

Kovářová, Pavla

## Použité výzkumné nástroje

In: Kovářová, Pavla. *Informační bezpečnost žáků základních škol : lekce v knihovnách*. Vydání první Brno: Filozofická fakulta, Masarykova univerzita, 2019, pp. 224-239

ISBN 978-80-210-9270-9; ISBN 978-80-210-9271-6 (online : pdf)

Stable URL (handle): <https://hdl.handle.net/11222.digilib/141127>

Access Date: 30. 11. 2024

Version: 20220831

Terms of use: Digital Library of the Faculty of Arts, Masaryk University provides access to digitized documents strictly for personal use, unless otherwise specified.

# PŘÍLOHA 1 POUŽITÉ VÝZKUMNÉ NÁSTROJE

## Příloha 1.1 Vzdělávání v knihovnách k bezpečnosti na internetu

### Představení

Vážené kolegyně a vážení kolegové,

jmenuji se Pavla Kovářová a jsem doktorandka na ÚISK FF UK a odborná pracovnice na KISK FF MU, kde se mj. zabývám informační bezpečností. Ráda bych Vás tímto požádala o spolupráci formou vyplnění krátkého dotazníku, jehož cílem je zmapování vzdělávání na téma bezpečnosti na internetu, především v knihovnách a se zaměřením na děti, ale i souvisejícího širšího kontextu. Výsledky dotazníku poslouží i k přizpůsobení několika plánovaných seminářů pro knihovníky na obdobná témata. Dále budou představeny na mezinárodní konferenci EU Kids Online (<http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Conference.aspx>) i v českých odborných periodikách.

Dotazník je složen z 10 otázek. Pokud je u některé možný výběr více odpovědí, budete na toto u ní upozorněni. Vyplnění by Vám nemělo zabrat déle než 10 minut.

Děkuji za spolupráci Pavla Kovářová

1. V jaké jste zaměstnán/a instituci (vyberte nejkonkrétnější možnost)? \*
  - školní knihovna
  - akademická knihovna
  - veřejná knihovna, která podle knihovního zákona není specializovaná knihovna
  - jiná knihovna
  - instituce školství mimo školní knihovnu

- instituce veřejné správy
  - soukromá firma
2. Organizuje tato instituce vzdělávací aktivity (ne pro zaměstnance samotné instituce)? \*
- ano
  - ne (přejděte na otázku č. 8)

### **Vzdělávací aktivity v instituci**

3. Jaké je obsahové zaměření vzdělávacích aktivit Vaší instituce? (možno více odpovědí)
- zkvalitnění zpracování informací bez ohledu na jejich zdroj (např. využití softwaru, online nástrojů, informační služby, informační etika, publikační činnost atd.)
  - zkvalitnění práce s tradičními informačními zdroji
  - zkvalitnění práce s elektronickými informačními zdroji
  - kulturní akce
  - jiné (uveďte jedno nejvýznamnější)
4. Víte o tom, že by se někdy některá/některé z nich věnovaly bezpečnosti na internetu? (možno více odpovědí)
- ano, jako samostatnému tématu (do pole poslední možnosti této otázky uveďte, zda pravidelně/nepravidelně a kolikrát během Vámi stanoveného časového období)
  - ano, v rámci jiných témat je zmiňován aspekt bezpečnosti na internetu (do pole poslední možnosti této otázky uveďte, zda pravidelně/nepravidelně a kolikrát během Vámi stanoveného časového období)
  - ne, ale podle mého názoru by měly
  - ne, podle mne to nemá smysl
  - pokud ano, jak často
5. Považujete děti za jednu z klíčových primárních cílových skupin vzdělávacích aktivit ve Vaší instituci (tj. vzdělávací akce pořádáte přímo pro ně a to minimálně 6 v roce)?
- ano
  - ne (přejděte na otázku č. 8)

### **Vzdělávací aktivity pro děti**

6. Jaké je obsahové zaměření vzdělávacích aktivit orientovaných na děti jako primární cílovou skupinu? (možno více odpovědí)
- zkvalitnění zpracování informací bez ohledu na jejich zdroj (např. využití softwaru, online nástrojů, informační služby, informační etika, publikační činnost atd.)
  - zkvalitnění práce s tradičními informačními zdroji

