NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

ROZCESTNÍK PRO UČITELE ZÁKLADNÍ ŠKOLY

www.nukib.cz

JAK (SE)VZDĚLÁVAT V KYBERBEZPEČNOSTI

Zamyslete se chvíli nad následujícími situacemi. Kolik z vás by se začalo bavit na ulici s naprosto neznámým člověkem? Kolik z vás by mu bylo ochotno sdělit přesnou adresu svého bydliště? Najde se mezi vámi někdo, kdo by mu poštou v obálce poslal své intimní fotografie, kdyby o ně požádal? Jak by se vám líbilo, kdyby vaše fotografie z firemního večírku visela na sloupech veřejného osvětlení v celém městě? Když odcházíte z domu na nákup, necháte odemčený dům? I kdyby to bylo jen na chvilku?… Všechny předchozí situace se vám pravděpodobně zdají zcela absurdní. Jistě, už od dětství si přeci osvojujeme znalosti a dovednosti, které nám pomáhají orientovat se ve světě. Tedy v tom reálném. Problém je, že velká část života se v dnešní době přesouvá do světa virtuálního. Všechny výše jmenované situace, které vám v reálném životě připadají natolik absurdní, jsou v kyberprostoru na denním pořádku. Před tím rozhodně nelze zavřít oči.

Budeme-li se držet pravidla, že primárním cílem vzdělávání je připravit žáky na život, pak je nezbytně nutné, aby učitelé drželi krok s rozvojem společnosti. A protože to není snadný úkol, vznikl tento vzdělávací web, který vám má pomoci se zorientovat v tom – co a jak v kyberbezpečnosti učit. Na internetu se nachází celá řada kvalitních materiálů, rozhodli jsme se proto je uspořádat do přehledných kapitol a doplnit „bílá místa“. Cílem nebylo vytvořit vyčerpávající seznam, ale především zaměřit se na zdroje, které považujeme za kvalitní. Pro přehlednost níže uvádíme seznam těch nejdůležitějších, s nimiž se při procházení webu budete setkávat.

Tento rozcestník Vám pomůže nejen se začleněním kyberbezpečnosti do výuky, ale především k získání potřebných znalostí. Věnujte tedy chvilku svého času jeho prostudování.

Profily

NAVIGACE

 Kliknutím se přesunete na dílčí kapitolu.

Obecné informace	Heslo	Pohyb v kyberprostoru	Závadové jednání v kyberprostoru
Pomoc	Obecné informace 2	Ochrana digitálních zařízení a malware	Ochrana a zabezpečení dat a informací
Heslo	Veřejný počítač a veřejná Wi-Fi síť	Podvodné praktiky a ochrana	Chování na internetu a komunikace
	Sociálně patologické jevy a rizikové chování	Práce s informacemi	

PROFILY

ABSOLVENT 1. STUPNĚ

ČÁST TECHNICKÁ:

Žák dokáže rozpoznat nestandardní chování digitálních zařízení a oznámit to dospělé osobě.

Žák zná pravidla tvorby bezpečného hesla, jeho ochrany a dokáže je aplikovat.

ČÁST NETECHNICKÁ:

Žák umí vysvětlit a aplikovat pravidla pro bezpečný pohyb v kyberprostoru (například online komunikace, užívání sociálních sítí, tvorba a péče o digitální stopu, online hry)

Žák dokáže rozpoznat a pojmenovat závadové jednání v kyberprostoru (například kyberšikana, sexting, kybergrooming, kyberstalking).

Žák se orientuje v možnostech pomoci v případě nebezpečí na internetu (například zná dostupné (online) linky pomoci, pedagogické pracovníky v místě školy, dospělé osoby ve svém okolí, na které se může obrátit)

ABSOLVENT 2. STUPNĚ

ČÁST TECHNICKÁ:

Žák zná základní pravidla ochrany digitálních zařízení (ochrana při ztrátě/krádeži zařízení, neoprávněný přístup do zařízení, počítačová infiltrace) a dokáže vysvětlit pojem malware.

Při práci s daty, žák aplikuje vhodné metody ochrany a zabezpečení dat (zná a dokáže aplikovat základní prvky obecné počítačové hygieny a zná způsoby zálohování dat).

Žák zná pravidla tvorby bezpečného hesla, jeho ochrany a dokáže je aplikovat.

Žák dokáže rozlišit jednotlivé druhy sítí (soukromou a veřejnou). Zná pravidla pro bezpečný pohyb na veřejných sítích.

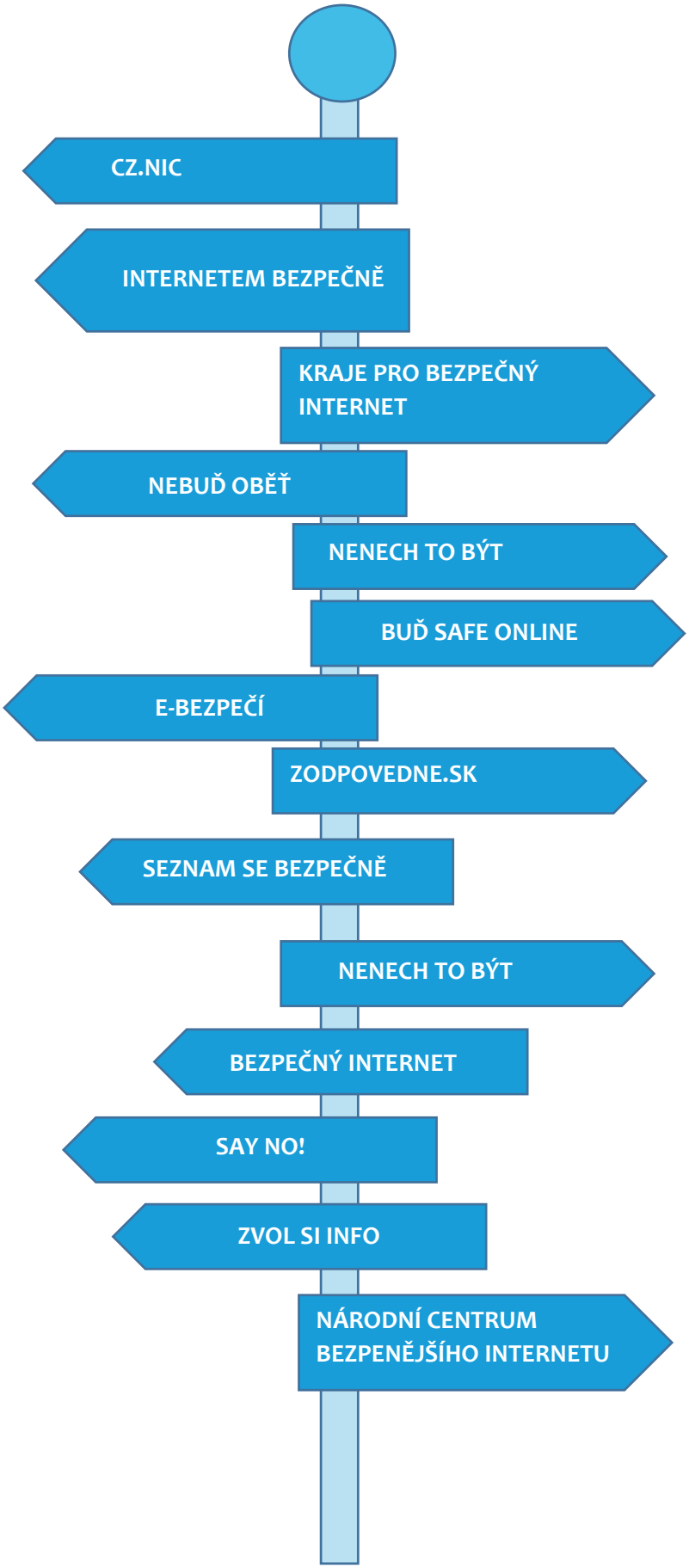
Žák dokáže rozeznat podvodné praktiky v prostředí internetu (například phishing, pharming) a uvést běžné způsoby ochrany (například neotevírat přílohy e-mailů od neznámých odesilatelů).

