

METODICKÉ MATERIÁLY DO VÝUKY NOVÉ INFORMATIKY ZAMĚŘENÉ NA BEZPEČNÉ POUŽÍVÁNÍ CHYTRÝCH MOBILNÍCH TELEFONŮ ŽÁKY ZŠ

SEDLÁČEK Michal, ŠEBÁKOVÁ Ivana, CZ

Resumé

Příspěvek se zabývá problematikou bezpečného používání chytrých mobilních telefonů žáky základních škol. V rámci příspěvku jsou prezentovány vytvořené konkrétní metodické materiály do výuky informatiky na základní škole navržené za účelem zvýšit u žáků povědomí o nutnosti bezpečného chování na internetu a zabezpečení mobilního telefonu, který k přístupu k internetovým zdrojům žáci používají. Součástí metodických materiálů jsou pracovní listy a doporučení pro učitele.

Klíčová slova: bezpečné chování na internetu, chytrý mobilní telefon, metodické materiály do výuky informatiky, žák základní školy.

METHODOLOGICAL MATERIALS FOR INFORMATICS TEACHING FOCUSED ON THE SAFE USE OF SMART MOBILE PHONES BY SCHOOL STUDENTS

Abstract

The paper deals with the issue of safe use of smartphones by primary school students. The paper presents concrete methodological materials for the teaching of computer science at primary school, designed to raise pupils' awareness of the need for safe behavior on the Internet and the security of the mobile phone that pupils use to access Internet resources. Methodical materials include worksheets and recommendations for teachers.

Keywords: safe behavior of students on the Internet, smart mobile phone, methodological materials for teaching computer science, elementary school student.

Úvod

Žáci v nové informatice získávají kompetence v porozumění základním principům digitálních technologií a rozvíjí si nenásilnými formami a metodami výuky informatické myšlení. Učí se, jak porozumět digitálnímu světu a jak si v něm chránit své soukromí. Získávají informace, učí se je správně diagnostikovat a aktivně hledají řešení a tím rozvíjí své znalosti, dovednosti a návyky. V rámcových vzdělávacích programech jsou uvedeny očekávané výstupy, které by měly základní školy naplňovat a na jejich základě tvoří vlastní školní vzdělávací program. Rámcový vzdělávací program je svými výstupy zaměřen na výuku Informačních technologií s obsahem, který se věnuje především práci s digitálními technologiemi, informačním systémům, algoritmizaci, programování a práce s daty. Co se týče konkrétně výuky bezpečnosti na sociálních sítích, zabezpečení chytrých dotykových a jiných osobních digitálních zařízení je v RVP věnovaná pozornost ochraně dat v posledním pilíři se zaměřením na digitální technologie. Studenti učitelství informatiky si negativní vlivy působení mobilních telefonů na současnou mladou generaci jasně uvědomují stejně, jako potřebu zařadit téma bezpečnosti do výuky informatiky na základních školách (Sedláček, 2022).

Nové technologie mohou usnadnit každodenní práci. Mezi technologické vynálezy, které náš život i život dětí ovlivňují, patří především chytré dotykové mobilní telefony. Chytrá zařízení

se mohou přizpůsobit našim zájmům a potřebám. Získávají ale od nás informace, které dále využívají pro marketingové účely firem a sledují naši činnost a zájmy na internetu. Nutnost bezpečného používání mobilních telefonů je aktuální a současně s tím potřeba vzdělávat nejen dospělé, ale především děti v této oblasti. Koncepce nové informatiky, která je aktuálně zaváděná na českých základních školách, je zaměřena na oblasti, jako jsou data, informace, modelování, algoritmizace a programování, informační systémy a digitální technologie. Simulačním modelům a možnostem jejich využití v nové informatice se věnujeme v dalších příspěvcích (Sedláček 2021). Simulačních modelů jako názorného demonstračního prostředku lze využít i ve výuce technicky orientovaných předmětů (Sedláček, 2019, Sedláček 2020). V rámci výuky nové informatiky by měla být věnovaná zvýšená pozornost právě bezpečnému používání chytrých zařízení, jako jsou již zmíněné chytré telefony či tablety, neboť aktuálně má přístup k chytrým zařízením většina dětí, které navštěvují základní školu. Děti používají mobilní telefony připojené k internetu především k zábavě, v hojné míře používají sociální sítě a komunikují mezi sebou a jsou stále online (Petrowski, 2014). Sledují videostreamy na YouTube a TikToku, používají cloud a další online služby. Obsah médií, který je dětem na internetu dostupný je silně ovlivňuje pozitivně, tak i negativně v chování a jednání. (Hauptová, 2019). Mezi pozitivní vlivy může patřit schopnost ovládat mobilní telefon a jiná digitální zařízení a také schopnost orientovat se v internetovém prostředí. Negativním vlivem pak je již zmíněné omezení verbálních komunikačních schopností a závislost na virtuálním komunikačním prostoru, který u dítěte nerozvíjí, a pokud tak jen velmi omezeně, verbální komunikační schopnosti.

