IMPULS
PRO KARIÉRU
A PRAXI

15

KYBERNETICKÁ BEZPEČNOST PRO ZŠ

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

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Jhk.cz

JIHOČESKÁ HOSPODÁŘSKÁ KOMORA

Jihočeský kraj

Pracovní postup „Kybernetická bezpečnost pro ZŠ“ je součástí publikace „Pracovní postupy pro workshopy digitalizace ve školách.“, která vznikla v rámci aktivity Asistenčního centra Impuls pro kariéru a praxi při Jihočeské hospodářské komoře díky realizaci projektu „Implementace Krajského akčního plánu Jihočeského kraje III“, který je spolufinancován Evropskou unií. Registrační číslo projektu CZ.02. 3. 68/0.0/0.0/19_078/0018246

Elektronická verze publikace je k dispozici na **www.impulsprokarieru.cz**

Autoři:
Ing, Rudolf Vohnout, Ph.D., Přírodovědecká fakulta, Jihočeská univerzita,
Ing. Petr Břehovský, Přírodovědecká fakulta, Jihočeská univerzita
Editor: doc. RNDr. Ing. Jana Kalová, Ph.D.
Publikaci připravila Přírodovědecká fakulta Jihočeské univerzity

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta
Centrum pro přírodovědné vzdělávání

Grafický design: Čestmír Sukdol – www.brandi.cz

Vydala: Jihočeská hospodářská komora

2021

Obsah

Cílem workshopu je na praktických ukázkách ukázat důsledky nezodpovědného chování v online prostoru. Workshop bude v první, teoretické části cílen na osvětu základních návyků chování na internetu. V části praktické pak bude osvětleno, jakým způsobem lze vysledovat informace o online chování jednotlivých uživatelů, jak lze získané informace propojit a jak je lze využít. V závěru bude na reálných případech ukázáno, kam může takovéto nezodpovědné chování vést.

Základní instrukce

Tento kurz je doporučován pro žáky druhého stupně základní školy a nižší ročníky osmiletých gymnázií. V přeneseném smyslu lze problematiku aplikovat také na žáky prvního stupně, kteří disponují chytrými zařízeními připojenými bez kontroly k internetu (smartphone, tablet, notebook apod.) Kurz je koncipován jako základní a je vstupenkou do uvědomělého chování v online prostředí, což je základní kámen kybernetické bezpečnosti.

Časová dotace tohoto kurzu je stanovena až na 7 hodin. Rozdělení 3+3(4) hodiny na teoretický a legislativní základ a získání praktických dovedností kybernetické bezpečnosti. Učitel by měl nejprve prostudovat všechny materiály dané k tomuto kurzu a pak se sám rozhodnout, kolik času kurzu věnovat.

Doporučený průběh a časové dotace podrobněji. Kurz lze rozčlenit do následujících částí:

1. Teoretický a legislativní úvod – především vymezení mantinelů a pojmu kybernetická bezpečnost, zákon o kybernetické bezpečnosti, co lze a nelze na veřejné síti provádět.
   a. Doporučuji jednu vyučovací hodinu.

2. Sdílení informací, digitální stopa a fotografická metadata – objasnění pojmů, jak vzniká digitální stopa, jak se dá vysledovat, co může prozradit a k čemu to může vést.
   a. Doporučuji také jednu až dvě vyučovací hodiny. Záleží na tom, zdali žáci jsou s tímto pojmem a problematikou k němu se vztahující obeznámeni či nikoliv.

3. Praktické ukázky důsledků nezodpovědného chování v online prostoru na konkrétních příkladech včetně jejich podrobné analýzy a diskuse. Co daný jedinec udělal špatně, k čemu to vedlo a jak tomu předejít. Sdílení vybraných odkazů s žáky nad rámec pracovních listů.
   a. Doporučuji dvě vyučovací hodiny.

4. Plnění zadaných úkolů dle pracovních listů. Připraveny jsou dva, práce s fotografickými metadaty a důsledky kyberšikany - viz metodická a didaktická část.
   a. Pro každý list doporučuji jednu vyučovací hodinu.