ČÁST NETECHNICKÁ:

Žák zná vhodné způsoby chování a komunikace v prostředí internetu a ví jak uvědoměle budovat a pečovat, o svoji digitální stopu (zejména ve vztahu k sociálním sítím).

Žák dokáže identifikovat a popsat rizika sociálně patologických jevů na internetu (netholismus, kyberšikana, sexting, nenávistné projevy, kybergrooming a sexting). Dokáže diskutovat jejich znaky, projevy a možné důsledky.

Žák dokáže analyzovat informace, s nimiž pracuje. Umí rozpoznat fake news a hoax.


CZ.NIC
INTERNETEM BEZPEČNĚ
KRAJE PRO BEZPEČNÝ INTERNET
NEBUĎ OBĚŤ
NENECH TO BÝT
BUĎ SAFE ONLINE
E-BEZPEČÍ
ZODPOVEDNE.SK
SEZNAM SE BEZPEČNĚ
NENECH TO BÝT
BEZPEČNÝ INTERNET
SAY NO!
ZVOL SI INFO
NÁRODNÍ CENTRUM BEZPENĚJŠÍHO INTERNETU

ABSOLVENT 1. STUPEŇ

OBECNÉ INFORMACE

Na prvním stupni základní školy se žák začíná více seznamovat s digitálními technologiemi. K prvnímu kontaktu dochází zpravidla již v rodinném prostředí, nicméně s nástupem povinné školní docházky se dítě setkává s digitálními technologiemi nejen ve výuce, ale také prostřednictvím svých spolužáků. Ačkoliv se v kyberprostoru začíná teprve orientovat, nelze vyloučit, že se již v tomto věku setká s nástrahami internetu. Cílem vzdělávání v kyberbezpečnosti na prvním stupni je osvojení základních pravidel pro pohyb v kyberprostoru, seznámení s možnými riziky a vybudování sítě pomoci.

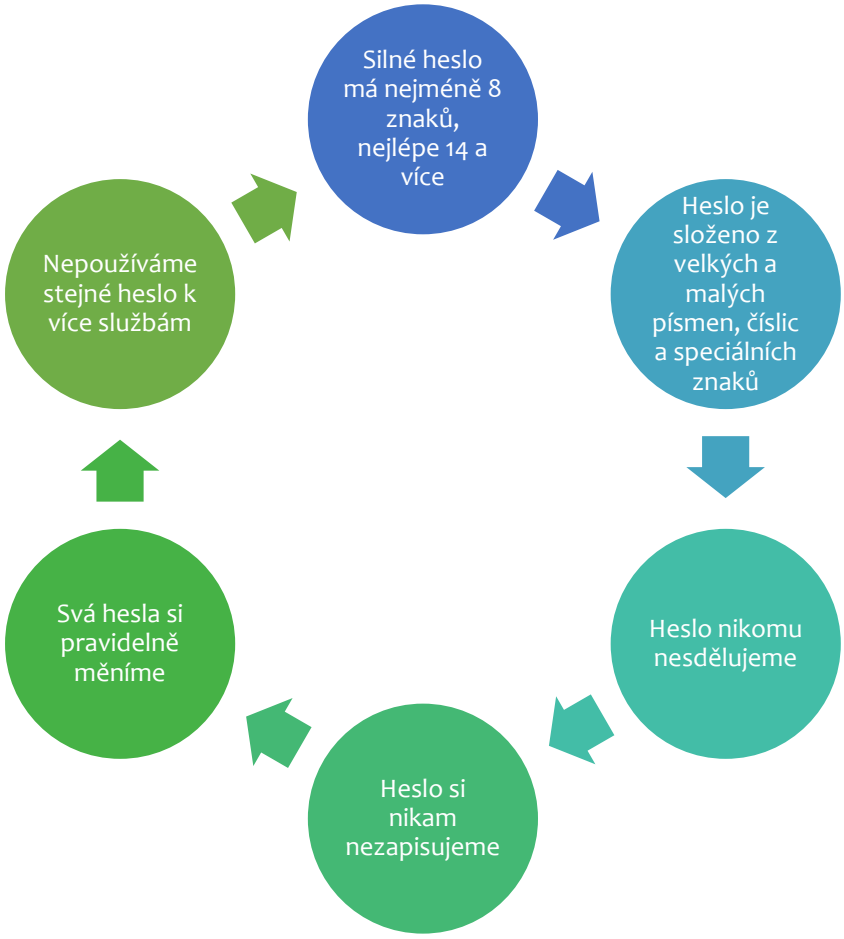
UŽITEČNÉ ZDROJE:

- Předtím než se budete věnovat jednotlivým tématům, prozkoumejte situaci ve třídě. Získáte přehled o tom, na co se ve výuce zaměřit. Mapování může probíhat různými způsoby, například formou diskuze nebo hrou. Jednou z takových her jsou Kyberškatulata.

ABSOLVENT 1. STUPEŇ

HESLO

Základem práce s počítačem a také pohybu na internetu je práce s hesly. Zvykli jsme si, že je po nás vyžadují nejrůznější internetové služby, jako například e-mail, sociální sítě, online hry nebo třeba elektronické bankovnictví. Proto, aby heslo bylo silné a bezpečné je potřeba dodržovat několik jednoduchých pravidel. Naučte žáky zásady tvorby bezpečného hesla a jeho ochrany.



