Systém podpory profesního rozvoje učitelů a ředitelů

Metodická příručka
NMK Informatika a ICT

KYBERNETICKÁ BEZPEČNOST A KYBERPROSTOR

WBS kód: 4.1.6.1.2

Autoři: Petra Vaňková a kolektiv autorů

www.projektsypo.cz

sypo.info@npi.cz

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

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Abstrakt

I vzhledem k situaci, která nastává v posledních letech, je hlavním motivem většiny škol, dalších organizací a vzdělávacích institucí fenomén internetu, kyberprostoru a s tím související bezpečnost v něm. Jedná se o velmi důležitou součást života všech žáků, pedagogických pracovníků i zákonných zástupců a všech dalších aktérů zajišťující nebo podporující vzdělávací proces. A právě z tohoto důvodu bylo Národním metodickým kabinetem Informatika a ICT zvoleno toto téma pro zpracování další, v pořadí třetí metodické příručky, která tak volně navazuje na příručku, zabývající se převážně online prostředím i příručku s prioritním zaměřením na cloudové technologie.

Metodická příručka vznikla jako jeden z výstupů projektu SYPO aktivit Národního metodického kabinetu Informatika a ICT a jejím hlavním cílem je motivovat a inspirovat učitele k realizaci aktivit zaměřených právě směrem ke kybernetické bezpečnost, kyberprostoru a internetu samotném. Reaguje na současné změny kurikulárních dokumentů nejen pro obor Informatika, ale ukazuje i možnosti přesahu této problematiky do dalších předmětů a oborů.

V příručce je obsaženo 7 aktivit, na kterých se podílel kolektiv autorů. Součástí příručky jsou také již vytvořené webové stránky, či aktivity se základní charakteristikou. Celkem jich bylo posbíráno 20. Nelze předpokládat, že by byl vytvořen ucelený systém nebo rozcestník aktivit nebo webových stránek. Jedná se o zajímavé příklady, které vybraly členové NMK ICT a další spolupracovníci projektu SYPO. Zároveň by měly ukazovat další možnosti v orientaci v tématu Kyberprostor a bezpečnost.

Obsah

1 Úvod

V současném světě, kde využíváme běžným způsobem digitální technologie a internet jak pro svou osobní potřebu, tak pro studium či práci, se začínají více rozkrývat hlouběji témata související i s ochranou v digitálním světě a tzv. kyberprostoru. Tato témata by měla zcela jistě promítat i do vzdělávacího procesu na všech stupních vzdělávání, a to nejen v rámci obsahu vzdělávacího oboru Informatika[1], ale dá se přemýšlet o kyberprostoru a bezpečnosti v něm jako o součásti digitální gramotnosti napříč obory[2]. Lze tedy uvažovat o tom, že se jedná o součást kompetence digitální, kterou by měly rozvíjet postupně v průběhu celého svého života. V rámci digitální gramotnosti se vymezuje dokonce dílčí kompetence bezpečnost, do které spadá například ochrana zařízení, ochrana osobních údajů a soukromí či ochrana zdraví a pohody. Zdá se být také nedílnou součástí dílčí digitální kompetence komunikace a kolaborace v tématech souvisejících se sdílením dat a spoluprací, netiketou nebo správou digitální identity.[3] Je totiž nutné podotknout, že je toto téma velmi stěžejní pro další obory, už vzhledem k tomu, že nevhodné využívání internetu a kyberprostoru obecně může mít pro žáka zásadní důsledky v jeho dalším vzdělávání, profesním životě i osobní rovině. Žáci se totiž v kyberprostoru pohybují stále více, a tudíž se dá předpokládat, že i hrozby a nástrahy s tím související budou pro ně čím dál častější. Nejde zde pouze o kyberšikanu nebo zapomenuté heslo. Témata spojená s kyberprostorem a bezpečností jsou provázaná s různými dalšími obory a oblastmi, nutno pamatovat i na etiku (či netiketu), či osobnostní a sociální výchovy. Nelze tedy říct, že aktivity spojené s tímto tématem jsou pouze technické, naopak se dostávají i do osobní a sociální roviny, či dokonce do finanční gramotnosti mnohem častěji, než tomu bylo dříve, a mohou mít velmi zásadní vliv na spokojený a bezpečný život žáka. Z těchto důvodů není možné ponechat témata spojená s kyberprostorem a kyberbezpečností pouze na učitelích informatiky, nebo na preventistech a preventivních programech pro školy. A škola by měla přemýšlet i o naplňování těchto témat v rámci klíčové kompetence digitální a zvyšování digitální gramotnosti žáků i učitelů v této problematice v dalších oborech a předmětech.

Zajímavostí u pojmu kyberprostor (cyberspace) by se mohlo zdát, že ve skutečnosti jeho zavedení vychází z povídek a románů. Příkladem může být román Williama Gibsona Neuromancer (1984)[4], v českém překladu od O. Neffa (1992). Nedá se zde sice vyložit tak, jak je v současnosti kyberprostor popisován, nicméně jisté konsekvence ještě ve spojení s umělou inteligencí či virtuální realitou by se zde jistě našly. O kyberprostoru se jako o „technickém pojmu“ hovoří více méně až na začátku 21. století a následně se přistupuje k popisu z technického, technologického, ale i sociálního hlediska. Kyberprostor se dá popsat jako nehmotný imaginární svět informací, které vznikají v důsledku propojování digitálních technologií, resp. informačních a komunikačních technologií, a prací s informacemi. Jeho součástí je například i internet.[5] V České republice je v legislativě ukotven pojem kybernetický prostor jako „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*“.[6]

[1] Dle revidovaného RVP ZV (2021)
[2] V rámci klíčové kompetence digitální dle revidovaného RVP ZV (2021)
[3] https://digigram.cz/vymezeni-digitalni-gramotnosti/
[4] https://muse.jhu.edu/article/21645
[5] https://wiki.knihovna.cz/index.php/Kyberprostor
[6] Zákon č. 127/2005 Sb. – zákon o elektronických komunikacích; Zákon č. 181/2014 Sb. – o kybernetické bezpečnosti

Již z výše čteného textu je jistě vidět jisté nutné propojení s bezpečností v kyberprostoru, tedy tzv. kybernetickou bezpečností. V České republice se problému bezpečnosti na národní úrovni věnuje Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) jako výkonná sekce Národního centra kybernetické bezpečnosti (NCKB), přičemž národní strategie a akční plány v této oblasti jsou k dispozici přímo na jejich stránkách.[7] Z hlediska legislativy se pak jedná o zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a kybernetickou bezpečnost lze tedy definovat dle těchto dokumentů jako *„soubor organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřující k zajištění zabezpečeného, chráněného a odolného kyberprostoru“.* S tím samozřejmě souvisí i kybernetické hrozby a rizika, kybernetická kriminalita, či kyberterorismus.

Pokud mluvíme o kyberprostoru, vždy bychom měli mít na paměti právě i bezpečnost v něm, a to i vzhledem k tomu, že se jedná o otevřený, veřejně přístupný virtuální prostor, ve kterém velkou roli hraje i „smyšlená anonymita“, která s sebou nenese na první pohled zodpovědnost. A právě síla informací, jejich komunikace, vytváření, sdílení či uchovávání v různých spektrech lidské činnosti ve virtuálním prostředí s sebou nese jistý potenciál nebezpečí, obzvláště pro děti, či žáky.

Zcela stěžejní je děti, žáky, vlastně i dospělé v této oblasti vzdělávat a pamatovat na to, jak rychle se tento kyberprostor mění. Ukázkové příklady jsou uvedeny v této příručce, nicméně netvoří ucelený soubor aktivit, které by dávaly dohromady příručku, jak vyučovat tuto oblast (a ani si takový cíl neklademe), ale měla by spíše přinášet vybrané nápady a aktivity, které je možné v této oblasti využít.

[7] https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

2 Aktivity

2.1 Popis aktivit

V této publikaci je popis aktivit obdobný jako v předchozích dvou metodických příručkách, aby byla podpořena kontinuita celé sady. Všechny aktivity byly vytvořeny a zpracovány s ohledem na nový RVP ZV, klíčovou aktivitu digitální a v případě aktivit spojených se střední školou jsou respektovány a podporovány aktivity s ohledem na rozvoj informatického myšlení a digitální gramotnosti.

Aktivity jsou popsány základními vlastnostmi:

- **stupeň vzdělání** – typicky 1. stupeň ZŠ, 2. stupeň ZŠ, popřípadě konkrétním ročníkem: 3. ročník SŠ;
- **naplňované indikátory/výstupy dle RVP, oblast, téma** – v případě RVP ZV je uvažováno již o revidovaném RVP ZV;
- **předpokládaný rozsah** – časové hledisko, typicky 1 vyuč. hodina, 30 min.;
- **vstupní požadavky na žáka** – reaguje na nutné požadavky jak z hlediska vědomostí, tak dovedností nejen z oboru Informatika, ale i dalších nutných; např. žák zvládá práci s procenty, žák zná hlavní města zemí sousedících s Českou republikou;
- **cíl aktivity** – jedná se o hlavní naplňovaný cíl aktivity (nejedná se o vzdělávací cíl), je možné připojit i dílčí cíle nesouvisející přímo s oborem Informatika;
- **potřebné vybavení** – jedná se o vybavení, které je nutné k hladkému průběhu aktivity, nemusí se jednat pouze o digitální technologie, ale i běžné pomůcky, např. fixy.

Následně je příspěvek popsán následujícím způsobem:

- **základní potřebné informace o aktivitě** – základní popis, abstrakt, myšlenka aktivity; měla by být vyjádřena v několika větách, aby vyučující pochopil samotnou podstatu aktivity;
- **příprava na výuku** – popisuje základní nutnou přípravu učitele na samotnou realizaci výuky, typicky, co musí připravit před samotnou výukou (např. instalace softwaru, příprava účtů žáka v konkrétním cloudovém prostředí, tisk pracovního listu);
- **organizace práce** – popisuje základní metody a formy výuky, které jsou v průběhu realizace výuky využity; je možné obecně popisovat organizaci práce např. dle E-U-R;
- **průběh výuky** – lze pojímat časově jak z hlediska vyučujícího, tak žáků; popř. rozpracované orientační časové hledisko.
- Reflexe výuky – v případě, že byla aktivita autorem výuka realizována, může reflektovat své konkrétní zkušenosti.
- Na co si dát pozor – autor aktivity popisuje rizika, která mohou souviset s realizací samotné výuky.

Další možné doplnění aktivity:

- **alternativní řešení** – autor může popsat další předměty, témata, ve kterém lze realizovat aktivitu, popř. aktivitu přizpůsobit;
- **další podobné příklady z praxe** – lze připojit již vytvořené aktivity, příklady aktivních učitelů, zahraniční příklady, webové stránky institucí aj.

2.2 Souhrn aktivit

Tabulka 1: tabulka vytvořených aktivit

	Název aktivity	Stupeň vzdělávání
1	Interpretace obrázků – Fake news	1. st. ZŠ
2	Spyware (jako součást Malware)	Základní vzdělávání
3	Úrovně internetu	2. st. ZŠ
4	Internet věcí mezi námi	Sekundární vzdělávání
5	Virtuální měny	2. st. ZŠ., popř. SŠ
6	Vishing	9. tř., SŠ, SOŠ
7	Opakování termínů v oblasti internetu a kybernetické bezpečnosti	SŠ, SOŠ

2.3 Jednotlivé aktivity

2.3.1 Interpretace obrázků – Jak nevěřit všemu

Tabulka 2: popis aktivity: Interpretace obrázků – jak nevěřit všemu

Stupeň vzdělávání	1. stupeň ZŠ (v případě modifikací obrázků je možné využít i na 2. stupni ZŠ)
Naplňované indikátory dle RVP ZV, oblast, téma	Obor Informatika, vzdělávací obsah Digitální technologie, téma Bezpečnost; Data, informace a modelování: data a informace – obrázek
Předpokládaný rozsah (časové hledisko)	1 vyučovací hodina
Vstupní požadavky na žáky	Bez specifických požadavků
Cíl aktivity	• Žák si uvědomí, že část obrázku nemusí mít vypovídající hodnotu. • Žák si uvědomí, že díky sledování části, nikoliv celku, obrázku se mohou informace na obrázku interpretovat nesprávně. • Žák je veden k diskuzi a vyjádření svých pocitů z obrázku. • Žák by si měl uvědomit, že díky vidění části obrázku se může celá situace na obrázku jevit nebo vysvětlovat úplně jiným způsobem a že věřit jen tomu, co vidíme bez ověření, může vést k dezinformacím (základ k tomu, aby žák porozuměl fake news).
Rozvíjené kompetence	Digitální kompetence: • Informační a datová gramotnost: hodnocení dat • Komunikace a kolaborace: netiketa • Bezpečnost: ochrana zdraví a pohody Klíčové kompetence: • K učení: formuluje, jaký význam má získaná informace pro běžný život, a propojuje nově získané – získané informace chápe včetně souvislostí a vysvětlí je. • K řešení problému: formuluje jednoduchou hypotézu; srozumitelně vysvětluje své řešení; změní své závěry na základě nových informací. • Komunikativní: pro jednotlivce i pro celou třídu srozumitelně vysloví svou myšlenku; vyslechne druhého, aniž by ho zbytečně přerušoval; odpoví na položenou otázku, řekne svůj názor na věc; různými způsoby vyjádří své názory, pocity a myšlenky.
Potřebné vybavení	Učitel využívá projekt ke spuštění prezentace.

Základní potřebné informace o aktivitě

Tato aktivita je vytvořená pro žáky prvního stupně, aby si uvědomili, že pohled na upravený a oříznutý obrázek na internetu nemusí mít vždy stejnou vypovídající hodnotu a že pokud nám někdo představí jen část obrázku (informace), tak nás může mystifikovat, zavádět nás, záměrně nám lhát

nebo zakrývat pravdu. To by mělo následně vést k tomu, že děti budou lépe připraveny na témata související s fake news a popř. práci s dezinformacemi, které se mohou na internetu nacházet.

Cílem aktivit je vyvolat v žácích emoce z toho, co vidí na kousku obrázku a co je pak následně na celém obrázku. Velmi důležité v této aktivitě je nechat žáky vyjádřit své názory, co se může dít na kousku obrázku a následně je nechat promlouvat o tom, co vidí na celém obrázku a jak se změnil jejich názor na část obrázku.

Příprava na výuku

Není nutná specifická příprava na samotnou aktivitu. Učitel může projít a doplnit připravenou prezentaci, popř. podobně vytvořit vlastní prezentaci dle typu obrázků, na kterých chce demonstrovat možnost vzniku dezinformace. K dispozici je i samotná sada obrázků, které jsou využity v prezentaci.

Organizace práce

Velmi důležitou součástí této aktivity je diskuze, motivace žáků mluvit o tom, co vidí a jak na ně působí to, co vidí, a jaké důsledky mohou mít takto upravené obrazové materiály.

Nemělo by se jednat zcela o frontální výuku, kdy učitel představuje prezentace, ale důležitou součástí je aktivizace dětí a jejich vedení k vyjádření vlastních názorů.

Průběh výuky

1. Zahájení hodiny: představení hodiny – žáci budou dneska sledovat, jak se může změnit pohled na informaci, která je na obrázku, pokud uvidí pouze část obrázku.
2. Práce s prezentací – prezentace je tvořená 6 dvojicemi obrázků, které nějakým způsobem ukazují to, jak se může změnit pohled na konkrétní situaci, když vidíme jen kousek obrázku nebo obrázek celý. První dvě dvojice by měly uvést děti do samotné aktivity a navodit u nich zájem a motivaci. Další čtyři dvojice pak vždy vykreslují konkrétní situaci, která se velmi zkreslí, pokud ukážeme jen část obrázku:

a. Emoce dětí (radost + smutek)
b. Hořící deštný prales
c. Demonstrace
d. Válka

Obrázek 1: ukázka z prezentace autora (viz prezentace autora)

- Velmi důležité je dát žákům dostatek prostoru pro vyjádření svých pocitů jak z části, tak celku. Zároveň je důležité s žáky mluvit o tom, jaké důsledky mohou mít takto zkreslené obrázky, pokud je někdo nesprávně pochopí, nebo nesprávně interpretuje.
- Poslední dva snímky prezentace pak již shrnují to, proč by lidé vlastně mohli dělat a co je důležité si z celé aktivity odnést – nedůvěřovat každému obrázku, který nalezneme na internetu. Může být buď zobrazena pouze jeho část nebo může být i jinak upravený (pokud učitel bude chtít dávat důraz na upravené obrázky, je vhodné využít a připravit jiný materiál).

Reflexe:

Na co si dát pozor

- Vhodné je nechat vyjádřit názor na jeden obrázek více dětí a nechat je diskutovat. Nepříjemné je, pokud se překřikují a nejsou vedeni k tomu, aby se poslouchali. Zároveň je pro učitele důležité slyšet názory více dětí, ne pouze těch aktivních. Dobré je pro aktivitu využít některou z metod formativního hodnocení (např. tahání špejlí se jmény dětí).
- Důležité je nezapomenout vysvětlit žákům situace, které jsou vyobrazeny na čtyřech dvojicích zabývajících se emocemi, ekologickou katastrofou, demonstrací a válkou, a snažit se děti upozornit na to, že každé zkreslení situace médii může mít velké důsledky.

Alternativní řešení

- Dalším typem aktivity by mohla být práce s upravenými obrázky (tj. přímo schválně modifikovanými), ne pouze obrazovými materiály, kde je předáván divákovi pouze výřez.
- Není nutné, aby aktivita probíhala pouze v předmětu Informatika.
- Aktivitu je možné s výběrem jiných obrazových materiálů modifikovat i pro žáky druhého stupně základní školy.

2.3.2 Spyware

Tabulka 3: popis aktivity Spyware

Stupeň vzdělávání	Základní vzdělávání (úprava pro 1. i 2. stupeň)
Naplňované indikátory dle RVP ZV, oblast, téma	Obor Informatika, vzdělávací obsah Algoritmitzace a programování, téma Animace ve Scratch
Předpokládaný rozsah (časové hledisko)	3 vyučovací hodiny, popř. projektový den (1. stupeň) 2 vyučovací hodiny (2. stupeň)
Vstupní požadavky na žáky	Žák zvládá základní práci s programem Scratch. 1. stupeň: žák rozumí čtenému textu. 2. stupeň: žák se orientuje v pojmové mapě.
Cíl aktivity	• Cílem aktivity je představit žákům spyware jako součást malwaru, jeho vlastnostem, typům a nebezpečí, které mohou způsobit zařízení (včetně mobilního telefonu). • Dílčím cílem je naprogramovat/naanimovat vlastní pojetí spyware prostřednictvím prostředí Scratch.
Rozvíjené kompetence	Digitální kompetence: • Tvorba digitálního obsahu (vytváření digitálního obsahu, programování) Klíčové kompetence: • K řešení problému: vytváří a využívá vizuální znázornění problému, posoudí, zda jeho výsledné řešení dává smysl • Komunikativní: při vyjadřování uspořádá informace logicky; obhajuje svůj názor asertivním způsobem • Sociální a personální: rozdělí si ve skupině úkol na části a přijme svou část, včetně zodpovědnosti za její plnění; samostatně (individuálně i jako členové skupiny) se postarají o hotové dílo;
Potřebné vybavení	Instalace prostředí Scratch či účet v online prostředí Scratch

Základní potřebné informace o aktivitě

Základní myšlenkou aktivity je představit žákům vlastnosti spyware prostřednictvím vlastní aktivity tvorba animace v prostředí Scratch. Díky základním údajům, které jim poskytne učitel, popř. které naleznou v příslušných internetových zdrojích, žáci vytvoří své pojetí spyware. Základními údaji pro první stupeň je krátký příběh, ve kterém se spyware představuje jako „zlý skřítek“, a v případě druhého stupně základní informace o spyware a malware.