Pro co největší dopad praktické části je více než vhodné zjistit, jací žáci budou v rámci výuky tohoto tématu vzděláváni a kolik veřejně dostupných informací lze o jednotlivých osobách (manuálně či pomocí robotické scraperu) dohledat. Z nich doporučuji vybrat jedince, o kterém lze dohledat ve veřejných informacích co nejvíce (jehož digitální stopa je největší) a na jeho příkladě demonstrovat slabiny, které mohou vést k případnému zneužití.

Teoretická část k dané problematice

Kybernetická bezpečnost

Nejprve je nutné si definovat pojem kyberprostor. Pro drtivou většinu laické veřejnosti KYBERPROSTOR = INTERNET = WEB, ale kybernetickým prostorem jsou vymezeny všechny počítačové systémy, služby (včetně aplikací a protokolů), uživatelé a data, která se v online světě nacházejí (a lze je tak využít k získání dílčích informací nutných pro definování digitální stopy).

Kybernetická bezpečnost nemá ucelenou definici. Zásadní je si uvědomit, že vždy představuje nějaký soubor opatření vedoucích k ochraně před kriminálním či neautorizovaným užitím elektronických dat. Jinými slovy, přijmutí takových opatření, která vedou k dosažení tohoto stavu. Tato opatření mohou být jak bezpečnostní, tak technické či organizační (administrativní) povahy.

Souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ***ochrany*** *počítačových systémů a dalších prvků ICT, aplikací,* ***dat a uživatelů***

+

schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených.

Dále je důležité se seznámit s kybernetickou hrozbou. Jedná se o možnost škodlivého pokusu o poškození nebo narušení počítačové sítě nebo systému. Kybernetickou hrozbu lze také definovat jako akt směřující ke změně informace, aplikací či systému samotného. Kybernetická hrozba může způsobit:

- Únik informace – stav, kdy dojde k vyzrazení chráněné informace neautorizovanému subjektu.
- Narušení integrity – poškození, změna, či vymazání dat.
- Potlačení služby – úmyslné bránění v přístupu k informacím, aplikacím, či systému.
- Nelegitimní použití je užití informací neautorizovaným subjektem či neoprávněným způsobem.

„Ten, kdo se ve jménu bezpečnosti vzdává svobody, nezaslouží si ani svobodu, ani bezpečnost.“

Benjamin Franklin

Základní legislativa

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
  - vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
- Zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů (aka GDPR)
- Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

„Každý má právo na ochranu před NEOPRÁVNĚNÝM shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“

Listina základních práv a svobod v čl. 10 odst. 2 a 3

Sdílení informací

Fyzické osoby samy a dobrovolně o sobě zveřejňují stále větší množství dat (fotografie, videa aj.), přičemž k distribuci těchto dat typicky využívají služby informační společnosti.

Nejvíce jsou osobní údaje zveřejňovány v rámci sociálních sítí, které z podstaty své funkce takovéto zveřejňování předpokládají a zakotvují ve smluvních podmínkách pravidla, na základě kterých je s takovýmito daty zacházeno.

Je nutné si uvědomit, že v dnešní době je většina fotografií pořizována chytrými telefony, které mají v sobě automaticky aktivovanou funkci geolokace [1]. Každá fotografie, která je zveřejněna v originální podobě si s sebou tuto informaci ve formě metadat nese [2]! Pokud tedy zveřejníte (bez potřebného nastavení zabezpečení sdílení [3]) na sociální síti, že Váš otec si právě koupil nové Porsche, je automaticky známo, kde jej také parkuje.

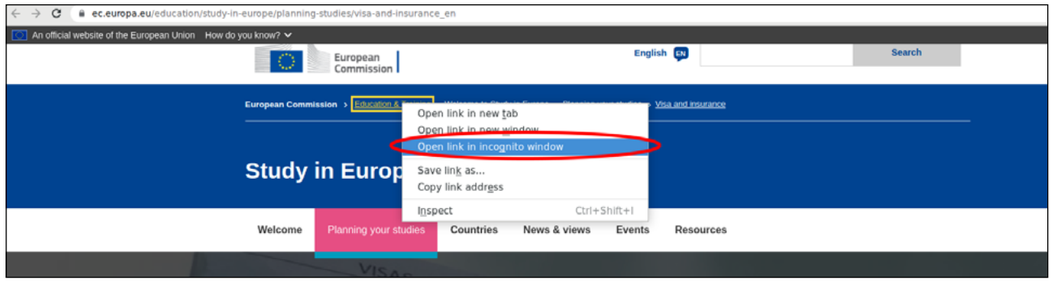
Nezapomeňte na dvě pomůcky:

- Napomáhání trestné činnosti není zákonem dovoleno.
- Neznalost zákona neomlouvá.