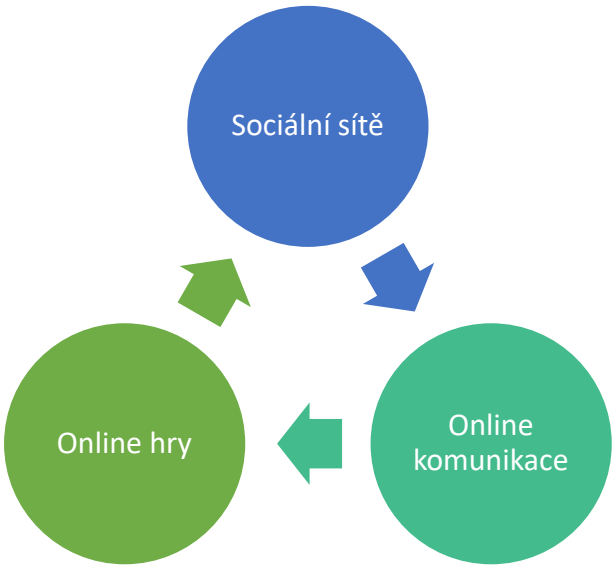
UŽITEČNÉ ZDROJE:

- Více o tom, jak správně nastavit heslo se dozvíte v seriálu CZ.NIC s názvem Nebojte se internetu nebo v seriálu Jak na internet. Pod videem naleznete komiks a výukový materiál ke stažení, případně doplňující informace a inspirativní zdroje.
- Pro výuku bezpečného hesla můžete použít seriál Kraje pro bezpečný internet s názvem Zkroť net. Hned! Pod videospoty naleznete metodiku, která vám poradí, jak s videospoty pracovat a mimo jiné v ní naleznete ukázkové pracovní listy.
- Tvorba hesla je pro menší děti popsána také v příručce s názvem Internetem bezpečně.
- Na stránkách E-bezpečí naleznete plakát s návodem na tvorbu bezpečného hesla.

ABSOLVENT 1. STUPEŇ

POHYB V KYBERPROSTORU

Možností jak trávit čas na internetu je mnoho. Můžeme prostřednictvím něj studovat, pracovat, ale také odpočívat. Co se týče volného času, pohyb v kyberprostoru se u menších dětí zužuje zpravidla na tři oblasti. Jsou jimi sociální sítě, online komunikace a online hry. Samozřejmě, řada dětí na internetu tráví čas například čtením knih nebo vyhledáváním informací do školy. Pozornost by ovšem měla směřovat k činnostem, u nichž je pravděpodobný zvýšený výskyt rizik.



SOCIÁLNÍ SÍTĚ

Sociální síť je služba na internetu. Díky sociálním sítím lidé sdílí informace, fotografie, videa, ale také komunikují s dalšími lidmi prostřednictvím chatu. Existuje celá řada sociálních sítí, jmenujme například Facebook, Twitter, YouTube nebo LinkedIn. V poslední době lze zaznamenat náklonnost k sociálním sítím s převážně obrazovým obsahem. Typickým představitelem takových sítí jsou Snapchat a Instagram, které jsou oblíbené zejména u mladší generace. O čem s žáky v souvislosti se sociálními sítěmi mluvit?

- **Věkové omezení na sociální sítích**

Založení profilu na sociálních sítích je omezen minimální věkovou hranicí. U řady sociálních sítí je věková hranice stanovena na 13 let. Jednotlivé země mohou tuto věkovou hranici zvýšit. Diskutujte s dětmi nastavení věkového omezení a rizika související s porušováním tohoto pravidla, například nebezpečí online komunikace, nevhodný obsah, navazování virtuálních vztahů namísto vztahů reálných

- **Sdílení informací na sociálních sítích**

Na sociálních sítích o sobě lidí prozradí hodně informací. Všechny tyto informace jsou součástí jejich digitální stopy a také jejich identity. Diskutujte s žáky o tom, které informace na internet nepatří. Zdůrazněte jim, že se jedná o veřejné prostředí. Nikdy si nemůžeme být jisti, kdo se k těmto informacím dostane.

- **Zveřejňování fotografií a videí**

Publikování nejrůznějších fotografií a videí na sociálních sítích je trendem dnešní doby. Jak již bylo zmíněno, sociální sítě s převážně obrazovým obsahem zastávají mezi ostatními sítěmi dominantní pozici. Mluvte s žáky o tom, že fotografie a videa jsou osobními údaji stejně jako například naše jméno, bydliště nebo třeba telefonní číslo. Leccos o nás vypovídají, ale hlavně jsme díky nim docela snadno identifikovatelní. Proberte s nimi, jaké fotografie a videa na sociální sítě nepatří.

UŽITEČNÉ ZDROJE:

- O tom, jak fungují sociální sítě se dozvíte například v seriálu CZ.NIC s názvem Nebojte se internetu. Pod videem naleznete další užitečné informace.
- Základní informace o fungování sociálních sítí se dozvíte také v seriálu CZ.NIC s názvem Jak na internet. Pod videem naleznete komiks a výukový materiál ke stažení, případně doplňující informace a inspirativní zdroje.
- Které informace na sociální sítě nepatří, zjistí žáci prostřednictvím e-learningového kurzu Kraje pro bezpečný internet s názvem Surfuj bez nehod.
- Vyzkoušejte s žáky hry, které nabízí Knihovna zdrojů pro digitální gramotnosti od Facebooku. V jednotlivých modulech (Soukromí a dobré jméno, Objevování identity, Pozitivní chování, Zabezpečení, Zapojení v rámci komunity) můžete následně vybírat z několika lekcí, v nichž naleznete ke stažení různé aktivity pro práci se třídou.
- Jedním ze současných trendů je publikování videí na YouTube a TikTok. Bavte se s žáky o tom, zda existují nějaká omezení, jaké video mohou na YouTube nahrát? Stejnými pravidly by se žáci měli řídit také na TikTok. Informace o pravidlech pro zveřejňování videí na YouTube najdete v Pokynech pro komunitu.
- Chcete-li se tématu věnovat hlouběji, vyzkoušejte s žáky hru s názvem „Semafor Bezpečně na YouTube“.

ONLINE KOMUNIKACE

Online komunikace se dnes stává stejně přirozenou jako komunikace osobní. Prostředí pro online komunikaci je celá řada. Mezi dětmi se těší velké oblibě zejména Messenger, Snapchat, Whatsapp nebo chat prostřednictvím hry Minecraft. Ať už tato prostředí znáte či nikoliv – nezoufejte. Přestože se každé z nich trochu liší, slouží ke stejnému účelu. Zpravidla prostřednictvím nich děti komunikují se svými spolužáky, kamarády nebo rodinnými příslušníky. Výjimkou ovšem není komunikace s cizími lidmi. Ne vždy se nutně jedná o internetové lovce. Například ve hře Minecraft, ale i dalších online hrách děti zpravidla komunikují s dalšími hráči. Tak či tak, je nutné s žáky probrat pravidla pro bezpečnou komunikaci.

- **Pravidla bezpečné online komunikace**

Na internetu lze najít řadu návodů, jak bezpečně komunikovat online. Jedním z nich je Desatero bezpečné komunikace, které naleznete v příručce s názvem Internetem bezpečně. Projděte si s žáky společně tato pravidla a diskutujte je. Zaměřte se na to, aby žáci pravidla pochopili a dokázali je uplatnit.

