidělili lajk, zapsali, **proč se jim obrázek líbí**. Ke každému obrázku s lajkem vymyslí členové skupiny alespoň dva různé důvody a zapíšou na samostatný lepicí papírek.
8. Fotografie nalepíme na tabuli a žáci čtou své věty a lepí je k danému obrázku. Vznikne tak soubor komentářů, proč se jim fotografie líbila.

REFLEXE AKTIVITY

Ptáme se žáků: *Jak se vám pracovalo? Je jednodušší lajkovat, nebo vysvětlovat, proč se mi něco líbí? Dá-li někdo někomu nebo něčemu lajk, musí to určitě znamenat, že se mu daná věc líbí? Že ho mají všichni rádi?*

Zmíníme, že **lajkovat je jednodušší než podporovat věci offline**. Vrátíme se k úvodu hodiny a k tomu, co žákům dělá radost a na čem jim záleží. Z diskuse by mělo vzejít jasné poselství, že lajkovat něco je jednoduché a často naše lajky ani nesouvisí s konkrétní fotkou nebo příspěvkem. Počtu lajků bychom proto neměli přikládat příliš velký význam.

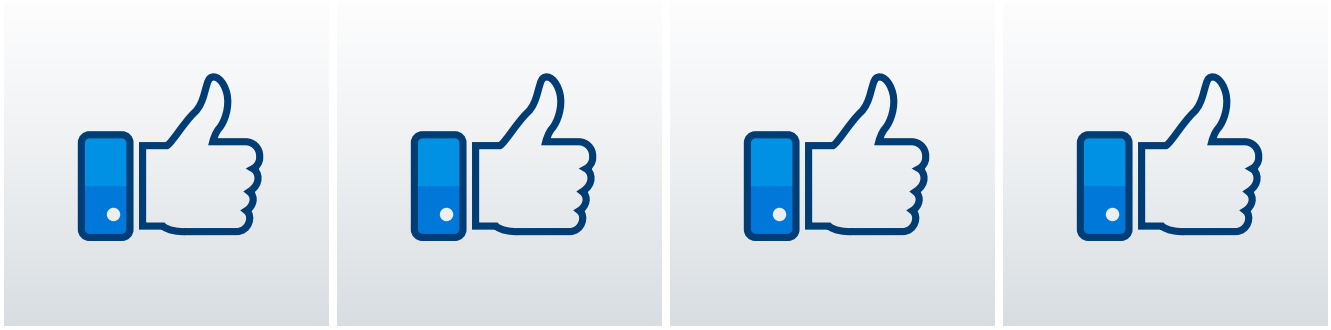
ZKUŠENOSTI Z PRAXE

Aktivitu jsem testovala v páté třídě s 24 žáky. Žáci jsou v pubertě, takže při aktivitě vtipkovali a lajkovali i věci kolem sebe, nejen fotky, s tím šlo ale dobře pracovat. Třída minulý rok absolvovala přednášku zaměřenou na nebezpečí na sociálních sítích, i tak ale pro ně bylo téma vcelku nové. Vše jsem si sice přichystala předem, naskytly se ale technické problémy, a tak byli žáci na film trochu nesoustředění. Na závěr jsme si zahráli psychohru, kterou jsem ukázala, že lajkovat na internetu je snadnější než v offlinu. Každý musel sousedovi po pravici říct: „Líbí se mi na tobě, že…“ Někteří se u přemýšlení zapotili, takže cíl byl myslím splněn.
Marie Valtrová, *ZŠ Kladno, Cyrila Boudy 1188*

POZNÁMKY

PRACOVNÍ LIST

Vystřihněte:



Zdroj: https://www.freepik.com/free-vector/facebook-like-icon_1105002.htm#page=1 & query=like & position=3

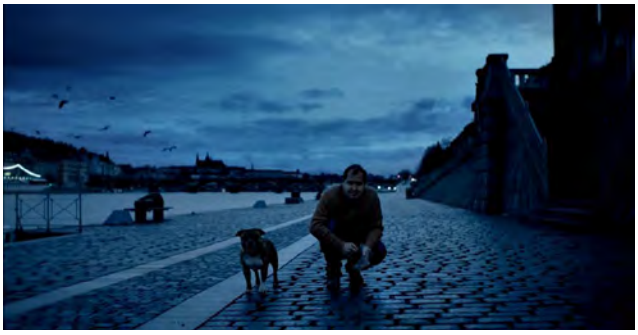
Vyberte obrázky, které se líbí všem ve vaší skupině, a dejte jim vystřižený lajk:

1.

2.

3.

4.



5.

Fotografie č. 1, 2, 3, 5 – zdroj: https://pixabay.com/, fotografie č. 4 – zdroj: Člověk v tísni

OTÁZKY A ODPOVĚDI

1. Jak se na sociálních sítích měří popularita?

Sociální sítě pracují s číslem jako hodnoticím prostředkem toho, jak je obrázek, text, video, jež jsme na sítě nahráli, oblíbené. S **palcem nahoru (lajkem)** jako ukazatelem popularity vloženého obsahu přišli provozovatelé sociálních sítí. **Lajky se postupně staly nedílnou součástí internetu.** Jsou všude, kam se podíváme – na sociálních sítích, videoplatformách, zpravodajských kanálech, webových stránkách a e-shopech. Ukazují nám, jak je příspěvek oblíbený mezi našimi „přáteli" a sledujícími nebo mezi ostatními uživateli internetu.

2. Jak lajky vznikly? Jaký je jejich smysl? Byl za nimi od počátku komerční záměr?

Lajk byl poprvé představen v roce 2005 na videoplatformě Vimeo, ale do širšího povědomí vstoupil až tehdy, když byl přijat Facebookem v roce 2009. Cílem lajků mělo původně být zbavit se zbytečných duplicitních komentářů jako „gratuluji", „dobrá práce" atd. Mimo to uživatelům tato funkce umožnila velmi rychle pochopit, jak populární nebo relevantní je příspěvek, aniž by museli číst všechny komentáře. **Od tohoto relativně jednoduchého záměru se podobné tlačítko rychle stalo fenoménem celého internetu.** Na Facebooku každý den jeho uživatelé dají celkově v průměru tři miliardy lajků.

3. Jak sociální sítě pracují s tím, co lajkujeme? Má to nějaký další dopad?

To, co vypadá jako jednoduchá a základní funkce, je ve skutečnosti jeden z nejvýkonnějších online nástrojů, jaké kdy byly vytvořeny.

V roce 2015 zveřejnili vědci z University of Cambridge a Stanford University studii ilustrující, jak mohou být data podobná těm, která publikujeme na Facebooku, použita k přesnému odhadu osobnostních rysů uživatelů. V roce 2007 tito vědci vytvořili online test osobnosti a zveřejnili jej na Facebooku. Podmínkou vyplnění testu bylo zprostředkování přístupu k osobním údajům na facebookovém profilu.

Test proběhl virálně mezi více než 80 000 lidmi, kteří vědcům dobrovolně poskytli obrovské množství osobních dat. Je důležité si uvědomit, že tato data mohou být kvůli licenčním podmínkám Facebooku (ano, to dlouhé, nudné, co jste nejspíše bez rozmyslu odklikli při registraci) poskytnuta za úplatu třetím stranám.

Pomocí údajů shromážděných z testu osobnosti a údajů z osobního profilu vědci vytvořili počítačový algoritmus, aby pochopili, jak přesně je možné určit osobní profil uživatele pouze na základě lajků na Facebooku. **Studie ukázala, že s pozoruhodně malým počtem lajků by algoritmus mohl určit osobnost uživatele do velmi vysoké míry a přinést podobně přesvědčivá data jako psychologické testy.**

Pokud se vám tedy od roku 2009 líbilo více než 300 příspěvků, Facebook vás pravděpodobně zná lépe než mnozí vaši kamarádi. Můžeme si snadno představit, jak by tento druh údajů a poznatků mohl být pro společnosti velmi cenný. Tak třeba: pokud se vám dříve líbila videa a příspěvky související s lyžováním a Facebook ví, kde se geograficky nacházíte, má smysl vám zobrazit příspěvek inzerující nový obchod s lyžařským vybavením, který byl otevřen blízko vaší lokality.

4. Je možné lajky koupit? Je to legální?

Na internetu dnes již existuje mnoho firem, které „prodávají lajky" – **programují speciální virtuální roboty (boty)**, kteří dokážou uměle pozvednout nějaký produkt nebo značku. Jde o legální byznys, i když většina seriózních firem k tomuto kroku nepřistupuje. Dnes totiž mají sociální sítě automatické mechanismy, které redukují možnosti virtuálních botů nebo na takové značky přímo aplikují ban – zákaz zobrazování.

5. Jak ovlivňuje sbírání lajků děti? Jaké psychologické efekty vyvolává, když získávají hodně lajků?

Nejmladší uživatelé online světa se s lajky často poprvé setkají prostřednictvím YouTube nebo sítě TikTok, kde se používají srdíčka.

Čím více lajků, tím více jste vidět díky hodnocení algoritmů. Ve světě sociálních sítí to pak pro mnohé uživatele znamená pocit, že „čím víc lajků máš, tím jsi oblíbenější". **Nejsilnější psychologický dopad má tento fenomén na dospívající.**

Podle teorie psychosociálního vývoje Erika Eriksona je ústředním tématem adolescence utváření osobní identity, které úzce souvisí s vývojem „ega". Než se objeví zralé „ego", musí člověk získat přiměřený pocit identity. Úspěšné zakotvení ve světě s jasným sebepojetím jedinci umožňuje vytváření jednoznačných a smysluplných vztahů k vlastní osobě i k druhým. V tomto období je pro každého jedince nanejvýš důležité ztotožnit se s určitým životním ideálem, skupinou, která mu je sympatická, a charakterem, který mu stojí za to rozvíjet.

Na jedné straně stojí silná potřeba být originální, na druhé straně podobně silná potřeba zapadnout do nějaké skupiny, být zkrátka oblíbený. Lajky se pak stávají zkratkovitým nástrojem, jak si ověřit, jak moc je moje osobnost zajímavá a jak ji přijímá skupina, o kterou stojím a jejíž součástí bych se chtěl stát.

Sociální média se stala jádrem mezilidských vztahů. Avšak **„hodnota" vztahu se na sociálních sítích kvůli lajkům měří naprosto jiným způsobem než v reálném světě.** Lajky jsou nástrojem jak hodnocení produktů a obsahů, tak i nástrojem hodnocení autora příspěvku.

V dnešní společnosti velká část mladých lidí (a nejen jich) upřímně věří, že jejich popularita, krása a vlastní hodnota pramení z množství lajků, které dostávají za svá selfie. To může být velice toxické a hluboce poškozovat sebevědomí – všechna ta dokonale vyretušovaná těla, tváře a životní příběhy, které na internetu vidí, mohou v uživatelích

vzbuzovat pocit, že jejich vlastní realita je přinejmenším nudná. Mnoho dospívajících si pak v online světě vytváří své falešné, ale dokonalé já. Zde získávají mnoho virtuální odměny v podobě lajků a povzbuzujících komentářů, nakonec se ale mohou cítit znechuceni a v depresi, když si v každodenním životě uvědomují propast mezi svou falešnou virtuální identitou a tím, kým skutečně jsou.

6. Mohou být děti na lajcích závislé?

Každý nový lajk u příspěvku znamená příliv velice příjemných hormonů (zejména dopaminu) a pocitů, které má lidský mozek v oblibě, a tak je často vyhledává. Mnozí uživatelé tak po publikování fotografie či jiného příspěvku neustále kontrolují sociální síť, aby zjistili, kolik nových lajků jim přibylo. Z takového jednání se stává jakási obsese.

Nedávná studie akademiků z University of California, ve které testovali mozkovou odezvu na vnímání lajků u adolescentů, potvrdila, že při konzumaci čokolády nebo výhře na výherních automatech se zapojují stejné mozkové obvody, jako když vidíme přibývající množství lajků. Studie také ukázala, že když vidíme lajky u cizího příspěvku, máme větší tendenci příspěvek chápat jako pozitivní a ztotožňovat se s ním.

Závislost na sociálních médiích sice není oficiálně klasifikována, ale nutkavá potřeba používat sociální média je u mnoha lidí realitou. Děje se tak i v situacích, které se tak stávají velmi nebezpečnými – například když někdo kontroluje sociální sítě při řízení auta.

Pokud člověk s nutkavou potřebou užívat sociální sítě k nim ztratí přístup, tedy například pokud rodiče dítěti zakážou je používat, je pravděpodobné, že se u takových uživatelů projeví úzkost nebo výkyvy nálad.

Nadměrné používání sociálních sítí je mnohem problematičtější u dětí a mladých dospělých, protože jejich mozek a sociální dovednosti se stále rozvíjejí. Odhaduje se, že 27 % dětí, které tráví tři a více hodin denně na sociálních sítích, vykazuje příznaky špatného duševního zdraví – výzkum ukázal, že adolescenti, kteří často používají sociální média, mají omezené sociální dovednosti, jako například schopnost empatie. Patrně mají rovněž vyšší skóre sociální úzkosti, vyšší míru deprese nebo negativně vnímají obraz vlastního těla.

7. Plánují velké sociální sítě nějaké změny v systému lajkování? Proč?

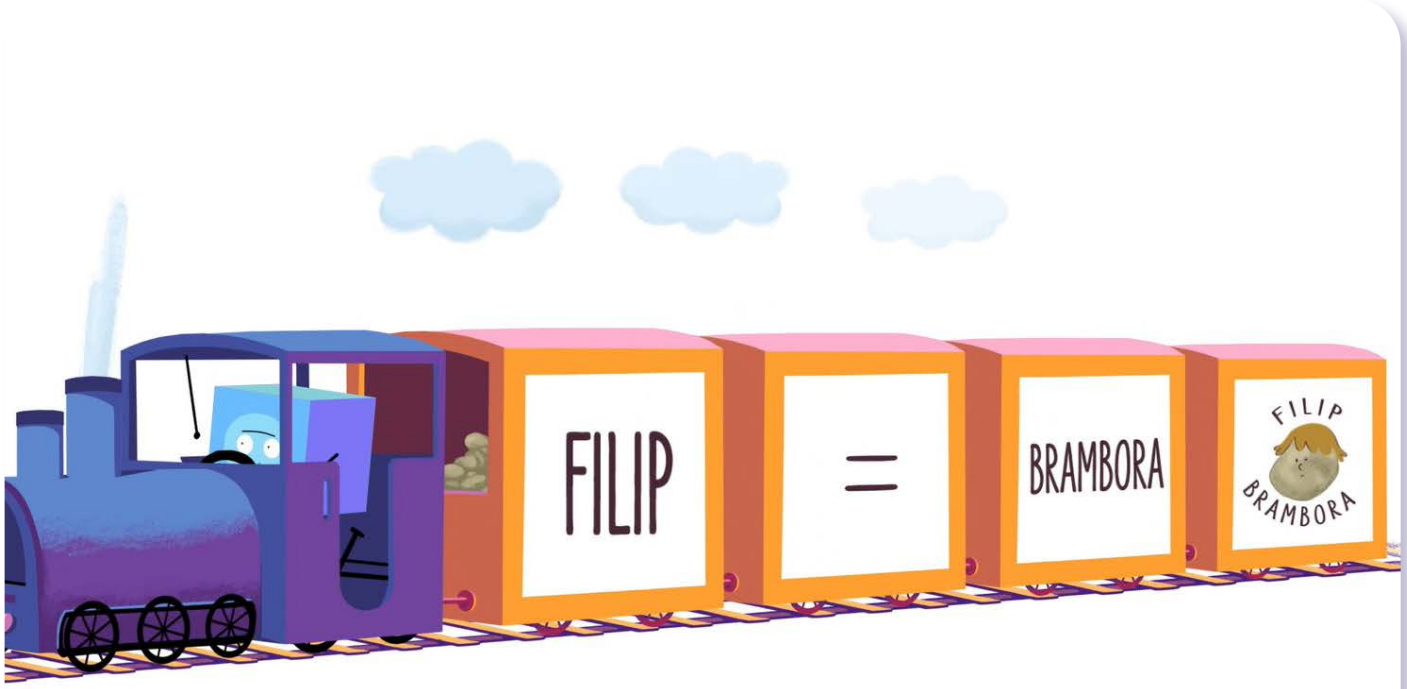
V červenci roku 2019 Instagram oznámil, že odstraní viditelné lajky v šesti zemích světa. Uživatelé zde mohou vidět počty přidělených lajků u svých příspěvků, ale ostatní tyto počty nevidí.

Podobný krok plánuje i Facebook. Tvrdí, že chce vytvořit **„méně natlakované prostředí“** a snížit negativní aspekty, jako jsou právě deprese a úzkosti (spojené s používáním lajků).

Odpovědi vypracovala:

Michaela Slussareff, Studia nových médií, Filozofická fakulta Univerzity Karlovy; zakladatelka Slow Tech Institute

Podívejte se na AV lekci V digitálním světě: Lajky na internetu na <jsns.cz/mv/lajky>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.



V digitálním světě

Jak mluvit na internetu

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Mína si za zády utahuje z Filipa, že mu to na fotkách moc nesluší. Jenže tato drobná poznámka míněná v legraci se při zveřejnění online nafoukne a oklikou se dostane až k babičce sourozenců. Rčení dvakrát měř, jednou řež platí pro komunikaci na internetu dvojnásob. Cokoliv vypustíme do online prostoru – názor, hlášku nebo fotku – je prakticky nemožné vzít zpět. Dřív než něco zveřejníme, je potřeba promyslet, jestli bychom stejnou myšlenku s klidným svědomím přednesli vlastním rodičům nebo spolužákům v reálném životě.

CÍLE LEKCE

1. osvojit si pravidla komunikace online
2. uvědomit si, že na internetu je „všechno navždy"

DOPORUČENÝ VĚK

8+ LET

AKTIVITA: Jak mluvit na internetu !!!