Digitální stopa

Veškerá aktivita v online prostoru zanechává digitální stopu [1]. Čím více času a aktivit v online světě děláme, tím je naše digitální stopa větší. [2] Digitální stopa (kromě příkladů uvedených v části „Příklady z praxe“) je poté využívána jako vstupní data pro algoritmy, které mají za úkol predikovat naše budoucí chování na internetu. To se využívá například u cílené reklamy, která poté slouží k co nejpřesnějším nabídkám na míru daného jedince. [3]

Pokud chcete svoji digitální stopu alespoň omezit (nikoliv eliminovat), používejte anonymní surfování. Nabízí jej každý prohlížeč.



Obrázek 1: Anonymní okno

Fotografická metadata

rvohnout@rvohnout-Latitude-E7440:~/ exif IMG_20210722_132304594.jpg

Na další straně je uveden výpis tzv. EXIF informací, což jsou metadata (data o datech) vybrané fotografie. Jsou to informace, které fotoaparát automaticky zapíše při pořízení fotografie a jsou její nedílnou součástí. EXIF k fotografii tak například přiřadí:

- informace o modelu fotoaparátu, kterým jste snímek pořídili, a o jeho výrobci,
- datum a čas pořízení snímku,
- údaje o rozlišení fotografie,
- GPS souřadnice,
- náhled fotografie.

Na další straně je uveden pouze příklad těch údajů, které by mohly být potenciálně využity v oblasti kybernetické bezpečnosti. Informací je daleko více (viz obrázek 1 či [4]). Každý žák by také měl vědět, jak se dá u jeho chytrého telefonu pořizování těchto informací automaticky vypnout (pro jednoduchost uvádím pouze odkaz na nejrozšířenější platformu Android, resp. Google program „Photos). [5]


```
EXIF tags in 'IMG_20210722_132304594.jpg' ('Motorola' byte order):
--------------------+-----------------------------------------------------------
Tag                 |Value
--------------------+-----------------------------------------------------------
Manufacturer        |motorola
Model               |moto g(7) plus
Orientation         |Right-top
X-Resolution        |72
Y-Resolution        |72
Resolution Unit     |Inch
Software            |lake_reteu_n-user 10 QPWS30.61-21-18-7 fac4a release-keys
Date and Time       |2021:07:22 13:23:05
YCbCr Positioning   |Centred
Compression         |JPEG compression
Orientation         |Right-top
X-Resolution        |72
Y-Resolution        |72
Resolution Unit     |Inch
Exposure Time       |1/50 sec.
F-Number            |f/1,7
ISO Speed Ratings   |139
Exif Version        |Exif Version 2.2
Date and Time (Origi|2021:07:22 13:23:05
Date and Time (Digit|2021:07:22 13:23:05
Components Configura|Y Cb Cr -
Shutter Speed       |5,64 EV (1/49 sec.)
Aperture            |1,53 EV (f/1,7)
Brightness          |1,95 EV (13,24 cd/m^2)
Exposure Bias       |0,00 EV
Metering Mode       |Centre-weighted average
Flash               |Flash did not fire, compulsory flash mode
Focal Length        |4,3 mm
Maker Note          |1115 bytes undefined data
Sub-second Time     |257539
Sub-second Time (Ori|257539
Sub-second Time (Dig|257539
FlashPixVersion     |FlashPix Version 1.0
Colour Space        |sRGB
Pixel X Dimension   |4608
Pixel Y Dimension   |3456
Sensing Method      |One-chip colour area sensor
Scene Type          |Directly photographed
Exposure Mode       |Auto exposure
White Balance       |Auto white balance
Digital Zoom Ratio  |1,00
Scene Capture Type  |Standard
GPS Tag Version     |2.2.0.0
North or South Latit|N
Latitude            |48, 58, 39,0503
East or West Longitu|E
Longitude           |14, 27, 0,5975
Altitude Reference  |Sea level
Altitude            |425,216
GPS Time (Atomic Clo|11:23:04,00
Geodetic Survey Data|WGS-84
Name of GPS Processi|12 bytes undefined data
GPS Date            |2021:07:22
Interoperability Ind|R98
Interoperability Ver|0100
--------------------+-----------------------------------------------------------
EXIF data contains a thumbnail (13929 bytes).
```