UŽITEČNÉ ZDROJE:

- Informace o online komunikaci získáte prostřednictvím seriálu CZ.NIC s názvem Jak na internet. Pod videem naleznete komiks a výukový materiál ke stažení, případně doplňující informace a inspirativní zdroje.
- Základy online komunikace získáte díky seriálu CZNIC s názvem Nebojte se internetu. Pod videem naleznete další užitečné informace.
- O pravidlech bezpečné komunikace se žáci dozvědí prostřednictvím e-learningového kurzu Kraje pro bezpečný internet s názvem Surfuj bez nehod.
- Osvěžit znalosti žáků, můžete prostřednictvím Pexesa bezpečné komunikace.
- Ověřit si, že žáci umí naučená pravidla aplikovat, můžete jednoduchou hrou s názvem Neználek Maxim.

ONLINE HRY

Oblíbenou zábavou dětí, ale i dospělých, jsou počítačové hry. Lze je rozdělit na online hry a offline hry. Přidanou hodnotou online her, ale zároveň i zvýšeným rizikem, je možnost komunikovat ve hře s dalšími hráči. O tom, že komunikace často připomíná spíše agresi, hovoří výzkumná zpráva Pedagogické fakulty Univerzity Palackého s názvem Fenomén Minecraft v českém prostředí z roku 2017.

UŽITEČNÉ ZDROJE:

- Více o online hrách se dozvíte prostřednictvím seriálu CZ.NIC s názvem Jak na internet. Pod videem naleznete komiks a výukový materiál ke stažení, případně doplňující informace a inspirativní zdroje.
- O možných nebezpečích se dozvíte například na stránkách Buď safe online.

ABSOLVENT 1. STUPEŇ

ZÁVADOVÉ JEDNÁNÍ V KYBERPROSTORU

Kyberprostor je místo, které nám usnadňuje řadu každodenních činností. Naučili jsme se v něm studovat, pracovat nebo trávit svůj volný čas. Některým lidem ale virtuální svět slouží k závadovému, tedy škodlivému jednání nebo dokonce k páchání trestné činnosti. Řada z nás o těchto rizicích ví, ale nepřipouštíme si, že by se mohly týkat naší osoby. Naučte žáky rozpoznat jednotlivé druhy závadového jednání pro případ, že by se stali jeho obětí nebo svědky. Pokud žák dokáže rozlišit, co je závadové jednání, zvyšuje se tím také pravděpodobnost, že se tomuto jednání bude vyvarovat. Typickým příkladem může být kyberšikana, která bývá mnohými žáky považována pouze za legraci.

- **Vysvětlení jednotlivých pojmů**

Informace o tom, co je to kyberšikana, sexting, kyberstalking a kybergrooming získáte prostřednictvím stránek Internetem bezpečně nebo stránek Nebuď oběť.

- **Možnosti ochrany/obrany**

Nezapomeňte se s dětmi pobavit o možnostech, jak se proti jednotlivým druhům závadového jednání chránit. Ale také, co dělat v případě, že se stanu obětí.

UŽITEČNÉ ZDROJE:

- K seznámení menších žáků s danou problematikou jsou určena videa formou pohádkových příběhů s názvem Ovce.sk. Na stránkách Zodpovedne.sk k nim naleznete Príručku pre učitel´ov, která vám poradí, jak s příběhy ve výuce pracovat.
- Pro starší žáky jsou určena videa Sezam se bezpečně s názvem Křečci v síti nebo seriál Kraje pro bezpečný internet s názvem Zkroť net. Hned! a jeho videospoty s názvem Kyberšikana a Kybergroming. Pod videospoty naleznete metodiku, která vám poradí, jak s videospoty pracovat a mimo jiné v ní naleznete ukázkové pracovní listy.
- K představení tohoto tématu může sloužit také příručka s názvem Internetem bezpečně.
- Na stránkách Internetem bezpečně rozhodně nepřehlédněte video zaměřené na kybergrooming.

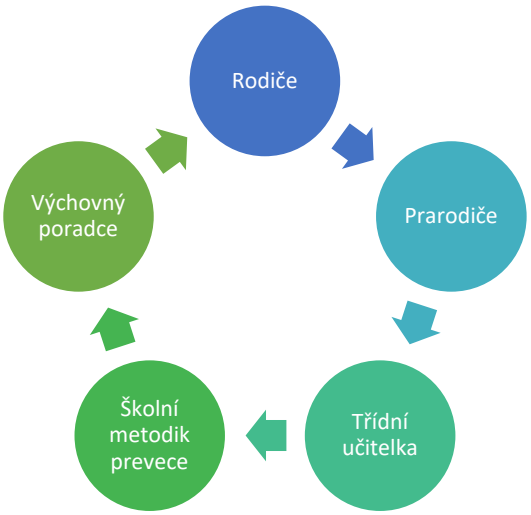
ABSOLVENT 1. STUPEŇ

POMOC

Základní znalost, kterou by měl žák při výuce kyberbezpečnosti získat, je vytvořit si síť osob, organizací,… na kterou se může obrátit v případě, že se dostane do nebezpečí na internetu. Síť žáka by měla mít dvě složky – osobní a profesionální.

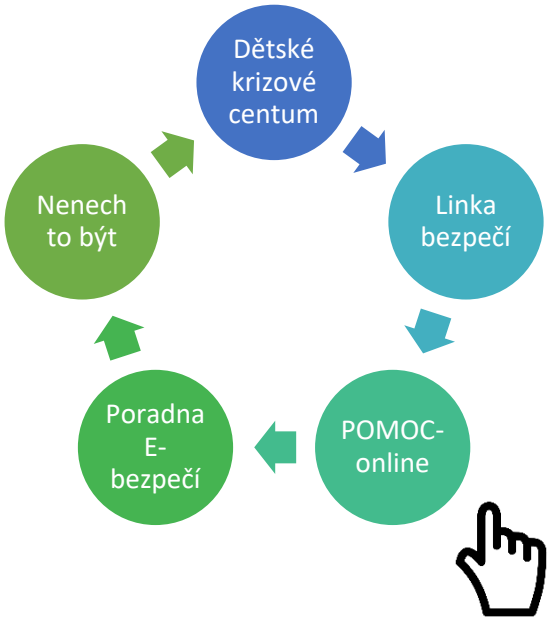
- **Osobní síť**

Diskutujte s žáky, které důležité osoby mohou patřit do jejich osobní sítě. Měly by v ní být dospělé osoby, se kterými jsou žáci v každodenním kontaktu a kteří jsou schopni jim v rizikové situaci podat pomocnou ruku. Aktivitu opět můžete pojmout pomocí hry. Dítě si například může obkreslit vlastní ruku a do každého prstu zaznačit stěžejní osoby ze svého okolí. Nabádejte žáky, aby přemýšleli také o osobách, na které se mohou obrátit ve škole.



- **Profesionální síť**

Je tvořena organizacemi, které umožňují poskytnutí odborného poradenství. Existuje jich celá řada, pomozte žákům poznat, alespoň některé z nich.