ANOTACE

Žáci si při zážitkové aktivitě se svými portréty, které formou hry „sdílejí na internetu“, uvědomí, jak se vytvořený obsah může nekontrolovatelně šířit a měnit. Společně formulují, jaká pravidla slušné a nezraňující komunikace by měla platit v reálném světě i online.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, umění a kultura, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k řešení problémů, komunikativní, sociální a personální, občanské

CÍLE

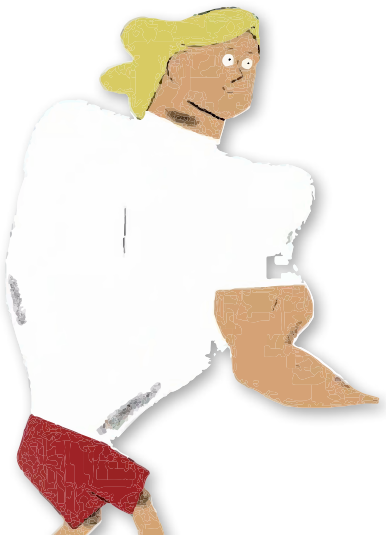
Žáci:
- si uvědomí, že na internetu je „všechno navždy“
- zjistí, že obsah sdílený na internetu mohou jiní uživatelé zneužívat
- formulují, proč je i na internetu důležité komunikovat ohleduplně a slušně

DÉLKA

45 min. (včetně projekce)

POMŮCKY

- papíry A4 pro každého žáka
- psací potřeby
- tabule nebo flipchart
- krabice či jiná nádoba s nápisem „internet“



POSTUP

1. Vyzveme žáky, aby říkali nahlas, jaká je napadají **pravidla slušného chování** během komunikace. Jejich postřehy zapisujeme na tabuli nebo flipchart.
2. Následuje **projekce epizody seriálu**.
   Poznámka: Snímek doporučujeme zhlédnout nejméně dvakrát.
3. Vybídneme žáky, aby zrekapitulovali příběh: do jakých potíží se postavy dostaly a **jak se cítily** (např. Nápis „Filip je brambora“ se začal rychle šířit. Míně bylo líto, co způsobila.).
4. Rozdáme žákům papíry a vyzveme je, aby **namalovali svůj jednoduchý portrét**. Žáci obrázek nepodepisují a během aktivity neříkají ani jinak nedávají najevo, který obrázek je jejich.
   Poznámka: Doporučujeme zdůraznit, že portrét má být opravdu jednoduchý, případně vymezíme přesný čas.
5. Doprostřed třídy dáme krabici/nádobu, na kterou napíšeme „internet“. Žáci umístí svůj obrázek do krabice. Upozorníme je, že právě „sdíleli svůj obsah na internet“. Ověříme si, že žáci pojmům „obsah“ a „sdílení na internetu“ rozumí, případně pojmy vysvětlíme.
   a/ Vyzveme je, aby si z krabice vylosovali obrázek a **připsali na něj vzkaz**.
   b/ Tento obrázek „přepošlou“ (tedy podají) někomu ze spolužáků. Nyní má každý obrázek, který od někoho dostal, a opět na něj napíšou vzkaz (z kterékoliv strany a kamkoliv).
   c/ Poté žáky vyzveme, aby opět obrázek umístili „na internet“ (do krabice) a znovu si vylosovali jiný.
   d/ Tentokrát obrázek trochu upraví, něco menšího k němu **přimalují**.
   e/ Vhodí ho zpět do krabice a každý si naposledy vylosuje obrázek.
6. Vyzveme pět dobrovolníků, aby nalepili obrázky, které drží v ruce, na tabuli. K nalepeným obrázkům připíšeme nadpis: „Osoby, které mají rády špenát.“ Dalších pět žáků obrázky v ruce zmačká.
7. Ptáme se žáků, kde se nyní nachází jejich obrázek, většina by to neměla vědět. Vyzveme žáky, aby zbylé obrázky položili do kruhu na zem. Každý by měl svůj obrázek najít a podívat se na něj.

REFLEXE AKTIVITY

Aktivitu se žáky důkladně rozebereme. Ptáme se: *Co se stalo s vaším obsahem (obrázkem) poté, co jste jej „umístili na internet“? Jakým způsobem se šířil? Měli jste kontrolu nad tím, kde se váš obrázek nachází? Jak jste se u toho cítili? Co asi symbolizoval zmačkaný obrázek? Jak jste se cítili, když se u vašeho obrázku objevil komentář nebo jste byli označeni, že „máte rádi špenát“? Můžeme námi sdílený obsah na internetu uhlídat? Co vše se s ním může stát? Co je třeba si uvědomit, než něco budu sdílet?*

Snažíme se dovést žáky k uvědomění, že vše, co sdílíme na internetu, se šíří bez naší kontroly a nelze to vzít zpět. Je třeba si řádně rozmyslet, co budeme sdílet.
Na závěr se vrátíme k pravidlům slušného chování při komunikaci. Ptáme se: *Jaká pravidla slušného chování při komunikaci platí v běžném životě i na internetu?* (V online prostoru, stejně jako v reálném životě, platí pravidla ohleduplného chování: Mluvíme slušně. Nikoho v komentářích neurážíme apod.)

ZKUŠENOSTI Z PRAXE

Aktivitu jsem testovala s 20 žáky druhé třídy. Krátký film se dětem líbil a dokázaly vystihnout jeho hlavní myšlenky. Po filmu jsme debatovali na téma, které se ve filmu objevilo. Žáky hodně bavilo dokreslovat portréty a psát anonymní vzkazy. Byli zvědaví, co a kdo napsal či nakreslil k jejich portrétu. Aktivita byla pro druháky vhodná spíše hraničně, doporučila bych ji pro trochu starší děti (třeťáky). Téma šlo díky materiálům dobře uchopit.
Aneta Pečonková, *ZŠ Kladno, Cyrila Boudy 1188*

POZNÁMKY

OTÁZKY A ODPOVĚDI

1. Jaká jsou specifika komunikace online oproti té tváří v tvář?

V online světě můžeme zůstat **anonymní**, můžeme se **vydávat za kohokoliv**, můžeme **komunikovat kdykoliv a odkudkoliv**. Při komunikaci tváří v tvář (face to face) vidíme **emoce** člověka, se kterým se bavíme, a jsme schopni na ně reagovat, ale při komunikaci online, třeba při chatování či komentování příspěvků, emoce nevidíme a nevíme, co člověk na druhé straně při čtení našich zpráv nebo komentářů prožívá a jak se cítí. Jednoduše nevíme, jaký na něj naše texty měly dopad, zda se smál, mračil, nebo dokonce plakal. Smajlíky a nálepky skutečné emoce nenahradí, přestože jsou často vtipné a zábavné.

Komunikace na internetu **má velký dosah**. Při veřejné komunikaci si může naše zprávy přečíst v podstatě kdokoliv, může si zprávy zkopírovat, udělat snapshot/screenshot (tedy pořídit si fotografii obrazovky). Přestože pak komunikaci smažeme, naše zprávy a komentáře se mohou šířit dále, bez našeho vědomí, **mimo naši kontrolu**.

2. Jaké typy příspěvků mohou ostatní zraňovat?

Na jedné straně jsou to příspěvky, kde šlo původně spíš o **legraci** než o snahu někomu ublížit. V online světě se ale obsah velmi často dostává **mimo kontrolu pisatele, šíří se virálně** a může se stát předmětem zveličování, zneužití nebo zesměšňování.

Druhou skupinu tvoří příspěvky, které již přímo **obsahují různé druhy agrese: nadávky, urážky, zesměšňování, ponižování** nebo jde o **šíření ponižujících fotografií či videí**. Ty se pak mohou stát součástí **dlouhodobější** a **opakované kyberšikany** či dalších komplexnějších forem rizikového chování, včetně trestných činů (např. vydírání či vyhrožování).

Další skupinu představují **předsudečné nenávistné slovní projevy (hate speech)**, které jsou součástí tzv. předsudečných trestných činů (hate crime). Jejich cílem je **šířit strach a nenávist** vůči konkrétním osobám či skupinám osob, a to například na základě náboženského vyznání či rasy.

3. Proč někdo publikuje takový obsah?

V některých případech jde jen o **nevinný žert**. Velmi často však autoři vulgárních a násilných textů jednají pod vlivem **strachu, frustrace, obav** a **především neznalosti či neschopnosti ověřit si fakta**. Nenávistné texty také mohou sloužit k poškozování oponentů, jsou **nástrojem pomsty**.

Řada autorů publikuje nenávistné texty z ryze pragmatických důvodů: **oslovit co nejvíce uživatelů, získat nad nimi kontrolu a postupně je využívat k dosahování vlastních cílů**. Obvykle dobře vědí, že šíří lež a že vyvolají nenávistné reakce, přesto se neštítí násilné chování ve svém publiku (tj. mezi sledujícími a fanoušky) probouzet. Tento způsob komunikace se v posledních letech objevuje například v diskusních fórech různých politických stran a hnutí, známé jsou případy vyvolání nenávisti například vůči novináři Marku Wollnerovi a dalším redaktorům veřejnoprávních médií.

4. Existují nějaké zákonné hranice pro svobodu projevu na internetu a sociálních sítích?

Každý má právo na vyjádření svého názoru, které je zaručeno řadou dokumentů, například Všeobecnou deklarací lidských práv, Mezinárodním paktem o občanských a politických právech nebo třeba Listinou základních lidských práv a svobod.

Svoboda projevu však má své hranice, lze ji omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti. Jinými slovy: **svoboda projevu neznamená, že si můžeme říkat a psát cokoliv**.

Existuje řada trestných činů, které s komunikací a sdílením informací na internetu velmi úzce souvisejí a za které hrozí uživateli až vězení, například **pomluva, křivé obvinění, podněcování k nenávisti, projev sympatií k hnutí směřujícímu k potlačování práv a svobod člověka apod.**

Je důležité vědět, že se svobodou projevu se pojí i zodpovědnost.

5. Jsou v ČR známé nějaké postihy za závadné chování na internetu?

V minulosti již byla potrestána řada uživatelů, kteří hranice svobody projevu v online světě překročili. Tresty padly například za výhrůžky zpěváku Radoslavu Bangovi (Gipsy.cz), za výhrůžky spojené s kauzou tabla prvňáčků z Teplic či za vyhrožování smrtí v případu úmrtí Roma v pizzerii v Žatci.

Jako přestupky proti občanskému soužití pak byly řešeny další situace, například vyhrožování studentovi, který se účastnil výstražné stávky za zachování ústavních a společenských zvyklostí a hodnot. Policie a státní zástupci rovněž upozorňují, že se budou případy hate-crime, kterých přibývá, stále intenzivněji zabývat. Viz odkazy níže.

6. Mohou sociální sítě zahrnovat do podmínek užívání další pravidla týkající se toho, co je zakázáno publikovat? Musím je dodržovat?

Každý provozovatel sociální sítě si může určit pravidla, která budou regulovat, jak se v jeho prostředí mají uživatelé chovat a kde jsou limity jejich projevu.

Například sociální síť Facebook zakazuje sdílet:

- Nenávistné, agresivní a ponižující slovní projevy chápané jako přímý útok na lidi na základě rasy, sexuální orientace, pohlaví, nábo-

ženského přesvědčení či vážného tělesného postižení nebo choroby;
- obsah, který glorifikuje násilí, utrpení či ponížení jiných (tento obsah je s výjimkami povolen v případě, že je jeho cílem zvýšit povědomí lidí o určitých problémech, např. podmínky, ve kterých žijí zvířata ve velkochovech, porušování lidských práv apod.);
- obsah zobrazující nahotu dětí a dospělých či sexuální aktivity dospělých;
- sexuální návrhy a otevřené vyjadřování o sexualitě, které může vést k obtěžování;
- obsah pobízející k sebevraždě a sebepoškozování.

Při porušení těchto pravidel může následovat sankce, například krátkodobé či dlouhodobé omezení používání konkrétních služeb nebo zablokování účtu.

7. Co mohu dělat, když mě někdo na sociálních sítích zesměšňuje nebo uráží?

Možností, jak se bránit, je několik:

- Uchovávat si veškeré **důkazy** (SMS zprávy, zprávy z chatu nebo e-mailu, screenshoty, tj. fotografie obrazovky, odkazy na webové stránky), nic nemazat a vše si ukládat.
- **Ukončit komunikaci s útočníkem**, nemstít se, nevyhrožovat a neoplácet útoky, i když se nás útočník bude snažit vyprovokovat.
- **Blokovat útočníka** a obsah, který rozšiřuje. Můžeme kontaktovat poskytovatele služby, zablokovat přijímání útočníkových hovorů a zpráv, zamezit útočníkovi přístup k účtu oběti či ke stránkám, které ke svým útokům využívá.
- Pokud to oběť neohrozí, pokusit se **identifikovat pachatele** (např. podle profilu).
- **Oznámit útok dospělému** (rodič, učitel, trenér, vedoucí v kroužku), jemuž důvěřujeme. Nenechávat si to pro sebe a požádat o pomoc. Případně kontaktovat specialisty, organizace, poradny, policii. Příklady organizací, které se touto problematikou zabývají: E-Bezpečí, Buď safe online, Bezpečně na netu, O2 Chytrá škola apod.

8. Dají se publikované věci úplně smazat? Co mohu dělat, když už jsem publikoval/a nějaký nevhodný obsah?

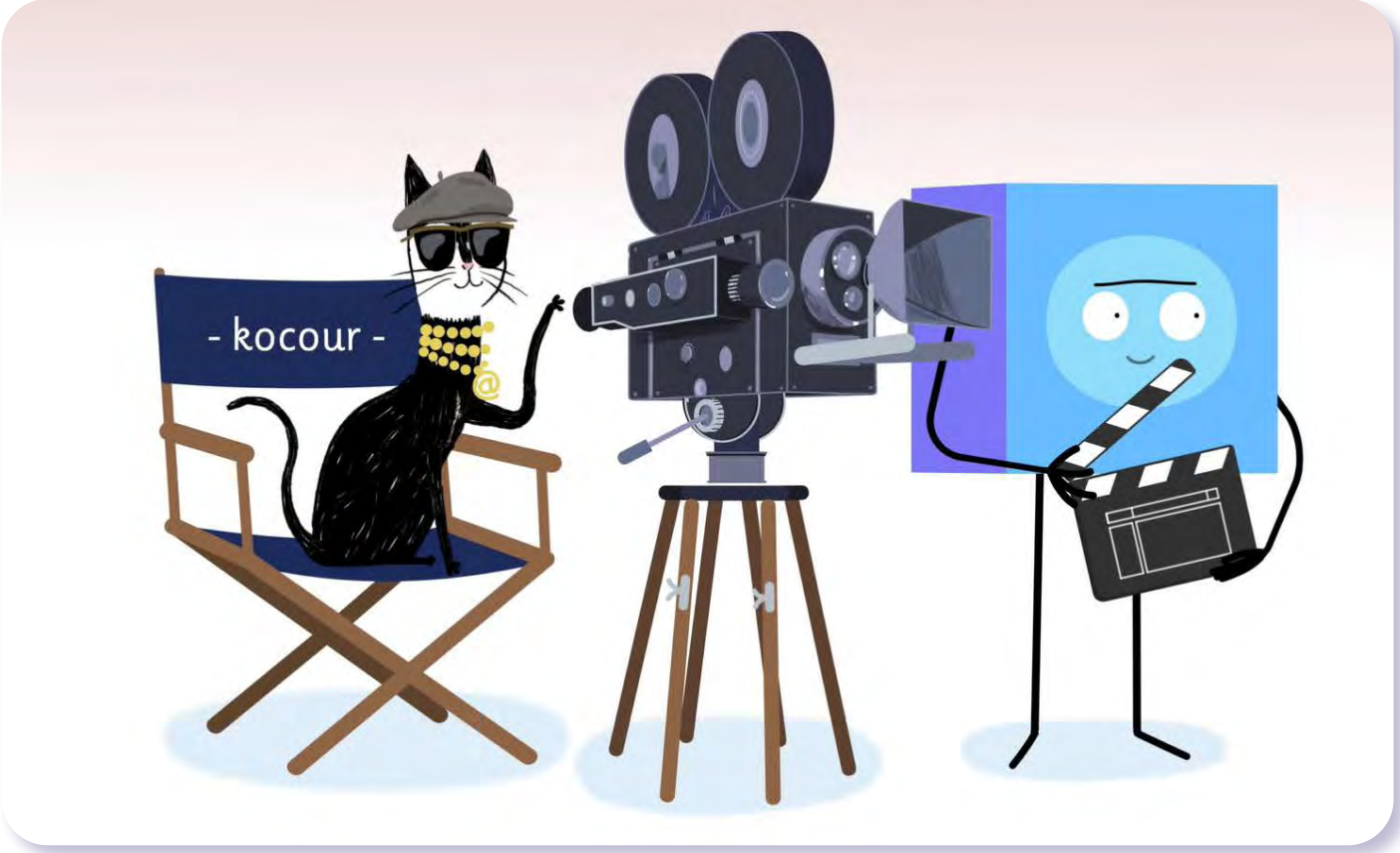
Je to jako s každým obsahem v online prostředí – přestože ho smažeme, nemůžeme si být stoprocentně jisti, že někde na internetu nekoluje. V online prostředí je velmi snadné kopírovat a rozmnožovat, a to v podstatě cokoliv. Proto je velmi důležité rozmyslet si, co vlastně budeme online publikovat a co se může vymknout naší kontrole. Pokud už se stane, že zveřejníme nevhodný příspěvek, měli bychom ho samozřejmě smazat a za své chování se omluvit.

Odpovědi vypracoval:

Kamil Kopecký, projekt E-Bezpečí, Univerzita Palackého v Olomouci

Navštivte lekci V digitálním světě: Jak mluvit na internetu na <jsns.cz/mv/jak-mluvit-na-internetu>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.

POZNÁMKY



V digitálním světě

Tvořit na internetu

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Mína a Filip tančí a zpívají ve videoklipu k narozeninám sestřenky Nity. Za kamerou sedí Kocour se svým bodrým okem zkušeného režiséra. Tvořit na internetu je dnes ve skutečnosti velmi snadné. Režisérem může být každý, kdo má telefon nebo tablet. Zbytek práce už udělají speciální aplikace, které dají amatérskému videu efektní kabát. Obtížnější už je však své dílo z internetu stáhnout, pokud nás třeba překvapí negativní reakce publika.

CÍLE LEKCE

1. seznámit se s možnostmi tvorby na internetu
2. uvědomit si úskalí, která mohou autora potkat
3. umět se rozhodnout, kde a kdy tvorbu uveřejnit

DOPORUČENÝ VĚK
8+ LET

AKTIVITA: Tvořit na internetu !!!

ANOTACE

Žáci si ve skupinách vyzkouší přípravy natočení videa. Vyberou si nebo vymyslí vlastní téma a námět videa, naplánují jeho přípravy – vytvoření scénáře i rozdělení rolí ve štábu. Zamyslí se nad možnostmi sdílet tvorbu na internetu a nad reakcemi uživatelů, které se mohou objevit.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k řešení problémů, komunikativní, sociální a personální, občanské

CÍLE

Žáci:
- zjistí, že dobré video vyžaduje nápad, dovednosti a úsilí
- si uvědomí úskalí, která mohou tvůrce potkat
- se seznámí s možnostmi internetu pro zveřejnění vlastní tvorby

DÉLKA

70 min. (včetně projekce)

POMŮCKY

- PRACOVNÍ LIST 1 a PRACOVNÍ LIST 2 do skupin
- papíry a psací potřeby do každé skupiny

POSTUP

1. Před projekcí se žáků zeptáme: *Sledujete YouTube nebo TikTok? Jaká videa vás zajímají? Vytvořili a zveřejnili jste někdy vlastní video?*
2. Společně se zamýšlíme nad **výhodami** (radost z tvorby a sdílení témat, nové dovednosti, zájem publika atd.) **a nevýhodami** (nesouhlas rodičů, kritické nebo urážlivé komentáře, odhalování soukromí atd.) zveřejňování videí na internetu. Postřehy žáků zapisujeme na tabuli a společně diskutujeme.
3. Následuje **projekce epizody seriálu**.
   Poznámka: Snímek doporučujeme zhlédnout nejméně dvakrát.
4. Krátce ověříme, zda žáci příběh pochopili, doporučujeme pamatovat i na reflexi emocí (*Jaké video připravovali Mína a Filip? Jak se u toho cítili? Sdíleli jej veřejně?*).
5. Žáky rozdělíme do skupin po pěti a rozdáme jim PRACOVNÍ LIST 1. Každá skupina vybere nejdříve **TÉMA videa a poté NÁMĚT**. Vybírají z nabízených možností nebo vymyslí vlastní.
6. V PRACOVNÍM LISTĚ 2 mají žáci za úkol ve skupině následně promyslet a specifikovat:
   - námět videa
   - přípravu na natáčení
   - role ve „štábu“
   - scénář, otázky

   Skupiny svoje náměty prezentují.