- zkvalitnění práce s elektronickými informačními zdroji
  - čtenářství
  - kulturní akce
  - doplnění výuky ve škole bez zaměření na aktivity knihovny (např. kreslení, fyzikální experimenty...)
  - jiné (uveďte jedno nejvýznamnější)
7. Víte o tom, že by se někdy některá/některé z nich věnovaly bezpečnosti na internetu? (možno více odpovědí)
- ano, jako samostatnému tématu (do pole poslední možnosti této otázky uveďte, zda pravidelně/nepřavidelně a kolikrát během Vámi stanoveného časového období)
  - ano, v rámci jiných témat je zmiňován aspekt bezpečnosti na internetu (do pole poslední možnosti této otázky uveďte, zda pravidelně/nepřavidelně a kolikrát během Vámi stanoveného časového období)
  - ne, ale podle mého názoru by měly
  - ne, podle mne to nemá smysl
  - pokud ano, jak často

### **Doplňující informace**

8. Myslíte si, že by se knihovny měly v rámci svých vzdělávacích aktivit věnovat bezpečnosti dětí na internetu? \*
- ano
  - ne
9. Jaké znáte online vzdělávací projekty k tématu bezpečnosti dětí na internetu (nejsou myšleny jednorázové kampaně)? (možno více odpovědí) \*
- Bezpecne-online.cz
  - E-Bezpečí
  - E-Nebezpečí
  - Internet Hotline
  - Nebud' obět'
  - Pomoconline.cz
  - Protišikaně.cz
  - Saferinternet CZ
  - Žádný
  - Jiný (uveďte jeden nejvýznamnější)
10. Chcete k tématům v dotazníku něco dodat? Pokud chcete být informováni o umístění publikovaných výsledků tohoto dotazníku, uveďte kontaktní e-mailovou adresu.

Vaše odpovědi byly úspěšně odeslány, děkuji za vyplnění dotazníku.

## Příloha 1.2 Rozšiřující deskripce vzdělávání

Dobrý den, jsme projekt iNeBe – informační (ne)Bezpečí, podporovaný Kabinetem informačních studií a knihovnictví Masarykovy univerzity v Brně. Chtěli bychom Vás požádat o vyplnění dotazníku zaměřeného na tematiku informační bezpečnosti, který nám pomůže zjistit, jaký zájem mají knihovny o vzdělávání v této oblasti. Vyplnění dotazníku Vám zabere přibližně 8 minut. V případě, že máte jakýkoliv dotaz nebo zájem o spolupráci, pište na e-mail: [inebe@seznam.cz](mailto:inebe@seznam.cz). Děkujeme za Váš čas!

1. Prosím uveďte název města, ve kterém se nachází Vaše knihovna: \*
2. Zde prosím vyplňte název Vaší knihovny: \*
3. Organizuje Vaše knihovna vzdělávací aktivity pro veřejnost? \*
  - Ano
  - Ne
  - Nevím
4. Je některá z těchto aktivit zaměřená na počítačovou gramotnost nebo práci s počítačem/internetem? \*
  - Ano
  - Ne
  - Nevím
5. Věnujete se v rámci některé vzdělávací aktivity problematice informační bezpečnosti? \*
  - Ano
  - Ne
  - Nevím
6. Myslíte si, že je důležité vzdělávání v oblasti informační bezpečnosti? \*
  - Určitě ano
  - Spíše ano
  - Spíše ne
  - Určitě ne
  - Nevím / nemohu odpovědět
7. Chtěli byste se vy osobně vzdělávat v oblasti informační bezpečnosti? \*
  - Určitě ano
  - Spíše ano
  - Spíše ne
  - Určitě ne
  - Nevím
8. Měli byste zájem o přednášku či kurz na téma informační bezpečnosti ve Vaší knihovně?\*

Příloha 1 Použité výzkumné nástroje

- Určitě ano
  - Spíše ano
  - Spíše ne
  - Určitě ne
  - Nevím / nemohu odpovědět
9. Pokud by vám byla nabídnuta možnost vzdělávat se v problematice informační bezpečnosti, jaká forma výuky by Vám vyhovovala?