NAVIGACE

ABSOLVENT 2. STUPEŇ

OBECNÉ INFORMACE

Na druhém stupni již většina žáků plně využívá digitální technologie. V rámci výuky informatiky se žáci učí pracovat s různými programy a také na internetu. Internet využívají také ve svém osobním životě. Ačkoliv se rozšiřuje pole činností, ke kterým internet využívají, sociální sítě, online komunikace a online hry mají v životě dospívajících stále dominantní pozici. Žáci druhého stupně jsou již také zpravidla vlastníky jednoho či více digitálních zařízení.

Cílem vzdělávání v kyberbezpečnosti na druhém stupni je prohlubování znalostí pro bezpečný pohyb v kyberprostoru, ale také ochrana digitálních zařízení, ochrana a zabezpečení dat a informací a v neposlední řadě práce s informacemi.

Přestože dnes většina žáků pokračuje ve studiu na střední škole a vysoké škole, nelze opomenout skupinu žáků, pro níž ukončení povinné školní docházky znamená také konec vzdělávání v rámci vzdělávacího systému České republiky. Právě s ohledem na to je nutné, aby žák v průběhu základního vzdělání získal všechny potřebné znalosti a dovednosti, které mu v životě umožní používat digitální technologie bezpečným způsobem.

ABSOLVENT 2. STUPEŇ

OCHRANA DIGITÁLNÍCH ZAŘÍZENÍ A MALWARE

Dříve než se s žáky začnete věnovat práci na digitálních zařízeních, promluvte si s nimi o možnostech jejich ochrany. Nejde o žádné složité technické úkony, ale pouze ty, které by měl zvládnout běžný uživatel. Díky nim zůstanou chráněna nejen zařízení samotná, ale především data, která v těchto zařízeních máme. Ochranu digitálních zařízení lze rozdělit na tři úrovně:

- **Ochrana při ztrátě/krádeži zařízení.**

Ne vždy se nám daří ochránit naše zařízení fyzicky. Je tedy nutné je zabezpečit proti případnému odcizení dat. Například tím, že pro vstup do zařízení je nutná autentizace. Autentizace slouží k jednoznačnému určení uživatele, který přistupuje do informačního systému. Nejčastěji je uživatel autentizován na základě uživatelského jména a hesla, například k přístupu do počítače. Případně pomocí číselného kódu, znaku nebo třeba otisku prstu, například u mobilního telefonu. Pokud je přístupové heslo dostatečně silné, zvyšuje se tím pravděpodobnost, že naše data zůstanou v bezpečí.

- **Neoprávněný přístup do zařízení.**

Nezvaný návštěvník může v našem zařízení udělat pěkný nepořádek. Nejenže může manipulovat s našimi daty, ale také může získat přístup do služeb a aplikací do nichž jsme na našich zařízeních trvale přihlášeni. Rizikem je také to, že nám upraví nastavení našeho zařízení, případně do něj zablokuje přístup kupříkladu změnou přihlašovacích údajů. Jedinou zaručenou ochranou je mít zařízení v případě, že jej nepoužíváme uzamknuta. Měli bychom také zvážit, zda je moudré zůstávat na svých zařízeních trvale přihlášen – například pro vstup na Facebook.

- **Ochrana před počítačovou infiltrací.**

Dalším z rizik toho, že se někdo neoprávněně dostane do našeho zařízení, je instalace škodlivého programu. Tomu se říká malware. Základní ochranu proti malware tvoří několik jednoduchých rad, řada z nich o nich ví, ale přesto se neustále porušují. Zopakujte je svým žákům.

UŽITEČNÉ ZDROJE:

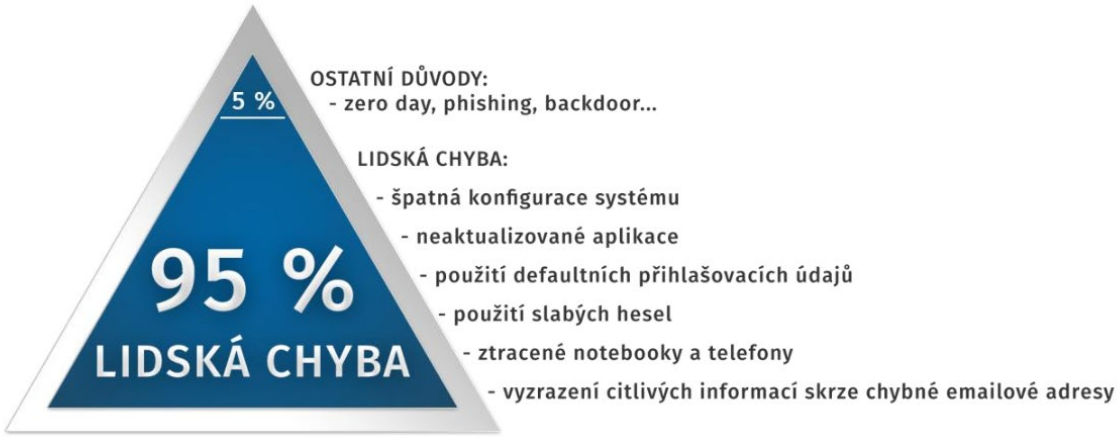
- Základní rady týkající se ochrany zařízení před malware se dozvíte na stránkách Internetem bezpečně.
- O tom, co je to malware a jaké druhy malware známe, se dozvíte z příručky Internetem bezpečně s názvem Bezpečnost v online prostředí.
- Informace o malware můžete získat také na stránkách Avast.

ABSOLVENT 2. STUPEŇ

OCHRANA A ZABEZPEČENÍ DAT A INFORMACÍ

Většinu dat a informací s nimiž pracujeme, máme uloženy na našich digitálních zařízeních, případně je máme zálohovány s využitím cloudové služby nebo na online uložištích. Je tedy namístě si připomenout pravidla jejich ochrany. Mluvte o zásadách ochrany dat a informací také s žáky. Jen díky včasnému osvojení těchto návyků lze do budoucna předejít situacím, kdy vysoce postavený odborník má přístupová hesla ke svému počítači na nástěncev kanceláři.

Zkuste se s žáky zamyslet nad následujícím obrázkem, který se zaměřuje na příčiny ohrožení našich dat a informací.



ZPŮSOBY OCHRANY DAT A INFORMACÍ

- **Bezpečné a silné heslo pro přístup do zařízení, ale také k jednotlivým účtům.**

Základem ochrany dat a informací je zabezpečení zařízení, ale také jednotlivých účtů silným a bezpečným heslem. Jak na to se dozvíte v části Heslo. Hesla nikdy nikomu nesdělujeme a zároveň je nikdy, opravdu nikdy, nezapisujeme nikam na papír nebo dokonce na nástěnku.

- **Přihlašovací údaje se nikomu nesdělují.**

Přihlašovací údaje nesdělujeme ani kamarádům, ani jiným lidem. Přihlašovací údaje nikdy nesdělujeme nikomu telefonicky ani e-mailem – a to ani v případě, že se člověk na druhé straně představí jako zástupce nějaké banky nebo třeba online hry. Tyto údaje po vás nikdo nemůže žádat.