Nabízí se několik možností, jak pojmout samotnou „animaci“:

představení spyware formou monologu (kdy „postava“, která symbolizuje spyware, o sobě vypráví);

animace toho, co spyware dělá (např. výběr některých nežádoucích činností spyware: přesměrování na jinou domovskou stránku, vyskakující reklamy, přesměrování telefonního čísla, sledování pohybu na klávesnici);

animace/představení toho, jak se proti spyware bránit.

V tomto pojetí aktivity by žáci měli hlouběji pochopit, co spyware představuje, na které vybrané typy spyware mohou narazit a jak se proti němu bránit. Zároveň je tato aktivita propojená s jednoduchou algoritmizací, či spíše animací v prostředí Scratch, kde si žáci (zejména ti mladší) mohou navrhnout pro ně přiměřenou grafickou podobu spyware.

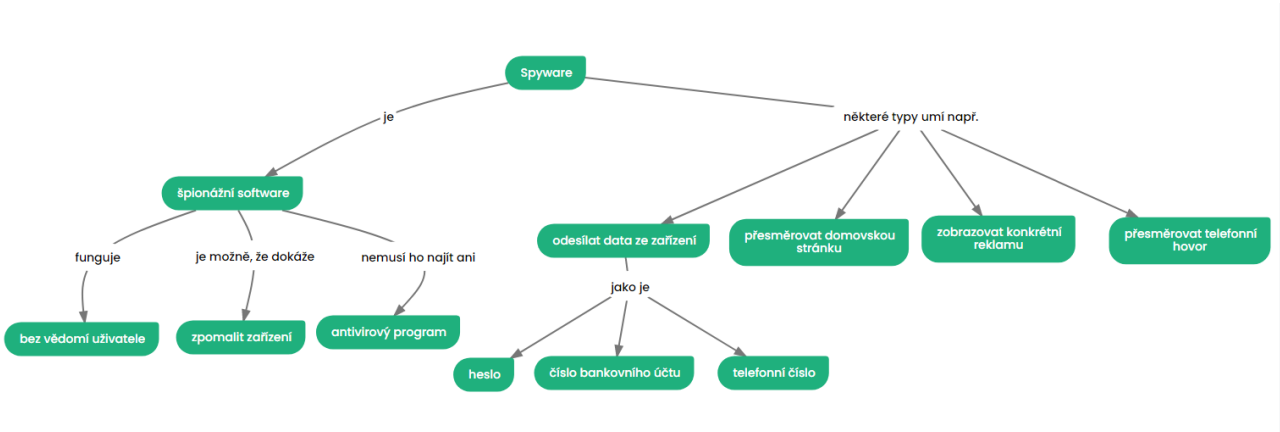
Příprava na výuku

- poskytnutí základních informací ohledně spyware:

1. stupeň: forma představení (odkaz)

> Já jsem takový malý špión v počítači. Jmenuji se Spyware.
> A co dělám? Procházím se po tvém počítači nebo telefonu a hledám informace. Hledám jen informace, které jsou pro někoho dalšího dobré a nemůže je získat. Některé informace se dají dokonce prodat. A ti lidé, co mě do tvého počítače a telefonu poslali, takové informace chtějí získat. Zajímá tě, co hledám? Tak třeba hesla nebo uložená telefonní čísla.
> Můžu být strašně nenápadný a ani si mě nevšimneš. Většinou mě dokonce nenajde ani antivirový program. Já ale vím, co v telefonu nebo na počítači děláš. A hned to pošlu dál. Kam? No, těm lidem, co mě vytvořili.
> Umím být i hodně zlý a posílat ti do webových stránek reklamu. Nebo tě dokonce umím přesunout na jinou webovou stránku. Dávej si na mě pozor. Já ti totiž dokážu zpomalit počítač nebo telefon.

2. stupeň: pojmová mapa se základními informacemi o spyware (odkaz na pojmovou mapu) – tato mapa představuje pouze základní hierarchii a učitel si ji může doplnit dle požadované úrovně znalostí žáků.



Obrázek 2: základní pojmová mapa: spyware

- v případě nutnosti dílčí příprava učitele v prostředí Scratch (např. instalace prostředí, příprava účtů v online prostředí, představení grafických možností Scratch, popř. příprava příkladů, jak samotnou aktivitu realizovat):

- náhledy připravených animací na jiná témata pro inspiraci žáků i učitele: (není cílem předvést výsledný produkt, aby žáci nepracovali nápodobou, ale naopak měli motivaci pro realizaci vlastního výstupu).
  - vtip: https://scratch.mit.edu/projects/249353135/
  - vysvětlení proměnné: https://scratch.mit.edu/projects/213960547/

Pokud se učiteli žádná z ukázek nezamlouvá, může využít části kap. 6 v učebnici vytvořené v rámci projektu PRIM Programování ve Scratch pro 2. stupeň základní školy[8] nebo libovolnou jinou animaci z databáze Scratch dle vlastního výběru: https://scratch.mit.edu/explore/projects/animations/.

Organizace práce (realizace na 1. stupni)

1. Společná práce – čtení textu
2. Skupinová práce, popř. práce ve dvojici – spyware a animace
3. Diskuze a představení vlastních výtvorů a animací

Organizace práce (realizace na 2. stupni)

1. Frontální výuka – představení spyware, popř. malware s využitím pojmové mapy
2. Práce ve dvojicích – grafická podoba, animace, popř. programování vymyšleného konceptu pojetí spyware
3. Představení vlastního konceptu představy o spyware

Průběh výuky na 1. stupni (časový harmonogram rozpracován pro projektový den)

1. Základní informace o tom, co je cílem hodiny, co budou žáci dělat a co bude výsledkem jejich práce. (5 min.)
2. Společné čtení připraveného textu. Učitel následně dotazy kontroluje, zda žáci porozuměli čtenému textu. (15 min.)
3. Rozdělení žáků do menších skupin a následná práce:
   a. Vymyšlení, jak bude spyware vypadat (tužka, pastelky, papír) (20 min.);
   b. Společný scénář, jak se bude spyware představovat (20 min.);
   c. Převedení podoby připraveného spyware do grafického prostředí Scratch (30 min.);
d. Vytvoření animace v prostředí Scratch (30 min.)
4. Diskuze a představení vlastních výtvorů a animací (dle počtu skupin a času, který je k dispozici vzhledem k délce projektového dne).

Průběh výuky na 2. stupni

1. Na začátku výuky je vhodné shrnout a přiblížit žákům malware, včetně některých rizik. Jedná se pouze o motivační část, aby se zajímali o jeden konkrétní druh, a to spyware. (10 min.)
2. Následně je žákům předána pojmová mapa (možné předat jak v elektronické, tak tištěné podobě) a učitel prostřednictvím dotazů kontroluje, zda žáci rozumí takové strukturaci informací. Poté probíhá krátká diskuze o tom, zda se žáci již s nějakým spyware setkali a jaké mají zkušenosti s těmito typy softwaru. (15 min.)

[8] https://imysleni.cz/images/vzdelavaci_materialy/Scratch2st_kapitoly/Kap6_zakovske_listy.pdf

3. Poté se žáci rozdělí do skupin (nejlépe dvojic) a rozdělí si úkoly v rámci zadané aktivity (20 min.): jejich úkolem je vytvořit krátkou animaci (dle preferencí učitele, nápady výše), např. výukovou, kde
   a. první žák: navrhuje grafickou podobu animace,
   b. druhý žák: navrhuje dialog, monolog, resp. samotný obsah krátké animace.
   Důležitá je spolupráce obou žáků mezi sebou. Jeden bez druhého nebudou schopni celou práci dokončit a je potřeba se domluvit na základních parametrech. První z žáků může začít okamžitě pracovat ve Scratch a vytvářet grafickou podobu. Druhý z žáků se následně přidá v momentě, kdy už má vymyšlený a sepsaný text (ve Wordu nebo v jiném textovém editoru).
4. Společnou prací již následně zpracovávají animaci. V případě, že jsou dříve hotovi, mohou přidat zvuk i další animační prvky. (30 min.)
5. V poslední fázi je zapotřebí, aby si žáci vyměnili své zkušenosti z takto pojímané práce, představili své výtvory a popř. ohodnotili své výtvory mezi sebou, např. hvězdičkami (1 min., 5 max.). (15 min. – nutné přihlédnout k počtu žáků a také délce představení, které jim vyučující poskytne. Je možné využít např. konkrétního úložiště a samostatného posouzení žáků jednotlivých děl.) Tato činnost je velmi důležitá pro samotné sdílení jednotlivých prací žáků a představení vlastní práce i spolupráce a je vhodné vyčlenit žákům i více času, než udává časový rozpis, který je pouze orientační.

Reflexe:

Na co si dát pozor

- 2. stupeň – jiný způsob práce ve dvojici může být pro žáky nevyhovující. Nicméně má částečně simulovat práci ve firmě, kdy se na začátku domluví práce na projektu a pak následně se pracuje odděleně ve skupinách nebo jednotlivcích, aniž by třeba věděli, co dělá druhá skupina. Důležitá je tedy prvotní výborná domluva obou žáků.
- 2. stupeň – žáci budou Scratch považovat za dětské prostředí a nebudou motivováni animaci v tomto prostředí připravit. Je vhodné jim předvést některé ze složitějších aktivit, které jsou ve Scratch vytvořeny, aby pochopili, že toto prostředí lze využít i na vyšším levelu znalostí o algoritmech a programování.

Alternativní řešení

- Je možné využít i další prostředí, která jsou vhodná pro animaci, např. Canva, nicméně se částečně ztratí lineární tvorba programu.

2.3.3 Dimenze webu

Tabulka 4: popis aktivity Dimenze webu

Stupeň vzdělávání	2. stupeň ZŠ
Naplňované indikátory dle RVP ZV, oblast, téma	Obor Informatika, vzdělávací obsah Digitální technologie, téma internet
Vyhovujte podpůrným výstupům RVP (příp. indikátor)	Ne
Předpokládaný rozsah (časové hledisko)	1–2 vyučovací hodiny
Vstupní požadavky na žáky	Žák obecně rozumí pojmu internet. Žák zná běžné služby a aplikace, dokáže přiřadit ke službám jejich loga nebo ikony.
Cíl aktivity	• Ukázat žákům různé úrovně internetu, jejich aplikace a služby. • Upozornit žáky prostřednictvím úrovní internetu na některé aplikace a služby (u prvních dvou úrovní) a upozornit na nebezpečí třetí úrovně.
Rozvíjené kompetence	Digitální kompetence: • Informační a datová gramotnost: Správa dat, informací a obsahu • Bezpečnost Klíčové kompetence: • Kompetence k učení: získané informace chápe včetně souvislostí a vysvětlí je. • Kompetence k řešení problému: problém analyzuje z různých hledisek; vyvozuje závěry ze získaných poznatků • Kompetence komunikativní: k vyjádření používá grafická znázornění a symbolické prostředky; různými způsoby vyjádří své názory, pocity a myšlenky, dívá se na věci z různých hledisek, vyhýbá se paušálním hodnotícím soudům. • Kompetence sociální a personální: rozpozná, kdy je úkol (jeho etapa) hotov a že je čas přejít k další etapě; dotahuje celý úkol do konce; samostatně (individuálně i jako členové skupiny) se postará o hotové dílo; podle svého uvážení využívá zpětnou vazbu pro své další jednání.
Potřebné vybavení	Bez nutného vybavení (unplugged aktivita); na závěr vhodné lepidlo, psací potřeby, popř. pastelky

Základní potřebné informace o aktivitě

Internet jako pojem je pro žáky možná docela neuchopitelný pojem a každý si pod ním představuje úplně něco jiného. Pro někoho to může být prohlížeč, pro jiného Wi-Fi, pro někoho je to prostě to, co má v mobilu (z výpovědí žáků 6. třídy). Každopádně s „ním“ žáci běžně pracují a je zapotřebí jim ukázat i různé služby a aplikace, se kterými se zřejmě v blízké budoucnosti budou setkávat.

Myšlenkou této vyučovací hodiny je seznámit žáky s úrovněmi internetu (surface web, deep web, dark web) na příkladech jednotlivých služeb a aplikací. Žáci by tak mohli snáze pochopit alespoň jednu z možností dělení internetu. Zároveň by měli porozumět tomu, jak se od sebe první dvě úrovně internetu liší a jaká nebezpečí může přinášet třetí úroveň.

Příprava na výuku

- dle počtu skupin připravit vytištěné pracovní materiály (podklad ve tvaru rovnoramenného trojúhelníku, názvy jednotlivých úrovní, popis jednotlivých úrovní, příklady služeb a aplikací pro jednotlivé úrovně), ukázky jsou ke stažení ZDE.

Organizace práce

1. řízená diskuze na téma: co je to internet,
2. skupinová práce, postupná vytváření konečného vyučovacího materiálu.

Průběh výuky

1. Řízená diskuze: co je to internet? – pokud se žáci zdráhají odpovědět, učitel může přinášet různé příklady toho, co by podle žáků mohl být internet a žáci následně „odhadují“, zda to internet je, nebo není (Nelze přesně odhadnout dobu diskuze, záleží na zapojení žáků a vysvětlujících informací učitelem). Příklady možných návodných otázek různého typu:
   a. Je internet uvnitř počítače?
   b. Kdy mohu říct, že pracuji s internetem?
   c. Jak to poznám, že pracuji s internetem? (Jak poznám, že jsem na internetu?)
   d. K čemu potřebuji internet?
   e. Co potřebuji k tomu, aby se mi webová stránka načetla? Co potřebuji k tomu, abych mohl/a poslat zprávu přes chatovací prostředí kamarádovi?
   f. Jak probíhá komunikace mezi mým telefonem a webovou stránkou?
   g. Jaké služby na internetu využíváme?

Pozn. Pro systematičtější pochopení je možné využít pořad Nezkreslená věda Jak funguje internet (https://www.youtube.com/watch?v=L05HGoaDkRo). V deseti minutách je zde vysvětlen důvod a způsob vzniku internetu, jak funguje posílání souborů z jednoho počítače na druhý (packety a TCP/IP), služba www, optická vlákna (to už je složitější a pro tuto aktivitu ne zcela důležité pro pochopení, co je to internet, ale více pro způsob přenosu dat a počítačových sítí).

2. Je vhodné před samotnou aktivitou žákům vysvětlit, že internet se dá rozdělit různými způsoby a že jeden z těchto způsobů si následně ve skupinách ukážou. Tento způsob se bude více blížit tomu, s jakými „typy informací“ se v které úrovni můžeme setkat.

3. Žáci se rozdělí do tříčlenných až čtyřčlenných skupin (popř. je učitel dle svého uvážení rozdělí). *Při takto realizované aktivitě se jde s žáky od známých konkrétních aplikací a služeb internetu ke společným vlastnostem a až následně k obecné terminologii*:
   a. Každá skupina dostane různé služby, aplikace či vlastnosti a má mezi nimi najít společné rysy taky, aby tyto služby, aplikace a vlastnosti všichni dokázali rozdělit do 3. skupin. Vždy po skončení nějaké fáze probíhá buď společná kontrola nebo kontrola s učitelem ve skupině. *Možná bude nutné žáky upozornit, že některé služby nebo aplikace mohou být i součástí dvou úrovní za nějakých konkrétních podmínek (přihlášení).*
   b. Po kontrole správnosti jim učitel dá šablonu rovnoramenného trojúhelníku a žáci mají rozhodnout, jak uspořádat tyto 3 skupiny (následně jednotlivé úrovně a pomyslně [tužkou] rozdělit, jakou část této trojúhelníku zabírají tři kategorie. K tomu jim již učitel dá i celkové vlastnosti všech tří úrovní, které mají přiřadit k rozřazeným službám a aplikacím. Následně opět proběhne kontrola: rozdělení vlastností jednotlivých úrovní a velikostí v rovnoramenném trojúhelníku, které zabírá. *Je dobré nechat žáky přijít na to, jakým způsobem se rovnoramenný trojúhelník natočí a podle čeho se to odvíjí (pokud se k tomu žáci samostatně nedostanou, učitel jim může poradit, že se úrovně internetu často z nějakého důvodu zobrazují jako kra, či podmořský ledovec).*
   c. Následně si žáci přiřadí názvy jednotlivých úrovní a proběhne poslední kontrola a žáci mohou doplnit vlastní známé aplikace a služby do různých úrovní a tím ozvláštnit svou pyramidu.
   d. Posledním krokem může být nalepení jednotlivých „papírků“ do rovnoramenného trojúhelníku a tím vytvoření vlastního vyučovacího materiálu.
   e. Pro ukončení aktivity může učitel žákům ukázat některé z typických vyobrazení úrovní internetu např.
      - https://upload.wikimedia.org/wikipedia/commons/0/06/Iceberg_of_Webs.svg
      - https://upload.wikimedia.org/wikipedia/commons/3/31/Deepweb.png

Reflexe:

V průběhu aktivity by mělo u žáků dojít nejen k získávání vědomostí, ale i k určitému posunu z hlediska osobnostní roviny a jejich pohledu na internet jako celek. Z tohoto důvodu je vhodné s žáky o tom diskutovat a poskytnout jim i prostor na to, aby vyjádřili, jak se změnil jejich pohled na internet po absolvování této hodiny.

Rozhodně velmi důležité je upozorňovat žáky, aby si ani v rámci své zvědavosti s Dark Webem nezahrávali, neriskovali a neexperimentovali, a to s důrazem na jejich vlastní bezpečnost i bezpečnost svých blízkých. Je vhodné žáky vést k tomu, aby se nepřidávali ke skupině uživatelů, kteří pouze chtějí nahlédnout.

Na co si dát pozor

- Učitel je hlavním „kontrolorem“ všech postupných kroků a je zapotřebí, aby dopředu rozhodl, jak se budou jednotlivé fáze kontrolovat, zda společně, nebo bude obcházet jednotlivé skupiny a pracovat s každou skupinou samostatně. Druhá varianta je optimální z hlediska individuálního přístupu, nicméně je pro učitele náročnější.