REFLEXE AKTIVITY

Ptáme se a diskutujeme: *Jak vám to šlo? Co vám připadalo snadné a co složitější? Co nejlepšího by se mohlo stát, kdybyste zveřejnili své video na internetu? Co nejhoršího by se mohlo stát?*
Vyzveme žáky, aby vyjmenovali **pravidla pro poučenou a bezpečnou tvorbu na webu**. Pravidla zapisujeme na tabuli.
Poznámka: Doporučujeme využít OTÁZKY A ODPOVĚDI k lekci.
Příklad pravidel:

1. Tvořit, ale nezesměšňovat.
2. Před zveřejněním video ukázat někomu, komu důvěřuji (rodičům, kamarádům).
3. Kritika může být přínosná.
4. Nikdy neuvádět žádné osobní údaje, své ani jiných lidí.
5. Zvážit publikování pod neutrálním jménem (nepoužívat občanské jméno).
6. Znát základní pravidla spojená s autorskými právy.
7. Vadilo by mi, kdyby se na video někdo podíval v budoucnu, až budu dospělý?

Poznámka: Aktivitu je možné zvládnout za jednu vyučovací hodinu, doporučujeme ale počítat spíš s její větší časovou náročností a nechat žákům čas na přípravu námětů a diskusi.

ZKUŠENOSTI Z PRAXE

Žáci v pátém ročníků již téměř všichni dobře znají videoprostředí na internetu, dobře se orientují ve výhodách a nevýhodách zveřejňování videí.
Nové pro mnohé žáky byly informace o právních souvislostech (např. z hlediska autorských práv). Mezi výhodami publikování videí z pohledu žáků je jasně na prvním místě zisk a sláva, teprve dlouho poté je jako výhoda uváděno potěšení a vlastní zábava pro svou osobu a své blízké. Z nevýhod jsou jasné největší obavy z kritiky a parodií své práce. Nejoblíbenějším tématem chlapeckých týmů byl „prank“, s námětem zesměšnění kamaráda – ovšem, byla to dobrá půda pro diskusi nad bezpečností a ochranou soukromí, například že s umístěním videa by musel kamarád souhlasit. Pro první stupeň ZŠ jako důležité vidím taky epizody Sociální sítě a Lajky.
Pavel Mikoláš, *ZŠ Benešova, Třebíč*

POZNÁMKY

PRACOVNÍ LIST 1

Vyberte si nejdříve TÉMA videa a poté NÁMĚT. Vybírejte z nabízených možností, nebo vymyslete vlastní.

TÉMA	NÁMĚT 1	NÁMĚT 2	VLASTNÍ NÁMĚT
Komentovat a recenzovat počítačovou hru	hra nebo aplikace s tematikou matematiky, angličtiny, Sluneční soustavy…	vymyšlená, zatím neexistující hra	
Recenze knížek nebo hraček	encyklopedie zvířat	robotická stavebnice	
TOP 5	top 5 učitelů školy	top 5 nejlepších míst školy	
Rozhovor	se spolužákem o netradičním sportu nebo koníčku	rozhovor s rodičem o jeho práci	
Challenge	dvojboj – kdo nejrychleji zvládne vyjmenovaná slova po P, k tomu násobky tří do třiceti	vyběhnout třikrát do prvního patra a zpět	
Tutoriál	jak začít s Minecraftem	návod na experiment	
Beauty videa	jak se nalíčit na haloweenskou školní oslavu	jak se líčit za anděla a čerta	
Prank	skrytá kamera: před vyučováním před školou tvrdit příchozím, že je škola zavřená	skrytá kamera: spolužákovi nenápadně nalepíme na záda nápis „Obejmi mě“ a sledujeme reakce	
DIY	videorecept na palačinky	návod na pletené gumičkové náramky	

PRACOVNÍ LIST 2

Ve skupině promyslete a zapište:

PŘÍPRAVA NA NATÁČENÍ

Co budeme potřebovat? Jakou máme techniku? Co musíme připravit/udělat před natáčením?

ROLE VE ŠTÁBU

Kdo bude točit? Kdo bude mluvit? Budeme video po natáčení upravovat, stříhat? Které další role ve štábu vás napadají?

SCÉNÁŘ

Jak budeme postupovat krok za krokem? Co přesně budeme snímat? Jaké budeme pokládat otázky?

OTÁZKY A ODPOVĚDI

1. Kde můžeme sdílet na internetu vlastní autorský obsah (hudbu, texty, fotky, videa)?

Web 21. století je z velké části tvořený **platformami, které uživateli umožňují zdarma sdílet obsah s ostatními a následně vydělávají na cílené reklamě**. Světově nejvýznamnějším videoportálem je Googlem vlastněný **YouTube,** a ačkoliv i mnohé jiné **služby sdílení videa** umožňují, nemá v oblasti videí zásadní konkurenci.

Pokud jde o krátká zábavná videa, těší se mezi mladými největší popularitě aplikace **TikTok** (jejíž součástí se stala i dříve velice populární aplikace Musical.ly). Oblíbeným kanálem pro sdílení kratších videí jsou také po 24 hodinách mizící **Stories** na Instagramu. Samotný **Instagram** je nejpopulárnější sociální sítí zaměřenou na fotografie a v dnešní době jde pravděpodobně o vůbec nejvýznamnější síť pro influencery (tj. uživatele, kteří mají vysoký počet sledujících, a tím i velký vliv).

Nejoblíbenější tzv. mikroblogovací platformou (tedy místem pro sdílení krátkých, primárně textových příspěvků) je **Twitter**.

Řada lidí píše svoje **blogy** (články), které je možné publikovat na některých zpravodajských portálech (např. iDNES), na blogovacích platformách (**Blogger.com** od Google) nebo si můžete založit vlastní blog (nejznámějším a nejrozšířenějším redakčním systémem pro blogy je **WordPress**). Hudebníci, kteří svůj obsah nechtějí sdílet rovnou s videoklipem na portálu YouTube, mohou využít například oblíbené služby **SoundCloud**.

2. Od kterého věku je možné publikovat na sociálních sítích vlastní videa?

Celosvětově obvyklou **minimální hranicí pro založení účtu** na některé ze sociálních sítí je **13 let**. Tento limit v podmínkách uvádějí například Facebook, Instagram nebo TikTok. **Google** má **pro Českou republiku** dokonce stanovenou minimální hranici **15 let**, a ta tím pádem platí i pro jeho službu YouTube. Mladšímu dítěti mohou YouTube účet založit **rodiče** a následně jej spravovat skrz aplikaci **Family Link**. Nemožnost založit účet ale nebrání uživateli sledovat obsah, pouze nemůže přidávat svůj vlastní (zveřejňovat videa, přidávat komentáře nebo lajky). **Sociální sítě navíc zadaný věk neověřují** a mladší uživatelé běžně uvádějí smyšlená data narození, která odpovídají věku vyššímu.

3. Které aplikace nebo programy pro tvorbu videí nebo úpravu fotek by se daly doporučit dětem?

Známý profesionální nástroj k **úpravě fotografií** – **Adobe Photoshop** – je k dispozici pouze za poměrně vysoké měsíční předplatné. Kvalitní profesionální alternativou může být software **Affinity Photo**, který je možné trvale zakoupit za cenu cca dvou měsíců předplatného Photoshopu a který nabízí velmi podobné funkce i prostředí.

Zcela zdarma jsou k dispozici například **GIMP** nebo **Paint.net**, případně aplikace **Photopea**, kterou není ani nutné instalovat, neboť běží přímo v internetovém prohlížeči.

Na **střih, barvení a další úpravy videa** zdarma je nejlepší volbou profesionální software **DaVinci Resolve**. Velmi populární alternativou je (opět měsíčně zpoplatněný) **Adobe Premiere**. V obou případech však jde o profesionální nástroje, jejichž složitost může nepřipraveného začátečníka spíš odradit.

Dostatečné **základní nástroje** (a jednodušší rozhraní) nabízejí programy **iMovie** (k dispozici pro mobilní i desktopová zařízení Apple), již trochu starší **Windows Movie Maker**, případně opensourcový **OpenShot** (Windows, OS X, Linux).

Střih videa je ideální zpracovávat na počítači, ale existují i mobilní aplikace, které umožňují alespoň základní úpravy. Kromě zmíněného iMovie pro iOS jsou to například androidové aplikace KineMaster, FilmoraGo, ActionDirector Video Editor, případně Adobe Premiere Rush, který je ale také poměrně drahý.

4. Na co si dát při natáčení videí pozor?

Automatické systémy portálů jako YouTube v rámci možností důsledně **kontrolují přítomnost autorsky chráněného obsahu**. Není tedy možné do vlastního videa například jako podklad použít libovolnou oblíbenou písničku, autoři musí **využívat hudby k tomuto účelu zdarma zpřístupněné** – například přímo v prostředí YouTube na youtube.com/audiolibrary nebo youtubery často využívané tvorby Kevina MacLeoda na webu incompetech.com.

To samé platí i pro audiovizuální materiál – **není možné na internet nahrávat filmy a seriály z televize, cizí videoklipy atd.** Americká legislativa má sice ustanovení zvané „**Fair Use**“, které dovoluje v určitých případech využít chráněného díla i bez souhlasu držitele autorských práv, je to například kritika, komentář, parodie, novinářské zpravodajství atd. Pohybovat se „na hraně“ je ale vždy trochu riskantní, neboť podmínky platformy i přístup k jejich vynucování se v čase vyvíjí (a takovým videím hrozí, že budou odstraněna).

I kdyby se tvůrci videa podařilo nahrát na server video s autorsky chráněnou hudbou a video tedy úspěšně prošlo všemi „filtry“, může k odhalení dojít kdykoliv v budoucnu. V lepším případě by odhalení mohlo znamenat, že **výdělky z reklamy videa půjdou původnímu autorovi** hudby, v horším může dojít na **smazání videa** nebo na sankce za **porušení autorských práv** (tzv. copyright strikes). Kritéria se navíc mohou kdykoliv změnit a na obsah se uplatňují i **retrospektivně**. Běžně dochází k hromadnému odstraňování obsahu, který byl dříve povolený.

5. Je možné publikovat videa zachycující jiné lidi bez jejich souhlasu?

Občanský zákoník uvádí, že o porušení práva osoby na ochranu soukromí rozhoduje především to, **jestli osoba k takovému jednání dala svolení**, respektive jestli **dala jasně najevo svůj nesouhlas** (musí o pořizování záznamu samozřejmě vědět). Udělit svolení může i mlčky tím, že se proti pořízení záznamu neohradí, tím umožňuje automaticky i následné šíření záznamu.

Složitější situace nastává, když jde o **činnost systematickou a výdělečnou**, neboť v některých případech namísto občanského zákoníku vstupuje do hry **regulace GDPR**. V obou případech má však zaznamenaná osoba vždy **právo svůj souhlas dodatečně odvolat** a domoci se odstranění videozáznamu – v tomto ohledu je pořizování záznamů jiných lidí vždy riskantní.

6. Jak reagovat na nenávistné komentáře k vlastní tvorbě?

Tvůrce obsahu jde vždy „s kůží na trh" a anonymita internetu dodává kritikům odvahu napsat v komentářích věci, které by tvůrci přímo do očí nikdy neřekli. Dává prostor k vyjádření i „trollům", kteří přišli pouze ublížit nebo si spravit náladu ponižováním druhého – s tím vším je při publikování obsahu online třeba počítat. Stává se to i těm největším a nejúspěšnějším a v **některých případech je lepší vůbec nereagovat**.

Mnozí influenceři sice nemohou zpětnou vazbu publika zcela ignorovat a komentáře například nečíst, ale je třeba, aby se tvůrce naučil v kritice najít to důležité a nezatěžoval se lacinými nenávistnými komentáři. Nemá smysl „krmit trolla" a hádat se s někým, kdo tvůrce přišel spíš virtuálně šikanovat. Neznamená to však číst pouze pozitivní komentáře. Znamená to **učit se rozeznávat konstruktivní kritiku (která pomáhá ke zlepšení) a nepouštět si k tělu samoúčelnou negativitu**.

Neexistují jednoduché odpovědi a jednoduché cesty – i zkušeného veterána může občas ošklivý komentář zaskočit. Měl by však mít dost rozumu nepouštět se s komentujícím do nelítostné hádky, byť online. Na YouTube je možné **komentáře** konkrétního uživatele v rámci celého kanálu **skrýt**, **nahlašovat nevhodné**, případně všechny komentáře pod konkrétním videem **podřídit schvalování** (nezobrazí se, dokud je vlastník kanálu neschválí) nebo je **úplně zakázat**.

7. Kteří influenceři jsou nejoblíbenější mezi dětmi ve věku 8–12 let?

Čeští **influenceři** zaměřující se na děti nejčastěji patří do kategorie **youtuberů** (jejich hlavní tvorbu najdeme na YouTube), ale obvykle mají i velmi úspěšné profily na **Instagramu** (a dnes i **TikToku**), které používají pro každodenní komunikaci se sledujícími. Oblibě se těší **letsplayeři** (hráči počítačových her) jako Ment, Gejmr, Pedro, Baxtrix, House, Wedry nebo FattyPillow.

Spíše na dívky cílí Anna Šulc, Týnuš Třešničková nebo Lea a další. K dalším velmi populárním tvůrcům mezi mladými diváky patří VladaVideos, Jmenuju Se Martin nebo Kovy (doporučovaný pro kvalitní obsah). Naopak kontroverzemi prosluli třeba TvTwixx, Fizi nebo Tary.

8. Jak mohou influenceři ovlivňovat okolí?

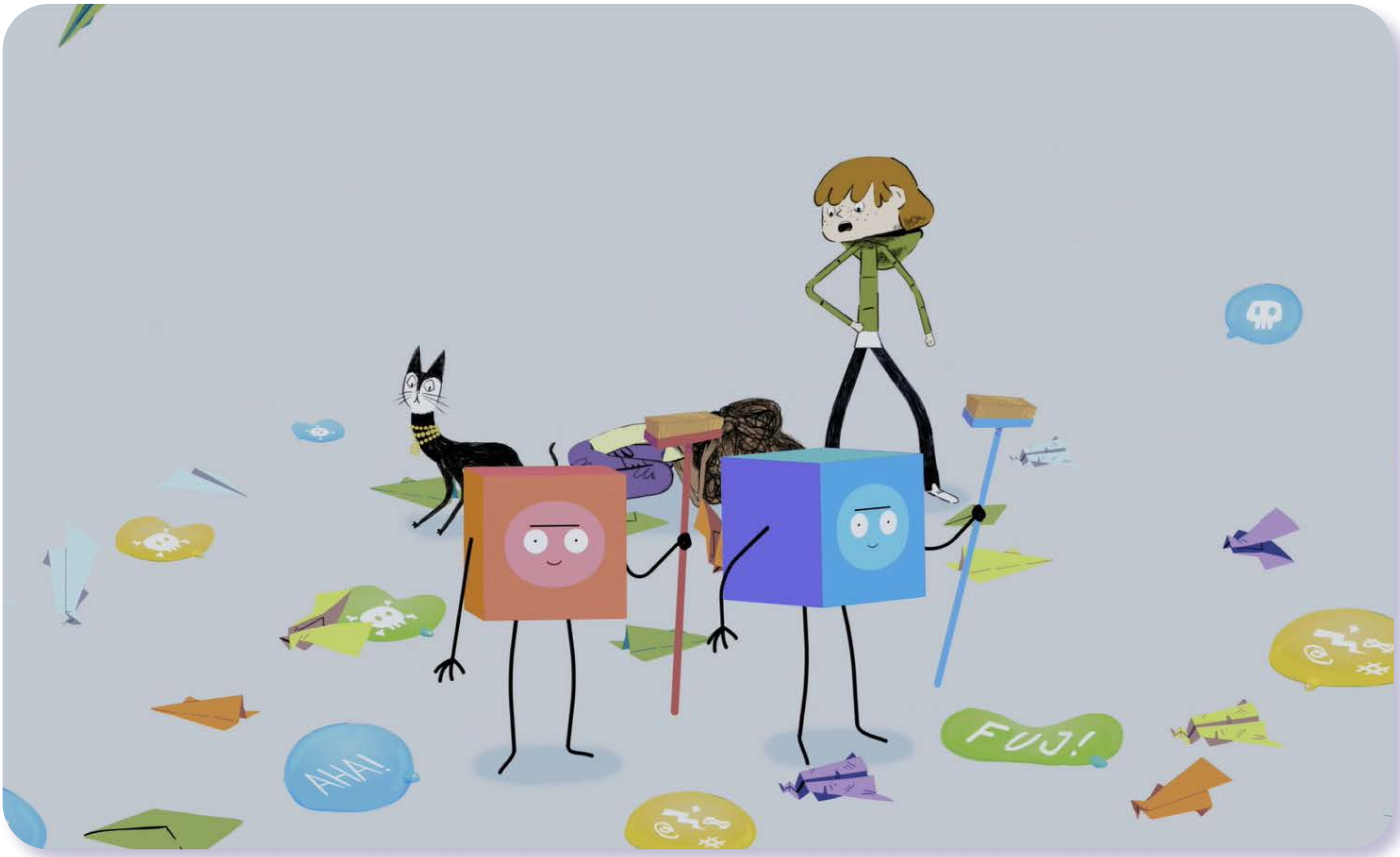
Nejčastěji medializovaná je **role influencerů v reklamě**, kde formou spolupráce se značkami pomáhají prodávat produkty, resp. různým způsobem ovlivňovat spotřební chování svých sledujících. **Mohou ale významně ovlivňovat** i jejich **názory, hodnoty nebo politické přesvědčení**. Je jen na influencerovi, jakou cestou se vydá. Může propagovat alkohol, elektronické cigarety a ve videích se pohybovat na hraně zákona, nebo naopak vyzdvihovat zdravý životní styl a zábavnou formou seznamovat diváky s krásami antické filozofie.

Sociální sítě jsou pouze platformy – nástroje. Je jen volbou tvůrce, jakým způsobem je použije (za předpokladu dodržení podmínek dané platformy a platných zákonů). Mladí influenceři si často vůbec neuvědomují svůj hodnotový vliv na děti a dospívající, nepřemýšlí o něm nebo nevědí, jak s ním vhodně naložit. Někteří z nich se zajímají pouze o to, jak získat zhlédnutí a lajky (tedy dát divákům co chtějí), případně peníze za spolupráci se značkami.

Odpovědi vypracoval:
Jakub Sedláček, Studia nových médií, Filozofická fakulta Univerzity Karlovy

Navštivte lekci V digitálním světě: Tvořit na internetu na <jsns.cz/mv/tvorit-na-internetu>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.

POZNÁMKY



V digitálním světě

Kyberšikana

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Mína dnes není ve své kůži. Filip nechápe, proč nechce soutěžit o nejhezčí fotku na internetu a neotevírá žádné zprávy. Udělá to za ní a v tom je zasype lavina „hejtů" na Mínino adresu. Na rozdíl od klasické šikany, oběť kyberšikany může být pod nenávistnou palbou 24 hodin denně. Vyřešit komplikovanou situaci pomůže především podpora dospělých a přátel. Svěřit se s trápením lidem, kterým důvěřujeme, je klíčové, stejně jako nemlčet v případě, že se staneme svědkem kyberšikany.

CÍLE LEKCE

1. seznámit žáky s pojmem kyberšikana a jejími podobami
2. osvojit si postupy, jak reagovat, když se staneme obětí či svědkem kyberšikany
3. uvědomit si, jaké chování může ubližovat

DOPORUČENÝ VĚK
8+ LET

AKTIVITA: Kyberšikana !!!