- **Nenechávejte své dokumenty volně přístupné – ani tištěné, ani v grafické podobě.**

Dávejte si pozor na to, abyste za sebou nenechali volně přístupné dokumenty. Pokud na něčem pracujete například ve škole a potřebujete si nutně odskočit, dokument uložte, zavřete a před ochodem z počítače se odhlaste. Vytvoření takového dokumentu vás jistě stálo mnoho a práce a přijít o něj by bylo nemilé.

- **Omezte přístup dalších osob k vašim soukromým zařízením.**

Vaše zařízení do rukou druhých lidí nepatří. Například v mobilu máme řadu věcí, o nichž nechceme, aby druzí věděli (třeba fotografie nebo videa).

- **Při odchodu od zařízení zamkněte obrazovku vašeho zařízení**.

Budete tak mít jistotu, že se k vašim datům a informacím nikdo nedostane. Důležité je to hlavně na zařízeních s veřejným přístupem. Tím je například počítač v knihovně nebo třeba v počítačové učebně. Na počítači lze uzamknutí provést například klávesovou

zkratkou  +

- **Přenosná paměťová média a jak s nimi nakládat.**

Pokud máte data a informace uloženy na přenosných paměťových médiích, jakým je například USB flash disk, nezanecháváme jej volně ležet bez dozoru. Zároveň pokud najdete takový USB flash disk, nepřipojujte jej do zařízení. Ať už jste jakkoliv zvědaví, nikdy nevíte, co se na něm skrývá a zda tím nemůžete ohrozit data a informace na svých zařízeních.

- **Pozor na stahování aplikací**

Aplikace, které stahujeme do svých zařízení, vyžadují přístup k některým našim datům. Vždy je nutné zhodnotit, zda okruh dat, ke kterým aplikace vyžaduje přístup, odpovídá jejímu účelu. Pokud aplikace, která primárně slouží k předpovědi počasí, žádá přístup k vašim fotografiím, je to podezřelé.

ZÁLOHOVÁNÍ DAT

Zálohování dat je nutné proto, abychom o ně nepřišli, v případě, kdy si je vymažeme my sami nebo někdo jiný, ať už omylem nebo záměrně. Zálohování naše data ochrání také v případě, že dojde k selhání, ztrátě nebo zničení našeho zařízení. Promluvte si s žáky o možnostech zálohování.

- **Záloha na fyzické zařízení**

Fyzickým zařízením se rozumí pevný disk, velkokapacitní USB flash paměť nebo třeba DVD. Výhodou je, že toto zařízení máme stále pod kontrolou. Je nutné toto zařízení skladovat bezpečně a odděleně od počítače. Toto zařízení by mělo být připojeno pouze po dobu zálohování.

- **Využití cloudové služby**

Jedná se o službu poskytovanou přes internet. Je charakteristická samoobsluhou podle potřeby; širokou dostupností přes internet – k datům tak můžeme přistupovat z různých míst a zařízení; sdílením prostředků cloudu prostřednictvím více uživatelů zároveň; Výhodou je, že data se u nás fyzicky nenachází a také to, že mnoho služeb je bezplatných. Příkladem takových cloudových služeb je Google Drive.

- **Online zálohování**

Tento princip se podobá cloudovým službám. Podstatným rozdílem je nemožnost tato data upravovat a sdílet s dalšími uživateli. Jde pouze o uložiště dat, ke kterému přistupujeme prostřednictvím internetu.

ABSOLVENT 2. STUPEŇ

HESLO

Jak pracovat s heslem by se měl žák dozvědět již na prvním stupni základní školy. Opakování je ovšem matka moudrosti a vytvoření bezpečného hesla, stejně jako jeho ochrany je naprostým základem.

- Silné heslo má minimálně 8 znaků (lépe 14) a je složeno z velkých a malých písmen, číslic a speciálního znaku – například *!
- Hesla si nikam nezapisujeme.
- Hesla nikomu nesdělujeme. Ani své nejlepší kamarádce nebo kamarádovi – co kdyby došlo na hádku a heslo se stalo nástrojem pomsty. Výjimku mohou tvořit rodiče, kteří mají právo na to vědět, s kým jejich dítě tráví čas na internetu. Dítě se ovšem může s rodičem domluvit, že si heslo ponechá pro sebe a rodiči pouze zpřístupní profil po přihlášení do sociální sítě nebo třeba počítačové hry.
- Nepoužíváme stejné heslo k více službám.
- Svá hesla si pravidelně měníme.

UŽITEČNÉ ZDROJE:

- Více o tom, jak si správně nastavit heslo se dozvíte například v seriálu CZ.NIC s názvem Nebojte se internetu. Pod videem naleznete další užitečné informace.
- Základní informace získáte také prostřednictvím seriálu CZ.NIC s názvem Jak na internet. Pod videem naleznete komiks a výukový materiál ke stažení, případně doplňující informace a inspirativní zdroje.
- Pro výuku bezpečného hesla můžete využít také seriál Kraje pro bezpečný internet s názvem Zkroť net. Hned! a jeho videospot Bezpečná hesla. Pod videospoty naleznete metodiku, která vám poradí, jak s videospoty pracovat a mimo jiné v ní naleznete ukázkové pracovní listy.
- Tvorba hesla je pro starší žáky a dospělé popsána také v příručce Internetem bezpečně s názvem Bezpečnost v online prostředí. Zde se mimo jiné dozvíte, co je to správce hesel a jak se používá.
- Na stránkách E-bezpečí naleznete plakát s návodem na tvorbu bezpečného hesla.

ABSOLVENT 2. STUPEŇ

VEŘEJNÝ POČÍTAČ A VEŘEJNÁ WI-FI SÍŤ

VEŘEJNÝ POČÍTAČ

Pro práci a přístup na internet nemusí vždy využívat pouze vlastní zařízení. Jsou to zařízení, která my sami nemáme pod kontrolou a má k nim přístup velké množství lidí. Jedná se například o zařízení v knihovnách nebo internetových kavárnách. Používání takových zařízení se řídí zvláštními bezpečnostními pravidly. Diskutujte tato pravidla s žáky.

UŽITEČNÉ ZDROJE:

- O tom, co je to veřejný počítač a jaká bezpečnostní pravidla při práci s ním platí zjistíte v seriálu CZ.NIC s názvem Jak na internet. Pod videem naleznete komiks a výukový materiál ke stažení, případně doplňující informace a inspirativní zdroje.
- O tom, jak bezpečně surfovat na veřejných počítačích se dozvíte na stránkách Bezpečný internet.

VEŘEJNÁ WI-FI SÍŤ

S veřejnými WiFi sítěmi se dnes běžně můžeme setkat například v dálkových dopravních prostředcích nebo obchodních domech. Naše chytrá zařízení je navíc umí samy vyhledávat. Pohyb na veřejných sítích má pravidla, díky kterým se surfování může stát bezpečnější. Využívání veřejných Wi-Fi sítí je mezi dospívajícími oblíbené. Proberte s nimi možnosti, jak se na veřejné Wi-Fi síti chránit.