Metodické materiály

Navržená výuka bezpečného chování na internetu je rozložena do pěti vyučovacích hodin informatiky. Časová náplň předpokládá 45minutový výukový cyklus, učitel si jej ale může dle aktuálních možností sám přizpůsobit. Návrhy nejsou námětem pro nový předmět, ale jsou vytvořeny jako doplnění aktuálního plánu výuky. Součástí návrhů jsou metodické listy s teoretickou i praktickou částí doplněnou prezentacemi. Pro žáky je také vytvořen pracovní list, který obsahuje celkem 12 motivačních úloh. Navržené metodické listy byly vytvořeny jako praktická část diplomové práce (Šebáková, 2022).

Každý metodický list začíná úvodem do tématu. Dále je zde popsána vhodná forma výuky, kdy ve většině případů je potřeba pro výuku pouze učebna s přístupem k promítání prezentací a časový rozpis vyučovací hodiny. Pedagog si prezentace i listy může přizpůsobit svým možnostem, ať už svému projevu, či časovým možnostem výuky. Obsahem listů je samotný výklad, který koresponduje se snímky v prezentacích. Po úspěšném dokončení výkladu je zde prostor pro dotazy žáků. Součástí metodického listu je krátké hodnocení a závěr.

Téma č.1 SMART zařízení

První hodina se bude zabývat základními pojmy a obecnými informacemi o chytrých zařízeních. Dnes je většina žáků již někdy setkala s chytrými zařízeními a žáci je také dokáží sami ovládat. Používají je v tomto mladém věku ale spíše pro zábavu, než pro práci a školu. První část hodiny se zabývá druhy těchto zařízení, aby žáci věděli, co mezi ně všechno může patřit. Také je zde uvedeno několik otázek přímo pro žáky, pro zpestření hodiny. Dalším tématem je aktualizace. Zde se žáci seznámí, k čemu aktualizace jsou a z jakého důvodu je dobré aktualizovat všechna svá zařízení. Třetí část hodiny je zaměřena na polohové služby, kdy by každý žák měl vědět, proč není dobré, aby smartphony sbíraly data o tom, kde se právě nacházíme. V poslední kapitole, by žáci měli získat informace o tom, že nejen poloha ale i sběr dat o sportovních

aktivitách, srdečním tepu apod. mohou být nebezpečné, pokud útočníci ví, jak s takovými informacemi naložit. Úvodní hodina věnovaná smart dotykovým zařízením je spíše teoretická, seznámí žáky s vybranými tématy, jak by měli se sdílenými informacemi zacházet. Jsou zde uvedeny také otázky, které lze žákům položit a jeden konkrétní případ nebezpečného sběru dat. Ke každému metodickému listu, kde je teoretický výklad, je vytvořena Powerpointová prezentace.