ANOTACE

Žáci se seznámí s pojmem kyberšikana a jejími projevy. Uvědomí si, jaké negativní prožívání se s ní pojí. Pomocí názorných příkladů sdílí ve skupinách svoje návrhy, jak situaci spojenou s kyberšikanou řešit. Třída společně reflektuje pravidla, která je dobrá znát jak z pozice oběti, tak svědka kyberšikany. Žáci se také dozví o anonymních možnostech podpory, kterou nabízí školní schránky důvěry, linky důvěry nebo online aplikace.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k řešení problémů, komunikativní, sociální a personální, občanské

CÍLE

Žáci:
- se seznámí s pojmem kyberšikana a jejími podobami
- si uvědomí, že internet nabízí nejen zábavu a poučení, ale jsou na něm i agresivní uživatelé
- se dozví, jak postupovat, když se stanou terčem nebo svědkem kyberšikany

DÉLKA

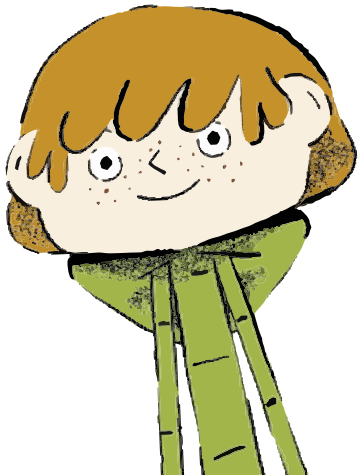
45 min. (včetně projekce)

POMŮCKY

- lepicí lístky, tužka, nůžky
- rozstříhaný PRACOVNÍ LIST
- tabule nebo flipchart

POSTUP

1. V úvodu hodiny položíme žákům otázku: *Proč si myslíte, že dospělí chtějí vědět, co na internetu děláte?* Odpovědi zapisujeme na tabuli.
2. Následuje **projekce epizody seriálu**.
3. Po projekci ověříme porozumění epizodě. Zaměříme se nejen **na příběh** (obsah epizody), ale také **na emoce, které mohou projekci doprovázet**. Do třídy rozdáme lepicí lístky. Požádáme žáky, aby každý na svůj lístek napsal, jak se Mína cítila nebo co si myslela (např. Myslela si, že to nikdy neskončí. Cítila se zoufalá apod.).
   Žáci lístky nalepí na tabuli a společně je přečteme a reflektujeme. Ptáme se: *Co se stalo Míně? Jak se cítila a proč? Co dělaly ostatní postavy? Jak jste se u sledování cítili? Cítila se Mína na konci příběhu jinak? Proč?*
   Poznámka: Pokud je to potřeba, **projekci epizody zopakujeme**.
4. Soustředíme se na pojem **kyberšikana**. Ptáme se žáků: *Dokážete uvést příklad jiné situace, kdy je někomu psychicky ubližováno v digitálním prostředí? Neboli kdy jde o opakovanou psychickou šikanu, která člověku ubližuje, zesměšňuje ho či ztrapňuje?*
   Poznámka: Doporučujeme využít materiál OTÁZKY A ODPOVĚDI k lekci, který obsahuje odborné informace pojící se s probíraným fenoménem.
5. Třídu rozdělíme do pěti skupin. Rozstříháme PRACOVNÍ LIST a každé skupině přidělíme **jednu situaci**. Žákům necháme čas přemýšlet o popsaných situacích a na diskusi ve skupině. Úkolem je ke konkrétním popsaným případům ve skupině promyslet:
   a/ jak se bude situace dál vyvíjet
   b/ jaká opatření by bylo možné udělat



REFLEXE AKTIVITY

V reflexi se zaměříme na analýzu odpovědí žáků k jednotlivým situacím, na jejich postřehy a doporučené postupy. Zapisujeme na tabuli. Společně vyvodíme **zásady, jak se ke kyberšikaně stavět** a co je možné udělat. Upozorníme, že kroky se týkají jak **oběti, tak svědků** kyberšikany.

Pokud to v diskusi nezazní, zdůrazníme tato pravidla:

- **Říct o problému dospělému, kterému důvěřuji** (rodič, vychovatel, trenér, babička, učitel/ka...).
- **Ponechat si důkazy** – nic nemazat.
- **Problém je lepší řešit** než (třeba ze strachu) nic nedělat.
- Pokud je člověk **svědkem kyberšikany, kamaráda/kamarádku podpoří** a pomůže mu/jí situaci řešit.

Další možnosti:

- V případě, že ji škola provozuje, upozorníme žáky na možnost použít schránku důvěry pro anonymní hlášení.
- Ve třídě je možné stabilně umístit:
  - Kontakt na bezplatné **linky důvěry** (např. Linka bezpečí – tel.: 116 111).
  - Odkaz na stránky iniciativy zaměřené na anonymní online řešení případů (kyber)šikany: **Nenech to být (nntb.cz)**.
  - Jméno a kontakt na **školního psychologa**.

Reflexi můžeme uzavřít tím, že na internetu chceme prožívat pozitivní emoce, ne negativní.

ZKUŠENOSTI Z PRAXE

S aktivitou jsem začala v páté třídě, vše jsme měla nachystané. Zvládli jsme začátek, u lístečků, kde měli žáci psát ty pocity, mi jeden kluk řekl: „Co když si to ani nemusím představovat, jak se ta postava cítila.“ To mě dost zaskočilo, ale zeptala jsem se, jak to myslí. Otevřeně řekl, že jeden kluk ze třídy dává na web videa, kde o něm nehezky mluví apod.
Nečekala jsem, že mi něco takové řekne. Takže jsem následně reagovala na to, co řekl, a využila toho. Samozřejmě po hodině už jsem to řešila s třídní a rozjel se kolotoč.
Jana Machovská, *ZŠ Liptál*

PRACOVNÍ LIST

Zamyslete se nad popsanými situacemi a zkuste si představit, jak by se situace mohla dál vyvíjet.

1.

Vaši kamarádku spolužáci vyfotili v hloupé pozici a nyní si fotografii přeposílají a píšou k ní nepříjemné komentáře.

Řekli byste o situaci rodičům nebo jinému dospělému?

Co by šlo ještě udělat?

Jak byste se zachovali, kdyby se situace týkala přímo vás?

2.

Vašeho kamaráda natočili na telefon, když ho spolužáci bili, a umístili video na sociální síť (např. TikTok).

Řekli byste o situaci rodičům nebo jinému dospělému?

Co by šlo ještě udělat?

Jak byste se zachovali, kdyby se situace týkala přímo vás?

3.

Vaše kamarádka se na sociální síti seznámila s neznámým klukem, líbí se jí a poslala mu fotku v plavkách. Kluk chce, aby to neříkala rodičům a sešla se s ním.

Řekli byste o situaci rodičům nebo jinému dospělému?

Co by šlo ještě udělat?

Jak byste se zachovali, kdyby se situace týkala přímo vás?

4.

Váš spolužák zjistil, že mu někdo zničil jeho stavby v Minecraftu.

Řekli byste o situaci rodičům nebo jinému dospělému?

Co by šlo ještě udělat?

Jak byste se zachovali, kdyby se situace týkala přímo vás?

5.

Zjistili jste, že spolužáci vytvořili urážející a zesměšňující video o učiteli a chtějí ho zveřejnit.

Řekli byste o situaci rodičům nebo jinému dospělému?

Co by šlo ještě udělat?

Jak byste se zachovali, kdyby se situace týkala přímo vás?

OTÁZKY A ODPOVĚDI

1. Co je kyberšikana?

Termínem **kyberšikana** označujeme **psychickou šikanu v digitálním prostředí**, která má za následek **ublížení, zesměšnění, ztrapnění nebo jiné poškození oběti**. Probíhá pomocí **informačních a komunikačních technologií** (např. pomocí mobilu nebo sociálních sítí).

2. Jaké může mít kyberšikana formy?

Kyberšikana může existovat ve dvou základních podobách:

- **Kyberšikana přímá** – **útočník přímo na svou oběť s pomocí IT nástrojů útočí** (např. nasdílí na sociální sítě ponižující foto, založí o někom dehonestující stránku či skupinu atd.).
- **Kyberšikana nepřímá** – probíhá **prostřednictvím jiných osob**, **které útočník zneužívá k útokům na oběť**, například o oběti rozšířil nepravdivé zprávy a motivoval tak ostatní k online útoku.

Kyberšikana může mít mnoho podob, mezi ty nejčastější patří:

- **Zasílání urážlivých a zastrašujících zpráv či pomluv** (např. přes SMS, v chatu, na sociálních sítích, na blozích apod.).
- **Vytváření internetových stránek, které urážejí, pomlouvají či ponižují** osobu nebo skupinu osob (např. falešné profily na sociálních sítích, zesměšňující skupiny a webové stránky apod.).
- **Pořizování zvukových záznamů, videí či fotografií** a jejich následné zveřejňování s cílem poškodit zachycenou osobu (např. sdílení nevhodné fotografie na sociálních sítích, natáčení a zveřejňování fyzického útoku, natáčení učitele apod.).
- **Krádež identity a její zneužití** (např. zcizení elektronického účtu a rozesílání nevhodných zpráv jménem majitele účtu apod.).
- **Provokování a napadání uživatelů v online komunikaci** (např. v rámci komentářů na sociálních sítích; nenávistným komentářům se říká také „hejty“).
- **Zveřejňování cizích tajemství s cílem zesměšnit oběť** (např. na sociálních sítích, blozích apod.).
- **Obtěžování a pronásledování voláním**, **psaním zpráv nebo prozváněním** (tzv. kyberstalking).
- **Vyloučení z virtuální komunity** (např. ze skupiny přátel v rámci sociální sítě).
- Speciální formou je pak kyberšikana **spojená s online hrami**, kde může docházet například ke krádeži herních postav, krádeži herních účtů, různým druhům podvodů, ničení vytvořených staveb (tzv. griefování) apod.

3. Proč ke kyberšikaně dochází? Co vede agresory k takovému chování?

Motivů pro páchání kyberšikany může být celá řada:

- **Pomsta** – kyberšikanu může páchat i ten, kdo byl šikanován v reálném světě a v tom virtuálním se snaží pomstít, oplatit bolest, kterou si sám prožil.
- **Nuda** – pro znuděného agresora představuje kyberšikana určité vzrušení, kterého se mu v životě nedostává. Je pro něj únikem a formou zábavy.
- **Skupinový tlak** – člověk se stane pachatelem, protože chce zapadnout do kolektivu, ve kterém je kyberšikana běžná a probíhá hromadně. Pod vlivem skupinového tlaku je pak schopen dělat to, co by sám od sebe neudělal.
- Projev **sociálního postavení** – slouží k posilování vlastní pozice a oslabování pozic druhých, kteří se stávají terčem útoků.
- **Anonymita internetu** – pachatelé věří, že je nelze vystopovat a chytit. Navíc nevidí reakci oběti, což jim usnadňuje dělat věci, které by v běžném životě nedělali.
- **Nedostatek empatie** – pachatel nevidí bolest a reakci oběti, a proto nemá ani výčitky svědomí a kyberšikanu vnímá naopak jako skvělou zábavu.
- **„Nevinný“ žert**, co se vymkl kontrole a začal si žít vlastním životem – pachatel nechtěl oběti ublížit a domníval se, že jde jen o neškodnou zábavu. Příkladem může být vtipné video, které unikne mimo uzavřenou skupinu, začne se šířit, sbírá negativní komentáře a další lidé si jej mezi sebou rozesílají pro pobavení.

4. Kdo je nejčastěji obětí kyberšikany?

Obětí kyberšikany může být **kdokoliv bez ohledu na věk**, pohlaví, zaměstnání, fyzickou sílu či oblíbenost v kolektivu. Tyto aspekty mohou hrát roli při komunikaci tváří v tvář, avšak **ve virtuální komunikaci nemají takový význam**.

Mezi společné znaky obětí kyberšikany můžeme řadit to, že **tráví více času na internetu, kde jsou také aktivní** (sdílejí o sobě hodně informací, aktivně využívají sociální sítě), a logicky pak roste příležitost, že se stanou potenciálním terčem útoku (zpravidla od svých spolužáků). Velkou roli hraje také přehnaná důvěra, kterou si mnozí útočníci umí od obětí získat. Oběti obvykle bývají **málo seznámeny s riziky spojenými s digitálním světem**, a proto se na internetu chovají méně opatrně. Může se také stát, že **oběť tradiční šikany** (tedy oběť šikany v reálném prostředí) se často stává **obětí kyberšikany**.

Existují určité charakteristiky, které riziko, že člověk může být šikanován, zvyšují. Může sem patřit třeba tělesný hendikep, psychické znevýhodnění (hyperaktivita, poruchy učení apod.), odlišnost od skupiny (např. rasová odlišnost, nízký socioekonomický status rodičů apod.). Oběťmi se mohou stát premianti třídy, ale také „zlobivé“ děti.

5. Jaké může mít kyberšikana na oběť dopady?

Dopad na oběť může být **i větší než u klasické šikany**, a to z několika důvodů. Během kyberšikany **nedochází k osobnímu kontaktu** útočníka s obětí. To může vést k tomu, že se bude útočník chovat **mnohem agresivněji a impulzivněji**, protože nevidí reakci oběti a to, jak moc jí ubližuje. Roli zde sehrává i **zdánlivá anonymita** útočníka, který si myslí, že je nedohledatelný, pokud vystupuje pod falešnou či skrytou identitou. Oběť pak může propadat beznaději, protože neví, jak se anonymnímu útočníkovi bránit.

Také **dopad** vlivu něčeho, co je zveřejněno **na internetu, trvá mnohem déle**, než například pomluva v reálném světě, na kterou se velmi rychle zapomene. Stačí, když si zesměšňující materiál stáhne jeden člověk, a kyberšikana může vypuknout znovu.

6. Kdo s kým se na sociálních sítích propojuje? Existují nějaká rizika?

Propojit se můžeme v podstatě **s jakýmkoliv uživatelem** dané sociální sítě, **aniž bychom ho znali nebo osobně potkali**. V případě, že s námi naváže kontakt **neznámý člověk**, měli bychom být velmi **obezřetní** a ověřit si, zda se nejedná o falešný účet, který si může snadno založit kdokoliv. Také internetoví predátoři si mohou vytvářet falešné profily s fotkami a údaji našich přátel, aby působili věrohodněji. Pomůže, když si ve svém účtu vypneme **viditelnost** našich přátel pro ostatní uživatele dané sociální sítě. Měli bychom myslet na to, že **nikdy nemáme jistotu, kdo sedí na druhé straně**.

Důležité je také hlídat, kdo sleduje nás. Svůj účet si nastavme tak, aby **nebyl veřejný** a mohli jsme sami schvalovat, kdo nás může a nemůže sledovat.

7. Jaký obsah bychom neměli na sociálních sítích sdílet? Proč?

Na sociálních sítích bychom **neměli sdílet osobní a citlivé informace**, jako je náš **věk, místo bydliště, telefonní číslo, kam chodíme do školy, kde pracují členové rodiny** apod. Tyto informace mohou velmi snadno zneužít internetoví predátoři. Když například zveřejníme místo svého bydliště, může predátor začít vyhrožovat, že ublíží nám a naší rodině, pokud neuděláme, co po nás chce.

Neměli bychom sdílet ani naše **intimní fotografie či videa**. Pokud se k tomuto materiálu někdo dostane, získává nad námi moc a může nás začít šikanovat nebo vydírat. Rodiče by zase měli myslet na to, že fotografie jejich dětí (např. nahé fotky v bazénku) mohou být zneužity a šířeny predátory jako dětská pornografie.

Na sociální sítě nepatří informace o **naší domácnosti, o jejím vybavení nebo kdy odjíždíme na dovolenou**. Tyto informace jsou pozvánkou pro zloděje, kteří mohou vykrást náš byt či dům ve chvíli, kdy nejsme doma.

Rozhodně bychom neměli sdílet **nevhodné fotografie** (ať už svoje, nebo druhých osob). Jedná se o fotografie, které nás zachycují při nelegálním chování (např. nelegální pití alkoholu, porušování rychlosti při jízdě autem apod.) nebo v nedůstojné situaci (např. v opilosti).

Hlídat bychom si měli také **geolokační informace**, jinak každý může vědět, kde se zrovna nacházíme.

8. Co dělat, když někdo sdílí fotky se mnou a já nechci, aby byly veřejné?

V případě, že byly fotky už zveřejněny, toho moc nezmůžeme. Můžeme **požádat osobu**, která fotky sdílela, aby je smazala. Avšak nemáme žádnou jistotu, že si fotografie někdo nestáhl a neuložil. Danou osobu můžeme upozornit, že si pro příště nepřejeme, aby fotografie sdílela bez našeho souhlasu.

Na mnohých sociálních sítí může nastavit, aby zveřejněná fotografie byla soukromá (viditelná jen pro naše přátele), a nikoliv veřejná. Kdyby se nám nelíbila fotografie, na které nás někdo označil, můžeme označení odebrat. Obecně ale platí, že i nastavení soukromí může nějaký útočník prolomit a cokoliv, co je jednou umístěné na internet, tam může být už „navždycky“.

Další možností je **závadný obsah na dané sociální síti nahlásit**. Tuto možnost dnes nabízejí v podstatě všechny sociální sítě. Pokud se pak jedná o vyloženě závadné materiály (dětská pornografie), případně nám někdo prostřednictvím těchto materiálů vyhrožuje nebo nás vydírá, **můžeme se také obrátit na Policii ČR**.

9. Jak se můžu bránit, když mě někdo šikanuje?

Pokud se staneme terčem kyberšikany, je potřeba snažit se zachovat klid a promyslet si, jak postupovat. Děti by se měli svěřit **někomu dospělému**, ideálně rodičům. Co dělat v situaci, když jsme terčem či svědky kyberšikany:

- **Sbírejte důkazy** – dohledejte a schovejte si veškeré důkazy kyberšikany. Udělejte si fotografie a kopie e-mailů, zpráv z chatu, SMS, fotografií, videí, příspěvků na sociálních sítích, odkazů na webové stránky, vše si pečlivě uložte.
- **Ukončete komunikaci s útočníkem** – nevyhrožujte a nemstěte se mu. Nesnažte se jej od jeho jednání odradit. Pokud budete reagovat, útočník bude rád, že vás vyprovokoval.
- **Zablokujte útočníka a obsah, který rozšiřuje** – zamezte útočníkovi přístup k dané službě (kontaktujte poskytovatele služby, zablokujte si přijímání útočníkových zpráv nebo hovorů, změňte svou virtuální identitu).
- **Útok vždy oznamte** – svěřte se blízké osobě, ideálně někomu dospělému, kterému věříte. Když vám někdo ubližuje, nenechávejte si to pro sebe.
- Nebojte se **vyhledat pomoc specialistů** – pokud je to potřeba, kontaktujte policii nebo pedagogicko-psycho-

logickou poradnu. Využít můžete i pomoci od anonymních internetových poraden (např. napisnam.cz, Dětské krizové centrum apod.).
- **Žádejte konečný verdikt** – pokud kyberšikanu řešíte ve škole, třeba s učitelem, školním psychologem či dalšími pracovníky, vždy žádejte informaci o tom, jak byla situace dořešena, zda/jak byl viník potrestán a zda/jak škola zajistí, aby se podobná situace nestala znovu (= prevence). To platí i v situaci, kdy kyberšikanu řeší za dítě rodiče s rodiči provinilce. Dítě by se mělo zajímat, zda byl viník potrestán.
- **Podpořte oběti** – pokud v okolí probíhá kyberšikana, nebuďte nevšímaví. Poraďte obětem, co mají dělat, a pomozte jim kyberšikanu nahlásit.
- **Zamezte dalším útokům prevencí** – veškeré účty si **zabezpečte dobrým heslem**, zároveň se nikdy nezapomeňte ze svého účtu odhlásit a neukládejte své heslo. Všude si soukromí nastavte tak, aby vaše příspěvky viděli jen ti, u kterých to chcete. Než něco budete sdílet, dvakrát nad tím popřemýšlejte.