UŽITEČNÉ ZDROJE:

- Jak funguje veřejná Wi-Fi síť a jak se na ni bezpečně pohybovat zjistíte v seriálu CZ.NIC s názvem Jak na internet.
- Tyto informace získáte také prostřednictvím stránek Bezpečný internet.

ABSOLVENT 2. STUPEŇ

PODVODNÉ PRAKTIKY V PROSTŘEDÍ INTERNETU A OCHRANA

Stejně jako v reálném světě, se také v online světě vyskytují podvodníci. Lidé, kteří se snaží dostat do našich zařízení a získat tak přístup k našim datům nebo třeba přihlašovací údaje k elektronickému bankovnictví. Mezi nejčastější podvodné praktiky patří spam, phishing a pharming. Právě poslední dvě zmíněné lze označit za techniky sociálního inženýrství. Ovšem není inženýr jako inženýr. Sociální inženýrství, o němž je řeč, je manipulativní technika, která k ovlivňování uživatelů využívá specifické psychologické metody. Metody sociálního inženýrství se zaměřují na nejslabší místo zabezpečení celého systému – člověka.

UŽITEČNÉ ZDROJE:

- O podvodných praktikách v prostředí internetu se dozvíte například prostřednictvím seriálu společnosti CZ.NIC s názvem Jak na internet. Pod videem naleznete komiks a výukový materiál ke stažení, případně doplňující informace a inspirativní zdroje.
- Pro výuku můžete využít seriál Kraje pro bezpečný internet s názvem Zkroť net. Hned! a jeho videospot Bezpečné chování online. Pod videospoty naleznete metodiku, která vám poradí, jak s videospoty pracovat a mimo jiné v ní naleznete ukázkové pracovní listy.
- Informace o podvodných praktikách a možnostech jak se před nimi chránit získáte také na stránkách Internetem bezpečně. Případně v jeho příručce Bezpečně v online prostředí.
- O internetových podvodech se dozvíte také ze stránek Hoax.
- Další zajímavé články na téma podvodných praktik naleznete na stránkách E-bezpečí.
- Jak rozpoznat phishing vám poradí stránky CSIRT.

ABSOLVENT 2. STUPEŇ

CHOVÁNÍ NA INTERNETU A KOMUNIKACE, PÉČE O DIGITÁLNÍ STOPU

CHOVÁNÍ NA INTERNETU A NETIKETA

Od dětství se učíme pravidlům chování. Zejména starší generace stále dbají na dodržování etikety, kterou lze zjednodušeně popsat jako pravidla slušného chování. Neexistují žádná pevně daná pravidla, jak se má člověk chovat online, jen nesmí porušovat zákon. Anonymita online prostředí často nahrává větší kurážnosti. Pokud se o tom chcete přesvědčit na vlastní oči, věnujte chvilku přečtení některé z internetových diskuzí. Myslíte, že by většina diskutujících dokázala být natolik otevřená a říct své názory ostatním tváří v tvář? Protože existují lidé, kterým takové chování vadí, vznikly nejrůznější seznamy pravidel slušného chování v kyberprostoru. Obecně se jim říká netiketa. Diskutujte s žáky o těchto pravidlech a pokuste se vymyslet další.

UŽITEČNÉ ZDROJE:

- Co je to netiketa a jaká pravidla obsahuje, se dozvíte například na stránkách Nebuď oběť.
- Informace o netiketě získáte také na stránkách Bezpečně online.

ONLINE KOMUNIKACE

Online komunikace se dnes stává stejně přirozenou jako komunikace osobní. Prostředí pro online komunikaci je celá řada. Mezi dětmi a dospívajícími se těší velké oblibě zejména Messenger, Snapchat, Whatsapp nebo chat prostřednictvím hry Minecraft. Ať už tato prostředí znáte či nikoliv – nezoufejte. Přestože se každé z nich trochu liší, slouží ke stejnému účelu. Zpravidla prostřednictvím nich děti komunikují se svými spolužáky, kamarády nebo rodinnými příslušníky. Výjimkou ovšem není komunikace s cizími lidmi. Ne vždy se nutně jedná o internetové lovce. Zejména dospívajícím slouží chatovací prostředí také k navazování partnerských vztahů. Kromě chatování využívají hlavně starší žáci také videohovory.

- **Pravidla bezpečné online komunikace**

Na internetu lze najít řadu návodů, jak bezpečně komunikovat online. Jedním z nich je Desatero bezpečné komunikace, které naleznete v příručce s názvem Internetem bezpečně. Projděte si s žáky společně tato pravidla a diskutujte je. Zaměřte se na to, aby žáci pravidla pochopili a dokázali je uplatnit.

UŽITEČNÉ ZDROJE:

- Informace o online komunikaci získáte prostřednictvím seriálu CZ.NIC s názvem Jak na internet. Pod videem naleznete komiks a výukový materiál ke stažení, případně doplňující informace a inspirativní zdroje.

- Základy online komunikace získáte díky seriálu CZNIC s názvem Nebojte se internetu. Pod videem naleznete další užitečné informace.

- Upozorněte žáky na riziko webcam trollingu. Vše potřebné o něm zjistíte na stránkách E-bezpečí. Na těchto stránkách naleznete ke stažení také plakát.

- O pravidlech bezpečné komunikace se dozvíte také na stránkách Bezpečný internet.

- S pravidly bezpečného pohybu a komunikace na sociálních vás seznámí seriál od Kraje pro bezpečný internet s názvem Zkroť net. Hned! a jeho videospot Sociální sítě 2. Pod videospoty naleznete metodiku, která vám poradí, jak s videospoty pracovat a mimo jiné v ní naleznete ukázkové pracovní listy.

SOCIÁLNÍ SÍTĚ

Sociální síť je služba na internetu. Díky sociálním sítím lidé sdílí informace, fotografie, videa, ale také komunikují s dalšími lidmi prostřednictvím chatu. Existuje celá řada sociálních sítí, jmenujme například Facebook, Twitter, YouTube nebo LinkedIn. V poslední době lze zaznamenat náklonnost k sociálním sítím s převážně obrazovým obsahem. Typickým představitelem takových sítí jsou Snapchat a Instagram, které jsou oblíbené zejména u mladší generace. O čem s žáky v souvislosti se sociálními sítěmi mluvit?

- **Sdílení informací na sociálních sítích**

Při používání sociálních sítí o sobě lidé sdílí řadu informací. Všechny tyto informace jsou součástí jejich digitální stopy a také jejich identity. Diskutujte s žáky o tom, které informace na internet nepatří. Zdůrazněte jim, že se jedná o veřejné prostředí. Nikdy si nemůžeme být jisti, kdo se k těmto informacím dostane.

- **Zabezpečení účtů a soukromí na sociálních sítích**

Informace na sociálních sítích je možné chránit více než pouze heslem. Jednou z možností je dvoufázové ověření, tedy dva nezávislé způsoby jak ověřit totožnost uživatele. Uživatel je chráněn v případě úniku nebo prolomení hesla. Věnujte se s žáky také možnostem nastavení profilu na sociálních sítích. Díky správnému nastavení omezíte přístup lidí k vašim informacím.