	Vyhovovala	Spíše vyhovovala	Spíše nevyhovovala	Nevyhovovala
E-learningový kurz *				
Klasické přednáškové lekce v rozsahu 5-10 lekcí *				
Jednorázový intenzivní workshop ve Vaší knihovně *				
Výuka ve virtuálním světě, např. SecondLife *				
Samostudium materiálů *				
Individuální školení s lektorem (max. 3 osoby) *				

10. Byli byste ochotni na výuku dojíždět? \*

	Ano	Ne
Praha *		
Brno *		
nejbližší krajská knihovna *		

11. Kolik času týdně byste byli ochotni věnovat takovému kurzu? \*

- Maximálně hodinu
- 1-2 hodiny
- 2-3 hodiny
- 3-4 hodiny
- 4 hodiny a více

12. Vyberte témata, která by Vás zajímala v kurzu: \* Můžete vybrat více možností

- problematika sociálních sítí
- nevyžádané zprávy (spam)
- malware (viry, červy, trojské koně...)
- zneužití osobních informací (vč. kyberšikany)
- autorské právo
- pornografie
- nevhodný a nelegální obsah (agresivita a násilí)
- specifictví uživatelé (děti, firmy, stát...)

- šifrování (hesla, elektronický podpis...)
  - prevence (jak svá data chránit)
  - jiné (napište prosím jaké)
13. Měli byste zájem o metodické materiály, které by vám umožnily orientaci v problematice tak, abyste sami mohli ve Vaší knihovně přednášet na téma informační bezpečnosti? \*
- Ano
  - Ne
14. Jakou formu výukových materiálů preferujete? \*
- podcasty (zvukové nahrávky)
  - teoretické texty
  - brožurky/letáčky
  - videa
  - zábavná forma (hry, komiksy, křížovky...)
  - teorie s možností ověření znalostí (test)
  - jiné (napište prosím jaké)
15. V případě, že máte zájem o spolupráci, výukové nebo propagační materiály, vyplňte prosím Vaši e-mailovou adresu:
16. Místo pro Vaše vyjádření nebo připomínky, a to ať už k dotazníku nebo problematice:

Děkujeme za Váš čas strávený vyplňováním dotazníku!

## Příloha 1.3 Didaktické testování

Dobrý den,

prosím o vyplnění dotazníku, jehož cílem je porovnat znalosti studentů oboru informační studia a knihovnictví a knihovníků o problematice digitálních stop. Výsledky budou použity pro tvorbu dizertační práce.

Vzhledem k cíli šetření prosím netipujte odpovědi, ale vyberte variantu „nevím“, pokud danou znalost nemáte. Vyplnění může být časově náročnější (přibližně 20 minut), výsledky ale budou o to přínosnější nejen pro publikování, ale také pro to, jaké vzdělávací aktivity Vám budou v budoucnu v souvisejících tématech nabízeny. Proto věřím, že vynaložený čas bude prospěšný i pro Vás.

Velmi děkuji za ochotu se tímto šetřením zabývat.

Pavla Kovářová

Kabinet informačních studií a knihovnictví, FF MU

Ústav informačních studií a knihovnictví, FF UK

### 1. Co jsou digitální stopy? (více možných odpovědí)\*

- *Historie vyhledávání, záznamy e-komerce (registrace, objednávky)*
- *Informace s vypovídací hodnotou, uložená či přenášená v digitální podobě, tedy dokumenty, „otisky“ činnosti technologického zařízení pracujícího s daty, metadata obsahující informace o daném souboru apod.*
- *Informace zpřístupněné vědomým nahráváním a sdílením samotným uživatelem i zpřístupněné online bez záměrného přičinění uživatele*
- *Jakákoliv digitální data, která mohou prokázat spáchání trestného činu nebo mohou poskytnout vazbu mezi trestným činem a jeho obětí či jeho pachatelem*
- *Profilů, které reklamním společností umožňují doručovat personalizovaná reklamní sdělení, vytvořené nejčastěji na základě sledování klíčových slov zadávaných do vyhledávačů a sledování pohybu napříč navštívenými webovými stránkami*
- *Soubor informací, které za sebou uživatel zanechává (ať již vědomě, či nevědomě) během využití informačních technologií*
- *Záznamy komunikace přes mobil, tablet i GPS a podobná zařízení*
- Nevím