Obr. 1. Ukázka z prezentace – sdílení informací na internetu

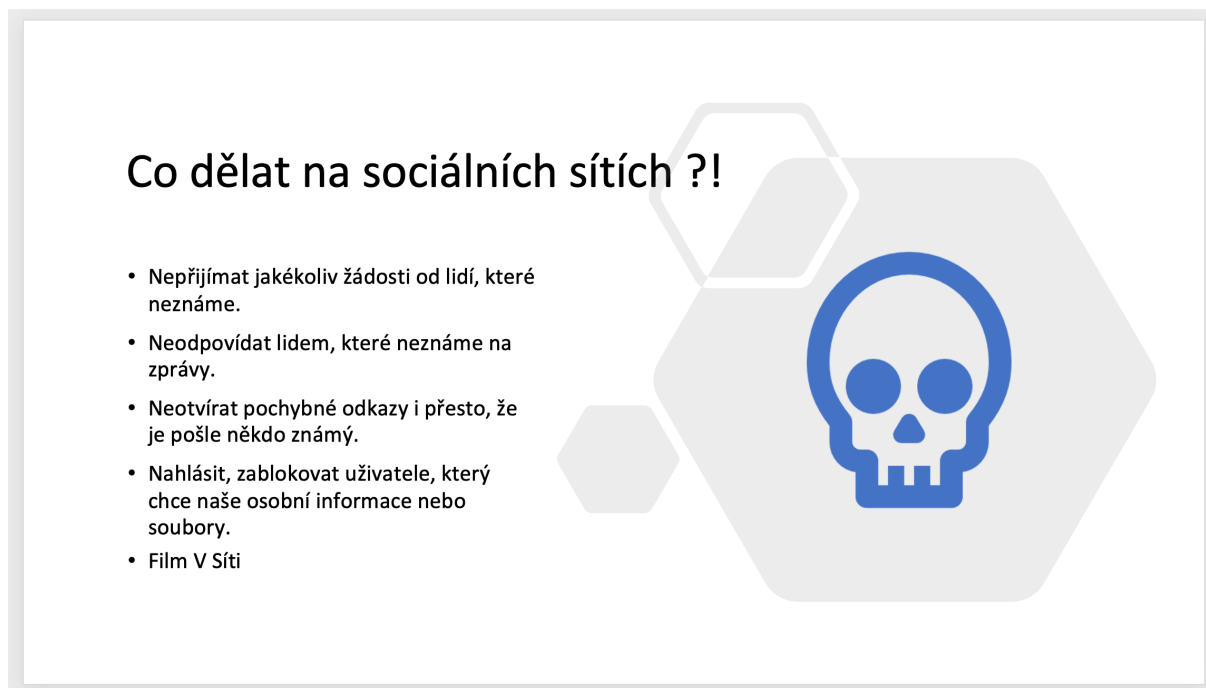
Téma č.2 Sociální sítě

Jak již bylo zmíněno, sociální sítě jsou moderním způsobem komunikace i zábavy. Žáci se těmto sítím věnují již v raném věku a nemají problém s tím, jak je používat. V tomto metodickém listu jsou tedy sítě popsány jen okrajově a neřeší konkrétní návod, jak je používat. Co je zde ale podstatné, jsou základní bezpečnostní informace u sítí Facebook, Instagram a TikTok. Jde, ale především o to, aby žáci na nich dokázali bezpečně komunikovat a sdílet informace, jelikož se dnes mohou velmi často potkat s podvodnými zprávami a lidmi právě na těchto sítích. Věnujeme se doporučení, koho si přidávat do přátel a koho ne, na jaké přijaté odkazy neklikat a také, proč si nastavit dobrou profilovou fotografii. Dále je zde ukázka toho, jak si lze na Instagramu nastavit profil, aby měl uživatel své příspěvky v soukromí a mohli je vidět jen ti, které si přidá do seznamu sledujících. Nakonec je zde několik doporučení pro žáky, co by neměli dělat na sociálních sítích. Také je zde uveden film natočený českou produkcí – V Síti. Ten je velmi dobrou ukázkou toho, co se může na internetu stát, pokud žáci věří cizím lidem, které nikdy neviděli.

Téma č.3 Ochrana soukromí

Ve třetí hodině jsou popsány další možnosti ochrany soukromí. Tématem je sdílení informací, konkrétně sdílení příspěvků ve formě aktuálních poloh mobilního zařízení a souborů. Žáci by měli vědět, že není dobré na sociální síti zobrazit svou aktuální polohu. Co obecně i konkrétně

patří do ochrany soukromí je vydané nařízením Evropskou unií, tzv. GDPR. Tato směrnice chrání uživatele v momentě, kdy zadávají své osobní údaje na různé internetové stránky (včetně sociálních sítí) a stanoví, jak poskytovatelé těchto stránek mohou nakládat s informacemi, které uživatelé musí vyplnit, pokud chtějí mít založený účet a využít služeb takových stránek. Pozornost je věnovaná také souborům Cookies. Žáci by měli vědět, z jakého důvodu se jim pokaždé, co poprvé zobrazí internetovou stránku s libovolným obsahem, zobrazí potvrzení souborů Cookies. Většina žáků ani nemusí tušit, co to je a je dobré jim toto téma přiblížit. Ve finále jsou popsány funkce hlasových asistentů a úskalí, která tyto služby přináší uživatelům možností odposlouchávání a shromažďování informací.