Je ale také potřeba **rozlišovat, za jakých okolností je vhodné útočníka blokovat a za jakých ne**. Rozdíl v blokaci je daný typem rizikového jevu a také tím, co blokujeme (obsah, profil).

U **běžné verbální kyberšikany**, kde jsou pachatelé v 80 % jiné děti, není problém stáhnout si důkazy a poté zablokovat komunikaci i pachatele – zde stačí screenshot (snímek obrazovky) komunikace (např. pro řešení v rámci školy). Takový důkazní materiál je dostatečný. U běžné kyberšikany je důležité potlačit šíření materiálu k dalším lidem.

U **útoku spojeného se sexuálními predátory**, kde dochází k vydírání a vyhrožování, šíření intimních materiálů apod., **NESMÍME útočníky blokovat**, protože bychom tím znemožnili policii problém vyšetřit. Zde je potřeba nechat profil neblokovaný a předat komunikaci policii. Samozřejmě můžeme blokovat šířený materiál, předtím si ale musíme uložit důkazy (výše zmíněnými způsoby – pořízením fotografie komunikace apod.). Zde už se jedná o trestné činy – například sexuální nátlak, navazování nedovolených kontaktů s dítětem apod.

Také v případě, že zažíváme vydírání či vyhrožování prostřednictvím sdílení intimních materiálů, bychom pachatele blokovat neměli. Opět z důvodu, aby policie mohla vypátrat jeho identitu.

10. Jak reagovat, když jsme svědky toho, že je spolužák obětí kyberšikany?

Nejdůležitější je **nabídnout mu pomoc a nedělat, že jeho problémy nevidíme**. Oběti kyberšikany se často bojí se svým trápením svěřit, a proto bychom jim měli podat pomocnou ruku v případě, že máme jistotu, že se něco děje. Pokud si například všimneme, že na internetu koluje urážlivá stránka o našem spolužákovi, nebojme se tuto stránku nahlásit nebo o ní informovat někoho dospělého. To samé se týká nevhodných fotek, videí či dalších projevů kyberšikany. Spolužákům-agresorům můžeme vysvětlit, proč je jejich chování špatné. Je to sice velmi obtížné, ale nebojte se postavit na stranu šikanovaného spolužáka.

11. Je kyberšikana trestná? Hrozí nějaký postih?

Samotný termín kyberšikana trestní zákoník nezná. Přesto však **řada skutků, které lze zařadit ke kyberšikaně, trestná je** – **například vydírání, vyhrožování, pomluva, nebezpečné pronásledování, mravnostní trestné činy**, v poslední době pak tzv. **hate-crime – předsudečné trestné činy** (nenávistné projevy).

S kyberšikanou se mohou pojit i další trestné činy, například **poškození cizích práv, křivé obvinění, hanobení, podněcování k nenávisti, šíření poplašné zprávy, podněcování a schvalování trestného činu** apod. Za tyto činy může být pachatel potrestán podmínkou nebo také odnětím svobody.

12. Jaká je situace v České republice? Jak je kyberšikana častá?

Podle dostupných dat z Česka i ze zahraničí (E-Bezpečí, EU Kids Online) **kyberšikanu v České republice zažívá přibližně 8–10 % dětí**. Daleko častěji se děti setkávají s běžnými formami agrese, která je pouze jednorázová a rychle odezní.

Z výzkumu *České děti v kybersvětě* vyplývá, že **některou z forem kybernetické agrese** zažilo v roce 2018 **41,29 % dětí**, což představuje celkem 11 221 incidentů. Dominantní je klasická **verbální agrese (27 % českých dětí)**, na dalších místech pak nalezneme **průnik do účtu (12,64 %)** a **zneužití ponižující fotografie dítěte (12,25 %)**.

13. Jaké panují mýty o kyberšikaně?

Útočník je anonymní a nedá se vystopovat.
Každý počítač s připojením k internetu má svoji IP adresu, která nám ukáže, kde přesně se daný počítač nachází. IP adresu si můžeme představit jako SPZ u auta nebo číslo domu. Útočníci někdy využívají toho, že si IP adresu „přesměrují" například do jiného státu, avšak i tento postup se dá odhalit.

Oběť si kyberšikanu zasloužila.
Přestože nám někdo není sympatický a nemáme ho rádi, nedává nám to právo mu ubližovat. Pokud máme s někým problém, ideální bude si s ním promluvit o tom, co nám vadí. Každý člověk je jiný a je potřeba se naučit tyto odlišnosti respektovat. Kyberšikana nikdy není řešením konfliktu.

Když nevhodnou fotografii (video, příspěvek, komentář) smažu, už ji nikdo neuvidí.
I když fotku (video, příspěvek, komentář) smažeme, nemáme žádnou jistotu, že si ji někdo předtím nestáhl a neuložil. Tento materiál může na internetu kolovat dál bez ohledu na to, že jsme jej smazali.

Kyberšikanu zastavíme vypnutím počítače nebo mobilního telefonu.
Zastavit kyberšikanu vypnutím mobilu nebo počítače je podobné jako zkoušet zastavit tradiční šikanu tím, že přestaneme chodit do školy. Je to nereálné a neefektivní.

Informační a komunikační technologie jsou velmi důležité nástroje, které slouží ke komunikaci, vzdělávání, zábavě, udržování sociálních kontaktů, získávání informací apod. Byla by škoda se o tyto benefity kvůli kyberšikaně ochuzovat.

Navíc řadu forem kyberšikany vypnutí počítače nezastaví – například kdokoliv může vytvořit útočnou stránku o konkrétní osobě a nezáleží na tom, zda je oběť aktuálně online.

14. Co je to griefing?

Osoba, která ve hře provádí tzv. griefing, se snaží **o cílené provokování ostatních hráčů ve hře využitím/zneužitím jednotlivých aspektů hry**. Z této cílené provokace ostatních hráčů získává vlastní potěšení či radost. Griefing je možné označit také jako specifickou podobu kyberšikany a „trollování".

Mezi **nejčastější metody a jevy v oblasti griefingu** patří:

- Spolupráce s oponenty ve hře, tedy škození vlastnímu týmu – vlastním spoluhráčům
- Různé akce podniknuté s primárním cílem plýtvat časem ostatních hráčů
- Zničení nebo demolování věcí vytvořených jinými hráči, bez povolení (např. hra Minecraft)
- Využívání chyb samotné hry ke škodě způsobené jiným hráčům
- Účelné porušování serverových pravidel nebo pokynů
- Písemné urážky (v herním chatu) včetně nepravdivých obvinění z podvádění

Termín griefing pochází z konce 90. let. V současné době se vyskytuje velmi často ve hrách typu battle royale, tedy ve hrách, které hraje najednou obrovský počet hráčů (MMORPG – online hra na hrdiny velkého počtu hráčů). Jedná se zejména o videohry Fortnite, PUBG – PlayerUnknown's Battlegrounds – či Call of Duty: Warzone.

15. V čem je griefing specifický oproti jiným formám kyberšikany?

Kyberšikana se v nejčastějších případech vyskytuje na sociálních sítích, kde mohou být útoky sahající až k psychickému teroru, zesměšňování či útlaku, ve zkratce tedy k útokům, které míří přímo na vaši reálnou osobu. Kyberšikana obecně probíhá ve virtuálním prostředí, ale ohrožuje oběti i v reálném životě (např. finanční vydírání).

Griefing ve videohrách můžeme řadit do podkategorií kyberšikany. Griefing „pouze" škodí virtuálně vytvořené postavě nebo prostředí přímo v samotné videohře.

16. Jak se lze vůči griefingu bránit?

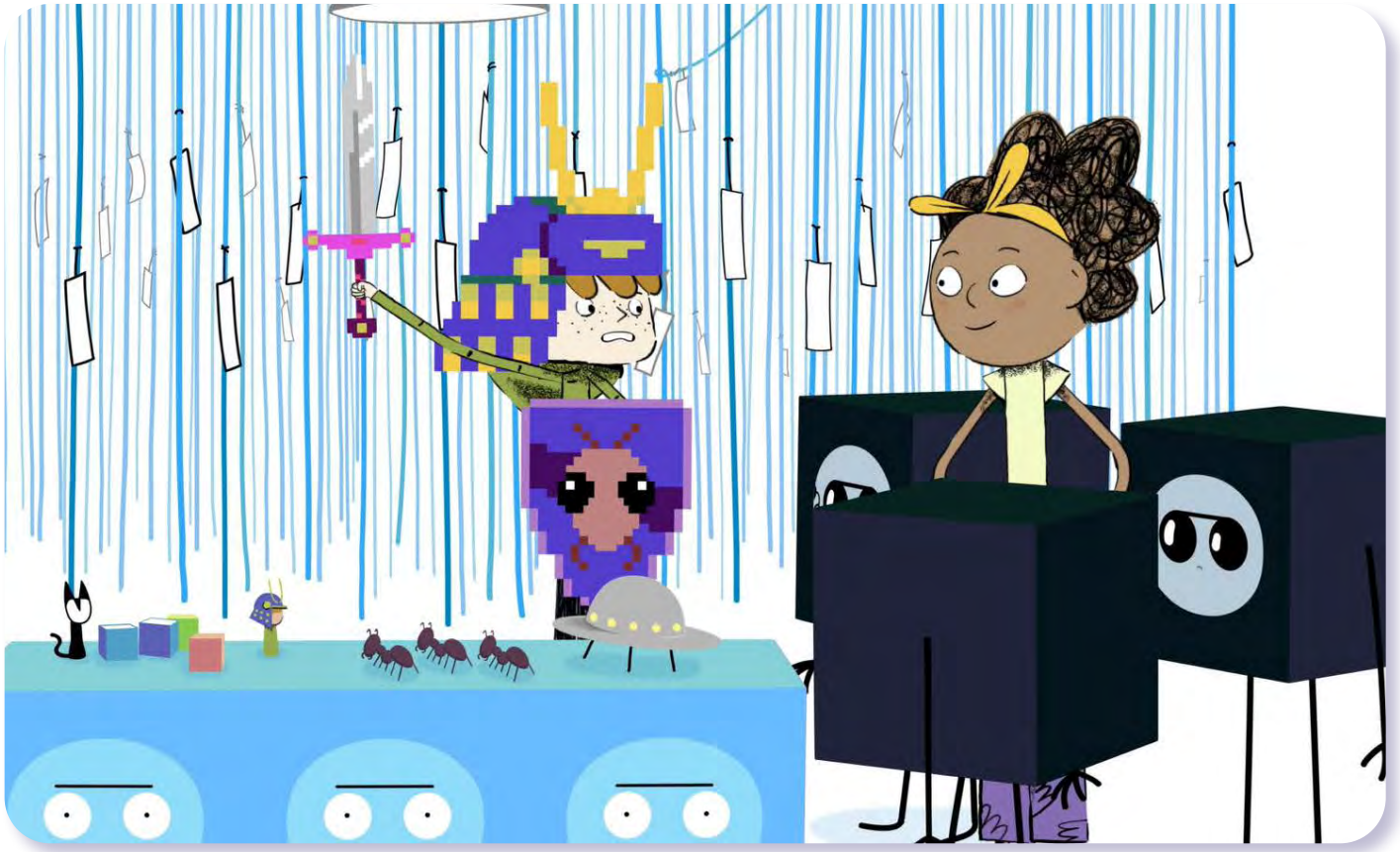
Pokud se hráč s griefingem setká výjimečně, jednoduše lze hru – herní mód ve videohře – opustit a připojit se do jiné, kde se škodlivá osoba již nenachází.

Především se ale lze bránit **nahlášením osoby, která škody působí**. Kdo griefing provádí, lze jednoduše poznat a převážně každá multiplayerová hra více hráčů má možnost tzv. nahlášení. Tím bude na dotyčnou osobu poukázáno a následně bude postižena menším či větším trestem, na základě toho, jakých škod se v samotné hře dopustila.

Odpovědi vypracovali:

Kamil Kopecký, Klára Mikulcová, Univerzita Palackého v Olomouci, E-Bezpečí (otázky 1–13)
Jiří Vimr, krajský protidrogový koordinátor, Krajský úřad Karlovarského kraje, oddělení bezpečnosti a prevence (otázky 14–16)

Podívejte se na lekci V digitálním světě: Kyberšikana na <jsns.cz/mv/kybersikana>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.



V digitálním světě

Pravda, nebo ne?

#DANSLATOILE / Emma Carré, Marjolaine Perreten / Francie, Švýcarsko / 2017 / 2 min.

Filip a Kocour táhnou do boje za záchranu světa před tajným spiknutím mravenců a mimozemšťanů. Při brouzdání internetem totiž naletěli na důvěryhodně vypadající fake news. Další díl seriálu radí, jak se v dnešní záplavě informací na webu orientovat a odlišit pravdu od fám a dezinformací. Ve svobodném prostoru internetu je totiž možné narazit na mnoho verzí téže události. Než vezmu jednu z nich za svou a pošlu ji dál, je dobré držet se několika zásad ověřování pravdivosti.

CÍLE LEKCE

1. uvědomit si, že ne všechny informace na internetu jsou pravdivé
2. naučit se několik zásad ověřování pravdivosti informací na internetu
3. přistupovat k informacím obezřetně a kriticky

DOPORUČENÝ VĚK
8+ LET

AKTIVITA: Pravda, nebo ne?

!!!

ANOTACE

Aktivita vede žáky k zamyšlení, jak se k nim dostávají informace. Zahrají si hru, při níž si uvědomí, že každá informace nemusí být pravdivá. Zamyslí se nad vlastními zkušenostmi s (ne)pravdou na internetu.

VZDĚLÁVACÍ OBLASTI A OBSAHOVÉ VZDĚLÁVACÍ OKRUHY

ZV a GV: člověk a jeho svět (1. stupeň ZŠ), člověk a společnost, jazyk a jazyková komunikace, informatika a informační a komunikační technologie

PRŮŘEZOVÁ TÉMATA

ZV a GV: MV, OSV

KLÍČOVÉ KOMPETENCE

ZV a GV: k řešení problémů, komunikativní, sociální a personální, občanské

CÍLE

Žáci:
- si uvědomí, že ne všechny informace na internetu jsou pravdivé
- si uvědomí, že musí k informacím přistupovat kriticky

DÉLKA

45 min. (včetně projekce)

POMŮCKY

- promítací technika
- tabule nebo flipchart

POSTUP

1. Vyzveme žáky, aby se zamysleli nad tím, jak se k nim dostávají nové informace. Odpovědi zapisujeme na tabuli.

   Poznámka: Pokud je potřeba, vysvětlíme pojem „informace“.

2. Následuje **projekce epizody seriálu**.
   Poznámka: Snímek doporučujeme zhlédnout nejméně dvakrát.

3. V reflexi po projekci zkoumáme, zda žáci porozuměli obsahu dílu a jaké emoce prožívaly postavy. Ptáme se například: *Co vystrašilo Filipa a kocoura? Proč chtěl Filip bojovat?*

4. Následně žáci dostanou za úkol promyslet si tvrzení o své osobě, které vždy začíná slovy
   a/ „Nikdo o mně neví, že...“ (např. „že mám rád ananas“). Důležitým pravidlem hry je, že informace **nemusí být pravdivá**. Úkolem ostatních je uhodnout, zda šlo o pravdu, či lež. Žáci, kteří mají zájem, postupně přečtou nahlas svá tvrzení. Ostatní si stoupnou vpravo, pokud si myslí, že je informace pravdivá, nebo vlevo, pokud nepravdivá. (Mohou také pouze zvedat ruku.) Kdo uhodne, započítá si bod, kdo se splete, bod si odečte. Nakonec si sdělíme své výsledky.
   b/ Ptáme se žáků, co jim pomáhalo poznat, že jejich spolužák nemluví pravdu. *Choval se jinak? Tvářil se jinak? Prozradila ho gesta nebo jiný postoj?*

REFLEXE AKTIVITY

Ptáme se: *Viděli jste na YouTube nebo jinde na internetu nějaká nepravdivá videa nebo jiné nepravdivé informace? Podle čeho jste poznali, že nejsou pravdivé? Co musíme udělat, abychom to zjistili? Proč myslíte, že někdo publikuje nepravdivé informace?*
Na závěr žáky vybídneme, ať říkají pravidla související s ne/pravdou, kterými se máme na internetu řídit. Zapisujeme je na tabuli. Důležité je, aby zaznělo, že ne všechno, co na internetu najdeme, je pravda.
Poznámka: Doporučujeme využít materiál OTÁZKY A ODPOVĚDI k epizodě seriálu.

ZKUŠENOSTI Z PRAXE

Aktivitu jsem testoval v 5. třídě s 23 žáky a poté ještě v 8. třídě, opět s 23 žáky. V pátém ročníku se zpočátku trochu ostýchali přede všemi mluvit a někteří jen zopakovali nebo upravili již vyřčená tvrzení. Třída je díky třídní učitelce velmi pospolitá a žáci se podrobně znají. Uměli tedy dobře odhadnout, zda někdo mluví pravdu, či ne. Osmáci pak byli kreativnější ve vymýšlení tvrzení a méně se styděli. Aktivita formou hry žáky bavila a měla úspěch, i bodování správných odpovědí je motivovalo k soutěživosti.
Po hře jsem pustil film, s upozorněním na to, že se budu na obsah filmu ptát. Podle následných otázek žáci film pochopili a bavil je.
Při reflexi jsem jako příklad nepravdivých sdělení žákům ukázal jimi používané kanály: YouTube, Facebook, Instagram a TikTok. Zdůrazňoval jsem nutnost kritického přístupu k informacím z internetu.
Bylo znát, že osmáci už mají s manipulací a informacemi větší zkušenosti. Bez ohledu na věk jsme ale v obou třídách došli ke stejným závěrům a k pochopení tématu.
Jan Chvojka, *ZŠ Kolín V.*

OTÁZKY A ODPOVĚDI

1. Co je kritické myšlení a proč je potřebné?

Žijeme v době, kdy jsme každý den vystaveni obrovskému množství informací – z klasických médií, ze sociálních sítí i od přátel. Mezi informacemi se však může vyskytovat řada nepravd, zkreslených zpráv nebo vyloženě úmyslných lží, které tvůrci šíří s cílem ovlivnit veřejné mínění, někoho poškodit apod. Zejména na internetu je šíření informací velmi jednoduché.

Kritické myšlení znamená schopnost nepodléhat prvnímu dojmu, obecnému mínění nebo naléhavosti nějakého sdělení. Rovněž znamená schopnost **naivně nepřebírat tradované názory či neprokázané mýty**. V moderním světě je třeba si od jakékoliv sdělené informace vytvořit odstup a připustit i odlišný pohled, popřemýšlet nad sdělením a nejlépe si je i **ověřit**.

Ne všechny informace, které se k nám dostávají, jsou nestranné (tedy co nejvíce objektivní) a ověřené. Kritické myšlení je důležité, protože v záplavě názorů a informací je třeba **informace analyzovat, vyhodnocovat a vysvětlovat**. Tím snižujeme riziko, že budeme přijímat povrchní informace, že budeme myslet a jednat na základě předsudků či stereotypů.