- Žáci některé z aplikací nebo služeb neznají. Pokud dojde k tomu, že ani jeden ze skupiny některou aplikaci nebo službu nezná, odloží ji stranou a při kontrole jednotlivých fází učitel nebo někdo z jiné skupiny vysvětlí, o jakou službu nebo aplikaci se jedná.
- Je vhodné, aby bod 3 z části Průběh výuky, proběhl v jedné vyučovací hodině. To znamená, že pokud se příliš protáhne diskuze, je lepší využít čas jiným způsobem a aktivitu nechat proběhnout v samostatné hodině.
- Učitel musí sám zvolit hloubku probírané tématiky, hlavně v případě Dark Webu.

2.3.4 Internet věcí mezi námi

Tabulka 5: popis aktivity: internet věcí mezi námi

Stupeň vzdělávání	Sekundární vzdělávání (vhodnější pro vyšší ročníky ZŠ a střední školy vzhledem ke znalosti různých čidel a senzorů)
Naplňované indikátory dle RVP ZV, oblast, téma	Obor Informatika, vzdělávací obsah Digitální technologie – HW a SW
Předpokládaný rozsah (časové hledisko)	2 vyučovací hodiny
Vstupní požadavky na žáky	znalost práce s aplikací Kahoot práce s prohlížečem a vyhledáváním informací
Cíl aktivity	• Představit žákům koncept internetu věcí a přiblížit jim ho na konkrétních příkladech z domácnosti.
Rozvíjené kompetence	Digitální kompetence: • Tvorba digitálního obsahu (vytváření digitálního obsahu, integrace a přepracování digitálního obsahu) • Bezpečnost (ochrana osobních údajů a soukromí) Klíčové kompetence: • K učení: získané informace chápe včetně souvislostí a vysvětlí je. • K řešení problému: problém analyzuje z různých hledisek; vytváří a využívá vizuální znázornění problému. • Komunikativní: před známým publikem přednese své sdělení uceleně a srozumitelně; v diskuzi využívá myšlenky druhých jako východiska pro svá sdělení a navazuje na ně. • Sociální a personální: samostatně (individuálně i jako členové skupiny) se postarají o hotové dílo; podle svého uvážení využívá zpětnou vazbu pro své další jednání.
Potřebné vybavení	Připojení k internetu – realizace aktivity v Kahoot Prohlížeč obrázků

Základní potřebné informace o aktivitě

V současnosti se čím dál více hovoří o internetu věcí, přesto se stále do povědomí žáků na základních a středních školách ne vždy dostává, a pokud ano, tak spíše nepřímo. Nicméně internet věcí jako síť zařízení, která se mezi sebou dokážou propojit a vzájemně si vyměňovat informace, se v současnosti stávají i součástí našich domácností a konkrétní povědomí by o této problematice měli získat i žáci. Tato aktivita má představit možnosti IoT v domácnosti a ukázat vše na konkrétních příkladech.

Příprava na výuku

- Kontrola funkčnosti videí z webu: https://www.jaknainternet.cz/
  - Internet věcí: https://www.jaknainternet.cz/page/1263/internet-veci/
  - Chytrá města: https://www.jaknainternet.cz/page/3647/chytra-mesta/

- aktualizace aktivity v aplikaci Kahoot vzhledem k novým informacím z této oblasti: https://create.kahoot.it/details/21016607-103e-48ce-8088-ed29d6e0cc4f
- příprava a aktualizace obrázků: kuchyně, obývací pokoj, koupelna (v posledním případě může jít o tisk a počet výtisků se odvíjí od počtu zamýšlených skupin)

Organizace práce

1. individuální práce s aplikací Kahoot (v případě nedostatku zařízení možnost práce v menších skupinách),
2. frontální výuka – představení možností IoT v obývacím pokoji a s žáky doplnění možností v kuchyni,
3. skupinová práce žáků – příprava možností IoT v koupelně,
4. individuální práce – příprava možností IoT ve vlastním dětském pokoji,
5. diskuze a reflexe na závěr – IoT ve vlastních pokojích.

Průběh výuky

1. získání povědomí o internetu věcí (možná diskuze, využití videa či využití aktivity v aplikaci Kahoot) (10 min.)
   - odkaz na video: https://www.jaknainternet.cz/page/1263/internet-veci/
   - odkaz na aktivitu v Kahoot: https://create.kahoot.it/details/21016607-103e-48ce-8088-ed29d6e0cc4f

Zde je velmi důležitá role učitele, který musí posoudit, jaký způsob představení IoT by pro žáky byl vhodný. Kupříkladu uvedené video může být pro nižší ročníky 2. stupně příliš abstraktní a učitel využije k představení připravený test v aplikaci Kahoot. Pro bližší představu žáků lze uvést ukázky z některého filmu (popř. traileru), ve kterém se vyskytuje IoT zcela běžně, např. Pátý element, či Ready Player One, Demolition Man. Každopádně by si žáci si měli uvědomit, že internet věcí je síť zařízení různého typu, která jsou vybavena senzory a čidly, ovládaná prostřednictvím softwaru, kde se data zpracovávají a zasílají do jiného zařízení (např. mobilního telefonu). Tato základní představa jim umožní si představit domácnost, která je těmito zařízeními ovládaná.

2. Představení internetu věcí v domácnosti, pomocí obrázku obývacího pokoje a kuchyně (15 min.) – obrázky jsou k dispozici ke stažení

Následně jim učitel představí příklady využití IoT v obývacím pokoji a kuchyni, kde společně s žáky doplňují možnosti, kde by se dalo využít IoT a jeho užitek. Výhodné je využití interaktivní tabule pro zakreslování prvků do obrázku. Vhodné je ale žáky upozornit i na riziko, které se sdílením dat přichází (např. kde se jejich data ukládají, kdo je může vidět a použít, jestli se na zařízení v domácnosti může připojit i někdo další…)

3. skupinová vlastní práce žáků s obrázkem koupelny (10 min.) – obrázek je k dispozici se ke stažení

Poté se žáci rozdělí do menších skupin a společně se zamýšlejí nad prvky domácnosti, které by bylo možné využít v koupelně, a následně mezi sebou své nápady sdílejí. Vhodné je, aby žáci měli představu koupelny před sebou vytištěnou a mohli si dělat poznámky, nebo minimálně pro názornost jim učitel nějaký ilustrativní obrázek promítne.

4. individuální práce žáků na zobrazení vlastního pokoje a možné prvky IoT (tuto práci lze zadat žákům jako domácí úkol či menší projekt, aby byli do následující hodiny připraveni k diskuzi, jinak je nutné počítat s časem na vypracování vlastních nápadů)

Učitel se snaží žáky motivovat k tomu, aby si uvědomili, že i jejich vlastní pokoj může obsahovat prvky, které jsou ovládány např. přes mobilní telefon a mohly by v budoucnu (nebo i současnosti) být součástí jejich vybavení.

5. závěrečné představení nápadů ohledně IoT v pokojích (15 min.)

Pro sdílení nápadů je důležitá následná diskuze, kde si žáci vyměňují ukázky svého řešení IoT u sebe v pokoji. Učitel může využít pro rychlejší sdílení nápadů např. aplikaci Padlet[9].

6. představení konceptu IoT pro města – tzv. chytrá města
    - odkaz na video: https://www.jaknainternet.cz/page/3647/chytra-mesta/

Závěrem je třeba žákům představit i možnosti, které se naskýtají mimo jejich pokoje a bydlení obecně. IoT je velmi důležitý i pro města, tzv. chytrá města. Dobré je žáky ale také upozornit na nebezpečí spojené se sdílením dat a jejich zneužitelnosti.

V případě, že se učitel dále chce této problematice věnovat, nabízí se vymýšlení IoT řešení ve škole, jejich možnosti a výhody (např. regulace teploty ve třídách, hlídání množství CO_2…)

Alternativní řešení

- Učitel může využít libovolný prostor, např. kadeřnický salón či samoobsluhu, dle zaměření žáků.
- Jako projektově orientovanou výuku může využít školu a žáci mohou navrhnout zlepšení přímo do známého prostředí školy.

[9] https://cs.padlet.com/

2.3.5 Virtuální měny

Tabulka 6: popis aktivity Virtuální měny

Stupeň vzdělávání	2. stupeň ZŠ, SŠ
Naplňované indikátory dle RVP ZV, oblast, téma	Obor Informatika, vzdělávací obsah Informační systémy, téma Úprava a doplnění tabulky, vytvoření spojnicového grafu (popř. Data, informace a modelování)
Předpokládaný rozsah (časové hledisko)	1 vyučovací hodina
Vstupní požadavky na žáky	Žák se umí orientovat v editoru pro práci s tabulkami a zvládá jednoduchou práci v něm, např. umí vytvořit graf. Žák dokáže samostatně pracovat se zadanou webovou stránkou.
Cíl aktivity	• V průběhu aktivity žák pochopí pojem virtuální měna. • Žák samostatně ze zadaných a doplněných dat vytvoří grafy dle zadání. • Žák z vytvořených grafů diskutuje tendence vybraných virtuálních měn.
Rozvíjené kompetence	Digitální kompetence: • Informační a datová gramotnost • Tvorba digitálního obsahu (Integrace a přepracování digitálního obsahu) Klíčové kompetence: • Kompetence k učení: získané informace chápe včetně souvislostí a vysvětlí je • Kompetence k řešení problému: rozpozná příčinu a důsledek a vztah mezi nimi, vytváří a využívá vizuální znázornění problému, formuluje hypotézy na základě dostupných informací • Kompetence komunikativní: k získání a výměně informací účelně využije různé informační a komunikační prostředky a technologie
Potřebné vybavení	Připojení k internetu a práce s prohlížečem, editor pro práci s tabulkami

Základní potřebné informace o aktivitě

Základní myšlenkou této aktivity je propojení oblasti virtuálních měn a jejich kurzů s tvorbou tabulky a přípravou spojnicových grafů. Žáci se na jednu stranu dozvědí, jaké jsou příklady virtuálních měn a jejich vlastnosti, či jaké jsou tendence jejich změny v časovém horizontu cca 1 roku vzhledem k CZK. A zároveň pracují s pro ně zajímavými a do budoucna možná užitečnými daty, které v tabulkovém editoru zobrazují do takové podoby, aby z nich dokázali přečíst vývoj a tendence.

Příprava na výuku

- Příprava/úprava připravené tabulky, resp. dat v ní, dle aktuálního roku, měsíce, či jiné „přesnosti“ dat, které chce učitel s žáky prezentovat a diskutovat.
- Aktualizace aktivity v Learning Apps (https://learningapps.org/view26109074).

Organizace práce

1. Frontální – vysvětlení virtuální měny, popř. následně ukázka, jak vytvořit spojnicový graf,
2. Individuální práce žáka – doplnění dat do tabulky, práce s grafem, porozumění zobrazovaným datům.

Průběh výuky

- zavést pojem virtuální měny (10 min.)
  - možná diskuze a využití vytvořeného materiálu v Learning Apps pro získání přehledu o základních vlastnostech virtuálních měn.
- Práce s tabulkou (30 min.)
  - Úkoly jsou popsané v samotné přiložené tabulce (ukázka tabulky viz níže).

CZK	01.10.2021	01.01.2022	01.03.2022	01.05.2022	aktuální datum
Bitcoin	1051415	1043051	968098	905263	
Ethereum	72267	82330	67927	67149	
Tether	21	22	23	23	
Ripple	22	18	18	14	
Litecoin	3628	3294	2571	2367	
vyber vlastní virtuální měnu					

Obrázek 3: ukázka z pracovního listu zpracovávané tabulky (viz odkaz na pracovní list autora)

Úkoly pro práci s tabulkou jsou velmi intuitivní a měly by navodit u žáků zájem ke sledování vývoje virtuální měny v průběhu konkrétního časového úseku.

Úkol 0:	Podívej se na tabulku a zjisti, co zobrazuje.
Úkol 1:	Doplň další vlastní virtuální měnu a její kurz.
Úkol 2:	Vytvoř souhrnný spojnicový graf. V levé části budou hodnoty CZK. Ve spodní části budou datumy.

Zamysli se: Proč nejsou data v grafu dobře čitelná a nepřináší přehlednost?

Úkol 3:	Vytvoř spojnicové grafy pro každou virtuální měnu zvlášť a popiš jejich tendence v roce 2022?

Obrázek 4: ukázka zadání pro práci s tabulkou (viz odkaz na pracovní list autora)

V prvním úkolu (Úkol 0) by žáci měli porozumět tabulce a tomu, co zobrazuje a jakým způsobem. Učitel může v rámci diskuze klást žákům doplňující otázky, aby zjistil, zda rozumí konkrétnímu zobrazení dat.

Následně (Úkol 1) žáci doplní tabulku vlastní vybranou virtuální měnou a zjistí aktuální stav konkrétních dalších příkladů. Pro vytvoření této tabulky a získání dalších dat pro tabulku je vhodné využití webové stránky kurzy.cz (konkrétně: https://www.kurzy.cz/kryptomeny/seznam-kryptomen/) a následně vždy kliknout na konkrétní kryptoměnu, vybrat období a měnu. V připravené tabulce je využito měny české koruny (CZK).

Poté žáci vytvoří spojnicový graf (Úkol 2), ve kterém budou všechny měny, nicméně měli by přijít na to, že se jim z grafu nepodaří dobře data přečíst vzhledem k tomu, že některé hodnoty jsou příliš vysoké, jiné příliš nízké a je potřeba tedy zobrazit konkrétní tendence kryptoměn samostatně (Úkol 3).

Po vytvoření všech spojnicových grafů je dobré zařadit na konec hodiny diskuzi, která směřuje k současné tendenci virtuálních měn, jejich možnostem vývoje, popř. diskuzi o investování do kryptoměn a rizicích s tím spojenými.

Reflexe:

Na co si dát pozor

- Žáci příliš dlouho sledují další příklady kryptoměn a nedokážou si vybrat další konkrétní – je dobré, aby si učitel připravil příklady doporučených kryptoměn a důvod, proč by si je žáci měli vybrat.
- Žáci nedokážou zjistit z grafu na kurzy.cz aktuální stav kryptoměny, popř. budou zmatení z toho, že se neustále situace mění a přepočítává.

Alternativní řešení

- Je možné využít libovolného tabulkového editoru včetně cloudových řešení, pokud dokážou vykreslit spojnicový graf, nebo jiný podobný graf.

2.3.6 Vishing

Tabulka 7: popis aktivity Vishing

Stupeň vzdělávání	Aktivita přímo nezávislá na věku žáků, doporučení pro 9. třídu ZŠ, 1. ročník SŠ
Naplňované indikátory dle RVP ZV, oblast, téma	Obor Informatika, vzdělávací obsah Digitální technologie, téma Bezpečnost
Předpokládaný rozsah (časové hledisko)	4 vyuč. hodiny, lépe pak dlouhodobý projekt pro skupiny žáků
Vstupní požadavky na žáky	Žák zvládá práci s mobilním dotykovým zařízením nebo kamerou. Žák se umí orientovat v práci s vybraným nástrojem pro střih a úpravu videa.
Cíl aktivity	• Představit žákům jeden typ podvodného chování, při kterém jsou cíleně získávány informace. • Nechat žáky ve skupině přemýšlet nad vytvořením scénáře a scénky, ve které si vyzkouší reakce na vishing. • Propojit Informatiku s Výchovou k občanství s preventivním programem školy.
Rozvíjené kompetence	Digitální gramotnost: • Vytváření digitálního obsahu • Ochrana osobních údajů a soukromí Klíčové kompetence: • k učení: aktivně využívá poznatky a dovednosti nabyté v určitém předmětu/oblasti i v jiných předmětech/oblastech; získané informace chápe včetně souvislostí. • k řešení problému: vytváří a využívá vizuální znázornění problému; srozumitelně zdůvodňuje a obhajuje svá řešení. • komunikativní: při vyjadřování uspořádá informace logicky podle časových, místních, příčinných a dějových souvislostí. • sociální a personální: rozdělí si ve skupině úkol na části a přijme svou část, včetně zodpovědnosti za její plnění; samostatně (individuálně i jako členové skupiny) se postará o hotové dílo.
Potřebné vybavení	• Aplikace Fotky (běžná aplikace OS Windows) nebo jiný nástroj pro úpravu a střih videa. • Textový editor (pro přípravu scénáře) • Připojení k internetu

Základní potřebné informace o aktivitě

Žáci se v současnosti již běžně ve škole setkávají s pojmy jako kyberšikana, stalking, či trolling. Školy pořádají preventivní programy v rámci projektových dnů, ale také v běžné výuce. Do škol mohou docházet i specialisté v této oblasti na přednášky či besedy. Tato výuková aktivita je také zaměřena na jeden z typů podvodného chování, a to vishing.

Vzhledem k tomu, že velké množství žáků již na prvním stupni disponuje mobilním telefonem, je také pravděpodobné, že je bude prostřednictvím tohoto zařízení někdo anonymní oslovovat a popřípadě i získávat informace.

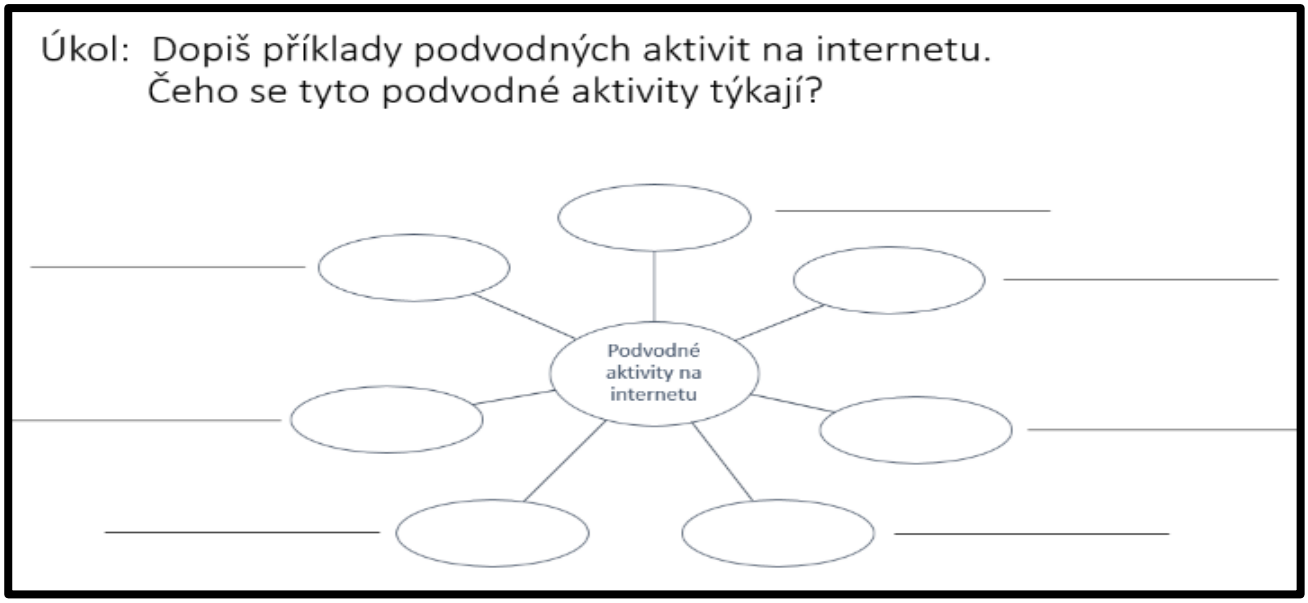
Tato aktivita by měla umožnit žákům se nad vishingem zamyslet jak z pohledu typu podvodné aktivity, tak samotného jednání, pokud se do takové situace dostanou.