Obr. 2. Ukázka z prezentace – bezpečnost na sociálních sítích

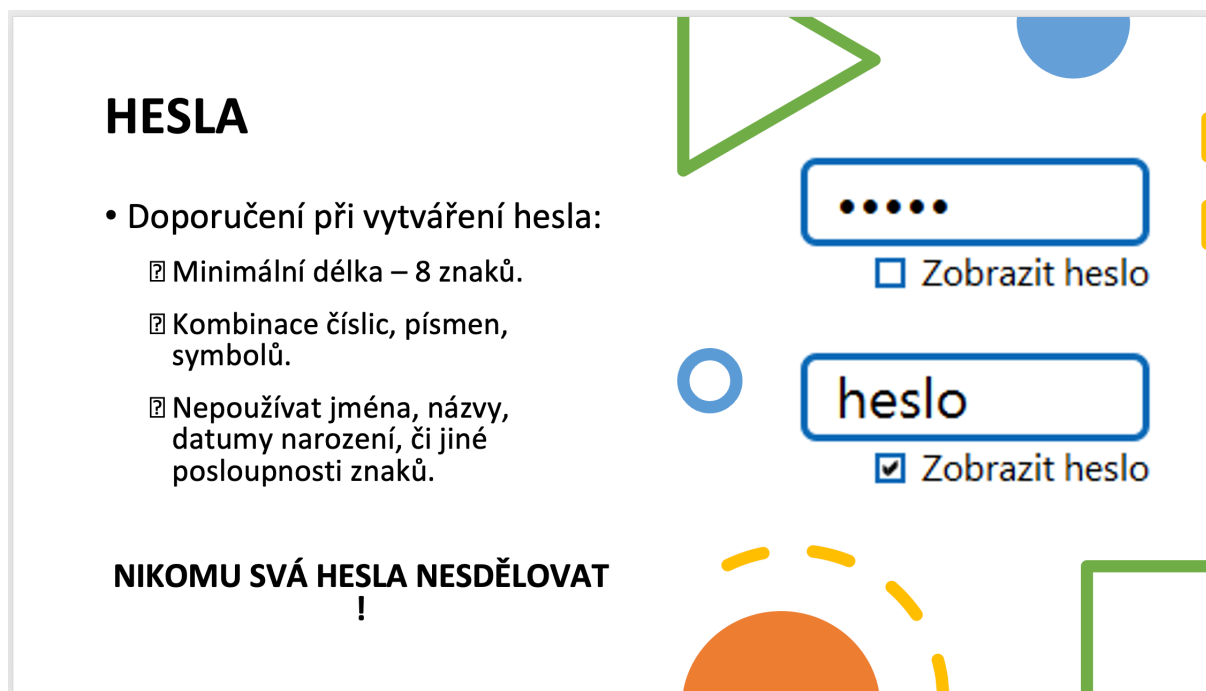
Téma č.4 Antivirus

Čtvrtá hodina je zaměřena na antivirové programy. Prezentace a výklad obsahují vysvětlení toho co je to antivirový program a jak fungují. Popsány jsou antivirové programy, které jsou zdarma ke stažení a používání. Pozornost je věnovaná také placeným antivirovým ochranám a porovnání funkcí s bezplatnými verzemi.

Téma č.5 Zabezpečení mobilního zařízení

Pátá a poslední hodina je zaměřena především na zabezpečení zařízení. První část se věnuje heslům a to konkrétně, jak by měla hesla vypadat, jak s vytvořeným heslem zacházet a chránit ho před únikem cizím lidem. Další důležitou součástí zabezpečení osobních zařízení je zámek, který je zobrazován vždy při aktivaci zařízení. Žáci by měli chápat nutnost chránit si svá hesla. Měli by vědět, že ani nejlepším kamarádům není dobré heslo sdělit, jelikož je to vstupenka do zařízení a také vstupenka ke všem datům, včetně přístupu na sociální sítě. Rozsáhleji je pozornost věnovaná dvoufázovému ověření uživatele jako důležité součásti zabezpečení. V první řadě je v metodickém materiálu vysvětleno, jak celý systém ověření funguje včetně konkrétních příkladů, jak se dvoufázové ověření nastavuje na konkrétním příkladu pro účet na

Google, Facebook a na mobilní aplikaci Instagram. Prostor je věnován také Spamu a jak se proti němu účinně bránit.