Obrázek 2: EXIF informace

Doporučené odkazy a materiály pro hlubší porozumění problematiky

[1] **https://www.mall.tv/martyisdead/digitalni-stopa**

[2] **https://blog.avast.com/cs/what-is-your-digital-footprint-avast**

[3] **https://www.youtube.com/watch?v=gcimRZF8g3Y**

[4] **https://www.milujemefotografii.cz/jak-rozumet-exifu-co-jsou-metadata**

[5] **https://support.google.com/photos/answer/6153599**

Příklady z praxe

Nedávej na Facebook nic, co bys neřekl své babičce, se říkávalo… Realističtější rada pro dnešní dny je – nedávejte na sociální sítě nic, co by neměl vidět Váš současný nebo budoucí zaměstnavatel, partner, či rodič.

Zásadní je si uvědomit, že to, co veřejně vystavíte na internet, je již navždy zveřejněno. Nic jako smazání dat neexistuje. [1]. V době, kdy jsme na škole, bohužel většinou neřešíme, že fotografie, které vystavujeme, mohou za 10 let být důvodem pro např. nepřijetí na vysoce společensky hodnocenou pozici.

Vystavení fotografie bez vědomí toho, kdo je na ní zachycen, je porušením nařízení GDPR (v ČR implementováno do legislativního prostoru jako Zákon č. 110/2019 Sb.). Vystavení takovéto fotografie může ovšem vést k vzedmutí vlny nenávistných reakcí, protože je dokázáno, že lidé se v online prostoru chovají jinak než v realitě. To může způsobit dotyčnému psychickou újmu, která v krajním případě může vést až k vyhledání psychologa, psychiatra či pokusu o sebevraždu. Uvědomte žáky, že si nesou (bez ohledu na věk) vždy následky takového jednání [2].

Relevantní odkazy

[1] **https://web.archive.org/**

[2] **https://www.mall.tv/martyisdead/pribeh-simony-a-kiany-jedna-fotka-na-instagramu-a-spousta-nenavisti**

https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybergrooming/33-112

https://o2chytraskola.cz/clanek/25/kybergrooming/4333

Pro ty, co si chtějí rozšířit obzory:

https://www.mall.tv/martyisdead/rizika-socialnich-siti

https://martyisdead.mall.tv/vyuka/

https://kyberbezpecnost.csirt.cz/cs/kyberbezpecnost/pro-uzivatele/

https://knihy.nic.cz/files/edice/cybersecurity.pdf

https://edu.ceskatelevize.cz/video/119-phishing

https://www.csfd.cz/film/812238-socialni-dilema/

https://www.documentaryarea.tv/player.php?title=The%20Social%20Dilemma

https://o2chytraskola.cz/video/8/nejsem-lovna-film-v-siti

https://o2chytraskola.cz/video/1/husta-lida

https://o.seznam.cz/wp-content/uploads/na_hory_metodika_Seznam_cz.pdf

https://www.e-bezpeci.cz/index.php/vzdelavani/tiskoviny-pro-ucitele-a-rodice

http://oldwww.upol.cz/fileadmin/user_upload/PdF/veda-vyzkum-zahr/2016/seminare/Zak_jako_obet_kybergroomingu.pdf

https://www.mesto-uh.cz/kybergrooming

Metodická a didaktická část

Na úvod je vhodné uvést, že pro tento kurz je mnohem vhodnější, pokud žáci obdrží pracovní listy v elektronické podobě ve formátu PDF, než vytištěné. Odkazy byly sice zkráceny pomocí nástroje „bit.ly“, ale i přesto přepisováním odkazů do internetového prohlížeče může dojít k překlepům a tudíž zbytečnému zdržování.

Jak bylo vysvětleno v první kapitole, kurz je rozdělen do dvou částí. Postupně se zastavíme u obou a uvedeme, co v nich učit.