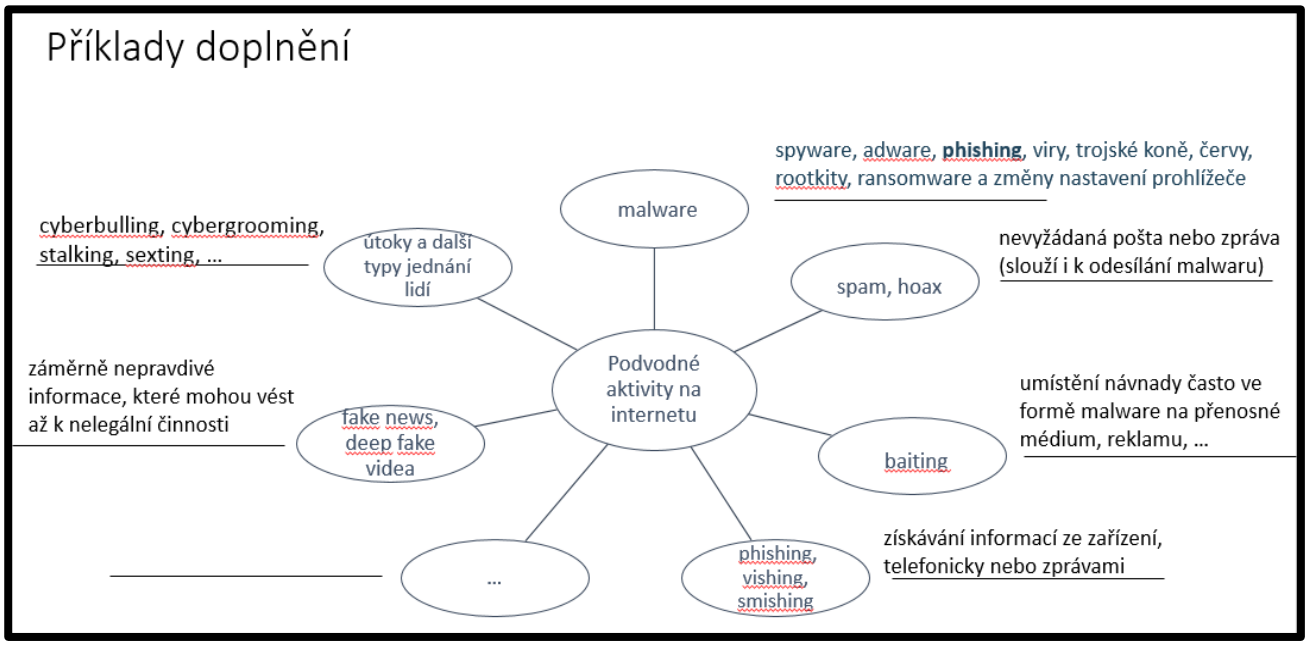
Příprava na výuku

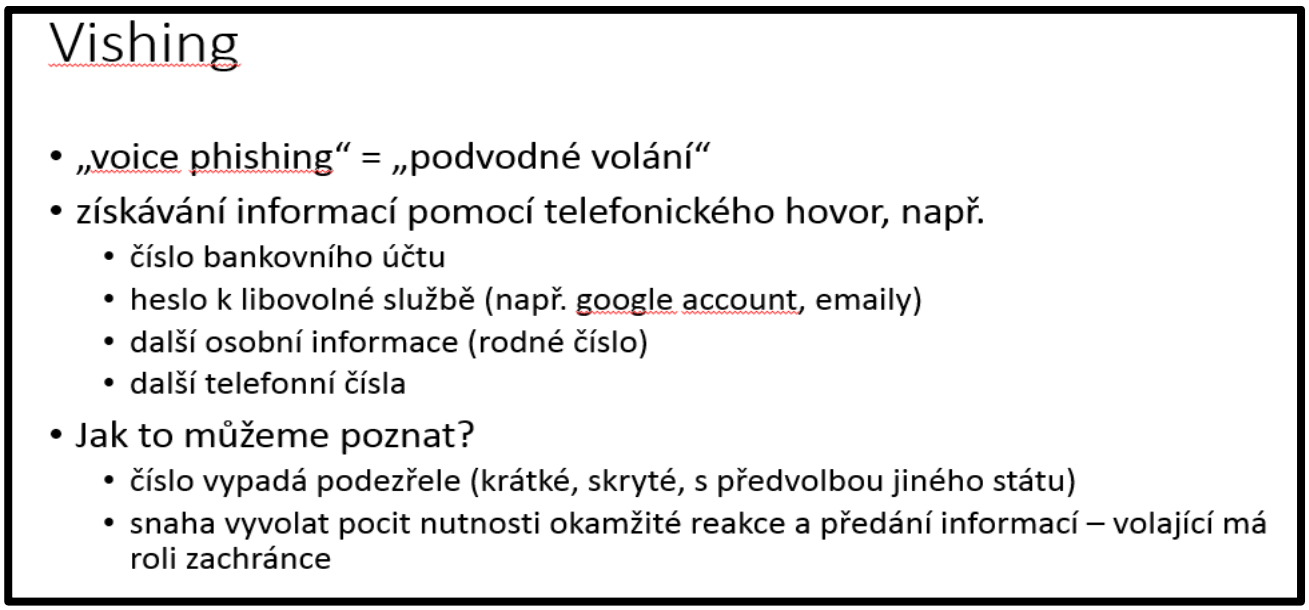
Pro samotnou přípravu na hodinu není nutná instalace žádného softwaru. Vzhledem k tomu, že žáci budou využívat mobilní dotyková zařízení (pokud je dovolí škola, tak i vlastní), je vhodné zajistit jejich nabití před samotnou hodinou.

Dále je nutné myslet na:

- příprava prezentace a diskuze na tématem vishing (možné využití připravené prezentace: náhled prezentace níže, stažení prezentace).







Obrázek 5: ukázky z prezentace (viz odkaz na prezentaci autora)

- vyzkoušení a výběr videí (možné ukázky, pro různé věkové kategorie):
  - https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/vishing
  - https://www.youtube.com/watch?v=tjAFobMn9ps
  - https://www.mbank.cz/blog/post,858,pozor-na-podvodne-telefonaty-aneb-co-je-to-vishing.html
  - https://edu.ceskatelevize.cz/video/121-phishing-a-skimming
- možné využití pracovního listu, pak je doporučený jeden výtisk pro každou skupinu (možné využití připraveného pracovního listu: náhled pracovního listu níže, stažení pracovního listu).

Celkové pojetí:

- Co konkrétně bude řešit scénka?
    - Počet herců a jejich charaktery
    - Kde se scénka odehrává (prostředí, situace)

Další poznámky:

- Jaké pomůcky/věci budete potřebovat a co je třeba si na natáčení donést?
- Na co je potřeba při scénce nezapomenout?

pohled kamery (posloupnost „scén", následný způsob střihu)	Způsob práce s kamerou (přiblížení, pohyb, namířena na konkrétní věc, herce)	Co se v dané chvíli děje (např. rozhovor)	poznámky (nutné pomůcky - telefon, oblečení, ...)	doba trvání

Obrázek 6: ukázka pracovního listu (viz odkaz na pracovní list autora)

- příprava prostředí, kam se budou výsledné scénky, popř. scénáře ukládat (např. OneDrive, Google Drive, síťové disky ve škole)

Organizace práce a průběh výuky:

1. diskuze s využitím prezentace (5–10 min.)
2. ukázka videí (5 min.)
3. rozdělení žáků do skupin (doporučuje se mít ve skupině min. 4 žáky: 3 aktéry, 1 kameramana) a stanovení postupu práce pro žáky:
   a. příprava scénáře (30 min.),
   b. samotné natočení scénky (40 min.),
   c. sestříhání scénky ve vybrané aplikaci, dokončení videa ve vybraném formátu (40 min.),
   d. prezentace vlastní scénky (dle počtu vytvořených scének, v případě 5–6 skupin na jednu třídu se jedná o přibližný odhad jedné vyučovací hodiny).

Formální požadavky na práci žáků ve skupině k vytvoření scénky:

- scénář – podrobný scénář, který žáci dopředu rozmyslí (možné využití pracovního listu):
  - nutné pomůcky,
  - minimálně 5× střídání pohledů kamery v jednom dialogu,
- scénka:
  - minimální a maximální délka: 1–2 minuty,
  - konečný produkt ve formátu mp4 odevzdaný do sdílené složky.

Reflexe:

Na co si dát pozor

- všichni žáci ve skupině jsou aktivní a zapojují se rovnoměrně do tvorby scénáře, scénky i výsledného videa;
- při využití vlastních zařízení se může stát, že žáci natočí video v takovém formátu, ve kterém nebudou moct pracovat prostřednictvím vybraného programu pro zpracování videa;
- žáci by mohli video začít natáčet na výšku, nikoliv na šířku; scénka by měla být natočena obdobně, jako se točí filmy, aby při promítání byla scénka pěkně vidět na projekci; bylo by vhodné žáky poučit o tom, jak využívat různého směru natáčení, scénka by neměla být natočena najedou z jednoho pohledu.

Alternativní řešení

- možné využití v rámci projektového dnu zaměřeného na bezpečnost;
- možné využití i v jiných předmětech, než je Informatika, např. ve Výchově k občanství.

Další podobné příklady z praxe a materiály:

- https://www.eset.com/cz/vishing/
- https://www.policie.cz/clanek/vishing-a-spoofing.aspx

2.3.7 Opakování termínů v oblasti internetu a kybernetické bezpečnosti

*Tabulka 8: popis aktivity Opakování termínu v **oblasti** internetu kybernetické bezpečnosti*

Stupeň vzdělávání	SŠ, SOŠ
Naplňované indikátory dle RVP ZV, oblast, téma	Obor Informatika, vzdělávací obsah Digitální technologie, téma Kybernetická bezpečnost
Předpokládaný rozsah (časové hledisko)	1–2 vyučovací hodina (záleží na učiteli, kolik prostoru dá žákům, pokud bude reflexe pro učitele a žáky stěžejní, je vhodné ji nechat jako samostatnou vyučovací hodinu)
Vstupní požadavky na žáky	Žák se orientuje v oblasti kybernetické bezpečnosti. Žák zvládá práci v prostředí Quizlet, s prohlížečem.
Cíl aktivity	• Upevnit pojmy související s kybernetickou bezpečností. • Spolupracovat v různých náhodně vytvořených skupinách. • Reflektovat a doplnit pojmovou základnu žáků v této oblasti.
Rozvíjené kompetence	Digitální gramotnost: • Informační a datová gramotnost: zpracování pojmů a definic k nim. • Komunikace a kolaborace: spolupráce prostřednictvím digitálních technologií. Klíčové kompetence: • Kompetence k učení: aktivně využívá různé zdroje informací, získané informace chápe včetně souvislostí a vysvětlí je (formuluje hlavní myšlenku). • Kompetence komunikativní: k získání a výměně informací účelně využije různé informační a komunikační prostředky a technologie, podle situace vybere a použije takové informační a komunikační prostředky nebo technologie, které nejlépe vyhovují situaci a okolnostem, při vyjadřování uspořádá informace logicky. • Kompetence sociální a personální: v případě potřeby nabízí svou pomoc, hledá spolu s druhými nejlepší návrhy na to, co by se příště mělo dělat stejně a co jinak.
Potřebné vybavení	Počítač / mobilní zařízení s připojením k internetu

Základní potřebné informace o aktivitě

Tato hodina by se dala nazvat opakovací, žáci si mají zopakovat a upevnit pojmy související s kybernetickou bezpečností, typy útoků a útočníků. Mělo by se tedy jednat o ukončení a reflexi znalostí žáků v této problematice.

Příprava na výuku

- připravený Quizlet: https://quizlet.com/_brdjam?x=1qqt&i=1dlzki
- připravený pracovní list (jednoduchá tabulka) pro každého žáka, či skupinu dle organizace práce (příklad viz níže)

Představení aplikace Quizlet:

Původním smyslem Quizletu (https://quizlet.com/) je využívání pro výuku cizích jazyků, hlavně pak slovíček (tzv. flash cards). Sice je možné využít aplikaci v rámci aktivit flash cards, learn, write, spell, text, match, gravity, ale zde je využívána live hra. Při této hře se žáci náhodně rozdělí do skupin. Důležité je žáky upozornit na to, že žádný z žáků nemá stejný pojem a vždy pouze jeden má ten správný. V případě, že někdo ze skupiny odpoví špatně, pak všechny získané body skupiny se vymažou. Pro výhru skupiny je nutné spojit všechny pojmy k jejich definicím.

Žáci se připojují pomocí www.quizlet.live a kódem nebo QR kódem v případě využití mobilních zařízení. Žáci pak zadají pouze své jméno pro přihlášení ke hře.

Učitel však musí hru nejdříve spustit. V případě této konkrétní aktivity se jedná o Random Teams a poté Definition and Terms. Následně čeká na připojení žáků a poté je rozdělí náhodně do skupin a hru spustí. Učitel nevidí hry žáků, pouze celkový počet bodů celé skupiny.

Žáci se nemusí do samotného Quizletu registrovat. V případě, že učitel chce vytvářet a spravovat Quizlety, je nutné přihlášení (např. pomocí Google account).

Tabulka 9: ukázka pracovního listu

Pracovní list:

Pojem	Definice

Organizace práce a průběh výuky:

1. uvedení do hodiny – vysvětlení, že se jedná o opakovací hodinu za účelem reflexe, kolik toho žáci vědí o probíraném tématu (2 min.),
2. skupinová práce: přihlášení do aplikace Quizlet a odehrání live hry, kdy se žáci rozdělí automaticky do skupin, kde musí spolupracovat, aby vyhráli (15 min.); možné opakovat dle preferencí žáků nebo učitele,
3. individuální práce (možná práce ve dvojici – dle preferencí učitele): doplnění chybějících pojmů, na které si žáci vzpomenou (15 min.),
4. diskuze a skupinová reflexe: společné procházení pojmů, které se ve hře nevyskytovaly (10 min.).

V případě, že by učitel kladl velký důraz na diskuzi a skupinovou reflexi, lze průběh hodiny a časové omezení jednotlivých částí upravit tak, aby poslední 4. bod probíhal v samostatné hodině.

Reflexe:

- Po realizaci aktivity ve výuce, autor shledal, že výhodné je, když žáci odehrají více live her v různých skupinách. Mají tak šanci spolupracovat s různými žáky ve skupině. Zároveň se pojmy střídají, a mohou tak hlouběji procvičit své znalosti.
- Důležitou částí takto koncipované hodiny je poslední bod, tedy skupinová reflexe. Zde se žáci mohou projevit a přidávat další pojmy a definice k nim. Zároveň je to také reflexí pro učitele, který může z aktivity žáků vyvodit další aktivity, např. doplnění vlastního Quizletu, popř. vytvoření dalšího seznamu pojmů, který žáci v této oblasti znají a využívají. Mohou učitele překvapit i pojmy, které doposud neslyšel a tím jsou vědomostně obohaceny obě strany.

Na co si dát pozor

- Učitel musí počkat na přihlášení všech žáků. Po rozdělení do týmů není možné další žáky ke hře přizvat.
- Žáci mohou zneužít anonymity přihlášení k aplikaci a výběru vlastní přezdívky nebo jména jiného žáka. Učitel může žáky, kteří nedodrželi jeho pokyny z hlediska přihlášení se jménem, ze hry vymazat a žáci jsou tak nuceni se opětovně přihlásit.

Alternativní řešení

- Pokud učitel nechce využít softwarové řešení, může pro žáky připravit kartičky, kdy na jedné bude definice, na druhé pojem. Úkolem žáků pak bude spojovat pojem a definici. V případě většího množství pojmů může pak vybrat do každé skupiny jiné pojmy. V tomto případě by se změnil průběh výuky. Před samotnou individuální prací je potřeba si všechny pojmy všech skupin doplnit, aby se v individuální práci žáků následně neopakovaly.
- Pro hromadnou reflexi může učitel využít i jiné aplikace, např. Kahoot.

3 Reflektované aktivity

V současnosti existují společnosti či subjekty, které se kybernetickou bezpečností systematicky a profesně zabývají. V jejich aktivitách se pak objevují i v rámci projektů možnosti realizace výuky od mateřské školy až po vysoké školy. Mezi nimi je možné jmenovat např. Avast, CZ.NIC, či NÚKIB.

Pro účely příručky byly vybrány ukázky aktivit, které lze přímo využít ve výuce. Většinou se jedná o popsané jednotlivosti, kdy se na portálech nachází mnohem více materiálů k využití ve výuce. Každá reflektovaná aktivita většinou nejdříve obecně popisuje projekt, počin či portál a následně přímo cílí na konkrétní ukázku. V tabulce níže jsou seřazeny vybrané reflektované aktivity dle abecedy a věku, reps. stupně, kdy je vhodné je ve škole využít.