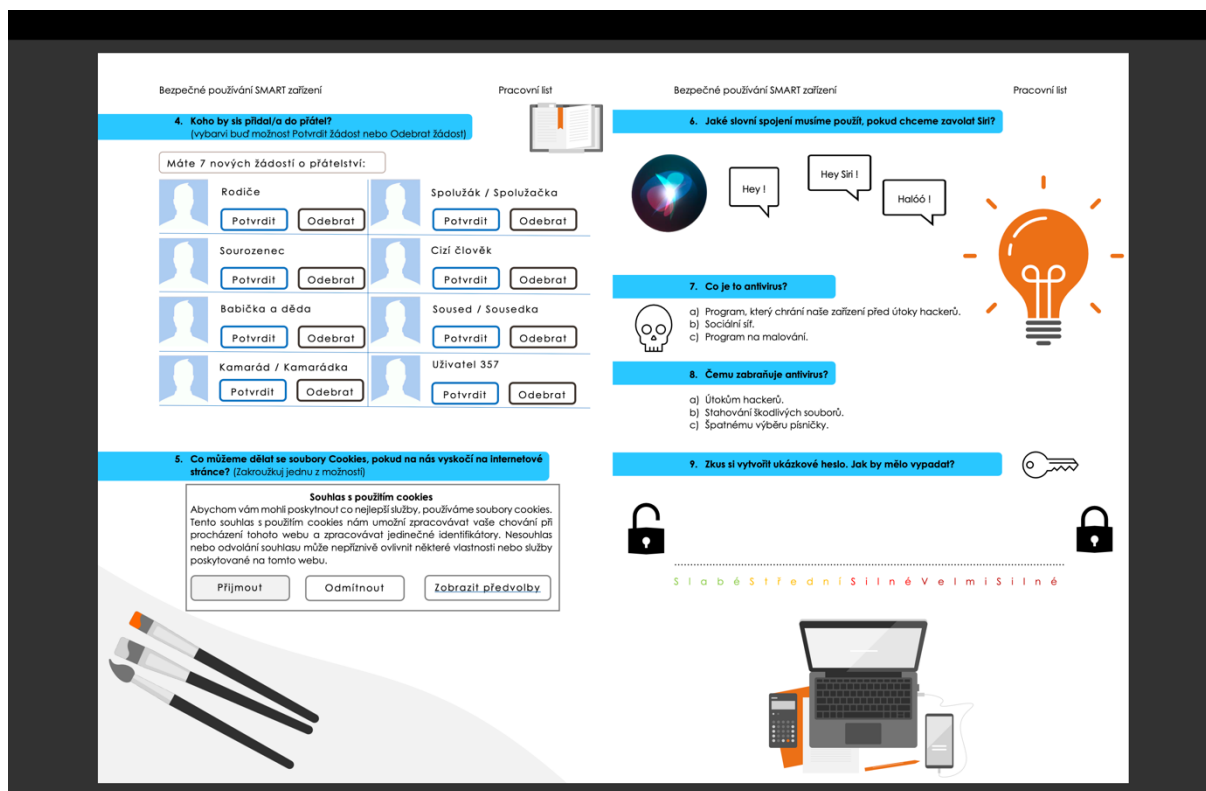


Obr. 3. Ukázka z prezentace – bezpečné a silné heslo

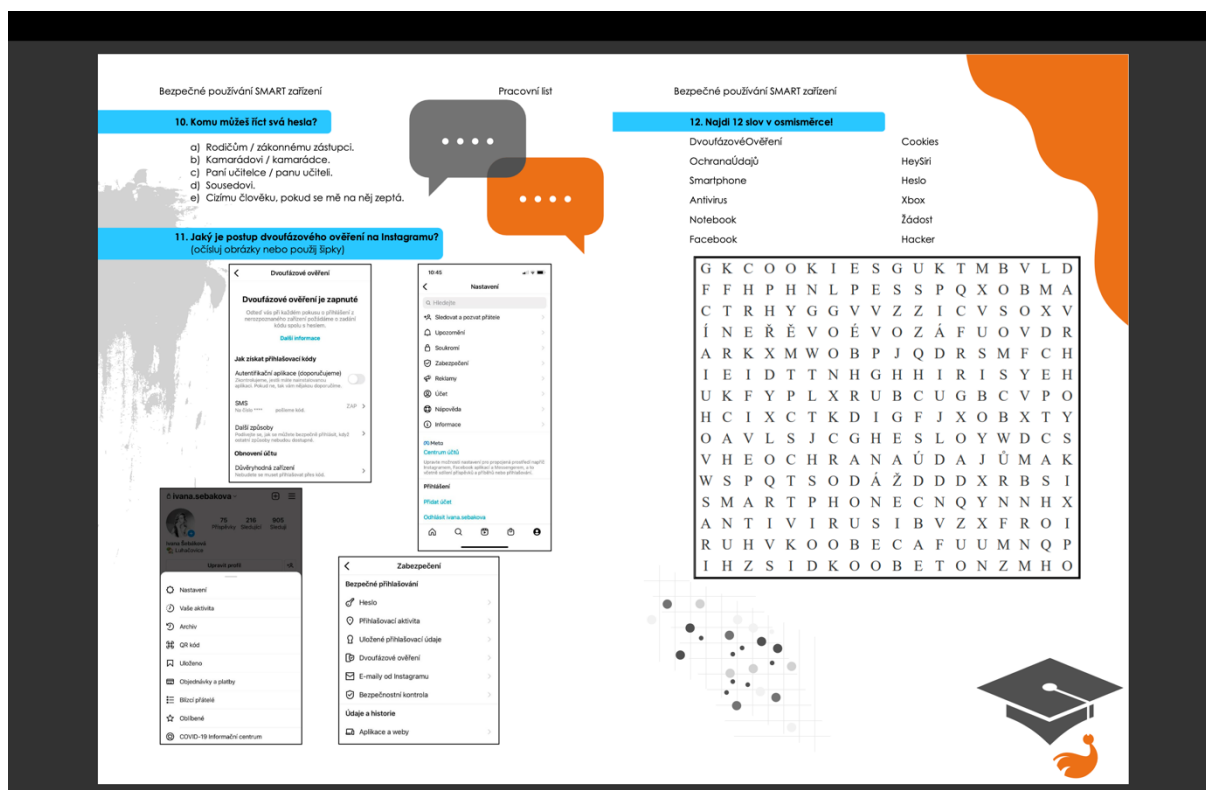
Pracovní listy pro žáky

Pracovní list má celkem pět stran a je nedílnou součástí vytvořených prezentací a metodických listů pro učitele. Obsahuje 12 otázek a úkolů pro žáky. V úvodní otázce mají žáci zakroužkovat zařízení, která vlastní. Druhá otázka je testová, kde žáci mají vybarvit správnou odpověď, kdo je zakladatelem Facebooku. Ve třetí otázce žáci zakroužkují správnou odpověď na otázku, kdo vydal nařízení GDPR. Čtvrtá otázka je úkol, který simuluje prostředí Facebooku, kde jsou vypsaní uživatelé, kde žáci mají vybarvit buď přijetím žádosti, nebo odmítnutím dle svého správného uvážení. Pátá otázka se zaměřuje na soubory Cookies. Zde není ani jedna správná odpověď. Je to ilustrovaný případ vyskakovacího okna na internetových stránkách, kde jde o souhlas s použitím těchto souborů. Žáci vyberou jednu z možností. Dále odpovádá na otázku, jaké slovní spojení musí uživatel použít, pokud chce zapnout Siri. Sedmá a osmá otázka je zaměřena na antivirovou ochranu, co je to antivirus a před jakými nebezpečími na internetu je chráněn. Devátý úkol je více kreativní, zde si žáci mohou sami napsat, jak by mělo vypadat silné heslo. Desátý úkol zjišťuje, komu žáci mohou říct svá hesla. V jedenáctém úkolu, žáci očíslojí snímky obrazovky z Instagramu tak jak si myslí, že je správný postup nastavení dvoufázového ověření na sociální síti Instagram. Poslední dvanáctý úkol je zábavný. Pro žáky je vytvořena osmisměrka, kde mají najít dvanáct slov týkající se převážně pojmů, které žáci měli možnost slyšet v prezentacích.