Fotografie není pouhý obrázek

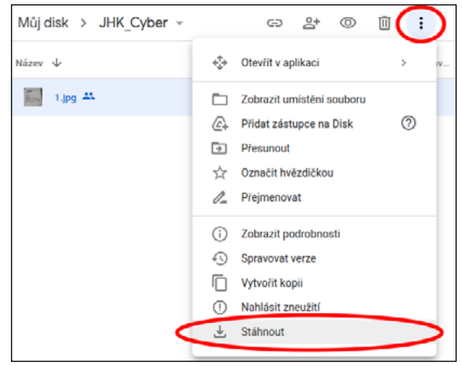
Účelem této části je zjistit, co jsou a jak vypadají metadata z fotografie a jaké všechny informace poskytují.

V této části je třeba zvládnout následující úkoly:

1. **Stáhnout si vybranou fotografii z datového úložiště.**
   Jako úložiště slouží Google Drive s veřejně dostupnou složkou „JHK_Cyber“. Zde je umístěno celkem 12 fotografií (pojmenovaných „1.jpg“ – „12.jpg“). Každá z nich byla pečlivě vybrána tak, aby obsahovala různá metadata, která se k dané fotografii vztahují. Tato metadata jsou původní a nebyla pro účely kurzu nijak účelově modifikována.

   Každou z fotografií je nutné nejprve stáhnout. Pro tento účel rozdejte žákům USB flashky, které dostanete během workshopu.

   Vybranou fotografii je nejprve nutné označit a až poté stáhnout, tak jak mají žáci uvedeno v příslušném pracovním listu. Fotografii (resp. soubor) ať žáci nepřejmenovávají.

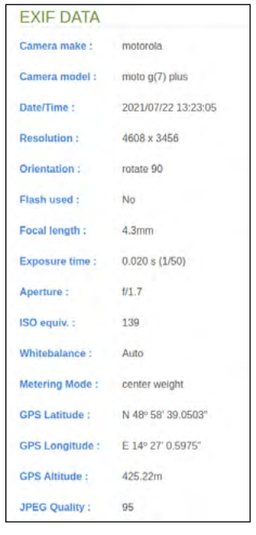


Obrázek 3: Google Drive

2. **Seznámit se s fotografií, včetně metadat prostředím online nástroje.**
   Pro tento účel slouží nástroj **https://www.verexif.com/en**

   Ten umožňuje jednak zobrazit důležitá metadata z fotografie, ale také je kompletně odstranit. Nástroj také kromě metadat zobrazuje náhled fotografie (vpravo nahoře) a (Google) mapu, na které je znázorněna lokalita, kde byla fotografie pořízena.

   V této fázi žáky vyzvete, ať Vám řeknou, kde a kdy byla fotografie pořízena.



Obrázek 4: EXIF Data z VerEXIF

3. **Použít stejný online nástroj k editaci (kompletnímu vymazání) metadat.**
   Pro tento účel slouží tlačítko „Remove Exif“

   Remove Exif

4. **Nahrát fotografie na USB flashku poskytnutou vyučujícím.**
   Aplikace poté nabídne takto pozměněnou fotografii uložit znovu pod názvem „foto_no_exif.jpg“. Požádejte žáky ať ji nahrají na zapůjčenou USB flashku a vrátí Vám ji.

Součástí tohoto pracovního listu je také diskuse ve třídě na téma, jaké údaje z metadat fotografií mohou vést k páchání trestné činnosti, proč je záhodno tyto informace před publikováním online vymazat/editovat a k čemu by potenciálně mohly tyto informace v rukou neoprávněné osoby vést.

Kyberšikana

Tato aktivita je rozdělena na dvě části:

Před začátkem se ujistěte, že je funkční audio výstup na počítačích, že studenti mají funkční sluchátka.

– Účelem první části je nejprve objasnit pojem kyberšikana a to takovým způsobem, aby se žákům dostal pod kůži a věděli přesně, co reprezentuje, a že se jedná o společenský problém chování v online světě.

Za pomoci instruktážního videa budou žáci písemně odpovídat na zadané otázky z videa a až budou mít hotovo, je nutné s nimi vést na toto téma diskusi (její délka, intenzita a míra detailu je plně ve Vaší kompetenci).