Tabulka 10: seznam reflektovaných aktivit

	Název	odkaz	Využití ve věkové skupině
1	Kuřátko Čiky a jeho přátelé	https://digifolio.rvp.cz/artefact/file/download.php?file=84758&view=15150	MŠ až 1. období 1. stupně ZŠ
2	Alenka v říši gifů	https://decko.ceskatelevize.cz/alenka-v-risi-gifu	1. st. ZŠ
3	Datová lhota: Cesta na se(r)ver	https://www.ceskatelevize.cz/porady/11933175266-datova-lhota/217543112110008/	1. st. ZŠ
4	Ovce.sk: Bez kožíšku	http://cz.sheeplive.eu/fairytales/bez-kozisku-titulky	1. st. ZŠ
5	Umím říct NE!	https://in-generation.jsi.cz/materialy/umim-rici-ne	1. st. ZŠ (3.–4. třída)
6	Internetem bezpečně: příručka pro děti: Happy slapping	https://www.internetembezpecne.cz/ke-stazeni/	2. st. ZŠ (6–12 let)
7	Buď safe online	https://www.avast.com/cz/besafeonline/online-kurz	2. st. ZŠ
8	Chytrá škola O2: Zdraví v kyberprostoru	https://vyuka.o2chytraskola.cz/data/files/zdravi-v-kyberprostoru-ds4b9omcse.pdf	2. st. ZŠ
9	Jak na internet: struktura internetu	https://www.jaknainternet.cz/page/1795/struktura-internetu/	2. st. ZŠ
10	Nebezpečné výzvy v online prostředí	https://e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/99-letak-nebezpecne-vyzvy-v-online-prostredi-pro-rodice-a-ucitele/file	2. st. ZŠ
11	Nebojte se internetu: online komunikace	https://www.nebojteseinternetu.cz/page/3416/on-line-komunikace/	2. st. ZŠ

12	Kybernetická bezpečnost	https://digigram.cz/dvz/#DVZICT01	9 tř. ZŠ, 1. ročník SŠ
13	Hoax	https://www.hoax.cz/cze/	2. st. ZŠ, SŠ
14	Khanova škola: Kybernetická bezpečnost a kriminalita	https://cs.khanacademy.org/computing/code-org/computers-and-the-internet	2. st. ZŠ, SŠ
15	#martyisdead	https://martyisdead.mall.tv/	SŠ
16	Kybertest	https://kybertest.cz/	SŠ
17	Soutěž v kybernetické bezpečnosti	https://www.kybersoutez.cz/	9–24 let
18	„DÁVEJ KYBER“ PRO UČITELE – Základy kybernetické bezpečnosti (pro zaměstnance škol)	https://osveta.nukib.cz/course/view.php?id=121	Zaměstnanci škol
19	Desatero dobrého kybernetického rodiče	https://www.zachranny-kruh.cz/osobni-bezpeci/dalsi-nebezpeci/internet/desatero-dobreho-kybernetickeho-rodice.html	Zaměstnanci škol, rodiče
20	Je ve virtuálním světě bezpečno?	https://bezpecnevkyberprostoru.cz/clanky/materialy-ke-stazeni/je-ve-virtualnim-svete-bezpecno----brozura/	Zaměstnanci škol, rodiče (na webové stránce uvedeny i materiály pro žáky 1. a 2. stupně)

3.1

Název: Kuřátko Čiky a jeho přátelé

Odkaz: https://digifolio.rvp.cz/artefact/file/download.php?file=84758&view=15150

Náhled:

Obrázek 7: ukázka z učebního materiálu

Popis:

V rámci Gramotnosti.pro život (Učíme v souvislostech) v části rozvoj digitální gramotnosti vznikly materiály i pro bezpečnost v kyberprostoru.

Využití:

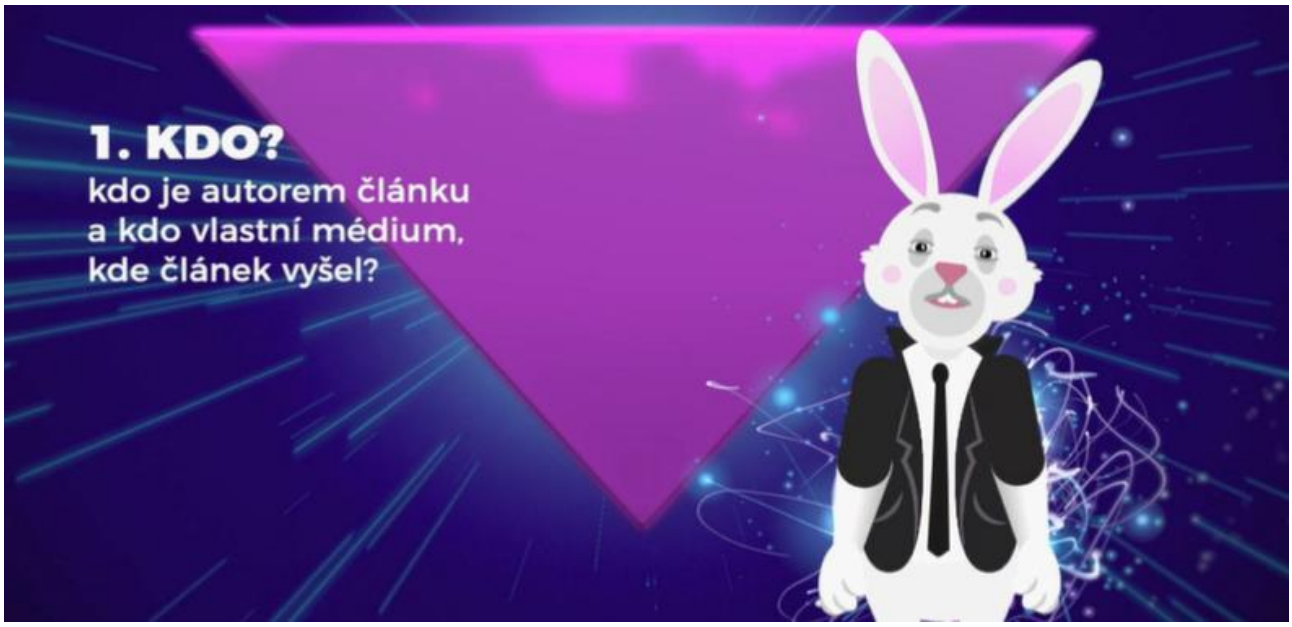
Vybrané téma cílí na nejmenší děti již z mateřské školy. Hlavní součástí aktivity je příběh pro 5–7leté děti. Součástí je i postup práce s příběhem. Před samotným vyprávěním se zdá být dle autorů důležité navození prostřednictvím diskuze, ve které se děti rozpovídají o současných zkušenostech s technologiemi, kyberprostorem a komunikaci v něm. V průběhu příběhu je pak vhodné dětem promítat obrázky nejen pro udržení jejich pozornosti, ale také kvůli vtahování dětí do samotného děje příběhu. Na konci příběhu nesmí chybět i ponaučení, které by děti měly samy vyslovit, a to: nepovídat si s cizími lidmi a nesdělovat jim osobní informace ani prostřednictvím digitálních technologií.

3.2

Název: Alenka v říši GIFů: Fake news. Čemu věřit?

Odkaz: https://decko.ceskatelevize.cz/alenka-v-risi-gifu

Náhled:



Obrázek 8: Ukázka z Alenka v říši GIFů

Popis:

Alenka v říši GIFů je 13dílný seriál vytvořený českou televizí a je možné ho shlédnout zdarma online. Pořad cílí na základní informace ze světa kyberprostoru a konkrétní produkty (např. Pot, slzy a YouTube; Je internet zadarmo?), součástí je i kyberbezpečnost (např. Šikana 2.0. Jak ji ustát na netu; Proč je tak těžké odtrhnout se od obrazovky). Hlavní roli zde hrají sourozenci a průvodcem je králík, součástí výkladů v příběhu jsou i konkrétní osoby, jako odborníci nebo youtubeři.

Využití

Vybraný díl se zabývá fake news a čemu věřit. Zkuste žáky požádat, aby si v průběhu sledování seriálu dělali poznámky a zaměřili se na to, co je zaujalo a z dané problematiky falešných zpráv. Po shlédnutí je vždy důležitá diskuze. Žáci by měli přijít na to, že ověřování informací je velmi důležité. Žáci by si měli v průběhu osvojit i pojem hoax, clickbait, či troll.

V rámci diskuze se ptejte žáků:

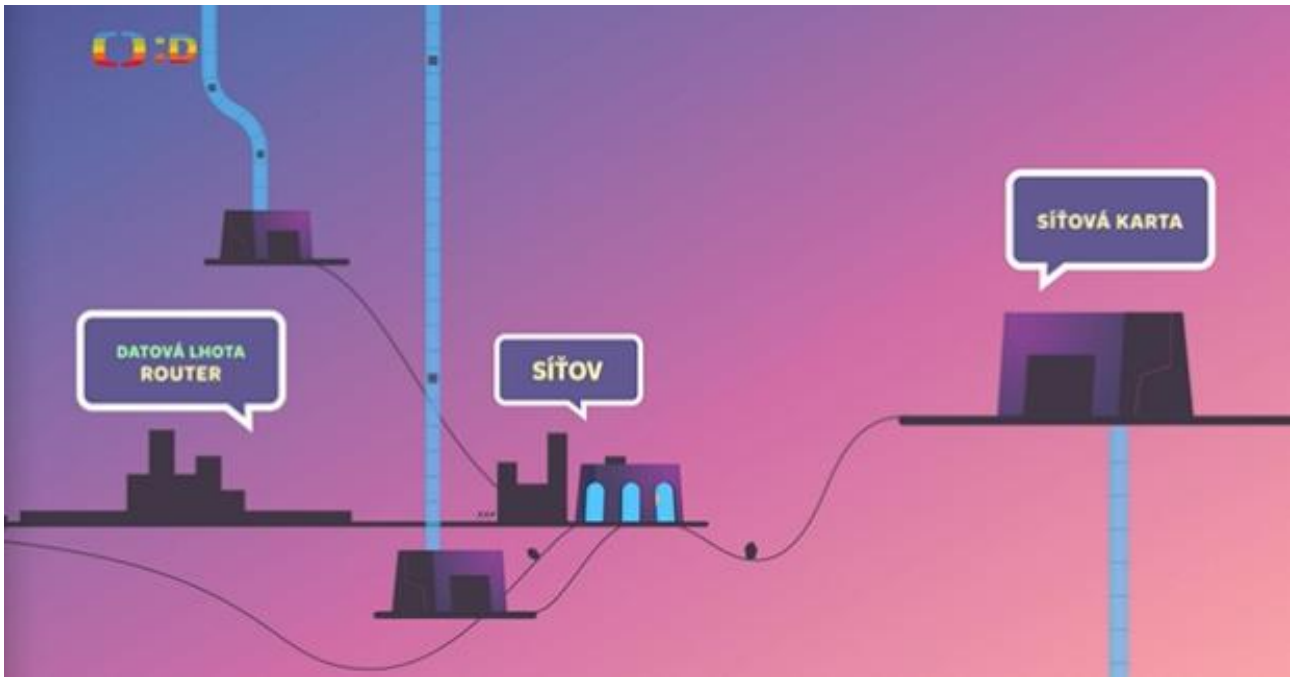
- jak poznat falešné nebo poplašné zprávy,
- co se snaží v nás vyvolat a jak na nás působí,
- proč to lidé dělají,
- proč lidi tak hodně fake news ovlivňují,
- jak se stává, že lidé naráží na fake news (vlastnosti prohlížeče).

3.3

Název: Datová Lhota – Cesta na se(r)ver

Odkaz: https://www.ceskatelevize.cz/porady/11933175266-datova-lhota/217543112110008/

Náhled:



Obrázek 9: Ukázka z Datová lhota

Popis:

Datová Lhota (https://decko.ceskatelevize.cz/datova-lhota) je obecně animovaný seriál, který vytvořila Česká televize ve spolupráci s MFF a CZ.NIC. Každý z deseti dílů si klade za cíl přiblížit svět počítačů a internetu. Vzhledem k zaměření této publikace byla vybrána ukázka s názvem Cesta na se(r)ver. Žáci by měli v průběhu krátkého videa získat informaci o tom, jak cestuje přihlašovací jméno a heslo na server, co je to IP adresa, router a DNS. V současnosti jsou vytvořené i některé modelové lekce, které učitel může využít pro práci s videi (https://decko.ceskatelevize.cz/datova-lhota/ve-skole). Pro tento konkrétní díl je vhodné projít si lekci, resp. metodický materiál s názvem Komunikace na internetu[10].

Využití:

Tento díl je vhodný pro využití v předmětu Informatika na prvním stupni při zavádění pojmu počítačová síť, přihlášení či heslo. Délka dílů nezatíží časově hodinu a zároveň umožňuje s žáky rozvíjet diskuzi nad konkrétním tématem.

[10] https://decko.ceskatelevize.cz/cms/porad-datova-lhota-data/docs/ML05-komunikace-po-internetu.pdf

3.4

Název: Ovce.sk: Bez kožíšku

Odkaz: http://cz.sheeplive.eu/fairytales/bez-kozisku-titulky

Náhled:

Obrázek 9: Ukázka z Ovce.sk

Popis:

Sheeplive je projekt podporovaný EU Safer Internet, jehož základ pochází ze Slovenska. Každopádně v současnosti je přeložen, respektive otitulkován v mnoha jazycích. Obecně se jedná o krátké příběhy zaměřené na bezpečnost práce s internetem pro žáky základní školy. Hlavní roli zde hraje bača, jeho syn, myslivec, zlí vlci a ovce. V každém příběhu je konkrétní poučení, o které se stará většinou myslivec nebo bača. Pro menší děti bude jistě matoucí slovenština, která má ještě nádech slovenského venkova z koliby. Nicméně je nutné přemýšlet nad samotným využitím nebo jejich doplněním. Videa byla vytvořena před téměř deseti lety, nicméně jako základ jsou využitelná i pro současné žáky.

Využití:

Pro ukázku bylo z 21 příběhů vybráno video nazvané „Bez kožíšku“. Zde je cíleno na to, jak je pro všechny nebezpečné dávat, resp. posílat komukoliv odhalené fotografie. Cílem je také žákům sdělit, že to, co je jednou dané, nahrané do internetu, se již prakticky nedá úplně smazat. Takto nahrané fotky může někdo využít nebo zneužít.

Stáří videa se dá využít a diskutovat s žáky, jakým způsobem se vyvinuly technologie a co je nyní zásadní při případném zveřejňování fotografií. Toto video je spíše motivační a jeho využití je možné předpokládat na uvození tématu zabývajícího se fotografiemi a jejich zveřejňováním na internetu.

3.5

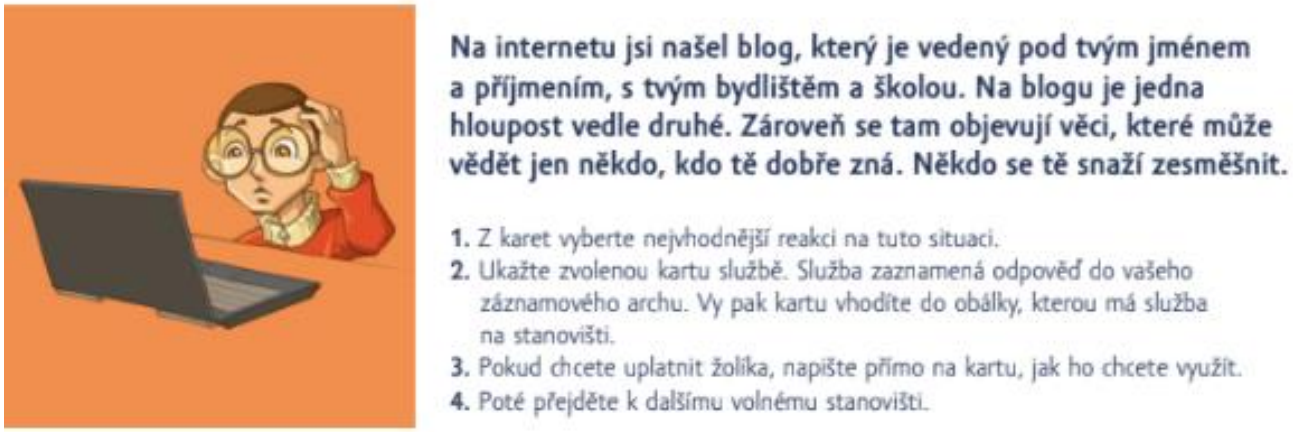
Název: Umím říct NE

Odkaz: https://in-generation.jsi.cz/materialy/umim-rici-ne

Náhled na kartičky:

Obrázek 10: ukázka kartičky z aktivity Umím říct NE

Náhled na situace:



Obrázek 11: ukázka situace z aktivity Umím říct NE

Popis:

IN(TERNET) GENERATION je obecně aktivita, která se zabývá internetovou gramotností. Vzniklo zde celkem 11 materiálů zaměřených na rozvoj internetové gramotnosti pro žáky 3.–4. tříd základní školy. Každý z materiálů obsahuje materiál pro žáky, učitele i rodiče. Tyto aktivity se dají využít bez přímého využívání dalších technologií nebo internetu, což může být na prvním stupni základní školy zásadní.

Pro krátký popis konkrétní aktivity byla vybrána hra Umím říct ne! Ta cílí na schopnost žáků bránit se proti šikaně, učí se podporovat asertivní obranu ve složitých situacích nejen v síti. Vzhledem k tomu, že se jedná o hru, učitel je zde v roli koordinátora, hlídá dodržování pravidel a diskutuje s žáky o tématu.

Celá hra je vhodná na dvě vyučovací hodiny, aby zbylo dost času na reflexi. Učitel předem musí připravit podklady: zadání pro stanoviště a pak následně stanoviště, záznamové archy, pravidla hry, dále nejlépe 7 razítek různého tvaru (popř. fixy různých barev).

Žáci se rozdělí do skupin, např. tříčlenných. Konkrétní pravidla jsou součástí pdf pro žáky. Učitel vytvoří stanoviště a na každém stanovišti je konkrétní situace, kterou žák má řešit pomocí kartiček. Kartičky má k dispozici každá skupina a každou může použít jen jednou. Své odpovědi také zaznamenávají do archu. V části připravené pro učitele je pak bodování jednotlivých odpovědí. Skupina, která získá nejvíce bodů, hru vyhrává.

Využití:

- při navození témat, která se týkají kybernetické bezpečnosti, či asertivního chování nejen na internetu;
- vhodný je výlet nebo větší prostor, kdy jsou od sebe dále stanoviště, než se dá zařídit ve třídě;
- vzhledem ke spolupráci ve skupině jde také o získávání poznatků i o reflexi aktuálních znalostí a postojů žáků.

3.6

Název: Internetem Bezpečně: příručka pro děti: Happy Slapping

Odkaz: https://www.internetembezpecne.cz/ke-stazeni/

Náhled:

Obrázek 12: ukázka z příručky (Happy slapping)

Popis:

Iniciátorem projektu Internetem Bezpečně je nezisková organizace you connected. V rámci projektu byly vytvořeny vzdělávací aktivity, které se zaměřují na kybernetické hrozby a jak se proti nim bránit. Vzhledem k tomu, že mezi hlavní cílovou skupinu patří i učitelé, přináší projekt aktivity přizpůsobené přímo do hodin. Na portálu je možné najít naučná videa i rady odborníků. Pro učitele důležitou kategorií budou příručky ke stažení (Internetem Bezpečně, Učebnice informatiky). Do šesti kategorií jsou pak rozděleny články: Jak se chránit, Rizika online komunikace, Malware, Rodiče, Podvodné praktiky a Dobré vědět.