2. Jaké cíle mohou sledovat mediální sdělení na internetu?

Cílem každé informace samozřejmě není někoho pomlouvat. Nejčastějším účelem mediálních sdělení je **informovat** o událostech, které se právě dějí. Například o dopravní nehodě, výsledcích sportovního utkání nebo o premiéře nového filmu.

Na internetu najdeme ale i další obsah, například příspěvky, které nás mají **pobavit** – nejrůznější vtipy, humorné obrázky či videa. Existuje řada webů, které šíří zprávy se smyšleným obsahem, jenž má být zábavný. Ne vždycky jsou ale takto pochopeny – mnozí lidé je berou na základě titulku vážně. Je tedy nutné se řídit nejen titulky, ale celým obsahem.

Na internetu najdeme i mnoho sdělení, kterými někdo chce **přesvědčit** ostatní o své pravdě: třeba o škodlivosti očkování, o víře v posmrtný život nebo o neexistenci změn klimatu. Tyto informace je třeba přijmout jako **názor**, nikoliv ihned jako fakt, a dále je zkoumat.

3. Jaký je rozdíl mezi fakty a názory?

Rozdíl se zdá být jednoduchý. **Zpráva** by měla informovat, **co** se stalo, **kdy** se to stalo, **jak** se událost odehrála, **kdo** byl aktérem a **jaká opatření** jsou učiněna.

Příkladem může být počasí. Faktickou informací je, že je dnes venku 24 °C, slabý vítr, jasno, nulové srážky. Názorem je, že je venku hezky nebo ošklivě, protože každý z nás hezké počasí vnímá trochu jinak.

To samé se může týkat společenských témat nebo třeba politiky. **Seriózní weby rozlišují faktické a názorové články**, v novinách a časopisech je pro názory určena stránka komentářů.

Neseriózní weby naopak s oblibou faktické informace a komentáře nerozlišují a články se snaží cíleně vyvolávat silné emoce, jako je strach nebo rozhořčení. Takový článek kombinující fakta (mnohdy neověřená) a názory čtenáře sice často zaujme, ale nesplňuje parametry seriózní žurnalistiky.

4. Kdo všechno může publikovat na internetu?

Jednoduše řečeno: kdokoliv. Internet je součástí životů nás všech. Stal se dostupným pro drtivou většinu obyvatel. Webové stránky si můžeme zřídit řádově za stokoruny ročně, pokud navíc máte dobrou čtenost, firmy pronajímající reklamní prostor za reklamu umístěnou na čteném webu s velkým dosahem rády zaplatí. Další příležitostí jsou sociální sítě nebo blogy, kde lze publikovat zcela zdarma. **Internet není nijak cenzurovaný a publikovat na něm může kdokoliv.** Každé sdělení tedy zdaleka nemusí být pravdivé jen proto, že je zveřejněné. Obsah však musí být **v souladu se zákony** a případně smluvními podmínkami platformy, na kterých daná osoba publikuje.

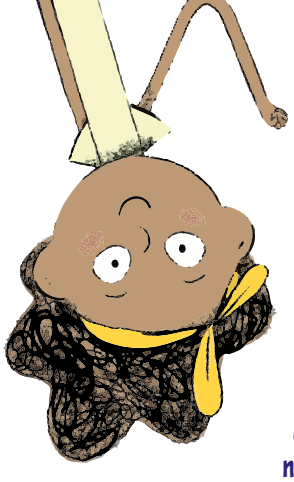
Společnosti vlastnící sociální sítě se snaží kontrolovat nahlášený obsah na sociálních sítích a vyvracet nejčastěji šířené hoaxy a konspirační teorie. Například společnost Facebook si na kontrolu faktů pro Českou republiku najala agenturu AFP. I přes to však na sociálních sítích kolují dezinformace, protože v silách editorů není kontrolovat všechna tvrzení a příspěvky.

5. Jak posoudit důvěryhodnost mediálních sdělení?

Při kritickém myšlení o mediálním sdělení je dobré klást si i následující otázky:

- Je článek **podepsán konkrétní osobou**? Pokud ne, je to podezřelé. Člověk se obvykle za dobře odvedenou práci nestydí. Svou identitu skrývá, když se jedná o pomluvu.
- Je dohledatelný **vlastník webu**? V případě, že není, je to znepokojivé. Weby či projekty mohou být řízeny třeba firmou s vlastními podnikatelskými záměry, například vám vnutit nějaký produkt.
- Obsahuje článek (či příspěvek na sociálních sítích) **ověřené zdroje**? Každá zpráva by měla obsahovat zdroje, odkud informace čerpá. Nejlépe formou odkazů či tvrzení skutečných autorit v daném oboru.
- Má příspěvek **bulvární titulek**? Pokud ano, je třeba být na pozoru a přečíst si důkladně celý text, neřídit se jen podle titulku.
- Jsou **zprávy a komentáře oddělené**? Pokud ne, nejedná se o seriózní žurnalistickou práci.
- Je **reklama viditelně označená**? Seriózní média jednoznačně oddělují reklamu od redakčního obsahu.

Existují projekty, které zkoumají důvěryhodnost jednotlivých médií, mapují



dezinformační weby nebo nabízejí detailní nástroje k ověřování pravosti videí a obrázků apod. Více viz Doporučené zdroje na konci této lekce.

6. Proč někdo publikuje nepravdivé nebo zavádějící zprávy? Co k tomu lidi nejčastěji vede?

Důvodů zveřejňovat nepravdivý obsah je celá řada. Kupříkladu daná osoba chce být **zajímavá** a chce, aby její příspěvek sdílely tisíce lidí.

Dalším důvodem mohou být **podnikatelské zájmy**. To se týká například webů slibujících rychlé zbohatnutí. Lidem praktikujícím takové nekalé metody se začalo říkat „šmejdi“, protože se často zaměřují na seniory nebo lidi v nesnázích (např. nabízejí rychlé půjčky).

Častou motivací je prostý **finanční zisk**. Takové weby lákají své čtenáře na „šokující informace“, aby získali co nejvíce návštěvníků. Na webu pak kromě nepravdivého obsahu najdete také **reklamy**. Čím více návštěv, tím vyšší příjmy z reklam.

A pak existují **politické zájmy**, které mohou například ovlivnit výsledek voleb, potažmo politiku daného státu. Na internetu najdeme i weby, které vyloženě hájí politiku zahraničních států. Příkladem může být Sputnik, který hájí zájmy Ruska, protože je řízen ruskou státní agenturou.

7. Co jsou deep fakes?

Deep fake je označení pro **realistickou úpravu videa**, především tváří zobrazených osob. V praxi tak můžeme osobám na videu vkládat do úst věty, které nikdy nepronesly, provádět záměny postav, obličejů atd. Deep fake využívá pokročilého počítačového zpracování dat s využitím umělé inteligence.

V českém prostředí se v květnu 2019 objevila dvě falešná videa s prezidentem Milošem Zemanem v souvislosti s jeho návštěvou Číny. V prvním předává Zeman starší čínské ženě svou hůl. V druhém mu obyčejný člověk pomáhá vstát a Zeman mu následně děkuje. K autorství videí se v roce 2020 přihlásil mystifikátor Kazma.

V zahraničí vznikla například falešná videa Angely Merkelové nebo Donalda Trumpa. Velký rozruch vyvolalo falešné video Baracka Obamy, které je natolik věrohodné, že nad ním žasnou i odborníci. Výměna tváří je považována za neetickou a nebezpečnou. Odhaduje se, že v průběhu dvou až tří let může představovat velký problém. Sestavit výkonný software, který by dokázal falešná videa poznat, se zatím nepodařilo. Proto je potřeba o těchto manipulativních technikách vědět a být na ně připraven.

8. Jak kriticky přemýšlet o informacích na Facebooku a dalších sociálních sítích?

Vždy je třeba si klást otázky, **kdo za informací stojí, zda jde o skutečnou osobu**. Běžně sice nejde zjistit, kdo za některými stránkami na Facebooku stojí, protože mají například falešná jména nebo na stránce není uvedeno, kdo ji spravuje. I tak ale existuje několik otázek, které nám v orientaci mohou pomoci. Setkáme-li se na Facebooku s pochybnou zprávou na nějakém profilu, vždy je třeba se ptát:

- Má tvůrce sdělení na svém profilu fotografii?
- Jedná se o nově založený profil, nebo existuje řadu let?
- Šíří informace jen z jednoho či dvou webů nebo se soustředí na jedno téma?
- Jaký slovník profil používá?
- Odpovídá profil na dotazy?
- V případě, že se jedná o stránku, je dohledatelné, kdo ji spravuje?
- Není stránka označena jako satirická?

To se samozřejmě netýká jen sociální sítě Facebook. Falešné profily jsou i na Twitteru nebo na Instagramu. Virálním prostředkem pro šíření dezinformací se poslední dobou stal i YouTube.

9. Hrozí za publikování nepravdivých nebo zavádějících informací nějaký postih?

Ano. Český trestní zákoník, konkrétně § 184 postihuje lidi, kteří **šíří** o někom **nepravdivé údaje** natolik závažné, že značnou měrou **ohrozí jeho vážnost** u spoluobčanů.

Dále § 357 určuje, že může být potrestán ten, kdo **úmyslně způsobí nebezpečí** vážného **rozšiřování nepravdivé poplašné zprávy**.

Rovněž je možné na některé nepravdivé zprávy aplikovat paragrafy týkající se **nenávistných projevů nebo ideologií**.

V těchto případech se můžete obrátit na **Policii České republiky**, případně **státní zastupitelství**. V případě poškození dobrého jména se může dotyčný člověk obrátit na **civilní soud** formou žaloby. Oběti chrání **občanský zákoník**, kde je stanoveno, že každý má právo hájit své jméno, vážnost, čest, soukromí a důstojnost.

10. Kontrolují vyhledávače, zda jsou zobrazované informace pravdivé?

Žádný vyhledávač zatím není schopen stoprocentně oddělit nepravdivé zprávy od pravdivých. Mnohé vyhledávače se ale **snaží hledat způsoby, jak dezinformace potlačit**. Vyhledávač Google je známý tím, že se snaží weby pravidelně šířící dezinformace upozaďovat a zvýhodňovat naopak projekty odhalující hoaxy. Společnost Seznam.cz taková opatření nedělá.

Proti dezinformacím více či méně úspěšně bojují sociální sítě. Velmi aktivní v tomto boji je Twitter, snahu vyvíjí i Facebook. Kromě již zmíněné editační činnosti a kontroly faktů nárazově odstraňuje falešné profily či stránky šířící dezinformace. I přesto však musíme být na sociálních sítích ostražití.

11. Co můžu dělat, když zjistím, že je nějaký článek či informace nepravdivá?

Na sociálních sítích je většinou možné diskutovat pod příspěvkem. Vložením poznatků, které se vám podařilo zjistit, se o ně jednak podělíte s ostatními pozornými čtenáři, jed-

nak tím kontaktujete autora. Stejně tak můžete příspěvek nahlásit správci nebo přímo sociální síti.

Autora je možné kontaktovat i u webu, pokud má uvedeny kontaktní údaje. V obou případech rovněž můžete o příspěvku dát vědět projektům kontrolujícím fakta jako www.hoax.cz nebo www.manipulatori.cz. Podobné projekty existují i v zahraničí.

12. Co jsou to média veřejné služby?

Veřejnoprávní média (neboli média veřejné služby) jsou média, která mají příjem především z veřejných peněz (koncesionářských poplatků) a v zákoně definovaný rozsah a povinnosti. V českém prostředí se jedná o Českou televizi, Český rozhlas a Českou tiskovou kancelář.

Cílem jejich provozování je **bránit zneužití médií politickými stranami a přinášet nestranné informace široké veřejnosti (tj. naplňovat tzv. veřejnou službu)**. Někdy bývají označována jako tzv. čtvrtý pilíř demokracie (vedle moci zákonodárné, výkonné a soudní). Média veřejné služby nejsou ale „státní“ média; ta obvykle fungují v diktaturách a autoritářských režimech, kdy vysílají to, co je v zájmu vládnoucích skupin.

Obecně lze říci, že média veřejné služby jsou důvěryhodnější než média soukromá, protože mají několik stupňů ověřování informací a následné kontroly obsahu. U veřejnoprávních médií je kladen zvláštní důraz na jejich povinnost poskytovat vyvážené, stranicky neutrální a objektivní zpravodajství. Mají rovněž veřejně dostupný etický kodex. Na vyváženost zpravodajství dohlíží Rada pro rozhlasové a televizní vysílání. Jednotlivá média pak mají i své kontrolní orgány, existuje tak Rada České televize, Rada Českého rozhlasu a Rada ČTK.

Odpovědi vypracoval:

Jan Cemper, Manipulátoři.cz

Podívejte se na lekci V digitálním světě: Pravda, nebo ne? na <jsns.cz/mv/pravda-nebo-ne>, kde najdete více informací, včetně doporučené literatury a dalších odkazů.

POZNÁMKY

5. REJSTŘÍK POJMŮ

REJSTŘÍK POJMŮ

Přinášíme vám rejstřík pojmů souvisejících s digitální a mediální tematikou, které se objevují v této publikaci.

Adware
Pojem vznikl zkrácením angl. výrazu *advertising-supported software* (program na podporu reklamy). Jedná se o různé formy reklamy, s nimiž se můžeme na internetu setkat – od bannerů po „vyskakovací" (pop-up) okna. Adware často přenastaví domovskou stránku v prohlížeči nebo do prohlížeče doinstaluje různé doplňky (např. lišty s alternativními vyhledávači či jinými nástroji). Adware se obvykle do počítače dostane tak, že uživatel si stahuje nějaký bezplatně šiřitelný program (freeware), k němuž je adware připojen jako doplněk.

Algoritmus
Přesně stanovený schematický postup pro řešení nějaké úlohy nebo situace. Algoritmy jsou používány vyhledávači (např. Google) či sociálními sítěmi (např. Facebook). Pro algoritmy sociálních sítí je typická *posloupnost* (po prvním kroku následuje druhý), *větvení* (pokud platí jedna podmínka, nastane určitá akce; pokud neplatí podmínka, nastane jiná akce) a *cykličnost* (opakování příkazu, dokud se nedosáhne požadovaného výsledku). Algoritmy nabízejí uživatelům pro ně co nejrelevantnější obsah, a tím je udržují na sítích co nejdéle, což majitelům sítí zajišťuje maximalizaci zisků z reklamy. Při výběru zobrazovaných příspěvků algoritmy využívají mnoho osobních dat uživatelů (např. lokalitu, sociodemografické charakteristiky, zájmy, koníčky, okruh přátel nebo obsahy, na které v minulosti uživatel reagoval).

Android
Nejpoužívanější operační systém pro chytré telefony.

Anonymní režim
Typ režimu v internetovém prohlížeči, při jehož používání se neukládá, co uživatel na internetu dělá – historie prohlížení, soubory cookies (viz samostatné heslo), data webů ani informace zadané do formulářů. Prohlížeč si vedle historie prohlížení nepamatuje ani seznam stažených souborů, byť samotné stažené soubory a vytvořené záložky jsou zachovány. Soubory cookies se v anonymním režimu ukládají jen dočasně (odděleně) a při zavření okna prohlížeče jsou z počítače vymazány.

Antivirus / antivirový program
Druh počítačového softwaru, jehož úkolem je chránit počítač nebo mobil. Antivirus se používá k nalezení, odstranění a zničení počítačových virů a malware (viz samostatné heslo). Tyto činnosti lze zajistit buď prohlídkou souborů na disku, kdy se vyhledávají sekvence odpovídající databázi počítačových virů, nebo zaznamenáváním nedůvěryhodných činností počítačového programu, které by mohly způsobit infekci. Antivirus se soubor pokusí opravit odstraněním viru, umístěním souboru do karantény nebo infikovaný soubor i vir smaže.

Binární kód / binární kódování
Způsob uložení informace v počítači založený na dvou hodnotách – 0 a 1. Právě do soustavy jedniček a nul si digitální přístroje překládají příkazy a informace, jež jim uživatel zadává. Binární kódování je tak univerzální metodou zpracování informací, přičemž využívá principu jednoduchosti, tedy pouze významu ano/ne, svítí/nesvítí, zapnuto/vypnuto (jev tedy nabývá pouze dvou hodnot – zmíněné nuly nebo jedničky). Tato základní jednotka binárního kódu se nazývá 1 bit (1 b) a z ní se tvoří větší bloky neboli bajty. 1 bajt (1 B) představuje 8 bitů (8 b), tedy osm po sobě jdoucích nul či jedniček.

Cookies
Malé datové soubory vytvořené webovou stránkou, které se přes prohlížeč ukládají do počítače či mobilního telefonu uživatele. Zaznamenávají informace o chování uživatele (resp. jeho zařízení) na webu a slouží k jeho pozdější identifikaci při opětovné návštěvě. Díky cookies si webová stránka pamatuje například přihlašovací a kontaktní údaje, položky v košíku nebo jazykové nastavení, a při pozdější návštěvě tak není nutné vše znovu vyplňovat.

Deep fake
Označení pro realistickou úpravu videa, především jde o úpravu tváře zobrazených osob. V praxi vypadá tak, že lze osobám na videu vkládat do úst věty, které nikdy nepronesly, provádět záměny postav, obličejů atd. Deep fake využívá pokročilého počítačového zpracování dat s využitím umělé inteligence.

Dezinformace
Nepravdivá nebo záměrně zkreslená informace, jejímž cílem je ovlivnit rozhodování nebo názory těch, kteří dezinformace přijímají. Mezi tvůrce a šiřitele dezinformací mohou patřit jednotlivci, organizované skupiny nebo i státní aktéři, což se týká zejména autoritativních a nedemokratických režimů.

Digitální gramotnost
Soubor digitálních kompetencí (vědomostí, dovedností, postojů, hodnot), které člověk potřebuje k bezpečnému, kritickému a tvořivému využívání digitálních technologií ve svém životě. Součástí digitální gramotnosti je například bezpečné používání internetu (včetně hesel, která nelze jednoduše odhalit) nebo vědomí, že digitální a reálný svět se liší. V době, kdy přibývá lidí závislých na digitálních technologiích, lze mezi prvky digitální gramotnosti řadit i užívání technologií v přiměřené míře.

Digitální stopa
Informace zanechaná uživatelem v prostředí internetu – buď vědomě a viditelně (např. příspěvek na sociální síti), nebo na první pohled skrytě jako součást souborů (např. jako součást cookies – viz samostatné heslo). Aktivní digitální stopu (tj. tu, co uživatel sám tvoří) může představovat fotografie, blog, osobní stránka, profil na sociální síti, e-maily, SMS a další typy obsahu. Pasivní digitální stopu tvoří informace, které jsou ukládány bez vědomí uživatele. Může se jednat o různá data, záznamy aktivit, četnost návštěvy webových stránek, činnosti na webech, IP adresu a jiné. Digitální stopy jsou zdrojem informací o uživateli. Tato data mohou být i zneužita, proto je potřeba digitální stopu pravidelně kontrolovat.

Digitální technologie
Technologie pracující s digitálním (nespojitým) signálem, který může nabývat dvou hodnot – 0 a 1. Digitální kód umožnil propojit text, obraz a zvuk a přinesl nové typy obsahu. Digitální technologie využívají počítače, mobilní telefony, DVD přehrávače, digitální fotoaparáty a kamery, MP3 přehrávače, wifi sítě apod.