Účelem druhé části je žákům na reálném příkladu demonstrovat ničivé důsledky kyberšikany. Na videu také uvidí, že lidé se v online světě chovají jinak než ve světě skutečném, kde si začnou uvědomovat důsledky svého chování teprve poté, když jsou konfrontováni s realitou.

Stejně jako v předchozí části, budou žáci písemně odpovídat na zadané otázky z videa a až budou mít hotovo je (zde extrémně) nutné s nimi vést na toto téma diskusi (její délka, intenzita a míra detailu je plně ve Vaší kompetenci).

Doporučené pomůcky

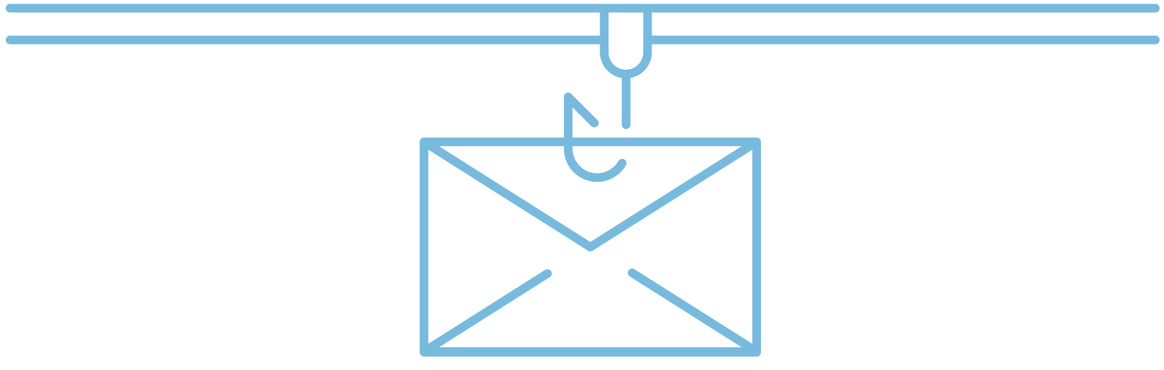
– Každý žák svůj počítač s (rychlým) připojením k internetu umožňujícím paralelně streamovat videa.
– Na PC s operačním systémem Windows bude funkční prohlížeč internetových stránek.
– Sluchátka a správně nastavený zvukový výstup.
– 20 ks USB flashek.

Pro správné zvládnutí úkolů je vhodné mít alespoň základní znalost anglického jazyka, protože pro pracovní list „Fotografie není pouhý obrázek“ jsou webové stránky v anglickém jazyce. I přesto, že je vše v pracovním listu objasněno, lze tímto předejít případným dotazům. Vysvětlete dětem, že znalost anglického jazyka je pro dnešní svět zásadní.

Pracovní listy

Přílohou tohoto materiálu jsou pracovní listy. Tyto pracovní listy jsou k dispozici v editovatelné elektronické formě, aby si je každý učitel mohl upravit, např. dle toho, co má již s žáky probráno.

Pracovní listy jsou pro základní pokrytí problematiky dva. V pracovních listech počítám s tím, že škola má k dispozici pomůcky výše uvedené.



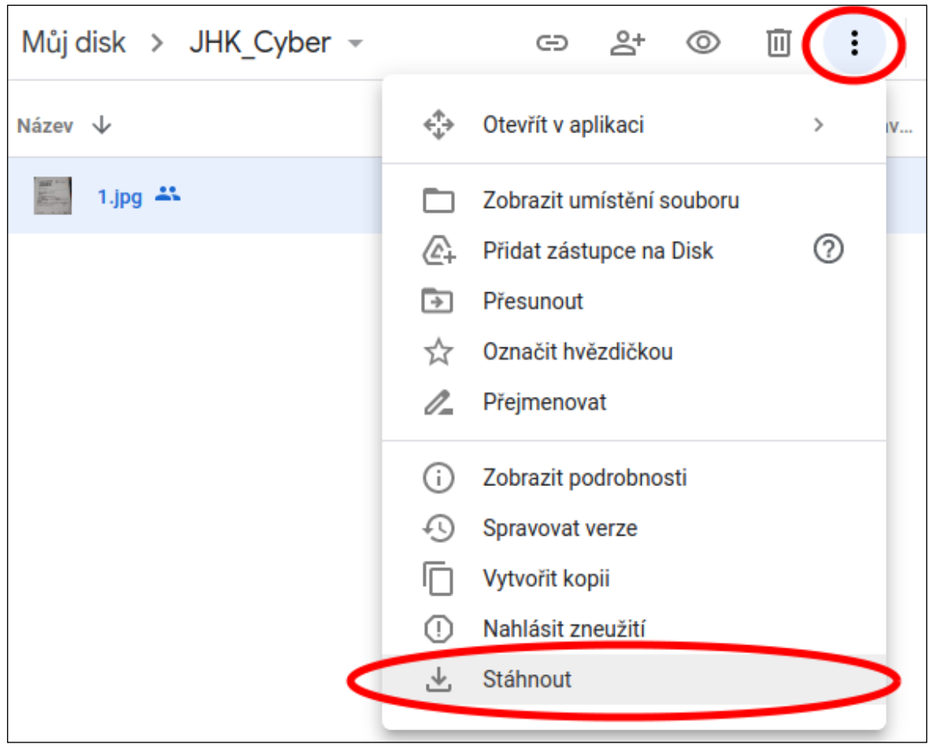
Pracovní list 1
Fotografie není pouhý obrázek