### 2. Ve které oblasti si dokážete představit legální využití a ve které nelegální zneužití digitálních stop?\*

	využití	zneužití	bez vlivu	nevím
hacking		X		
kriminalistika	X			
management (kontrola a monitoring)	X	X		
marketing	X	X		
mezilidská komunikace, např. zprávy i zed' na Facebooku	X	X		



	využití	zneužití	bez vlivu	nevím
personalistika	X	X		
správa informačních systémů a sítí	X	X		
státní správa	X			

3. Jak silně zneužitelné jsou informace, které je za určitých okolností možné zjistit z digitálních stop? (označte jednu možnost pro každý řádek)\* (1 silně zneužitelné – 5 samostatně nezneužitelné)

	1	2	3	4	5	Nevím
cestovní plány		X				
citlivé údaje s potenciálem diskriminace (náboženství, přestupky proti zákonu...)	X					
číselné identifikátory a autentizační údaje (rodné číslo, uživatelské jméno a heslo...)	X					
dokumenty k osobě (vlastní i oblíbené cizí výtvary, fotky s ním...)			X			
identifikační údaje pro stát či firmy (jméno, příjmení, datum a místo narození, adresa trvalého pobytu...)	X					
informace o denní rutině (pravidelný dopravní spoj, zájmová sdružení, rozvrh...)		X				
navštívené webové stránky			X			
osobní informace možná za hranicí soukromí (podrobnosti přátelství a partnerství, nahé fotky v kojeneckém věku...)		X				
podrobnosti o movitém či nemovitém majetku			X			
povolání					X	
přibližná výše platu					X	
telefonní číslo, e-mailová adresa			X			
věk				X		
zájmy (koníčky, zdroje, názory...)			X			
zaměstnavatel, vzdělání				X		

4. Co je výsledkem deaktivace účtu na Facebooku? Vyberte jednu nejpřesnější odpověď.\*

- Informace vyprodukované uživatelem, který účet deaktivuje, budou odstraněny
- Účet bude neaktivní, ale vše zaznamenané na Facebooku zůstane, dokud nebudou podniknuty komplexnější kroky ke smazání
- Účet nebude přístupný, dokud ho uživatel znovu neaktivuje přes daný postup (např. potvrzení e-mailem, když byl účet deaktivován kvůli prozrazení přístupových údajů)
- Všechny informace spojitelné s uživatelem budou odstraněny

- Nevím
5. Jaké nástroje jsou využívány pro automatický pasivní (bez uživatelské aktivity) sběr digitálních stop? (více správných odpovědí)\*
- CAPTCHA
  - *cookies*
  - crawler
  - *historie v prohlížeči*
  - hotspot
  - link farma
  - PageRank
  - *plugin v prohlížeči*
  - *sociální síť*
  - *vyhledavač*
  - *webbug (pixelový tag)*
  - jiný (doplňte)
6. Zhodnoňte upotřebení digitálních stop v problémech uvedených v tabulce. Pokud je pro realizaci digitální stopu nezbytné využít, zatrhněte pole „vyžaduje“. Pokud digitální stopa jen přispívá k úspěšnosti, ale není nezbytná, zatrhněte pole „podporuje“. Pokud problém s digitální stopou nepracuje, zatrhněte „bez vlivu“. Pokud pojem neznáte, zatrhněte „nevím“. (označte jednu či více možností)\*

	<b>Vyžaduje</b>	<b>Podporuje</b>	<b>Bez vlivu</b>	<b>Nevím</b>
Krádež identity	X			
Kyberšikana		X		
Kyberstalking	X			
Kybergrooming	X			
Sexting	X			
Vydírání	X			
Malware		X		
Spam			X	
Scam		X		
Hoax			X	
Phishing		X		
Prolamování hesel		X		