Facebook
Celosvětově největší sociální síť (2,23 miliard aktivních uživatelů, z toho 5,2 milionu v České republice). Platformu založil v roce 2004 Američan Mark Zuckerberg. Umožňuje vytvoření osobního profilu, firemních stránek nebo skupin uživatelů. Ve všech je možné sdílet statusy, fotografie, videa, zajímavé odkazy nebo pozvánky na události. Správci stránek mohou používat (a mnozí používají) k šíření svých sdělení placenou propagaci.

Fake news
Úmyslně vytvořená nepravdivá zpráva, která je vydávána za pravdivou. Pojem tvoří angl. slova *fake* (falešný, nepravdivý) a *news* (zpráva). Může být buď zcela vymyšlená, nebo se opírat o účelově vybraná fakta, která jsou zasazena do neúplného kontextu. Cílem fake news je ovlivnit příjemce sdělení podle záměru autora smyšlené zprávy (např. vyvolat nenávist k určité skupině lidí, posílit podporu nějakého politika nebo názoru). Často přitahuje příjemce senzačním titulkem, slibuje šokující odhalení a vzbuzuje silné emoce. Nepravdivé zprávy se někdy také označují pojmem dezinformace nebo hoax (byť jsou mezi nimi drobné významové rozdíly).

Freemium
Pojem odvozený z angl. slov *free* (zdarma, volný) a *premium* (prémiový). Popisuje obchodní model, který nabízí základní produkt či službu zdarma a zisk je generován prodejem doplňkových prémiových služeb a funkcionalit. Například u hraní online (video)her je základní verze hry volně dostupná (tzv. free to play), ale uživatel přímo ve hře nakupuje dodatečné prvky.

GDPR
Mechanismus, který má za cíl chránit osobní údaje uživatelů a zabránit tomu, aby s nimi firmy či státní aktéři nelegálně nakládali, například tím, že využijí telefonní číslo uživatele k telemarketingovým akcím, aniž by k tomu uživatel dal předem souhlas. Oficiální název tohoto právního rámce, který je platný v celé Evropské unii, zní obecné nařízení o ochraně osobních údajů (angl. *General Data Protection Regulation* – GDPR). GDPR se týká všech firem a institucí, ale i jednotlivců a online služeb, které zpracovávají data uživatelů.

Google
Google je jedna z nejvýznamnějších globálních technologických firem světa, která provozuje řadu celosvětově rozšířených služeb – vyhledávač Google, e-mailovou aplikaci Gmail, Google Maps, prohlížeč Google Chrome nebo nástroj Google Analytics. Google založili během studií dva spolužáci ze Stanfordské univerzity, Larry Page a Sergey Brin.

Google začínal jako internetový vyhledávač, který díky revoluční technologii PageRank dosahoval nesrovnatelně lepších výsledků hledání než jeho tehdejší konkurenti. Mnohé nástroje Googlu jsou uživatelům k dispozici zdarma (Gmail apod.), přičemž Google především profituje ze získávání dat o chování uživatelů, které pak využívá při prodeji reklamy.

Hate speech
Vyjádření, která rozšiřují, podněcují, podporují či ospravedlňují nenávist vůči skupině osob. Pojem pochází z angl. slov *hate* (nenávist) a *speech* (řeč). Nenávist vůči skupině je podněcována zejména na základě rasy, národnosti, etnicity, náboženství, věku, sexuální orientace, genderové příslušnosti, fyzického nebo mentálního hendikepu, sociálního postavení, životního stylu nebo politické orientace.

Hoax
Zpráva obsahující nepravdivé či zkreslené informace (angl. slovo *hoax* znamená podvod, falešná zpráva). Obvykle zahrnuje žádost o další šíření a rozesílání mezi co nejvíce příjemců. Zpravidla bývá šířena e-mailem nebo na sociálních sítích. Hoaxy často varují před nějakým smyšleným nebezpečím a mohou tak splňovat definici poplašné zprávy. Jiné hoaxy se snaží ovlivnit názory a jednání příjemců.

HTTP
Komunikační protokol, který umožňuje „přenášení" webových stránek mezi počítači. V praxi se zkratka http (*hypertext transfer protocol*) objevuje ve webových adresách (např. http://www.jsns.cz), případně v upravené zabezpečené podobě jako https. Protokolem se nazývají celosvětově platné konvence, podle nichž probíhá elektronická komunikace a přenos dat.

Influencer
Člověk, který svými názory ovlivňuje významné množství lidí. V praxi jsou jimi v marketingu nejčastěji označováni youtubeři, instagrameři a další lidé, kteří jsou populární na sociálních sítích a sleduje je tak velký počet lidí (v českém prostředí mezi takové patří např. moderátor Leoš Mareš, kterého na sociální síti Instagram sleduje více než milion uživatelů). Influencery nemusí být jen celebrity s miliony fanoušků, ale mohou mezi ně patřit i lidé, kteří jsou populární jen v určité menší komunitě v rámci svého oboru.

Instagram
Jedna z celosvětově nejpopulárnějších sociálních sítí založená zejména na sdílení fotografií nebo krátkých videí. Vlastníkem Instagramu je společnost Facebook.

Instagram Stories / Insta Stories
Nástroj sociální sítě Instagram, který umožňuje uživateli natáčet vlastní krátké (video)příběhy a ty pak zveřejnit. Tyto příběhy se na Instagramu zobrazují 24 hodin, poté se automaticky mažou. Insta Stories obvykle zachycují každodenní momenty či několikavteřinové koláže z fotografií, často doplněné o texty, barevné kresby i emotikony.

Internet parenting
Soubor kompetencí, které by měly rodičům pomoci vést děti ke správnému užívání internetu. Ve chvíli, kdy se dítě začne aktivně pohybovat na internetu, by mu rodiče měli objasnit, jak internet funguje, jak ho bezpečně používat a jaká má rizika. Někteří rodiče, kteří sami vyrůstali bez internetu, ale na tento úkol často nejsou připraveni. Na tuto potřebu tak reagují různé neziskové projekty, které rodičům nabízejí informace a podporu.

Internetový vyhledávač
Služba umožňující najít webové stránky, které obsahují požadované informace. Uživatel zadává do vyhledávače klíčová slova související s hledanou informací a vyhledávač obratem ze své databáze vygeneruje seznam odkazů na stránky, které hledané informace obsahují. Vedle organického vyhledávání (přirozených výsledků) vyhledávače obvykle nabízí i odkazy, jejichž zvýraznění majitel stránky podpořil reklamou. V českém prostředí jsou nejpoužívanější vyhledávače Seznam a Google, který dominuje vyhledávání celosvětově.

Konspirační teorie
Soubor fakticky nepodložených názorů, které mají za cíl – obvykle šokujícím způsobem – vysvětlit nějaký jev nebo dění. Konspirační teorie často tvrdí, že události, které se odehrávají, utajeně řídí mocní jednotlivci nebo skupiny, které chtějí ovládnout svět. Konspirační teorie se často šíří formou řetězových e-mailů nebo jsou publikovány na dezinformačních webech.

Kritické myšlení
Způsob myšlení, během něhož jsou zkoumána a hodnocena předkládaná tvrzení s cílem posoudit jejich platnost či pravděpodobnost, relevanci a záměr. Hodnocení se netýká pouze tvrzení druhých osob, ale i vlastních myšlenek. Kritické myšlení slouží jako ochrana proti klamům, lžím, manipulaci a mylnému chápání sebe samých a světa kolem nás.

Kyberšikana
Psychická šikana v digitálním prostředí, která má za následek ublížení, zesměšnění, ztrapnění nebo jiné poškození oběti. Probíhá pomocí informačních a komunikačních technologií (např. pomocí SMS zpráv nebo sociálních sítí).

Kyberprostor
Digitální prostředí, v němž dochází ke vzniku, zpracování a výměně informací. Jde o imaginární prostor bez časoprostorových souřadnic.

Malware
Program, který má za cíl poškodit počítač či data. Mezi malware patří počítačové viry, trojské koně, ale třeba i spyware, což jsou tzv. špionážní programy, které po nevědomém nainstalování na počítač uživatele (např. při stahování jiného souboru) začnou o uživateli odesílat data, která shromažďuje útočník.

Mediální gramotnost
Soubor poznatků a dovedností, které člověku umožňují se orientovat ve světě médií. S nárůstem počtu informací, kterým jsme v digitální době denně vystaveni, roste i nutnost umět od sebe odlišit zprávy pravdivé a nepravdivé, porozumět fungování médií a jejich zájmům (např. média veřejnoprávní vs. média soukromá) a chápat souvislosti vzniku tzv. mediálních obsahů (tj. zpráv, videí, příspěvků na sociálních sítích apod.).

Mediální výchova
Výchova směřující k mediální gramotnosti. Ve většině rozvinutých zemí je součástí formálních vzdělávacích systémů, v České republice je součástí školních kurikul základních a středních škol (především gymnázií) od roku 2007.

Messenger
Populární komunikační aplikace, která umožňuje posílání zpráv, obrázků, videí a vytváření skupin uživatelů. Messenger je vlastněn společností Facebook.

Minecraft
Populární počítačová hra vyvíjená společností Mojang. Hra obsahuje různé stupně obtížnosti a lze ji hrát samostatně nebo i s jinými uživateli. Hráčům nabízí velmi volné pole působnosti k různým aktivitám (typ tzv. sandboxové hry). Minecraft patří do kategorie her s tzv. adventure tematikou.

Personalizovaná reklama
Forma reklamy, která využívá údaje o online aktivitách uživatelů a zobrazuje jim tak relevantnější reklamní obsah, který může uživatele zaujmout.

Počítačový vir
Program (nebo část kódu), který se spustí v počítači po navštívení infikované webové stránky, otevření přílohy podezřelého e-mailu či instalaci závadného softwaru. Viry mohou napadat i chytré mobilní telefony.

Prank
Oblíbený typ obsahu na sociálních sítích, zejména na YouTube, jehož podstatou je někoho nachytat nebo si z něj vystřelit. Anglické slovo *prank* znamená „kanadský žertík“, vylomeninu či rošťárnu. Tyto chytáky, zesměšnění nebo vtípky jsou pečlivě připravené a natáčejí se a zveřejňují se na internetu.

Jejich cílem není postiženému ublížit, ale autoři pranku se snaží spíše své okolí pobavit. Nejde jim tedy ani o obohacení, ani o zlý úmysl. Ne vždy se toto podaří a mnohé pranky mohou být až kruté nebo na hranici zákona.

Programování
Činnost, na základě které počítač provádí požadované úkony, například přehrává hudbu nebo zobrazuje webové stránky. Základem programování je tzv. programovací jazyk, pomocí kterého specialisté zapisují, co má počítač dělat, a to lidsky čitelnými příkazy. Následně se tyto čitelné příkazy pomocí speciálního nástroje přeloží do binárního kódu v podobě nul a jedniček, kterému už počítače „rozumí“.

Ransomware
Škodlivý program, který omezuje uživatelům přístup k jejich počítačovému systému nebo souborům. Za obnovení přístupu požaduje program zaplacení výkupného. Pro podobné programy se používá také označení rogueware nebo scareware.

Screenshot
Snímek (fotografie) obrazovky. Na počítači lze screenshot pořídit obvykle pomocí klávesové zkratky nebo klávesy Printscreen. Screenshot komunikace může fungovat například jako důkaz při kyberšikaně.

Selfie
Fotografický autoportrét, který člověk pořizuje vlastní rukou digitálním fotoaparátem nebo mobilním telefonem. Selfie (z angl. *self* – já, vlastní osoba) se většinou sdílí a publikuje na sociálních sítích. Jedná se o neformální snímky, někdy pořizované i s pomocí zrcadla. Na selfie je buď jen ten, kdo fotografuje, nebo společně s lidmi, kteří se vejdou do záběru (*group selfies*). Selfie je známo již od roku 1900, kdy byl poprvé používán přenosný fotoaparát Kodak. Vzestup selfies umožnilo fotografování pomocí předního fotoaparátu mobilního telefonu nebo tabletu.

Sexting
Zasílání textových zpráv, fotografií nebo videí se sexuálním obsahem.

Snapchat
Aplikace určená především k zasílání obrázků a fotografií. Specifikem Snapchatu je, že zaslané materiály se samy po určité době (např. 24 hodin) smažou. Teoreticky tak není možné zaslaný materiál dále zkopírovat či rozšířit, což uživatelé ale v praxi obcházejí tím, že si pořídí snímek obrazovky (screenshot).

Sociální bublina
Komunita lidí, která sdílí podobné postoje (politické, náboženské atd.), názory nebo zájmy. Skutečnost, že lidé mají tendenci se sdružovat a komunikovat s lidmi, kteří jim jsou podobní, vede k utváření klamu, že jejich žitý svět je ten jediný normální a běžný. Dostávají se tak do sociální bubliny ve vztahu k lidem s odlišnou sociální pozicí a životním stylem. Členové jednotlivých bublin se ve svých názorech navzájem utvrzují, což jim poskytuje pocit bezpečí. Na druhou stranu se však vzdalují názorům dalších skupin, a sociální bubliny tak mohou vést k vzájemnému nepochopení a štěpení společnosti.

Sociální síť
Internetová služba umožňující svým uživatelům tvořit a sdílet s ostatními osobní obsah (textové příspěvky, videa, fotografie apod.) a komunikovat s nimi (formou zpráv či komentováním příspěvků ostatních uživatelů). Nejznámějšími sociálními sítěmi jsou v současnosti Instagram, Facebook, YouTube, Twitter či TikTok. Existují také specializované sociální sítě, například profesní sociální síť LinkedIn nebo ResearchGate, která slouží vědecké komunitě.

SoundCloud
Název celosvětově oblíbené internetové stránky pro online distribuci hudby nebo mluveného slova (tzv. podcastů).

TikTok
Sociální síť založená na sdílení patnáctivteřinových videí, často hudebních videoklipů. Ty lze velmi snadno vytvářet a sdílet, k dispozici je také celá řada předpřipravených filtrů, díky kterým působí videa kvalitněji. TikTok je populární především u dětí do 13 let věku, starší uživatelé se již orientují na jiné sociální sítě a služby. TikTok využívá více než miliarda uživatelů (stav k létu 2020).

Trojský kůň
Typ škodlivého kódu, který se často ukrývá v bezplatných aplikacích nebo filmech. Jeho cílem je ovládnout počítač uživatele, krást nebo mazat data, získat hesla a jinak škodit.

Troll
Slangový výraz pro uživatele internetu, který v diskusních fórech, chatech či komentářích rozdmýchává hádky a mnohdy slovně napadá ostatní uživatele. Trollové se obvykle nezabývají argumenty, ale jejich cílem je provokovat, urážet a vyvolávat konflikty. Činnosti trollů se říká trolling. Vedle osamocených trollů, kteří si tak ventilují svoji frustraci a nudu, existují i organizované skupiny (tzv. trollí farmy), které působí i v mezinárodním kontextu a snaží se debatu svést pro ně výhodným směrem (rozšiřují tak např. i dezinformace, fake news a útočí na politické protivníky).

Twitter
Sociální síť umožňující zveřejňování zpráv v rozsahu 240 znaků. Tyto zprávy se nazývají tweety a mohou obsahovat i odkazy na další obsah nebo je lze doprovodit fotografií.

Veřejnoprávní média
Média tzv. veřejné služby, jejichž fungování je upraveno zákonem. Smyslem existence veřejnoprávních médií není generovat zisk jako komerční média, ale naplňovat veřejný zájem poskytováním „objektivních a všestranných informací pro svobodné vytváření názorů“ a vytvářet a poskytovat vyváženou nabídku pořadů pro všechny skupiny obyvatel. V našem prostředí patří mezi veřejnoprávní média Česká televize (ČT), Český rozhlas (ČRo) a Česká tisková kancelář (ČTK). ČT a ČRo jsou většinově financovány z televizních a rozhlasových poplatků, ČTK vydělává na svůj provoz prodejem agenturního zpravodajství. Na činnost každého veřejnoprávního média u nás dohlíží speciálně zřízená rada. (Média veřejné služby se někdy mylně ztotožňují s tzv. státními nebo oficiálními médii, jejichž existence je typická pro autoritářské režimy.)

Vlog
Krátké video, jehož tvůrce mluví do kamery na libovolné téma od vlastních zážitků přes společenské komentáře. Vlog se poté veřejně publikuje (nejčastěji na YouTube).

WhatsApp
Aplikace, která umožňuje vyměňování zpráv a multimediálních souborů mezi jednotlivými vlastníky chytrých telefonů. Přes WhatsApp lze zaslat audia, videa, fotografie, obrázky nebo i sdílet polohu. Název odkazuje k účelu aplikace a tvoří ho kombinace formulace *What's up* (co se děje, co je nového) a *App* (univerzálně používaná zkratka pro slovo aplikace).

WWW
WWW je zkratka slov World Wide Web. Označuje celosvětovou počítačovou síť, díky níž si můžeme prohlížet obsah internetu.

YouTube
Celosvětově nejrozšířenější internetová platforma pro sdílení a sledování videí. Majitelem YouTube je společnost Google.

Youtuber
Tvůrce videí, který sdílí svůj obsah na portálu YouTube. Youtubeři natáčejí videa na rozmanitá témata podle skupin uživatelů, na které cílí. Populární jsou například videa zaměřená na líčení, hraní počítačových her apod. Autoři převážně tvoří pro mladší publikum, ale mezi youtubery jsou i lidé střední generace, kteří se věnují závažnějším společenským tématům. Mezi populární youtubery v českém prostředí patří například Kovy nebo Shopaholic Nicol.

KVÍZ PRO ŽÁKY: Co víte o digitálním světě?

**Vyzkoušejte si, co všechno už víte o digitálním světě.
Z každé dvojice tvrzení je vždy jen jedno správné.
Poznáte které?**

- ☐ Digitální svět tvoří nuly a jedničky.
  nebo
- ☐ Digitální svět tvoří hvězdičky a tečky.

- ☐ Internet vznikl teprve nedávno a stále se učíme, jak ho využívat chytře a bezpečně.
  nebo
- ☐ Internet existuje od pradávna a nemůže se nám v něm stát nic špatného.

- ☐ Informace na internetu se nám objevují zcela náhodně.
  nebo
- ☐ Informace na internetu třídí vyhledávače a algoritmy.

- ☐ Počítač je sám od sebe chráněn před všemi hrozbami.
  nebo
- ☐ I počítač může onemocnět. Musíme ho chránit před viry.

- ☐ Silná hesla chrání naše soukromí i peníze.
  nebo
- ☐ Silná hesla nám jenom komplikují život, protože je složité si je pamatovat.

- ☐ Cookies mažou informace o našem pohybu na internetu.
  nebo
- ☐ Cookies sbírají informace o našem pohybu na internetu.

- ☐ Při nákupu během hraní hry nikdy nejde o skutečné peníze.
  nebo
- ☐ Při nákupu během hraní počítačové hry může jít o skutečné peníze.

- ☐ Důležitější než mobily a počítače jsou kamarádi, rodina a koníčky.
  nebo
- ☐ Důležitější než mobily a počítače už není vůbec nic.

- ☐ Všechno na internetu je vhodné pro děti.
  nebo
- ☐ Na internetu můžeme narazit na obsah, který není vhodný pro děti.

- ☐ Veškerý obsah na internetu se pravidelně promazává.
  nebo
- ☐ Cokoliv na internet umístíme, tam zůstane navždy.

- ☐ Lajky nejsou všechno – více lajků neznamená více dobrých kamarádů.
  nebo
- ☐ Lajky jsou důležitější než skutečné kamarádství.

- ☐ Pravidla slušné a ohleduplné komunikace by měla platit i online.
  nebo
- ☐ Na internetu nemusíme být slušní ani nemusíme na nikoho brát ohledy.