Využití:

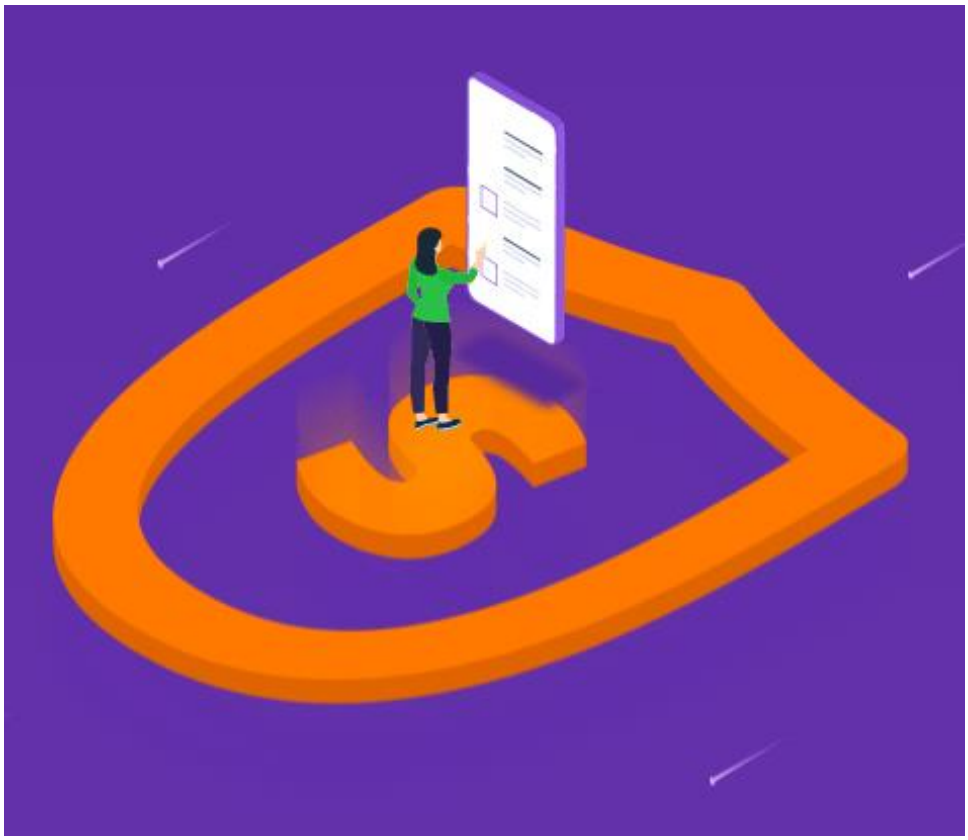
„Internetem Bezpečně“ je koncipováno přímo pro žáky, dalo by se říct jako příručka či učebnice. Obsahuje vysvětlení 13 témat (neobsahuje aktivity, má spíše informativní charakter), mezi kterými se vyskytuje i internetová komunikace, kyberšikana, nebo jak zabezpečit heslo. Pro ukázku byl vybrán Happy Slapping, který se jeví jako velmi nebezpečný z hlediska zdraví žáka, protože si žák nemusí uvědomit, kde končí hra a začíná trestná činnost. Důležité je žáky informovat, že jakékoliv takové jednání je postihováno zákonem, i když by to vypadalo jako legrace.

3.**7**

Název: Buď safe online

Odkaz: https://www.avast.com/cz/besafeonline/online-kurz

Náhled:



Obrázek 13: ilustrativní obrázek z Buď safe online

Popis:

Avast a E-Bezpečí ve spolupráci s bývalým youtuberem/influencerem Jiřím Králem připravili online kurz, ve kterém žáci druhého stupně mohou otestovat, jestli se dokážou bezpečně chovat na internetu. Celý výukový materiál se skládá ze čtyř částí se 14 tématy, ve kterých žáci získávají hvězdičky za úspěšné odpovědi na otázky. Před samotnými otázkami je vždy konkrétní situace navozena chatem a následně videem, ve kterém figuruje právě youtuber.

Webová stránka obsahuje i informace pro rodiče, co dělat pro bezpečí svých dětí, a 11 dílů podcastů Máma a táta v síti.

Využití:

Učitel může s žáky využít test v rámci jedné vyučovací hodiny jako ukončení k tématu Bezpečnost na internetu a zároveň využít doplňující informace a podklady pro diskuzi, které jsou připraveny (na vyžádání e-mailem).

3.8

Název: Chytrá škola O2: Zdraví v kyberprostoru

Odkaz: https://vyuka.o2chytraskola.cz/clanek/12/zdravi-v-kyberprostoru/ (https://vyuka.o2chytraskola.cz/data/files/zdravi-v-kyberprostoru-ds4b9omcse.pdf)

Náhled:

Obrázek 14: Ukázka z Chytrá škola O2

Popis:

V rámci tzv. Chytré školy z nadace O2 vznikaly metodické materiály pro učitele ve čtyřech částech: online bezpečnost, mediální gramotnost, počítačová gramotnost a technologie ve vzdělávání. Nutno

podotknout, že některé materiály jsou převzaté z jiných webových stránek, což nesnižuje jejich relevanci nebo velký rozsah materiálů. Dále popisovaná aktivita byla vybrána z části online bezpečnost, kde se učitelé mohou inspirovat ve 14 tématech. Zdraví v kyberprostoru obsahuje infolist i metodického rádce pro učitele. Každá taková aktivita se skládá z východisek, cílů a následně témat, aktivit či diskuzních otázek.

Využití:

Cílem vybraných výukových aktivit Zdraví v kyberprostoru je vést žáky k dodržování hygieny práce s technologiemi i s vysvětlením, proč je důležité si dělat přestávky nebo před spaním nesledovat telefon. Tento metodický rádce se zabývá obecnými pravidly hygieny práce s technologiemi, závislostí na internetu, nomofobií a syndromu FOMO, sledování světelného zdroje před spaním a kybernemocemi.

Pro žáky by mohl být nejzajímavější test úrovně nomofobie, který skládá z 20 otázek a měl by poukázat na to, jak jsou žáci spjatí se svým mobilním zařízením a jaký mají strach z toho, že pokud nebudou u svého mobilního telefonu, tak něco v kyberprostoru zmeškají. Před samotným testem je také vhodná diskuze, kdy učitel může využít připravené otázky v samotné metodice.

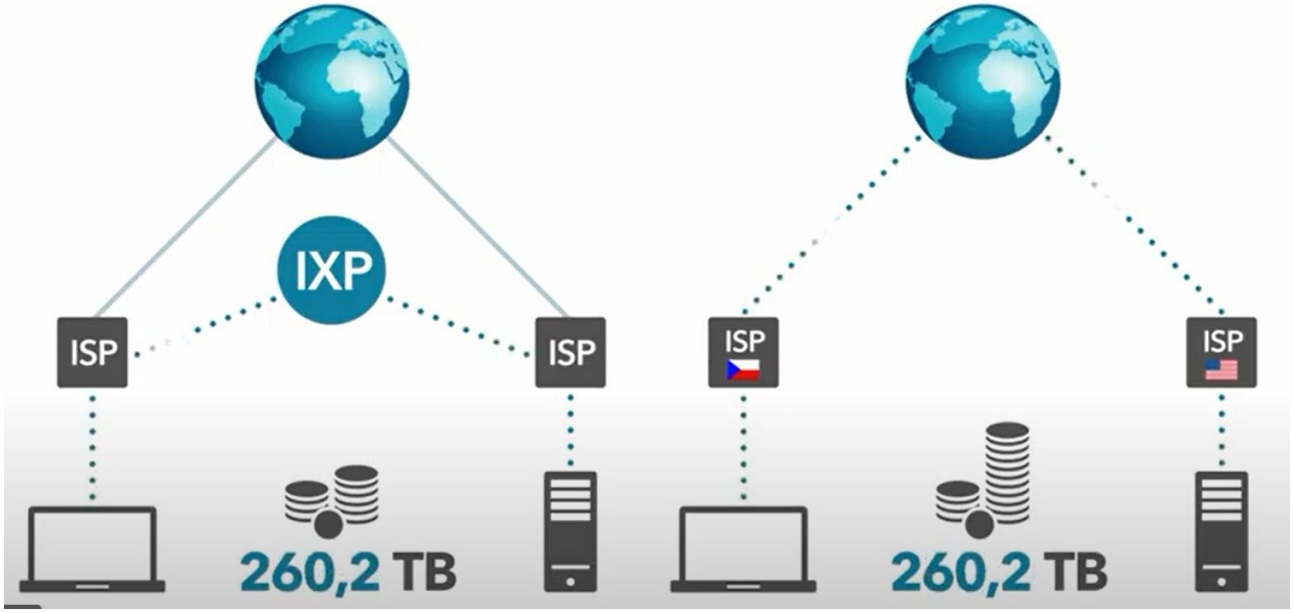
3.9

Název: Jak na internet: struktura internetu

Odkaz: https://www.jaknainternet.cz/page/1795/struktura-internetu/

(https://www.jaknainternet.cz/public_media/JNI_materialy/JNI_Struktura_Internetu_pracovni_list.pdf)

Náhled:



Obrázek 15: ukázka z Jak na internet

Popis:

Projekt „Jak na Internet“ je osvětová činnost CZ.NIC, pro kterou bylo vytvořeno osm kategorií (a následně devátá s nejnovějšími epizodami 2017). V přibližně dvou minutách se videa snaží osvětlit prostřednictvím průvodce konkrétní problematiku související s internetem (např. správa a fungování internetu, sdílení a publikování na internetu, nakupování i bezpečí na internetu) a reaguje i na současné IoT. Nutno podotknout, že je vhodné přihlédnout k období, kdy seriál vznikal, tedy 2012–2014 a následně v 2017, a reagovat na vývoj technologií.

Využití:

Jako ukázka bylo vybráno video s názvem struktura internetu. Žáci by si v rámci videa měli připomenout, že internet má decentralizovanou strukturu a jakým způsobem se připojujeme k internetu (ISP, IXP).

Pro učitele je zde připojen i výukový materiál, který obsahuje otázky k diskuzi, úkoly a případné další informace, kterých může učitel, či žáci využít. Pod videem se nachází i doprovodný článek vysvětlující co je to internet, způsoby propojování v rámci internetu.

Vzhledem k délce videa/videí je učitel může zařadit jako doprovodný materiál do výuky. Jeví se i jako vhodný informační zdroj v rámci případné hybridní či distanční výuky.

3.10

Název: Nebezpečné výzvy v online prostředí (E-Bezpečí)

Odkaz: https://e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/99-letak-nebezpecne-vyzvy-v-online-prostredi-pro-rodice-a-ucitele/file

Náhled:

Obrázek 16: ukázka z materiálu na e-bezpečí

Popis:

Obecně projekt E-Bezpečí obsahuje různé materiály pro podporu výuky, pro rodiče, učitele i žáky. Portál provozuje Centrum prevence rizikové virtuální komunikace na Pedagogické fakultě Univerzity Palackého v Olomouci. Součástí jsou tedy i nejrůznější články, výzkumné zprávy, kurzy (včetně videokurzu) či poradna. Tento projekt má i mezinárodní ocenění a spolupracuje nejen na materiálech a podkladech např. s O2, Avastem, Policií ČR, linkou bezpečí, MŠMT. Učitel si zde jistě najde snadno podklady pro výuku.

Využití

Ukázka je netradiční vzhledem k běžnému obsahu výuky a její zařazení do výuky by se dalo považovat spíše za informativní, popř. by se dalo využít na nástěnku či projektovou práci pro žáky i vzhledem k tomu, že se zabývá riziky spojenými s tzv. Challenges (výzvy). Na informačním letáku je popsané, co výzvami rozumíme a proč jsou pro děti tak nebezpečné. Uvedeny jsou i konkrétní příklady, včetně obrazové dokumentace (např. Duck Tape Challenge, Choking Challenge). Všechny tyto výzvy mohou být nebezpečné, dokonce i smrtelně, a proto je nutné o nich vědět, informovat žáky, ale na druhou stranu takovým způsobem, aby se nesnažili takové výzvy vyzkoušet, což může mít pro ně nedozírné následky do budoucího života. Z toho důvodu je důležitá prevence a diskuze.

3.11

Název: Nebojte se internetu: online komunikace

Odkaz: https://www.nebojteseinternetu.cz/page/3416/on-line-komunikace/

Náhled:

Obrázek 17: ukázka z Nebojte se internetu

Popis:

Desetidílný seriál Nebojte se internetu je projektem CZ.NIC a jeho cílem je informovat o technologiích především dospělé a ty, které se v technologiích tolik neorientují jako net generation. Nicméně se dá využít v některých částech i pro vzdělávání žáků, např. i na střední odborné škole. Tento seriál se orientuje na digitální prostředí od práce s prohlížečem přes bezpečné chování a komunikaci v online prostředí, včetně online nakupování. Součástí nejsou doprovodné materiály pro učitele, ale články pod videi, které mají hlouběji informovat o situaci, která se v části seriálu děje a vysvětlovat konkrétní pojmy a fungování vybraných služeb internetu.

Využití:

Vybraný díl se týká online komunikace a v rámci doprovodného článku se více zaměřuje na typy komunikace (synchronní a asynchronní), včetně fungování chatovacích nástrojů. U žáků je možné vyvolat domnění, že se učitel nesnaží poučovat je, ale doporučovat jim, aby se snažili působit i na své rodiče. Ověření, zda žáci dané problematice rozumí, může docházet formou návodných otázek:

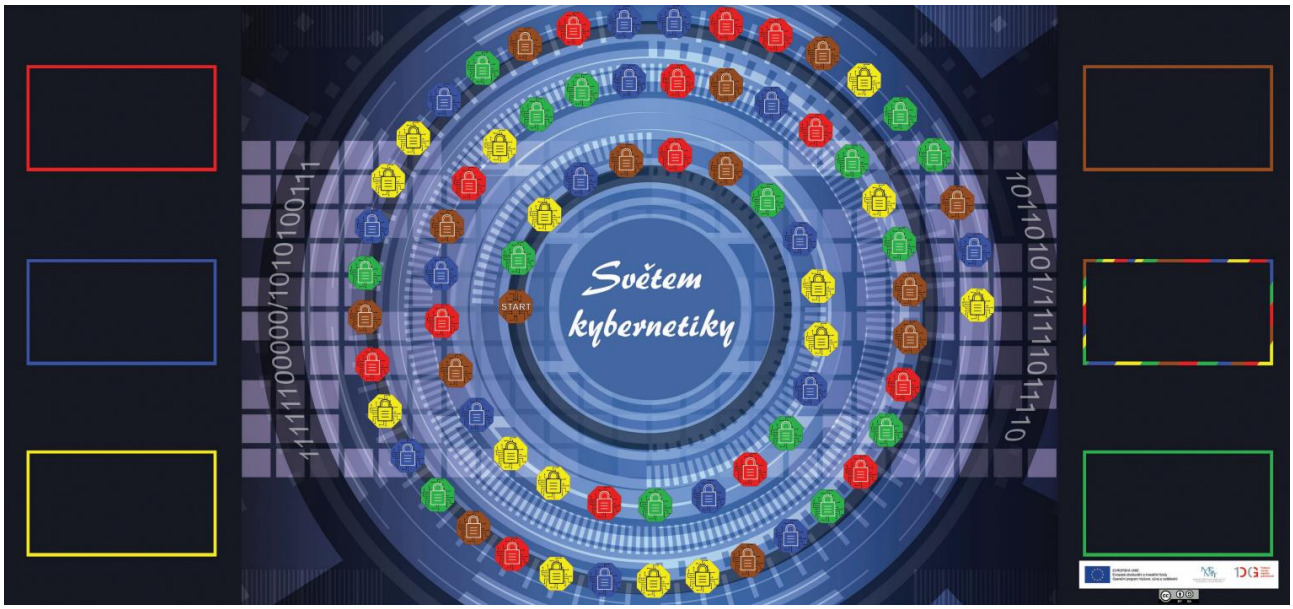
- Jaký je rozdíl mezi synchronní a asynchronní komunikací?
- V jakých případech je možné a vhodné využívání synchronní a asynchronní komunikace?
- Jaké možnosti a vlastnosti mají synchronní nástroje?
- Podle jakých vlastností si vybíráte chatovací nástroje?

3.12

Název: digigram.cz: Kybernetická bezpečnost

Odkaz: https://digigram.cz/dvz/#DVZICT01

Náhled:



Obrázek 18: hrací pole z Kybernetická bezpečnost

Popis:

Tento digitální vzdělávací zdroj zaměřený na bezpečnost se obejde bez využití počítačů. Jedná se o hru podobnou Aktivitám, kde se žáci pohybují po jednotlivých polích a dle barvy si vybírají otázku, na kterou mají odpovědět. Otázky na kartičkách jsou rozděleny do pěti oblastí: elektronická komunikace, bezpečnost v kyberprostoru, bezpečnost a finance, počítačové viry. Na každé kartičce jsou kromě otázky i 3 možnosti, z nichž pouze jedna je správná. Výhodou je, že si učitel může dle svého uvážení kartičky doplnit či modifikovat. Nevýhodou může být nutnost přípravy a tisku podkladů.

Mezi DVZ na digigram.cz je možné pro téma kyberprostor a bezpečnost využít i další aktivity, např:

- Netiketa v sociálních sítích
- Čí je to obrázek?
- Chraň svá data

Využití:

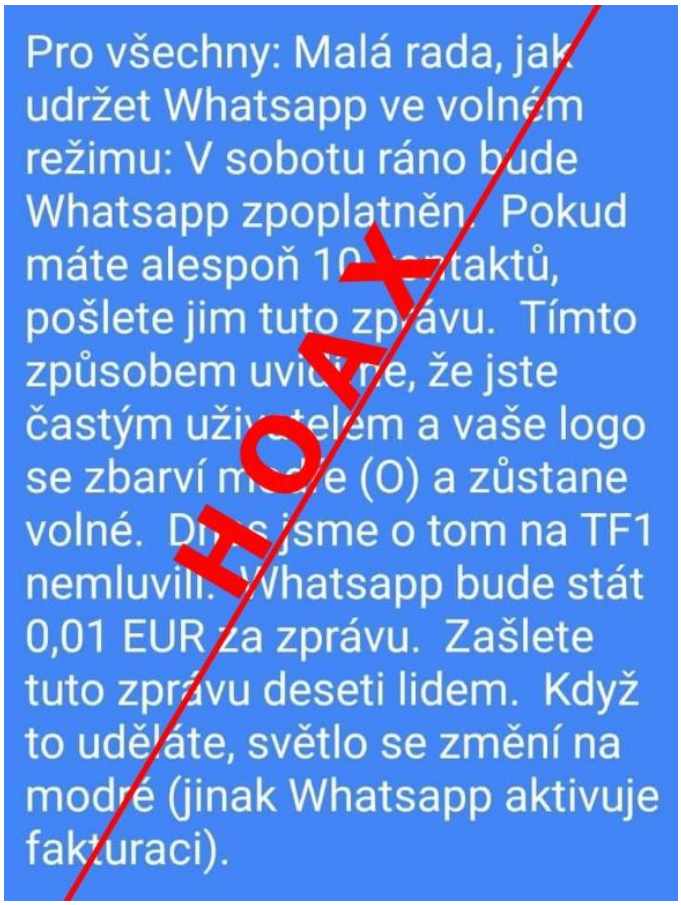
Žáci se hravou formou dozvídají informace prostřednictvím tzv. aktivit. Zajímavým aspektem se může jevit i práce ve skupině a společná diskuze nad otázkami. Hra by neměla být však pouze odehraná bez souvislostí či dalšího (popř. předcházejícího) výkladu nebo společné diskuze nad jednotlivými tématy.