7. Jaká varování mohou předznamenávat to, že se Vás někdo snaží zmanipulovat? (více možných odpovědí)\*
- „ohánění se“ autoritou (*nadřizený, známá organizace...*) a znalostí bez kontextu
  - časový limit, naléhavost
  - formální (*jazykové, typografické*) chyby
  - napodobení očekávaného vzhledu (*např. webu, adresy, vizuálu...*)

- *nebezpečí (finanční či jiné)*
  - *nemožnost či omezení ověření*
  - *symboly pro zvýšení pozornosti (velká písmena, vykřičníky, \$\$\$...)*
  - *útok na emoce (vína, soucit, ego přes flirtování či lichocení...)*
  - *vybuzení zájmu (zvědavost, finanční či jiný zisk s malými náklady)*
  - nic z uvedeného
  - jiné
8. Jaká preventivní opatření ve vlastním chování proti vytváření a využití digitálních stop znáte a která používáte?\*

	<b>znám a používám</b>	<b>znám, ale nepoužívám</b>	<b>neznám</b>
Bezpečné používání silných hesel			
Čtení certifikátů, licenčních podmínek, varování, potvrzení...			
Egosurfing (vyhledání informací o konkrétním člověku)			
Nedůvěra k deklarované identitě (uvědomění si možnosti změny identity, např. spoofing, falešné údaje v registraci...)			
Nezjednodušování si práce na úkor bezpečnosti (např. pamatování hesel v prohlížeči)			
Prověřování aplikacemi typu antivir všeho staženého z internetu (soubory, e-maily...)			
Při neobvyklé žádosti (o informace, činnost...) ověřit oprávněnost			
Sledování aktuálních problémů a bezpečnostních řešení			
Šifrování (e-mailů, spojení...) či elektronický podpis, kde je to možné			
Uváživá práce s uživatelskými účty, především v operačním systému			
Uváživé publikování fotografií, videí a osobních údajů			
Vhodné nastavení soukromí u všech služeb, zejména sociálních sítí (např. nastavení aktualizací)			
Vhodné nastavení prohlížeče (např. správa cookies)			
Nejsou navštěvovány weby a stahovány soubory s nevhodným a nelegálním obsahem			
Využití více přihlašovacích jmen (přezdívek)			
Zamýšlení se nad možnými negativními i pozitivními důsledky a jejich zhodnocení před aktivitou			

9. Co znamená anonymní mód (InPrivate apod.) v prohlížeči? Vyberte jednu nejpřesnější odpověď.\*
- Nejsou ukládány nikam žádné informace o uživateli a zařízení, které využívá
  - Nejsou ukládány informace spojitelné s konkrétním uživatelem, ale jen obecné (např. preferovaný jazyk)
  - *Jsou ukládány informace jako při běžném použití prohlížeče, ale po ukončení jsou smazány záznamy (historie, cookies apod.), kromě stažených souborů*
  - Nevím
10. Jakou anonymizaci umožňují webové proxy servery? Vyberte jednu nejpřesnější odpověď.\*
- Úplné skrytí veškerých technických informací o uživatelově zařízení, díky čemuž webové stránky mohou zjistit jen technické informace o proxy serveru
  - Úplné skrytí IP adresy za adresu proxy serveru, o zařízení uživatele mohou weby zjistit jen obecné technické informace (např. rozlišení obrazovky pro správné zobrazení)
  - *Skrytí IP adresy, které je ale neúčinné, pokud nejsou blokovány HTTP hlavičky nebo není důvěryhodný správce*
  - Nevím
11. Jak fungují služby založené na onion routingu (např. TOR, JonDonym)? Vyberte jednu nejpřesnější odpověď.\*
- *IP adresa a další údaje jsou skryty za údaji několika proxy serverů, navíc lze přenos šifrovat a použít plugíny pro šifrovaný přenos a blokování Flash a Java skriptů*
  - Dostatečná anonymizace je zajištěna skrytím veškerých technických informací o uživatelově zařízení několikanásobným zašifrováním (jako vrstvy cibule), jiné funkce by službu nevhodně zpomalovaly
  - Různé pakety jsou přes různé uzly sítě (routing), proto žádný uzel nezíská kompletní informaci o uživatelově zařízení či osobě
  - Nevím
12. Co se stane při zablokování cookies s úmyslem zamezit vzniku digitální stopy? Vyberte jednu nejpřesnější odpověď.\*
- *Některé služby nebudou správně fungovat, zejména pokud jsou spojeny s uživatelským účtem.*
  - Služby nebudou moci shromažďovat žádné informace o uživateli, takže mu nebudou moci zasílat cílenou reklamu.
  - Nezobrazí se některé části stránky (např. interaktivní, Flash videa apod.).
  - Zvýší se bezpečnost uživatele, ale použití internetu to neovlivní, je to pro něj transparentní opatření.
  - Nevím.
13. Jaké specializované nástroje proti vytváření a využití digitálních stop znáte a které používáte? (označte jednu možnost pro každý řádek)\*