Co budeme potřebovat

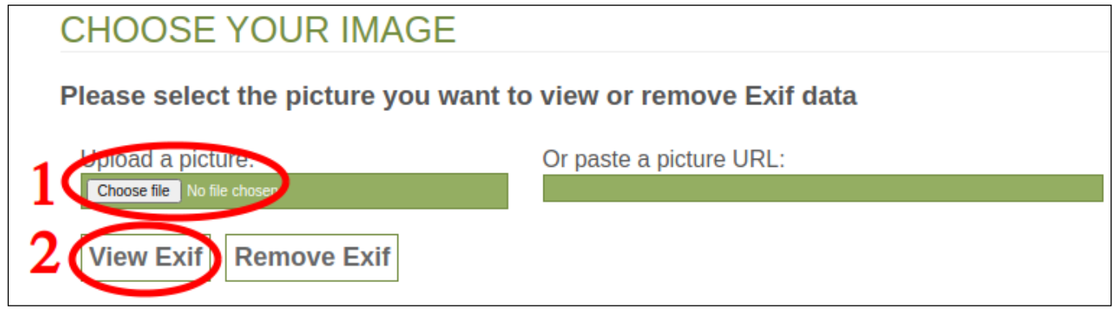
- Počítač s přístupem na internet a prohlížečem webových stránek.
- Základní znalost anglického jazyka.
- USB flashku.

A jdeme na to

1. Na nastartovaném počítači otevřete prohlížeč webových stránek a zkopírujte následující adresu do adresního řádku (případně pokud máte tento pracovní list jako soubor na počítači ve formátu PDF, přímo na odkaz níže klikněte):
   https://bit.ly/3iIDnQf
2. Zobrazí se seznam (souborů) fotografií pojmenovaných „1.jpg“ – „12.jpg“. Vyberte a označte si libovolnou fotografii a stáhněte ji na USB flashku dodanou vyučujícím (soubor nepřejmenovávejte).



3. Otevřete si nové okno v prohlížeči (nebo jej spusťte znovu, pokud jste prohlížeč zavřeli) a do adresního řádku napište následující webovou adresu (nebo jako v předchozím případě - pokud máte tento pracovní list jako soubor na počítači ve formátu PDF přímo na odkaz níže klikněte)
   https://www.verexif.com/en
4. Vyberte soubor nahraný na USB flashce a klikněte na tlačítko View Exif



5. Zobrazí se Vám kromě náhledu nahrané fotografie také tzv. EXIF data, což jsou informace o fotografii (tzv. Metadata = data o datech).
   a. Vhodným způsobem sdělte učiteli, jaká z těchto dat se podle vás dají využít k páchání trestné činnosti a proč. Zaměřte se na mapu.
6. Nyní přistoupíme k výmazu EXIF informací. Z fotografie se tak stane pouhý obrázek, bez dodatečných informací. Klikněte na tlačítko Remove Exif a soubor uložte opět na USB flashku.
7. Přesvědčte se, že nově nahraný soubor (obrázek) již neobsahuje žádné dodatečné informace (to můžete udělat více způsoby – volba je vás).
8. USB flashku s oběma soubory odevzdejte učiteli.