UŽITEČNÉ ZDROJE:

- O tom, jak fungují sociální sítě se dozvíte například v seriálu CZ.NIC s názvem Nebojte se internetu. Pod videem naleznete další užitečné informace.

- Základní informace o fungování sociálních sítí se dozvíte také v seriálu CZ.NIC s názvem Jak na internet. Pod videem naleznete komiks a výukový materiál ke stažení, případně doplňující informace a inspirativní zdroje.

- Informace o sociálních sítích, jejich rizicích, ale také rady pro bezpečné používání sociálních sítí získáte na stránkách Bezpečného internetu.

- O tom, které informace na sociální sítě nepatří, se žáci dozvědí například prostřednictvím e-learningového kurzu Kraje pro bezpečný internet s názvem Surfuj bez nehod.
- Vyzkoušejte s žáky hry, které nabízí Knihovna zdrojů pro digitální gramotnosti od Facebooku. V jednotlivých modulech (Soukromí a dobré jméno, Objevování identity, Pozitivní chování, Zabezpečení, Zapojení v rámci komunity) můžete následně vybírat z několika lekcí, v nichž naleznete ke stažení různé aktivity pro práci se třídou.
- Věnujte se s žáky možnostem nastavení profilu na sociálních sítích. Díky správnému nastavení lze omezit přístup některých lidí k informacím, které jsou zveřejňovány na profilu. Jak na to, se dozvíte na stránkách Sdílej bezpečně.
- Jak zvýšit bezpečnost sdílení na sociálních sítích zjistíte také prostřednictvím seriálu Kraje pro bezpečný internet s názvem Zkroť net. Hned! a jeho videospot Sociální sítě. Pod videospoty naleznete metodiku, která vám poradí, jak s videospoty pracovat a mimo jiné v ní naleznete ukázkové pracovní listy.

ABSOLVENT 2. STUPEŇ

SOCIÁLNĚ PATOLOGICKÉ JEVY A RIZIKOVÉ CHOVÁNÍ NA INTERNETU

Kyberprostor je místo, které nám usnadňuje řadu každodenních činností. Naučili jsme se v něm studovat, pracovat nebo trávit svůj volný čas. Každá mince má dvě strany, a tak jindy účinný nástroj, je současně zdrojem rizik. Internet sám o sobě rizikovým není, rizikovým ho činí chování lidí. Již na prvním stupni by měl žák získat základní povědomí o tom, co je to kyberšikana, kybergrooming, kyberstalking a sexting. Na druhém stupni by se těmto pojmům měl žák věnovat hlouběji a umět diskutovat jejich znaky, projevy a důsledky. Žák by se měl také dozvědět, co je to netholismus.

KYBERŠIKANA, KYBERGROOMING, KYBERSTALKING, SEXTING

O jednotlivých pojmech se dozvíte například prostřednictvím stránek Internetem bezpečně: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/ nebo stránek Nebuď oběť: http://nebudobet.cz/

UŽITEČNÉ ZDROJE:

- Zajímavé a inspirativní články k jednotlivým druhům závadového jednání naleznete na stránkách E-bezpečí pod záložkou Rizikové jevy.
- Na stránkách E-bezpečí také naleznete záložku Materiály pro učitele, rodiče a žáky. Jsou zde nejrůznější skládačky, přehledové listy, ale především příručka pro rodiče a pedagogy v níž se taktéž můžete dočíst potřebné informace k jednotlivým druhům závadového jednání.
- Pro starší žáky jsou určena videa Sezam se bezpečně.
- S problematikou seznamuje žáky také seriál Kraje pro bezpečný internet s názvem Zkroť net. Hned! a jeho videospot s názvem Kyberšikana a Kybergroming. Pod videospoty naleznete metodiku, která vám poradí, jak s videospoty pracovat a mimo jiné v ní naleznete ukázkové pracovní listy.
- K představení této tematiky může sloužit také Příručka Internetem bezpečně s názvem Bezpečnost v online prostředí.
- Diskuzi na téma závadové jednání v kyberprostoru lze podnítit také videem, které je součástí kampaně #Say no! O té si můžete přečíst na stránkách Policie ČR. Na těchto stránkách také naleznete zmíněné video.

NETHOLISMUS

Již samotný název napovídá, že se tento pojem týká závislosti. V tomto případě závislosti na virtuálních drogách. Někdy také označované jako online závislosti. Více o netholismus se dozvíte na stránkách Internetem bezpečně nebo stránkách Nebuď oběť.

UŽITEČNÉ ZDROJE:

- Zajímavé a inspirativní články k online závislosti naleznete také na stránkách E-bezpečí.
- Vyzkoušejte si Kurz pro pedagogy od Kraje pro bezpečný internet. Jednou z výukových lekcí je také Netholismus a online gambling
- K představení netholismus může sloužit také příručka Internetem bezpečně s názvem Bezpečnost v online prostředí.
- Podnětným může být také seriál CZ.NIC s názvem Jak na internet. Pod videem naleznete komiks a výukový materiál ke stažení, případně doplňující informace a inspirativní zdroje.
- Vyzkoušejte si s žáky Kurz pro děti a studenty od Kraje pro bezpečný internet. Jednou z lekcí je také Internet jako droga.

ABSOLVENT 2. STUPEŇ

PRÁCE S INFORMACEMI

Každý den jsme doslova zavaleni množstvím informací. Jsou to informace z médií a ze sociálních sítí. Všechny tyto informace musíme nějakým způsobem zpracovávat. Dospělí lidé už si osvojili určité dovednosti třídění informací, děti a dospívající v této oblasti potřebují pomocnou ruku. Ne vždy mají děti a dospívající možnost naučit se pracovat s informacemi v rodinném prostředí. Škola je místem, kde by si dítě mělo osvojit základy kritického myšlení. O práci s informacemi se často mluví ve spojitosti s mediální výchovou. Zdaleka ne na všech školách je jí věnovaný dostatečný prostor. Přesto práce s informacemi a osvojení kritického myšlení je základní kompetencí přežití v současné společnosti, která bývá také označována jako společnost „informační".

UŽITEČNÉ ZDROJE:

- Dítě a dospívající mnoha informacím nerozumí a nedokáže je zasadit do širšího kontextu. Velmi často tak přijímá názory na základě zprávy z jednoho zdroje. Pomozte žákům zorientovat se ve světě informací. Inspirací a pomocníkem vám mohou být stránky Zvol si info a jejich Surfařův průvodce po internetu.
- O tom jak pracovat s informacemi se dozvíte prostřednictvím plakátů E-bezpečí s názvem Jak ověřit informace na internetu nebo s názvem Fake news.
- Cenným zdrojem informací může být také Jeden svět na školách a jeho sekce Mediální vzdělávání.
- Máte rádi hry? Vyzkoušejte si se svými žáky hru na vytváření dezinformací na internetu. Naleznete ji na iRozhlas.