	znám a používám	znám, ale nepoužívám	neznám
Anonymizér			
Antiphishingový nástroj			
Antirookit			
Antispam			
Antispyware			
Antivirus			
Filtry obsahu			
Firewall			

14. Co jsou osobní údaje, které chrání český zákon a jeho evropské obdoby díky směrnici EU? Vyberte jednu nejpřesnější odpověď.\*

- *Informace, které jednoznačně identifikují konkrétní fyzickou osobu ve fyzickém prostředí (např. jméno, příjmení, adresa trvalého pobytu, datum narození)*
- Informace, které jednoznačně identifikují konkrétní osobu ve fyzickém i v elektronickém prostředí (např. přístupové údaje)
- Informace, které jednoznačně identifikují konkrétní fyzickou nebo právnickou osobu (např. IČO, vedení organizace)
- Informace, které chce konkrétní člověk uchovat v soukromí (např. společenské vztahy, sociální vazby)
- Nevím

15. Když někdo přinese počítač na opravu, může se technik legálně podívat na data v počítači? Vyberte jednu nejpřesnější odpověď.\*

- Ano, pokud je jeho úkolem i zálohovat data
- Ano, protože co mu zákon nezakazuje, to má povoleno a toto mu zákon nezakazuje
- Ne, pokud by musel nějak neoprávněně proniknout do systému (uhodnout heslo, využít bezpečnostní mezery informačního systému atp.); v opačném případě ano
- Ne, ale musí mu to zákazník výslovně zakázat
- *Ne, jde o narušení soukromí zákazníků a to není legálně možné*
- Nevím

16. Jste:\*

- muž
- žena

17. V jaké fázi vysokoškolského vzdělávání v oboru informační studia a knihovnictví se nacházíte? (jedna odpověď)\*

- studuji bakalářský stupeň
- studuji navazující magisterský stupeň
- studuji doktorský stupeň

Příloha 1 Použité výzkumné nástroje

- studuji jiný obor než informační studia a knihovnictví
- mám již dostudován obor informační studia a knihovnictví a pracuji nebo chci pracovat v knihovně
- mám již dostudován jiný obor než informační studia a knihovnictví a pracuji nebo chci pracovat v knihovně
- jiné

18. Jak byste popsali/a svůj zájem o téma digitálních stop? Vyberte jednu nejpřesnější odpověď.\*

- vůbec mne to nezajímá a myslím, že nemá smysl tomu věnovat čas
- nezajímá mne to, ale myslím, že má smysl v této oblasti vzdělávat
- zajímá mne to jako běžného uživatele
- zajímá mne to a chci se této problematice věnovat hlouběji než běžný uživatel nebo o ní chci vzdělávat ostatní

19. Přiřaďte rozsah vzdělávání v tématu digitálních stop (nebo obecněji informační bezpečnosti), který jste absolvoval/a. (označte ve vybraném řádku jednu či více možností)\*

	<b>Žádné vzdělání</b>	<b>1-3 přednášky</b>	<b>Více přednášek</b>	<b>Samostatný předmět či seminář</b>
před vysokou školou				
na vysoké škole mimo obor ISK				
na vysoké škole v rámci oboru ISK				
po vysoké škole mimo akce určené pro knihovníky				
po vysoké škole v rámci akce určené pro knihovníky				

20. Přiřaďte varianty vyjadřující Vaš názor, jak by se mělo vzdělávat o digitálních stopách na ZŠ, VŠ a v knihovně. Vzdělávat by se...