Vytvořené metodické materiály byly využity při výuce informatiky na konkrétní základní škole Zlínského regionu, kde zpětnou vazbu poskytli učitelé informatiky. Ti hodnotili předložené metodické materiály pozitivně, dle pedagogů jsou vytvořené prezentace vhodným metodickým materiálem, který výuku informatiky na základní škole obohatí.



Obr. 4. Ukázka pracovního listu pro žáka – pracovní list č.1



Obr. 5. Ukázka pracovního listu pro žáka – pracovní list č.2

Závěr

Otázkám bezpečného chování na internetu s využitím mobilního telefonu považujeme za důležité věnovat dostatečnou pozornost ve výuce nové informatiky na základních školách. Žáci by měli být vědomi rizik, která online prostředí přináší. Měli by si být jasné vědomi toho, jak se na sociálních sítích zodpovědně a bezpečně chovat, aby byli v bezpečí nejen oni sami, ale také jejich data. Měli by si být vědomi, že nemohou na internetu sdílet libovolné soubory a uvědomit si, jak chránit svá data i soukromí. Učitelé na základních školách by se měli tématům bezpečnosti ve výuce informatiky věnovat a zaměřit se na problematiku bezpečného přístupu k webu, nastavení dvoufázového ověření přístupu, silných a bezpečných hesel správy dat a používání antivirových programů. Vytvořené metodické materiály mohou pomoci dosáhnout těchto cílů ve výuce informatiky.

Literatura

- ŠEBÁKOVÁ, I. (2022). *Bezpečné využívání chytrých zařízení žáky základní školy*. Zlín. Diplomová práce. UTB, FaI.
- MCCARTHY, L., WELDON, D. (2013). *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha: CZ.NIC, 2013, 316 s. CZ.NIC. ISBN 978-80-904248-6-9.
- HAUPTOVÁ, Š. (2019). *Vliv internetu a sociálních sítí na oblast komunikace a vytváření mezilidských vztahů u dětí a mládeže*. Pardubice. Diplomová práce. Univerzita Pardubice.
- PETROWSKI, T. (2014). *Bezpečí na internetu: pro všechny*. Liberec: Dialog. Tajemství (Dialog). ISBN 978-807-4240-669.
- SEDLACEK, M. (2020). *Modelování výrobních procesů s využitím programu simul8 v kontextu výuky technických předmětů*. Olomouc, Univerzita Palackého, TVV 2020, 14(2):25-26. RIV/61989592:15410/20:73612053
- SEDLACEK, M. (2020). *Simulační modely a možnosti jejich uplatnění ve výuce technických předmětů v kontextu průmyslu 4.0*. Olomouc, Univerzita Palackého, TVV 2020, 13(1):28-34 | DOI: 10.5507/tvv.2020.005.
- SEDLACEK, M. (2020). *Modelování výrobních procesů s využitím programu Simul8 v kontextu výuky technických předmětů*. Olomouc, Univerzita Palackého, TVV 2020, 13(1):12-19 | DOI: 10.5507/tvv.2020.002.
- SEDLACEK, M. (2021). *SWOT analýza a její aplikace při řešení vnitřních a vnějších faktorů současné online výuky z pohledu studentů učitelství informatiky*. Olomouc, Univerzita Palackého, TVV 2021, 14(2):24-25. RIV/61989592:15410/21:73612048
- SEDLACEK, M. (2021). *Aplikace simulačního modelu v kontextu rozvoje inženýrského myšlení*. Olomouc, Univerzita Palackého, TVV 2021, 14(2):94-100. DOI: 10.5507/tvv.2021.010.

Kontaktní adresa:

Ing. Mgr. Michal Sedláček, Ph.D., Katedra technické a informační výchovy, Pedagogická fakulta, Univerzita Palackého v Olomouci, Žižkovo nám. 5, 771 40 Olomouc, Česká republika, e-mail: michal.sedlacek@upol.cz

Mgr. Ivana Šebáková, Ústav informatiky a umělé inteligence, Fakulta aplikované informatiky, Univerzita Tomáše Bati ve Zlíně, Nad Stráněmi 4511, 760 05 Zlín, Česká republika.