*Vyzkoušejte si výše uvedené na některé z vašich fotografií – např. z vašeho mobilního telefonu a to tak, že přímo z mobilního telefonu půjdete na výše uvedenou stránku **https://www.verexif.com/en** a nahrajete vámi vybranou fotku (nemusíte mít strach, webová stránka fotografie neukládá). Přesvědčte se, že pozice na mapě opravdu souhlasí s tím, kde byla fotografie původně pořízena.*

Na závěr se se svým vyučujícím pobavte, jaká metadata mohou podle Vás být potenciálně nebezpečná a mohou sloužit k páchání například Kyberšikany.

Co jste se naučili

Že fotografie není pouhý obrázek. Co všechno dodatečné informace (metadata, EXIF data) obsahují a jak tyto informace vymazat před publikováním fotografie na internet či sociální sítě.

Pracovní list 2
Kyberšikana

Co budeme potřebovat

- Počítač s přístupem na internet a prohlížečem webových stránek.
- Funkční audio výstup vyvedený na sluchátka.
- USB flashku.

A jdeme na to

První část

1. Na nastartovaném počítači otevřete prohlížeč webových stránek a zkopírujte následující adresu do adresního řádku (případně pokud máte tento pracovní list jako soubor na počítači ve formátu PDF, přímo na odkaz níže klikněte):
   https://bit.ly/3iJEy1L
2. Nasaďte si sluchátka a podívejte se na video.
   a. Ujistěte se, že ve sluchátkách slyšíte zvuk. Pokud ne a nevíte si rady, zavolejte na pomoc učitele.
3. Zodpovězte následující otázky vztahující se k tomu, co jste právě viděli. Nebojte se video si pustit opakovaně.

Jak byste vlastními slovy definovali pojem „kyberšikana“?
Jak se liší od šikany klasické a proč může být šikana v online prostoru ještě horší?

Pokud se k již probíhající kyberšikaně „nachomýtnete“, jak je správné se zachovat?
Měli byste se k ní přidat?

Pokud jste obětí kyberšikany, jak byste měli postupovat, aby Vám někdo druhý uvěřil a měli jste proti agresorům důkazy? Co je pravidlo „tři N“?

Je správné kyberšikanu nahlásit? Co je Sexting?

Druhá část

4. Znovu otevřete prohlížeč webových stránek a zkopírujte následující adresu do adresního řádku (případně pokud máte tento pracovní list jako soubor na počítači ve formátu PDF, přímo na odkaz níže klikněte):
   https://bit.ly/3yNkiC1
5. Nasaďte si sluchátka a podívejte se na video.
   Nezapomeňte kliknout na ikonu u videa :

   Zapnout zvuk

   a. Ujistěte se, že ve sluchátkách slyšíte zvuk. Pokud ne a nevíte si rady, zavolejte na pomoc učitele.
6. Zodpovězte následující otázky vztahující se k tomu, co jste právě viděli. Nebojte se video si pustit opakovaně.

Co udělala Simona a Kiana podle tebe špatně? Kde nastala zásadní chyba?

Jak se zachovali jejich spolužáci? Jaký byl rozdíl v jejich chování v online prostoru (na sociálních sítích) a ve skutečnosti?

K čemu u Kiany vedlo chování jejích spolužáků v online světě? Jakou pomoc musela vyhledat?

Na Facebooku si vždy nastavte, aby pokud Vás někdo označí na fotografii, jste tuto akci museli schválit. Pokud ji neschválíte, fotografie se neobjeví na Vašem profilu.

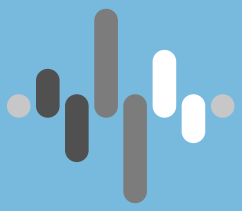
https://www.facebook.com/help/226296694047060

Dále si povolte, kdo může co přidávat do Vašich příspěvků, a že takováto označení vždy podléhají Vašemu schválení

https://www.facebook.com/help/247746261926036

Co jste se naučili

Definovat pojem kyberšikana a především mu porozumět. Základy chování na sociálních sítích a etiku při publikování a sdílení fotografií. Důsledky kyberšikany a nepřirozené chování dětí v online prostoru.



IMPULS
PRO KARIÉRU
A PRAXI