- ☐ Internet je prostor pro sdílení. Vytvořit dobrý obsah ale vyžaduje nápady, přípravu a úsilí.
  nebo
- ☐ Na internetu nic nikomu nepatří, jakýkoliv obsah můžeme bez dovolení upravovat a vydávat za vlastní.

- ☐ Hrubé nebo jinak nevhodné chování na internetu je v pořádku.
  nebo
- ☐ Pokud se k nám na internetu někdo chová hrubě nebo jinak nevhodně, požádáme dospělého o pomoc.

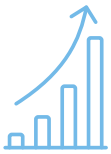
- ☐ Na internetu jsou pravdivé i nepravdivé informace. Nemůžeme proto všem informacím na internetu automaticky věřit.
  nebo
- ☐ Na internetu jsou pouze pravdivé informace.

BONUSOVÝ MATERIÁL.

INFOGRAFIKA
K VYBRANÝM TÉMATŮM
MEDIÁLNÍHO VZDĚLÁVÁNÍ

Historie internetu

Významné světové a české milníky



2030

Odhadem 90 % světové populace* online

2020

60 % světové populace online

– tj. 4,57 miliardy lidí

2007

Představen iPhone

– mění svět smartphonů a mobilního internetu

2005

První video na YouTube

2004

Přichází Facebook

– hybatel sociálních sítí

1997

Spuštěn vyhledávač Google

1996

Seznam.cz

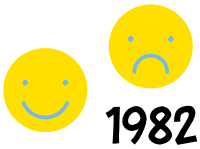
– katalog s žebříčkem TOP českých stránek

1992

Československo připojeno k internetu

1991

Internet je veřejný & První webové stránky na světě



1982

První emotikony

1978

První spam

1971

První e-mailový program

1966

Zárodek internetu

– první přenos informací mezi počítači propojenými v armádní síti ARPANET (USA)

*Ve věku 6 let a starších; zdroj: Cybersecurity Ventures.

HISTORIE INTERNETU – VÝZNAMNÉ SVĚTOVÉ A ČESKÉ MILNÍKY

1969 – Zárodek internetu

První výměna informací mezi prvními dvěma počítači se uskutečnila na Kalifornské univerzitě v USA. Stalo se tak po síti ARPANET, která byla zřízena americkým ministerstvem obrany pro výzkumné účely. Z této sítě se později vyvinul internet.

1971 – První e-mailový program

Jednalo se o první systém schopný odeslat zprávy mezi uživateli různých počítačů připojených k síti ARPANET.

1978 – První spam

Poprvé byla odeslána nevyžádaná pošta celkem 393 lidem v síti ARPANET.

1982 – První emotikony

První emotikony v podobě usmívajícího :-) se a smutného :-(smajlíka spatřily světlo světa díky Američanovi Scottu Fahlmanovi.

1991 – První webové stránky na světě; začátek komerčních provozovatelů webových stránek.

Veřejnosti byla zpřístupněna první webová stránka na světě. Šlo o jednoduchou textovou stránku s odkazy, které ji napojovaly na další stránky. Vytvořil ji a pustil do světa Tim Berners-Lee ve výzkumné organizaci CERN ve Švýcarsku. Podoba první webové stránky je k vidění na http://info.cern.ch/.

Téhož roku byl v USA obsloužen první zákazník přes internet, což bylo důležitým krokem pro masové zavedení internetu.

1992 – Československo připojeno k internetu

K připojení Československa k internetu došlo na Českém vysokém učení technickém (ČVUT) v Praze.

1996 – Založení Seznam.cz

Seznam.cz byl první katalogový server a vyhledávač na českém internetu. Obsahoval žebříček nejlepších českých stránek.

1998 – Spuštění vyhledávače Google

Do konce téhož roku uměl Google vyhledávač najít přibližně 60 milionů webových stránek.

2004 – Přichází Facebook

Ačkoliv Facebook nebyl prvním existujícím sociálním médiem, stal se významným hybatelem světa sociálních sítí.

2005 – Zveřejněné první video na YouTube

Video s názvem Me at the zoo (Já v ZOO) zveřejnil spoluzakladatel YouTube Jawed Karim.

2007 – Představen iPhone

Steve Jobs, zakladatel firmy Apple, představil iPhone slovy „Apple znovu vynalezl telefon“. A vskutku – svými řešeními definoval první iPhone moderní smartphone.

2020 – 60 % světové populace online

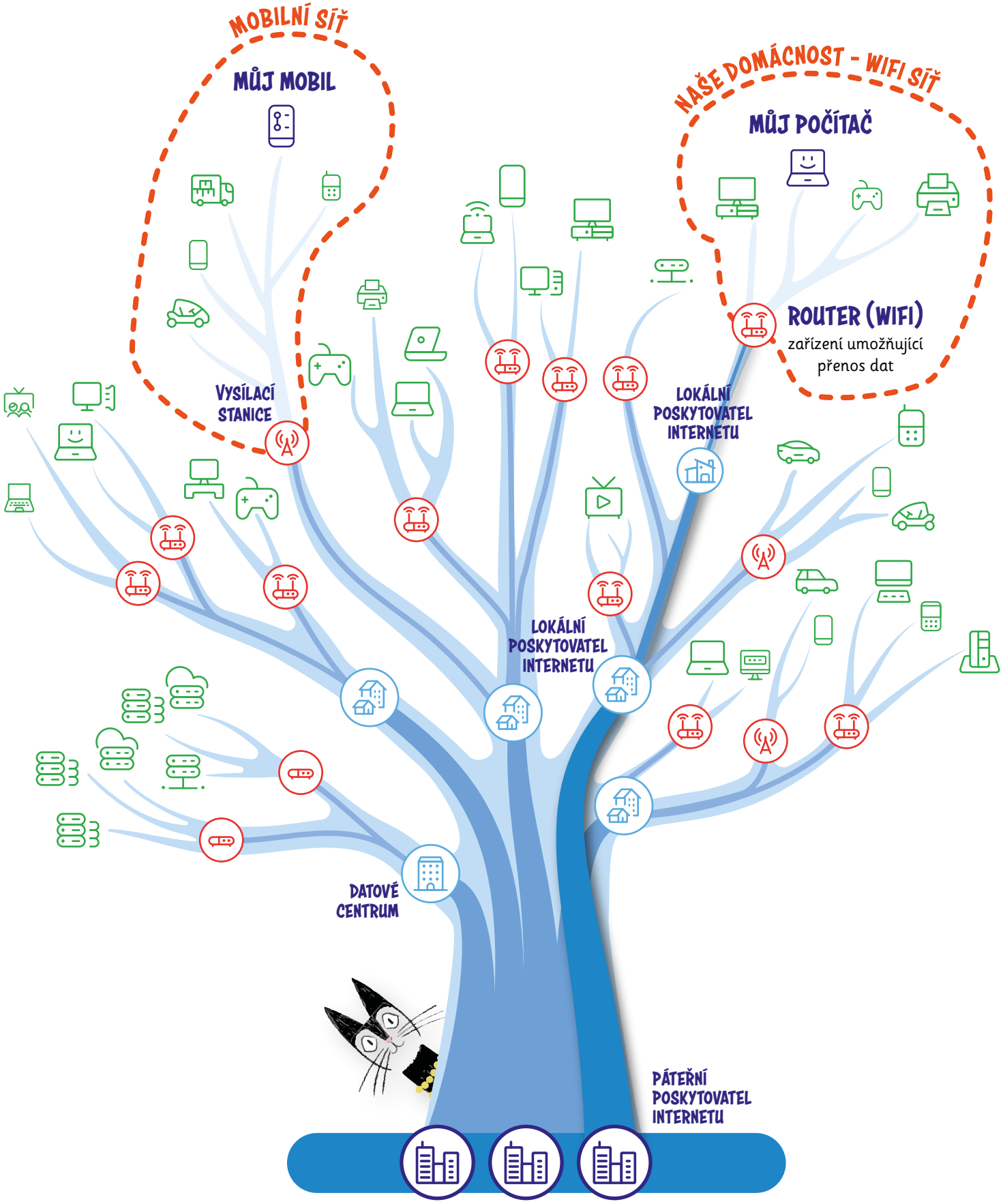
Internet má 4,57 miliardy aktivních uživatelů.

2030 – Odhadem 90 % světové populace online

Předpokládá se, že v roce 2030 bude mít internet přes 7,5 miliardy uživatelů (ve věku 6 let a starších), což odpovídá 90 % světové populace z předpokládaných 8,5 miliardy lidí (zdroj: Cybersecurity Ventures).

JAK VYPADÁ INTERNETOVÁ SÍŤ?

Velmi zjednodušeně si můžeme strukturu internetu představit jako strom.



JAK VYPADÁ INTERNETOVÁ SÍŤ?

Internet je největší počítačová síť, která se skládá z velkého množství menších sítí. Je v ní zapojeno obří množství zařízení z celého světa – počítače, mobily, televize, tiskárny a další různá zařízení.

Kde se ale internet bere? Jak se dostane až do našeho mobilu nebo počítače? Jakou trasu musí informace projít, než se dostanou do našeho zařízení? **Velmi zjednodušeně si můžeme infrastrukturu internetu představit jako strom.**

Když se podíváme na strom, vidíme spoustu jednotlivých lístků. Počítač nebo smartphone, který máme před sebou, je jedním lístkem na větvičce. Na této větvičce je spousta dalších lístků (např. zařízení připojená k internetu v naší domácnosti nebo ve třídě).

Tyto lístky propojuje větvička (např. wifi router nebo vysílací stanice pro zařízení v mobilní síti).

Větvička roste ze silnější větve (lokální poskytovatel internetu), která je napojena na silnější a silnější větve. Kmen pak ty nejsilnější větve propojuje, stejně jako páteřní poskytovatel internetu propojuje největší sítě internetu.

Stejně jako jsou na stromě propojené všechny listy skrze větve a kmen, jsou v internetové síti propojena jednotlivá koncová zařízení.

Důležitou součástí internetové sítě jsou datová centra. Slouží k provozu webových aplikací, ukládání a zpracovávání dat.

ZABEZPEČENÁ VS. NEZABEZPEČENÁ KOMUNIKACE

NEPUSŤTE HACKERA KE SVÉMU HESLU

HTTP://WWW.CHCIVSECHNO.COM

FILIP

HESLO: STAR_*WARS28!

ODESLANÉ BEZ ZABEZPEČENÍ

HACKER UVIDÍ
STAR_*WARS28!

HTTPS://WWW.NECHCIVSECHNO.COM

MÍNA

HESLO: NIC!NEUVIDIS4

ODESLANÉ ZABEZPEČENĚ

HACKER UVIDÍ
JEN ZMĚŤ ZNAKŮ

JE STRÁNKA POD ZÁMKEM?

HTTP://WWW.CHCIVSECHNO.COM

HTTPS://WWW.CHCIVSECHNO.COM

ZABEZPEČENÁ VS. NEZABEZPEČENÁ KOMUNIKACE

NEPUSŤTE HACKERA KE SVÉMU HESLU

Na obrázku si Filip otevřel stránku *http://www.chcivsechno.com*. Chtěl se přihlásit ke svému profilu, a tak zadal svoje přihlašovací údaje spolu s heslem Star_*Wars28! a odeslal je. Nevšimnul si však, že **spojení se stránkou není zabezpečené**. Útočníkovi (hackerovi) se podařilo zachytit údaje, které Filip při přihlašování odesílal, **ve stejné podobě**, jako je Filip zadával.

Mína si otevřela stránku *https://www.nechcivsechno.com*. Při přihlašování ke svému profilu zadala své údaje a heslo Nic!Neuvidis4 a odeslala je. **Spojení se stránkou je naštěstí zabezpečené**, a tak se útočníkovi nepodařilo Míniny údaje zachytit. **Hacker vidí pouze změť znaků**, kterou nedokáže jednoduše rozluštit.

Co je to tedy zabezpečená a nezabezpečená komunikace na internetu?

Internetovou komunikací rozumíme přenášení jakýchkoliv informací na internetu. Zabezpečená komunikace pak znamená, že informace, které na internet odešleme nebo jeho prostřednictvím získáme, jsou chráněné a soukromé. Proto je před zadáváním citlivých informací (jako je zadávání údajů z platební karty) důležité zkontrolovat, že prohlížeč s webem navázal soukromé, zabezpečené spojení – například tak, že u adresního řádku zpravidla vidíme symbol zámku. Zabezpečenou komunikaci také znázorňuje prefix https:// (pozor, ne http://) před adresou stránky. Avšak prohlížeče někdy tento prefix skrývají.

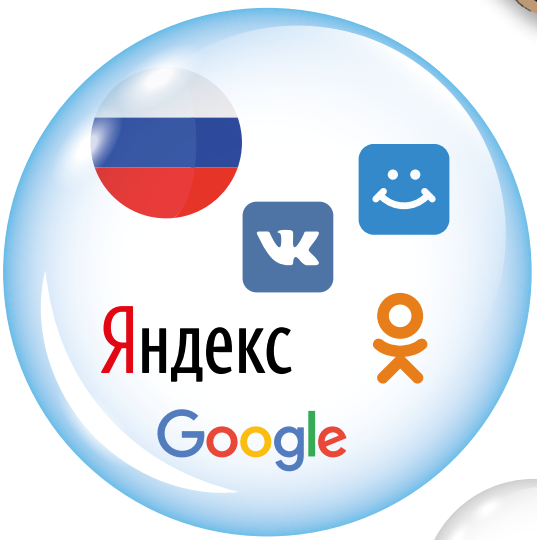
Dnešní prohlížeče standardně na zabezpečení webu upozorňují, ale i přesto je důležité být při sdílení soukromých informací vždy opatrný a zkontrolovat, zda jsme opravdu na webu, který chceme navštívit.

Úrovní zabezpečení internetové komunikace může být více. **Musíme být zvlášť obezřetní například při využívání veřejné wifi**, kde je riziko, že útočník zjistí naše citlivé údaje, vysoké.

RŮZNÉ INTERNETOVÉ SVĚTY

Žijeme v bublinách

WEBOVÉ STRÁNKY, KTERÉ VYUŽÍVÁM, JSOU JENOM VELMI MALOU ČÁSTÍ INTERNETU. JE TO POUZE MOJE INFORMAČNÍ BUBLINA.



LIDÉ V RŮZNÝCH KOUTECH SVĚTA VYUŽÍVAJÍ KE STEJNÝM ČINNOSTEM JINÉ WEBOVÉ SLUŽBY, NEŽ JSME ZVYKLÍ V ČESKU.

RŮZNÉ INTERNETOVÉ SVĚTY – ŽIJEME V BUBLINÁCH

V různých koutech světa lidé mnohdy využívají ke svým činnostem jiné webové služby. V Česku a jiných zemích například běžně využíváme vyhledávač Google, zatímco v Číně je zakázaný a namísto něj internetový uživatelé využívají zejména vyhledávač Baidu. U nás je populární i vyhledávač Seznam.cz, v Rusku pro změnu Yandex.ru. Jednotlivé vyhledávače se však neliší pouze jazykem, ale i svým obsahem.

Také sociální sítě jako Instagram, TikTok, Facebook či YouTube jsou sice rozšířené celosvětově (včetně Česka), ale v některých zemích lidé využívají služby své – v Číně je nejrozšířenější WeChat, v Rusku je velmi oblíbená síť VKontakte.

Po celém světě bychom takových příkladů našli spousty.

Je důležité si tedy uvědomit, že se k **internetovým uživatelům z různých zemí dostávají často odlišné informace**. Například v Číně státní moc otevřeně hlídá a cenzuruje obsah internetu. Záměrně či nezáměrně mohou být tedy uživatelé izolováni od určitých informací, což může vést k omezení různorodosti názorů. Tomuto efektu říkáme **informační bublina**. Internet je proto vhodným nástrojem pro šíření propagandy.

Mějme proto na paměti, že webové stránky, které využíváme, jsou ovlivněné naší informační bublinou a jsou jenom velmi malou částí internetu.

JAK FUNGUJÍ SOCIÁLNÍ SÍTĚ

MÍNA

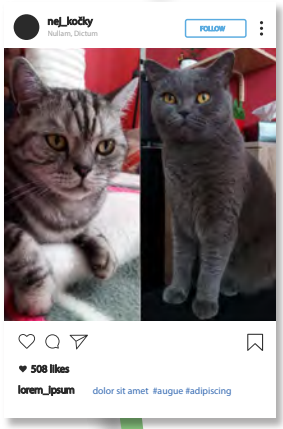
ZAJÍMÁ SE O KOČKY

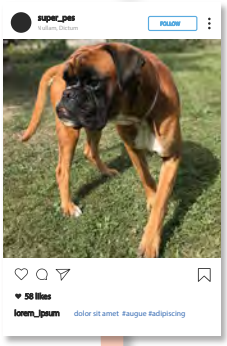
NEZAJÍMÁ SE O PSY

ZOBRAZOVANÉ PŘÍSPĚVKY

KOČKY ANO

PSY NE





PROHLÍŽÍ SI NEBO LAJKUJE KOČKY

MÍNĚ SE ZOBRAZUJE VÍCE KOČEK

KOČKY, KOČKY, KOČKY...

MÍNĚ SE ZOBRAZUJE MÉNĚ PSŮ

NEPROHLÍŽÍ SI PSY

Automatický výběr příspěvků

JAK FUNGUJÍ SOCIÁLNÍ SÍTĚ?

Každému z nás se na sociálních sítích zobrazují příspěvky na základě našeho chování online. **Sociální sítě tedy nabízí obsah přesně na míru** – takový, aby nás co nejvíce bavil a zajímal. A jak vědí, co nás bude bavit a zajímat?

Ukážeme si příklad na Míně.

Mína má ráda kočky. Když si prohlíží obsah své sociální sítě, věnuje příspěvkům s kočkami pozornost. Kdykoliv jí vyskočí příspěvek o kočce nebo s kočkou, se zájmem si jej prohlíží, lajkuje ho nebo okomentuje. Algoritmus sociální sítě (neviditelný proces, který vybírá příspěvky k zobrazení) si toho všímá a podle toho přizpůsobuje zobrazovaný obsah. Míně se pak zobrazí další a další fotky, videa, reklamy či jiný obsah související s kočkami.

Zároveň se Mína nezajímá o psy. Když si prohlíží svou sociální síť, příspěvky se psy přeskakuje a nevěnuje jim tolik pozornosti. Algoritmus si toho taktéž všímá, a obsah související se psy jí proto nenabízí tak často.

Výsledkem je, že se Míně zobrazuje více příspěvků souvisejících s kočkami a méně příspěvků se psy. Dokud Mína nezmění na sociální síti své chování, tento koloběh se bude opakovat.

To může způsobit, že Mína toho sice bude hodně vědět o kočkách, ale o psech se toho moc nedozví. Je to sice škoda, ale není to žádná katastrofa.

Větším problémem může být, když se **filtrování informací** (a uzavření se ve své informační bublině) **týká důležitých témat**, jako je například politika, názory na veřejné dění nebo zdraví.

POZNÁMKY

POZNÁMKY

POZNÁMKY

JSNS.CZ

LEPŠÍ ŠKOLA PRO VŠECHNY

nadační fond avast

Jan Barta
Dušan Šenkypl
David Holý

Hana Dvořáková **Ondřej Fryc** **Martin Hájek** **Libor Winkler**

Seriál V digitálním světě, který je i včetně doprovodných výukových materiálů součástí metodické příručky V digitálním světě, byl podpořen z programu O2 Chytrá škola.

O2 Chytrá škola

o2chytraskola.cz