- nemělo.
- mělo několika přednáškami nezaměřenými na informační bezpečnost, ale souvisejícími.
- mělo několika přednáškami o digitálních stopách v předmětech/vzdělávacích cyklech nezaměřených na informační bezpečnost.
- mělo celým předmětem zaměřeným na informační bezpečnost.\*

Základní škola \_\_\_\_\_  
Vysoká škola \_\_\_\_\_  
Knihovna \_\_\_\_\_

## Příloha 1.4 Rozhovory v akčním výzkumu

### Poučený souhlas

Tímto uděluji PhDr. Pavle Kovářové, r. č. \_\_\_\_\_, poučený souhlas k neanonymnímu publikování autorizovaných výsledků rozhovoru v její dizertační práci. Cílem publikovaných informací bude popsat názory a argumenty k vzdělávání v knihovnách o tématu digitálních stop a jejich zneužívání s důrazem na spolupráci škol a knihoven při tomto vzdělávání. Ke zpracování dojde na základě polostrukturovaného rozhovoru zaznamenaného ve formě videa pro potřeby vyhodnocení zjištění. Videozáznamy nebudou publikovány, po zpracování budou uchovány jen pro potřeby pozdějšího přezkoumání.

Jméno:

Pozice pro výzkum:

Podpis:

### Seznam otázek pro rozhovor: Aktuální pohled na knihovnu a informační bezpečnost

1. Jak byste definoval/a digitální stopy a jaké problémy jsou s nimi spojeny?
2. Má podle Vás smysl vzdělávat v oblasti digitálních stop a (proti) jejich zneužití?
3. Jak byste popsal/a svůj aktuální názor na to, jestli knihovny mají vzdělávat v tématu digitálních stop a (proti) jejich zneužití?
4. Jak se na spojení vzdělávání o digitálních stopách v knihovnách podle Vás dívají obecně knihovníci/školy/veřejnost či její určité části?
5. Jaká subtémata by se měla při tomto vzdělávání v knihovnách řešit?
6. Pro koho by měla být nabízena?
7. A jakou formou?
8. Při srovnání s jinými tématy, co by měla knihovna upřednostnit (knihy X internet; témata v rámci internetu; v subtématech digitálních stop)?
9. Dokážete si Vy osobně představit, že by se toto téma řešilo v každé knihovně?
10. Co by pro to muselo být zajištěno?
11. Proč myslíte, že dnešní aktivní knihovníci jsou či nejsou připraveni vzdělávat v této problematice?
12. Vzdělávají podle Vás střední, vyšší a vysoké školy budoucí knihovníky, aby toto téma mohli řešit?
13. Co by tyto školy měly dělat, aby to jejich absolventi mohli řešit?
14. Co by měli absolventi pro to znát a jak hluboce?



15. Jak jste dříve pohlížel/a na to, že by knihovny vzdělávaly v problematice digitálních stop?
16. Kdy a čím se to měnilo?
17. Jakou jste měl/a představu o možnosti lekcí a jejich reálnosti?
18. Bylo nějak téma digitálních stop řešeno dřív v nějaké lekci knihovny?
19. Jak to vypadalo?
20. Jak byste popsala stav před lekcí, tj. do jakého prostředí byla implementována, co mohlo ovlivnit její realizaci?
21. Co podle Vás přesvědčilo knihovnu pustit se do realizace lekce?
22. A co přesvědčilo školu (paní učitelky)?
  
23. Co si myslíte o uskutečněné lekci?
24. Změnila nějak právě ona Vaše názory? V čem?
25. Mělo by se podle Vás něco v uskutečněné lekci změnit?
26. Jaké pozitivní či negativní výsledky podle Vás má a na koho?
27. Myslíte, že je rozšiřitelná na další prostředí (školy, knihovny, věk cílové skupiny...)?
28. Na jaká a za jakých podmínek?
29. Co si myslíte, že si z ní děti odnesly?
30. Myslíte si, že by se na ni mělo navázat? Jak?