3.13

Název: ho@x.cz: ZPOPLATNĚNÍ WHATSAPP

Odkaz: https://www.hoax.cz/cze/, konkrétně: https://hoax.cz/hoax/zpoplatneni-whatsapp/

Náhled:



Obrázek 19: ukázka hoaxu

Popis:

Portál ho@x.cz se soustředí na 6 typů podvodné činnosti na internetu, konkrétně: hoax, phishing, loterie, scam419, malware a řetězové e-maily. Nicméně se zde nachází i témata z netikety a diskuzní témata. Jsou zde nejen informace, ale i konkrétní aktualizované ukázky. Pro učitele, žáky i další uživatele se může stát stránka velmi užitečná pro ověření, zda s k nim nějaká poplašná zpráva dostala.

Využití:

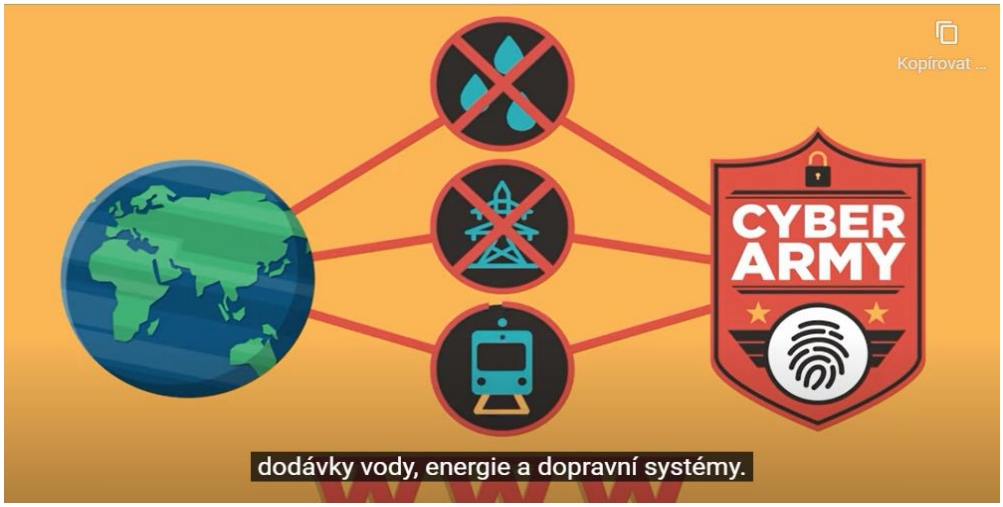
Právě ukázkou takové poplašné zprávy je zpráva o zpoplatnění aplikace WhatsApp. Anglická verze zprávy je již deset let stará, nicméně v roce 2022 se opět objevila s informací, že tuto chatovací aplikaci koupila jiná firma. Žáci si by si měli připomenout, co je vlastně hoax a proč je pro člověka důležité informace ověřovat a nedůvěřovat ani tomu, co jim pošle kamarád.

3.14

Název: Khanova škola: Kybernetická bezpečnost a kriminalita

Odkaz: https://cs.khanacademy.org/computing/code-org/computers-and-the-internet

Náhled:



Obrázek 20: ukázka z Khanovy školy (z videa)

Popis:

Khanova škola vychází z Khan Academy, která je spojená s databází bezplatných vzdělávací videí. Tato videa jsou pro české účely buď titulkována nebo přímo dabována. Sama udává, že se zde nachází již přes 1000 českých videí. Soustředí se více na oblast přírodovědných předmětů (Matematika, Fyzika, Chemie, Biologie, Ekonomie, Informatika), ale také Dějepis a Dějiny umění. V případě Informatiky se zde nachází devět témat, včetně tématu Počítač a internet. Zároveň je vhodné dodat, že videa jsou za sebou logicky poskládaná a u některých částí jsou i aktivity pro žáky.

Využití:

Pro ukázku bylo vybráno video Kybernetická bezpečnost a kriminalita, které se zaměřuje na tři oblasti: viry, DDoS útoky a phishing. Každopádně je nutné upozornit, že toto video je v řadě až poslední a pro žáky je vhodné pro úplnost projít i videa předchozí. Nicméně lze spustit i nezávisle na předchozích. Obecně se dá říct, že tato videa nejsou vhodná pouze na jedno shlédnutí, ale je vhodné je vidět vícekrát vzhledem k tomu, že obsahují dost často velké množství informací předávaných v relativně krátkém čase. Záleží ovšem na způsobu využití ve výuce a cíli, který si učitel stanoví.

Dotazy do diskuze:

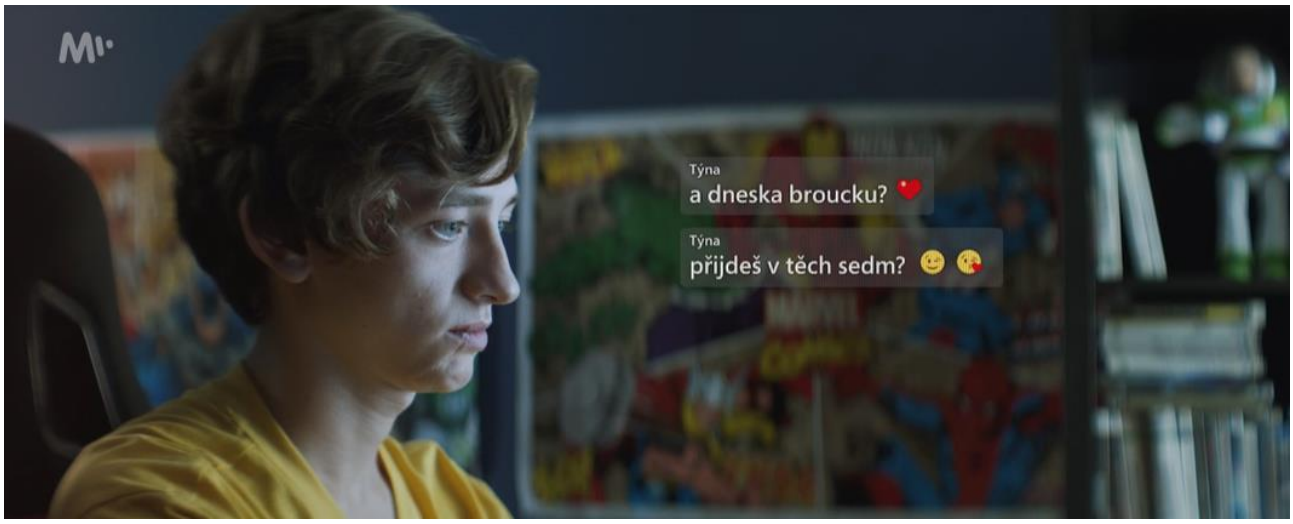
- Proč se vlastně zabývat kybernetickou bezpečností?
- Proč je bezpečnost důležitá z globálního hlediska?
- Co je to virus a jak se šíří? Proč je virus tak nebezpečný pro zařízení?
- Jak se stane, že hackeři napadnou webovou stránku?
- Jak se člověk může stát obětí phishingu?

3.15

Název: #martyisdead

Odkaz: https://martyisdead.mall.tv/

Náhled:



Obrázek 21: ukázka z #martyisdead

Popis:

Jedná se o osmidílný seriál, ve kterém postupně rodiče odkrývají, proč jejich „bezproblémový“ 15letý syn přišel o život. Prostřednictvím technologií se dozvídají, do jakých situací se Martin dostával, a hlavně otec se snaží zorientovat v posledních týdnech života svého syna.

Nutno poznamenat, že i pro potřeby online výuky vznikly výukové materiály k tématu kyberšikany ve spolupráci s Mall.TV a CZ.NIC. Příkladem může být osm pravidel chování na internetu. Součástí webové stránky se seriálem je i pět skutečných příběhů.

V případě, že se učitel v rámci prevence dotkne i filmu V síti, je možné na Mall.TV sledovat i Deník predátora.

Využití:

Kromě samotných připravených výukových aktivit jsou k dispozici i další fakta a pravidla, se kterými se učitel i žáci mohou seznámit, týkají se např. trollingu, sociálního inženýrství i sociálních sítí.

Zřejmě není možné, aby učitel s žáky sledoval všech osm dílů seriálu, ale důležitá je diskuze poté, co samostatně žáci seriál shlédnou. Rozhodně zajímavé by měly být reakce žáků po shlédnutí posledního dílu, kdy se ve skutečnosti dozví, že všechny špatnosti, kterých se musel dopouštět Marty, byly z popudu jeho nejbližšího okolí.

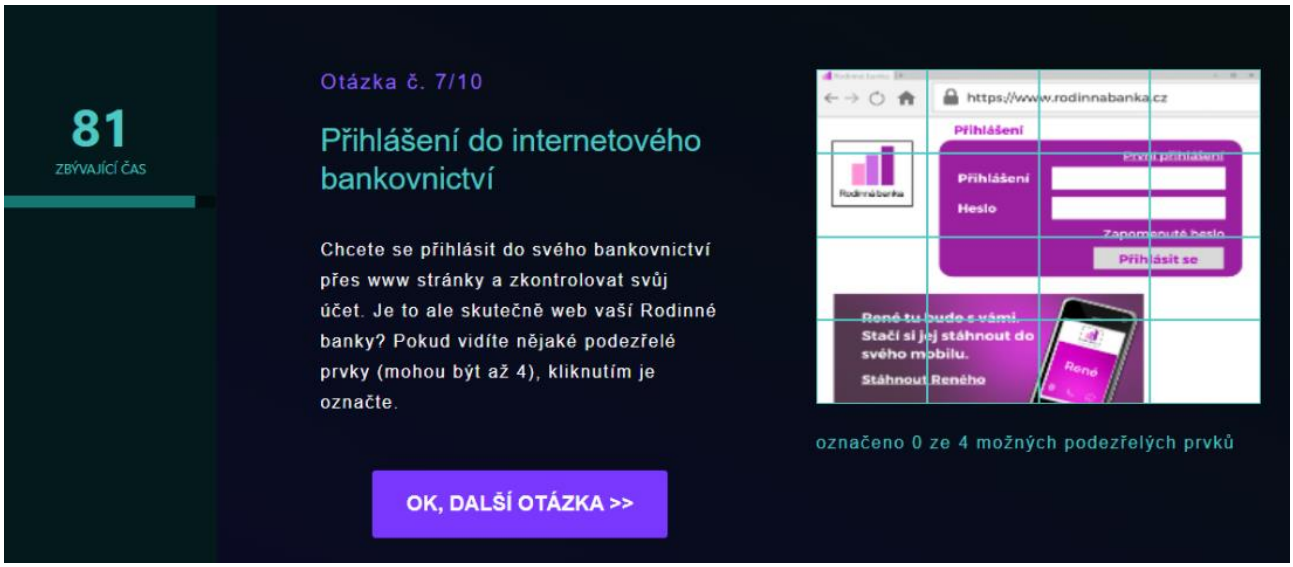
Vzhledem k fatálním důsledkům této kyberšikany, je potřebné opět zdůrazňovat nutnost prevence rizik spojených s užíváním kyberprostoru.

3.16

Název: Kybertest

Odkaz: https://kybertest.cz/

Náhled:



Obrázek 22: ukázka z kybertestu

Popis:

Jedná se o vědomostní test složený z 10 otázek, kdy na každou odpověď má účastník 90 sekund. Je tedy jasné, že test není nikterak časově náročný. Okamžitě po ukončení testu dojde k jeho vyhodnocení a následně může učitel s žáky test rozebrat. Tento test byl součástí průzkumu chování Čechů v online prostředí v souvislosti s bezpečností a elektronickým bankovnictvím v roce 2020. Od té doby je k dispozici volně a mohou ho využít i učitelé jako součást výuky. Součástí webové stránky, na které se nachází test, jsou i popisy nejčastějších útoků na klienty bank a zásady bezpečnosti chování v kyberprostoru.

Testování se může zdát netradiční, protože se nejedná o otázky a volbu odpovědí či jejich doplnění. Ten, kdo si chce testem projít, musí označovat části obrázků, na kterých se nachází konkrétní bezpečnostní prvek. Podle takového se dá odvodit, zda se jedná o podvod, či oprávněnou žádost.

Využití

Učitel může test využít ve chvíli, kdy tématem výuky je bezpečnost na internetu v souvislosti např. s elektronickým bankovnictvím. Nemusí se jednat o výuku informatiky, ale nachází využití i v ekonomicky zaměřených předmětech a je přímou součástí vzdělávacích oborů Výchova k občanství a Člověk a svět práce. Tyto znalosti a dovednosti jsou součástí digitální gramotnosti člověka, který pracuje s elektronickým bankovnictvím.

3.17

Název: Soutěž v kybernetické bezpečnosti

Odkaz: https://www.kybersoutez.cz/

Náhled:

Obrázek 23: ilustrativní obrázek z kybersoutěže

Popis:

Tato soutěž je pro všechny žáky a studenty základních, středních i vysokých škol (ve věku 9–25 let). V roce 2022 byl ukončen 6. ročník, na podzim konkrétního roku bývá zahájen další ročník. Soutěž, kterou pořádá Centrum kybernetické bezpečnosti a je součástí European Cyber Security Challenge, probíhá ve třech kolech: osvětové, výběrové a finálové. Cílem je zvyšovat povědomí o rizicích a hrozbách kyberprostoru, poskytnout informační podporu učitelům i v neposlední řadě ověřit a doplnit znalosti v této oblasti jak na straně žáků, tak učitelů. Soutěž se obsahově skládá z 11 oblastí, např. principy ochrany kybernetického prostoru, hrozby a zranitelnosti kybernetického prostoru, či legislativa a právní aspekty, ochrana osobních údajů a digitální stopa, dokonce i LINUX. Do každého kola pak existují doporučené materiály k prostudování.

Je velmi výhodné dobře prostudovat pravidla soutěže. Každý soutěžící má právo vyplnit jeden soutěžní test, ve kterém závisí na správnosti i rychlosti odpovědi. V případě špatných odpovědí jsou body odečítány.

Pro učitele jsou připraveny i metodické a podpůrné materiály připravené NÚKIB, AFCEA, CZ.NIC či NCBI.

Využití:

- prevence v oblasti kyberbezpečnosti,
- metodické materiály pro učitele,
- příprava žáků v oblasti kybernetické bezpečnosti.

3.18

Název: „DÁVEJ KYBER“ PRO UČITELE – Základy kybernetické bezpečnosti

Odkaz: https://osveta.nukib.cz/course/view.php?id=121

Náhled:

Obrázek 24: ilustrativní obrázek z NÚKIB

Popis:

Tento online kurz vytvořený NÚKIB za podpory MŠMT se zaměřuje přímo na zaměstnance škol. Je rozdělený do dvou částí: témata zaměřená na učitele a témata zaměřená na třídu. Mezi osmi tématy zaměřenými na učitele se objevuje i část zaměřená na bezpečnou online výuku, digitální identitu učitele či učitele jako oběť kyberšikany. Sedm témat zaměřených na třídu se orientuje na obecně na kyberprostor a nebezpečí v něm, např. kyberšikanu, nenávist a online agrese.

Každé téma se skládá ze slovníčku důležitých pojmů, úvodního slova, konkrétního příběhu, doporučení a tipů do praxe. Popis i samotné vyjádření dané problematiky je vytvářeno velmi příjemně a užitečně, nikoliv příliš odborně. I z tohoto důvodu je tento kurz, nebo jeho jednotlivá témata, vhodný i pro učitele neinformatických předmětů.

NÚKIB připravuje i kurzy pro žáky různých věkových kategorií:

- Vanda a Eda v onl@jn světě (1.–3. ročník ZŠ)
- Digitální stopa: příběh svůdníka (4. –5. ročník ZŠ)
- Digitální stopa: příběh Báry (5. –7. ročník ZŠ)
- Jsem netvor na základce (8. –9. ročník ZŠ)
- Jsem netvor na střední (1. –2. ročník SŠ)

Využití:

Jedná se o MOOC kurz, do kterého není nutné se přihlašovat, ale učitel může prostudovat jen témata, která ho aktuálně zajímají. Jedná se o osobnostní rozvoj a rozvoj práce se skupinou žáků či třídním kolektivem.

3.19

Název: Desatero dobrého „kybernetického“ rodiče

Odkaz: https://www.zachranny-kruh.cz/osobni-bezpeci/dalsi-nebezpeci/internet/desatero-dobreho-kybernetickeho-rodice.html

Náhled:

Obrázek 25: ilustrativní obrázek ze Záchranného kruhu

Popis:

Portál Záchranného kruhu se zabývá nejen například bezpečnou dopravou, první pomocí, ale i osobním bezpečím (https://www.zachranny-kruh.cz/osobni-bezpeci/), do kterého lze řadit i kybernetickou bezpečnost. Zde je formou krátkých článků vysvětlena vždy konkrétní problematika, např. mobbing, botnet či bezpečné nákupy. Každopádně činnosti této neziskové organizace, která shlukuje především záchranářské subjekty a další instituce, necílí pouze na děti, ale i dospělí včetně seniorů zde naleznou zajímavé články pro své vzdělávání. Tato asociace Záchranný kruh mimo jiné umožňuje vznikat také vzdělávacím materiálům pro učitele, a tudíž jejich žáky, či realizuje preventivně výchovné činnosti.

Využití:

Vybraný článek se zaměřuje na deset konkrétních rad, které je vhodné si v roli učitele a rodiče osvojit, resp. na co se v rámci vzdělávání dětí zaměřit. Jak je psáno v úvodu tohoto článku, dítě v rodičích hledá svůj vzor, pomoc a pochopení i v případě technologií. Tento článek je vhodné využít pro osobní vzdělávání učitele či rodiče, resp. k uvědomění si základních pravidel a strategií, na které se při práci s dětmi v oblasti bezpečnosti soustředit.

Desatero se zaměřuje na netiketu, osobní bezpečnost při práci s technologiemi, fake news i elektronickou komunikaci. Kromě samotného textu ve spodní části učitelé i rodiče naleznou další zajímavé materiály.

3.20

Název: Je ve virtuálním světě bezpečno?

Odkaz: https://bezpecnevkyberprostoru.cz/clanky/materialy-ke-stazeni/je-ve-virtualnim-svete-bezpecno----brozura/

Náhled:

Popis:

Projekt Bezpečno v kyberprostoru vznikl již před více než deseti lety ve spolupráci v Jihomoravském kraji. Snaží se reagovat na aktuální trendy a rizika v kyberprostoru a je určen pro širokou veřejnost, školy nevyjímaje. V rámci projektu se realizuje i soutěž právě pro žáky Jihomoravského kraje. V rámci portálu je možné se dostat i k výzkumným zprávám, článkům, či slovníčku pojmů (včetně komunikačních akronymů).

V materiálech ke stažení je možné získat 3 typy materiálů: pro 1. stupeň, 2. stupeň a Je bezpečno ve virtuálním světě. První dva zmíněné jsou vytvořeny jako pracovní listy pro žáky konkrétních stupňů vzdělávání a jsou okamžitě využitelné (popř. s korekcí učitele) ve výuce.

Velmi jednoduše je pak zpracována příručka Je ve virtuálním světě bezpečno, která se zaměřuje na rizika a nástroje sociální sítí a jak jim předcházet. Obsahuje i důležité odkazy na případnou další pomoc.

Využití:

Brožura je spíše informační text než učebnice vhodná pro žáky 2. st. ZŠ. Její části mohou sloužit pro přípravu učitele na vyučování. Také může sloužit pro zákonné zástupce, aby se v dané oblasti mohli zorientovat.

4 Závěr

V této příručce by se měl učitel inspirovat různými možnostmi, jak v jednotlivých aktivitách, prostředích, či s využitím různých didaktických postupů zařadit témata související s kybernetickou bezpečností a kyberprostorem obecně. Úmyslně byly aktivity navrženy různým způsobem a s tématy, která nejsou zcela typická (a tudíž se příliš nevyskytují a neopakují v rámci jiných již vytvořených aktivit a metodických pomocníků) a ukazují i další možnosti, jak žáky v dané oblasti rozvíjet. Jedná se o útržkovité ukázky a inspiraci, nikoliv dogma, jak by se měla v rámci představených aktivit vyučovat na školách kybernetická bezpečnost či internet nebo kyberprostor.

Učitel v příručce může narazit na již vytvořené aktivity různých společností, firem či institucí, které se minimálně o danou problematiku zajímaly, či se v ní neustále svou orientací pohybují. Výčet není jistě kompletní, ale měl by učiteli minimálně napovědět, jak je možné k této oblasti a těmto tématům přistupovat.

Za autory Vám přeji, aby se Vám vytvořené i sesbírané aktivity líbily a abyste si dále rozšiřovali portfolio aktivit, které se v této oblasti pro základní i střední školy vyskytují.

5 Seznam informačních zdrojů

Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025. *NUKIB* [online]. 2021 [cit. 2022-7-5]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan

Akademie věd České republiky. Nezkreslená věda. *Jak funguje internet.* In: Youtube [online]. 4. 5. 2020 [cit. 2022-06-03]. Dostupné z: https://www.youtube.com/watch?v=L05HGoaDkRo. Kanál uživatele Otevřená věda.

Alenka v říši GIFů. *Ozvěny budoucnosti* In. ČT Déčko [online]. [cit. 2022-05-31]. Dostupné z: https://decko.ceskatelevize.cz/alenka-v-risi-gifu

Bankovkovi. *Phishing a skimming.* In. ČT EDU [online]. [cit. 2022-05-31]. Dostupné z: https://edu.ceskatelevize.cz/video/121-phishing-a-skimming

Bezpečně v kyberprostoru. *Je ve virtuálním světě bezpečno?* Krajské ředitelství Policie Jihomoravského kraje. Brno. [cit. 2022-06-1]. Dostupné z: https://bezpecnevkyberprostoru.cz/clanky/materialy-ke-stazeni/je-ve-virtualnim-svete-bezpecno----brozura/

Buď save online. *Online kurz.* Avast. [cit. 2022-03-20]. Dostupné z: https://www.avast.com/cz/besafeonline/online-kurz

Centrum kybernetické bezpečnosti. *Cyber Security Competition.* [online]. [cit. 2022-06-03]. Dostupné z: https://www.kybersoutez.cz/

Centrum prevence rizikové virtuální komunikace. Nebezpečné výzvy v online prostředí (pro učitele a rodiče). [online]. Univerzita Palackého. Olomouc. 2017. [cit. 2022-05-31]. Dostupné z: https://e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/99-letak-nebezpecne-vyzvy-v-online-prostredi-pro-rodice-a-ucitele/file

CZ.NIC. *On-line komunikace.* Nebojte se internetu. [online]. [cit. 2022-06-01]. Dostupné z: https://www.nebojteseinternetu.cz/page/3416/on-line-komunikace/

CZ.NIC. *Struktura Internetu.* In. Jak na internet. [online]. [cit. 2022-05-31]. Dostupné z: https://www.jaknainternet.cz/page/1795/struktura-internetu/

Česká bankovní asociace. *Kybertest.* [online]. [cit. 2022-06-03]. Dostupné z: https://kybertest.cz/

Česká bankovní asociace. *Podvodné volání (vishing).* In: Youtube [online]. 13. 7. 2021 [cit. 2022-04-03]. Dostupné z: https://www.youtube.com/watch?v=tjAFobMn9ps

Datová lhota. *Cesta na se(r)ver.* iVysílání ČT. [online]. [cit. 2022-03-19]. Dostupné z: https://www.ceskatelevize.cz/porady/11933175266-datova-lhota/217543112110008/

ESET. *Vishing: co je to a jak se bránit?* [online]. [cit. 2022-8-1]. Dostupné z: https://www.eset.com/cz/vishing/

FANFULOVÁ, Eva a Zuzana KOZLOVÁ. Kuřátko Čiky a jeho přátelé. *Gramotnost pro život. Učíme v souvislostech.* [online]. březen 2019, 12 [cit. 2022-03-19]. Dostupné z: https://digifolio.rvp.cz/artefact/file/download.php?file=84758&view=15150

Hoax.cz. *Hoax.* [online]. [cit. 2022-05-03]. Dostupné z: https://www.hoax.cz/cze/

IN(TERNET) GENERATION. *Umím říci NE.* Jednota školských informatiků. [cit. 2022-03-20]. Dostupné z: https://in-generation.jsi.cz/materialy/umim-rici-ne

Khanova škola (z Khan Academy). *Jak fungují počítače.* In. Počítače a internet. [online]. [cit. 2022-6-3]. Dostupné z: https://cs.khanacademy.org/computing/code-org/computers-and-the-internet

KOHOUT, Roman a Sandra KUBÍČKOVÁ. Internetem bezpečně: příručka pro děti od 6 do 12 let. *Bezpečně internetem.* [online]. [cit. 2022-05-31]. Dostupné z: https://www.internetembezpecne.cz/ke-stazeni/

Kurzy.cz. *Seznam kryptoměn* [online]. [cit. 2022-5-20]. Dostupné z: https://www.kurzy.cz/kryptomeny/seznam-kryptomen/

Learning Apps [online]. [cit. 2022-5-1]. Dostupné z: https://learningapps.org

MYERS, Tony. „The Postmodern Imaginary in William Gibson's Neuromancer." *MFS Modern Fiction Studies*, vol. 47 no. 4, 2001, p. 887-909. *Project MUSE*, doi:10.1353/mfs.2001.0100.

NÚKIB. *„Dávej kyber" pro učitele.* [online]. [cit. 2022-06-03]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=121

O2 Chytrá škola. *Zdraví v kyberprostoru: Metodický rádce pro učitele.* E-bezpečí. Univerzita Palackého Olomouc. [cit. 2022-05-31]. Dostupné z: https://vyuka.o2chytraskola.cz/data/files/zdravi-v-kyberprostoru-ds4b9omcse.pdf

Policie České republiky. *Vishing a spoofing.* [online]. [cit. 2022-8-1]. Dostupné z: https://www.policie.cz/clanek/vishing-a-spoofing.aspx

Quizlet [online]. [cit. 2022-05-15]. Dostupné z: https://quizlet.com/

RAMBOUSEK, Vladimír a Tomáš JEŘÁBEK. Vymezení digitální gramotnosti. *Podpora rozvoje digitální gramotnosti* [online]. Praha, 2019 [cit. 2022-06-20]. Dostupné z: https://digigram.cz/vymezeni-digitalni-gramotnosti/

Sheeplive. *Bez kožíšku.* Sheeplive. [online]. [cit. 2022-03-20]. Dostupné z: http://cz.sheeplive.eu/fairytales/bez-kozisku-titulky

tým mBank. *Co je to vishing a jak se bránit podvodným telefonátům?* [online]. [cit. 2022-07-20]. Dostupné z: https://www.mbank.cz/blog/post,858,pozor-na-podvodne-telefonaty-aneb-co-je-to-vishing.html

VAJEN, Irena. *Kybernetická bezpečnost.* Podpora rozvoje digitální gramotnosti. [online]. 2020. [cit. 2022-06-01]. Dostupné z: https://digigram.cz/dvz/#DVZICT01

Vishing. *Česká spořitelna* [online]. [cit. 2022-04-03]. Dostupné z: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/vishing

Záchranný kruh. *Desatero dobrého „kybernetického" rodiče.* [online]. [cit. 2022-06-03]. Dostupné z: https://www.zachranny-kruh.cz/osobni-bezpeci/dalsi-nebezpeci/internet/desatero-dobreho-kybernetickeho-rodice.html

Zákon o elektronických komunikacích. Zákon č. 127/2005. In: *Sbírka zákonů ČR*. 2005. Dostupné také z: https://www.mpo.cz/cz/e-komunikace-a-posta/elektronicke-komunikace/narodni-legislativa-a-predpisy/zakon-o-elektronickych-komunikacich--37746/

Zákon o kybernetické bezpečnosti. Zákon č. 181/2014. In: Sbírka zákonů ČR. 2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

#martyisdead. In. Mall TV. [online]. [cit. 2022-06-03]. Dostupné z: https://martyisdead.mall.tv/

6 Seznam odkazů na obrazové materiály:

[Deep web]. In. *Wikimedia.org*. [online]. [cit. 2022-05-10] Dostupné z: https://upload.wikimedia.org/wikipedia/commons/3/31/Deepweb.png

[Demonstrace]. In. *Flickr.com.* [online]. [cit. 2022-07-03]. Dostupné z: https://live.staticflickr.com/740/22978737539_1617c19258_b.jpg

[Deštný prales]. In. *ccb.cz*. [online] [cit. 2022-07-03]. Dostupné z: https://ccbc.cz/wp-content/uploads/2020/12/doskol-tropicky-destny-les-prednaska-2.jpg

[Deštný prales]. In. *forest-atlas.fs.fed.us.* [online]. [cit. 2022-07-03]. Dostupné z: https://forest-atlas.fs.fed.us/assets/shapes/fires/Understory-Fire_PantherNWR-FL_Wildfire0306%20.jpg

[Dimenze internetu]. In. *Wikimedia.org*. [online]. [cit. 2022-05-10] Dostupné z: https://upload.wikimedia.org/wikipedia/commons/0/06/Iceberg_of_Webs.svg

[Koupelna]. In. *Publicdomainpictures.net*. [online]. [cit. 2022-07-03] Dostupné z: https.://www.publicdomainpictures.net/pictures/10000/nahled/87-1222002804D8gw.jpg

[Kuchyně]. In. *Pexels.com*. [online]. [cit. 2022-07-15] Dostupné z: https://images.pexels.com/photos/5353945/pexels-photo-5353945.jpeg

[Mikulášská nadílka]. In. *Omalovanky.webgarden.cz.* [online]. 4. února 2009. [cit. 2022-07-03]. Dostupné z: http://www.detskeomalovanky.cz/wp-content/mikulas3.gif

[Obývací pokoj]. In. *Baumax.cz*. [online]. [cit. 2022-07-15] Dostupné z: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQHIG3chLPsW-x0F5LrD2DRU02Rvkxst0R5aQ&usqp=CAU

[Šachy]. In. *istockphoto.com*. [online]. [cit. 2022-07-03] Dostupné z: https://media.istockphoto.com/photos/vivid-emotions-after-the-game-of-chess-picture-id586945434?k=20&m=586945434&s=170667a&w=0&h=G-DjDst-2NmIXUPYXDTmKBU3colpjEAP9RHsRi-Lg8M=

[Válka]. In. *Lidovky.cz* [online]. 16. ledna. 2022 [cit. 2022-07-03]. Dostupné z: https://1gr.cz/fotky/lidovky/22/012/vidw/RKJ90cb8b_data1.jpg

7 Seznam obrázků

8 Seznam tabulek

9 Seznam často využívaných pojmů a zkratek

AFCEA – Armed Forces Communications & Electronics Association – hlavní zaměření je dlouhodobá podpora rozvoje informačních a komunikačních technologií ozbrojených sil
asynchronní komunikace – vzhledem k digitálním technologiím probíhá s časovým odstupem (např. e-mail)
Avast – Avast Software s.r.o. je česká nadnárodní společnost zabývající se počítačovou bezpečností
botnet – malware, druh „internetového robota“, který funguje autonomně dle své určené činnosti (např. rozesílání spamu)
Centrum prevence rizikové virtuální komunikace – je součástí Pedagogické fakulty Univerzity Palackého
clickbait – tzv. návnada po kliknutí, např. titulek nebo odkaz, pod kterým se může schovávat škodlivý software
CZK – česká koruna
CZ.NIC – poskytovatelé internetových služeb, registrace pod doménou CZ, starají se i o zabezpečení a provoz domén na nejvyšší úrovni a zároveň o osvětu v oblasti kyberprostoru a kybernetické bezpečnosti
dark web – web se „specifickými vlastnostmi“, ke kterému je třeba přistoupit, a často je spojován s nelegální kybernetickou i jinou činností
DDoS – (z angl. Denial of Service) – typ útoku např. na webovou stránku, ve kterém jde o znepřístupnění nebo znefukčnění přístupu, či služeb
deep web – web se „specifickými vlastnostmi“, ke kterému je třeba přistoupit i přes běžný internetový prohlížeč, např. přihlášením
digitální gramotnost – soubor dílčích digitálních kompetencí, které potřebuje člověk k bezpečnému, jistému a kritickému využívání digitálních technologií (detailnější popis na digigram.cz)
digitální identita – jedná se o soubor informací o naší osobě v kyberprostoru (popř. veřejně dostupný)
DNS – (z angl. Domain Name System) – hierarchický decentralizovaný systém doménových jmen
DVZ – digitální vzdělávací zdroj, metodický materiál pro učitele ve spojitosti s učebním materiálem pro žáka
e-bezpečí – projekt zabývající se bezpečností na internetu, který provozuje Centrum prevence rizikové virtuální komunikace na Pedagogické fakultě Univerzity Palackého
fake news – tzv. falešné zprávy, které úmyslně šíří dezinformace
FOMO – (z angl. Fear of Missing out) – úzkostný strach z toho, že člověku utíká nějaká důležitá událost nebo příležitost, kterou ostatní zmiňují (často spojeno se sociálními médii)
Happy slapping – (z anglického spokojené fackování) – fyzické napadení oběti, které je nahráváno např. na mobilní telefon
hoax – tzv. poplašná zpráva, která má za cíl útočit emočně
challenge – výzva na internetu, může být zpracovaná formou videa, v některých případech může mít i smrtelné následky (např. Duck Tape Challenge, Choking Challenge)
chatovací nástroj – aplikace, která umožňuje synchronní komunikaci (např. messenger)
Internet – propojené počítačové sítě, kdy počítače komunikují skrze protokoly TCP/IP

Internet věcí (z angl. IoT – internet of things) – síť zařízení vybavených elektronikou a potřebným softwarem pro komunikaci a propojení s dalším zařízením, se kterým si jsou schopny vyměňovat data
IP adresa – číslo, které identifikuje počítač v síti
Kahoot – online prostředí pro přípravu testů a jejich následnou realizaci pro poskytování okamžité hromadné zpětné vazby žákům
klíčové kompetence – představují souhrn vědomostí, dovedností, schopností, postojů a hodnot důležitých pro osobní rozvoj a uplatnění každého člena společnosti; v tomto případě dle RVP ZV a komplexní rozvoj žáka
kybernetická bezpečnost – aktivity nezbytné k ochraně sítí, informačních systémů, digitálních technologií i koncových uživatelů v kyberprostoru
kyberprostor (z angl. cyberspace) – virtuální počítačový svět, který tvoří globální počítačovou síť
kyberšikana – šikana realizovaná skrze nebo prostřednictvím digitálních technologií
malware – (z angl. malicious software) je v současnosti obecné označení pro škodlivý software, který provádí změny v digitálních technologiích, které uživatel neodsouhlasil (např. trojský kůň, spyware)
MFF – Matematicko-fyzikální fakulta Univerzity Karlovy
mobbing – druh šikany na pracovišti
MOOC kurz – (z angl. Massive Open Online Course) – hromadný vzdělávací online kurz bez omezeného počtu účastníků, řadí se do neformálního vzdělávání a je založen na principu zprostředkování konkrétního vzdělávacího obsahu široké veřejnosti
nomofóbie – úzkostný strach, který spočívá v závislosti na vlastním mobilním dotykovém zařízení
MŠMT – Ministerstvo školství, mládeže a tělovýchovy
NCBI – National Center for Biotechnology Information
NCKB – Národní centrum kybernetické bezpečnosti
net generation – označení „lidí“, kteří se narodili již v době, kdy informační a komunikační technologie jsou běžnou součástí lidské potřeby (podobné termíny: mileniáni, digitální domorodci)
netiketa – etiketa v kyberprostoru
NMK ICT – Národní metodický kabinet Informatika a ICT
NÚKIB – Národní úřad pro kybernetickou bezpečnost
Obor Informatika – vzdělávací obor dle RVP ZV (2021)
OS – operační systém
O2 – obchodní značka telekomunikační sítě společnosti Telefónica
phishing – útok na digitální technologie pomocí technik sociálního inženýrství, při kterých se získávají data o uživateli a následně se předpokládá jejich zneužití
počítačový vir – malware, který se šíří bez vědomí člověka digitálními technologiemi a napadá software
podcast – digitální pořad, často formou mluveného slova
QR kód – data zakódovaná specifickým algoritmem (podobně jako EAN, jen s větším množstvím dat)
Quizlet – online prostředí pro přípravu aktivit (flash cards, learn, write, spell, text, match, gravity, live)
router – tzv. směřovač je aktivní síťový prvek, který spojuje dvě sítě mezi sebou přenáší mezi nimi data
RVP ZV – Rámcový vzdělávací program pro základní vzdělávání

stalking – opakované dlouhodobé sledování aktivit určité osoby, obtěžování této osoby nebo jejího okolí a sběr dat o této osobě
surface web – běžně dostupný web, ke kterému lze přistoupit přes běžný internetový prohlížeč
synchronní komunikace – vzhledem k digitálním technologiím probíhá okamžitě v reálném čase (např. chat)
troll – účastník diskuzí, chatů a dalších sociálních médií, který se snaží vyprovokovat další osoby k reakci
virtuální měna – kryptoměna, digitální decentralizovaná měna
vishing – (z angl. Voice phishing) – podvodná praktika, kdy se z oběti vylákávají peníze nebo informace prostřednictvím telefonického hovoru
you connected – nezisková organizace zabývající se bezpečností na internetu

Systém podpory profesního rozvoje učitelů a ředitelů

Metodická příručka NMK Informatika a ICT
KYBERNETICKÁ BEZPEČNOST A KYBERPROSTOR

WBS kód:4.1.6.1.2

Autoři: Petra Vaňková a kolektiv autorů

Národní pedagogický institut České republiky

Senovážné nám. 872/25, 110 00 Praha 1

Tel./fax: +420 222 122 112

E-mail: sekretariat@npi.cz

Praha, 2023

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

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY