Financováno
Evropskou unií

prostor +

METODIKA

Snooper 2026

Financováno Evropskou unií

prostor +

Realizováno v rámci projektu Snooper, reg. č.: CZ.03.02.02/00/22_027/0001216

V organizaci Prostor plus o. p. s. dlouhodobě usilujeme o rovné příležitosti a spravedlivý přístup ke všem lidem, se kterými v naší práci přicházíme do kontaktu. Vnímáme také význam jazyka jako nástroje, který může rovnost podporovat, a jsme si vědomi důležitosti genderově senzitivního vyjadřování.

V tomto dokumentu pracujeme s pojmy jako „zaměstnanec“, „pracovník“, „zaměstnavatel“, „klient“ v mužském rodě. Toto jazykové řešení vychází z praktických důvodů a snahy o srozumitelnost a jednotnost textu, nikoli z neznalosti či nezájmu o genderovou rovnost.

Na tomto místě je nutné jasně říci, že použití mužského rodu není vedeno záměrem zneviditelňovat ženy ani jinak se identifikující osoby v organizaci Prostor plus.

Vážíme si práce všech odbornic i odborníků v našich službách a podporujeme všechny osoby bez ohledu na jejich pohlaví, genderovou identitu, věk, etnicitu, sociální situaci či jiné charakteristiky. Prosíme proto čtenářky i čtenáře této metodiky, aby všechna označení osob v mužském rodě chápali jako otevřená a zahrnující — tedy ve významu „zaměstnanec / zaměstnankyně“, „pracovník / pracovnice“, „klient / klientka“ a obdobně i v dalších případech.

Úvod

Kontext vzniku metodiky

Projekt Snooper vznikl jako reakce na deficit digitální gramotnosti a na nárůst problematického používání digitálních technologií mezi dětmi, mladými lidmi a jejich rodinami. Sociální služby dlouhodobě upozorňují na to, že digitální kompetence se stávají jedním z klíčových faktorů sociální inkluze: ovlivňují vzdělávací dráhu, možnost zapojit se do vrstevnické skupiny, uplatnění na trhu práce i psychické zdraví. Nedostatečné digitální dovednosti nebo rizikové užívání technologií tak mohou významně prohlubovat znevýhodnění jednotlivců i celých komunit a přispívat k jejich sociálnímu vyloučení.

Na základě těchto zjištění vznikl projekt Snooper, jehož cílem je vytvořit inovativní a prakticky využitelný program zaměřený na podporu digitální gramotnosti, prevenci digitální závislosti a rozvoj bezpečných návyků v užívání technologií. Projekt Snooper (č.p. CZ.03.02.02/00/22_027/0001216) je financován Evropskou unií z Operačního programu Zaměstnanost plus a realizován v období od 1. 9. 2023 do 28. 2. 2026. Jeho ambicí je nabídnout sociálním službám, školám i dalším aktérům metodicky ukotvený nástroj, který pomůže lépe reagovat na digitální realitu života dětí, mladých lidí a jejich blízkých. Více informací o projektu je k dispozici na www.mrsnooper.cz.

Cíl metodiky

Cílem této metodiky je vytvořit ucelený, přehledný a prakticky využitelný dokument, který popisuje podobu programu Snooper, jeho teoretické ukotvení, metodické nastavení i praktické postupy práce. Metodika slouží především pracovníkům sociálních služeb, odborníkům, školám a institucím, které se věnují práci s dětmi, mladými lidmi, jejich rodinami a komunitou v oblasti digitální gramotnosti.

Charakteristika projektu

Projekt Snooper je inovativní preventivní a vzdělávací program, který reaguje na dynamické změny v digitálním prostředí a jejich dopad na duševní zdraví a sociální stabilitu dětí, dospívajících a jejich rodin. Na rozdíl od běžných IT vzdělávání, která se zaměřují primárně na technické dovednosti, Snooper integruje technologické znalosti s metodami sociální práce a peer podpory. Součástí projektu je také vývoj hardware řešení Snoopbox, se kterým lze provést praktická cvičení přímo ve třídě.

A. Komplexní přístup k digitální realitě

Snooper vnímá online svět jako jako integrální součást každodenní reality. Projekt je charakteristický svým holistickým přístupem, který pokrývá tři klíčové oblasti:

1. Technická bezpečnost: Ochrana dat, zabezpečení účtů a prevence kyberútoků.
2. Psychosociální odolnost: Práce s emocemi v online prostoru, zvládání kyberšikany, haterských útoků a prevence digitálních závislostí (netolismu).
3. Informační gramotnost: Schopnost kriticky vyhodnocovat obsah, rozpoznávat dezinformace, hoaxy a algoritmy, které ovlivňují naše vnímání světa.

B. Unikátní metodické pilíře

Projekt je postaven na několika specifických prvcích, které jej odlišují od standardních preventivních programů:

- **SnoopBox**: Vlastní technologické zařízení, které slouží jako interaktivní prvek v hodině. Umožňuje anonymní hlasování, sběr dotazů v reálném čase a okamžitou zpětnou vazbu bez nutnosti připojení k veřejnému internetu, což zvyšuje bezpečí a otevřenost žáků.
- **Peer zapojení:** Využití peer průvodců (osob se sdílenou zkušeností), kteří vnášejí do témat autenticitu a pomáhají překonávat nedůvěru cílové skupiny k institucionálnímu vzdělávání.
- **Peer to peer dynamika :** Využívá dynamiku skupiny k posílení vnitřní motivace a srozumitelnosti sdělení.
- **Odborná garance:** Jak bylo zmíněno v teoretických východiscích, obsah je konzultován s expertem Janem Šalomounem, což zajišťuje historický a civilizační přesah nad rámec běžných „příruček o bezpečnosti“.

C. Flexibilita a adaptabilita

Metodika Snooperu je navržena jako modulární systém. Je adaptována pro různé věkové skupiny (1. stupeň ZŠ, 2. stupeň ZŠ, SŠ a G) a specifické potřeby různých školních či sociálních kolektivů. Obsah je průběžně aktualizován tak, aby reflektoval nejnovější trendy (např. vliv umělé inteligence, aktuální podvody na sociálních sítích).

D. Cíle a výstupy

Primárním cílem projektu je rozvoj komplexních digitálních kompetencí, které participujícím umožňují bezpečný a autonomní pohyb v kyberprostoru. Program směřuje k dosažení

psychosociální rovnováhy (digitálního wellbeingu) skrze efektivní využívání rozvojového potenciálu technologií při současné kultivaci seberegulačních mechanismů v offline interakcích. Projekt tak konstituuje základy zodpovědného digitálního občanství, postaveného na kritickém myšlení a etické integritě.

Cílové skupiny

Program Snooper operuje na principu hierarchizované intervence. Design programu je citlivě modulován dle vývojových fází a socio-digitálních charakteristik aktérů. Pro dosažení maximální efektivity je edukace primární cílové skupiny (Žáci) integrována do širšího rámce multi-stakeholder spolupráce, zahrnující pedagogické pracovníky a rodičovskou veřejnost. Tím je vytvořeno stabilní protektivní prostředí, které překračuje rámec jednorázové intervence.

A. Primární cílové skupiny (Žáci a studenti)

Vzdělávací moduly jsou strukturovány v soudalu s gradováním sekvencového obsahu, kde se témata cyklicky vracejí a zvyšují míru komplexity. Rozčleněné do tří sekvenčních modulů reflektujících vzdělávací stupně.

1. **Mladší školní věk (Pre - adolescence, 1. stupeň ZŠ):**
    - Zaměření: Budování základů digitální gramotnosti a prosociálního chování v kyberprostoru. Důraz je kladen na vymezení specifikace mezi privátní a veřejnou sférou a na prevenci technologického excesu
    - Metodika: Využití projektivních technik a narativní pedagogiky. Akcentována je afektivní rovina učení – rozvoj emoční inteligence (identifikace pocitů v digitální interakci) a ustavování bezpečných vazeb na dospělé autority jakožto primární protektivní faktor.
2. **Starší školní věk (Adolescence, 2. stupeň ZŠ):**
    - Zaměření: Rozvoj analyticko-kritických kompetencí. Rozbor mechanismů sociálních platforem (algoritmizace, komerční využití dat) a hloubková analýza fenoménu kybernetické agrese. Implementace principů ochrany digitální identity a správy digitálního otisku.
    - Metodika: Zkušenostní učení s využitím strukturovaného dramatu a kazuistických seminářů. Klíčovým nástrojem je SnoopBox, který umožňuje facilitovanou sebereflexi skupiny skrze depersonalizovaný sběr dat a sdílenou zkušenost.
3. **Dospívající (Pozdní adolescence, SŠ a Gymnázia):**
    - Zaměření: Komplexní problematika kognitivní bezpečnosti (dezinformace, kognitivní zkreslení, informační válka) a právní rámec digitální interakce. Strategické zacílení na digitální wellbeing a vliv sociálních architektur na duševní integritu jedince.
    - Metodika: Sokratovský dialog, analýza mediálních diskurzů a metoda peer-to-p**eer mentoringu**. Studenti jsou vedeni k roli aktivních nositelů preventivních hodnot, schopných metodicky instruovat mladší kohorty uživatelů.

B. Specifické skupiny

Program Snooper věnuje zvýšenou pozornost žákům vyžadujícím podpůrná opatření či specifické

intervenční přístupy:

Žáci ohrožení sociálním vyloučením: V tomto kontextu je rozvoj digitálních kompetencí primárně chápán jako nástroj sociální inkluze a vertikální mobility. Intervence se zaměřuje na eliminaci digitální propasti a posilování funkční gramotnosti, která brání další sociální exkluzi jedince v informační společnosti.

Žáci se SVP (Specifickými vzdělávacími potřebami): Obsah je modifikován tak, aby byla zajištěna jeho přístupnost a emoční bezpečnost. Možnost uzpůsobování pracovních materiálů umožňuje individualizaci tempa a hloubky reflexe s ohledem na specifika konkrétních potřeb.

C. Sekundární cílové skupiny (Dospělí v okolí dítěte)

Pro zajištění udržitelnosti preventivního efektu integruje program Snooper tyto další cílové skupiny skupiny:

Zákonní zástupci: Cílem intervence je posílení rodičovských kompetencí v oblasti digitální mediace. Prostřednictvím specializovaných výstupů (informační materiály, participativní workshopy) program stimuluje přechod od restriktivních strategií k aktivnímu monitoringu a otevřenému dialogu. Důraz je kladen na redukci technofobie a budování vzájemné důvěry v rámci rodinného systému.

Pedagogičtí pracovníci a školní metodici prevence: Program Snooper může pedagogům sloužit jako praktická metodická opora při práci s tématy digitální gramotnosti a prevence. Nabízí srozumitelné didaktické materiály a nástroje (např. SnoopBox), které lze flexibilně začlenit do školního vzdělávacího programu (ŠVP) podle potřeb konkrétní školy. Cílem je podpořit pedagogy v tom, aby se při řešení digitálních rizik cítili jistěji a měli k dispozici konkrétní inspiraci pro práci s třídním kolektivem.

Proč je toto rozdělení důležité?

Rozdělení cílových skupin je důležité proto, že děti a dospívající procházejí odlišnými vývojovými fázemi a setkávají se s různými riziky v digitálním prostoru. Program Snooper proto přizpůsobuje obsah věku – u mladších dětí se zaměřuje především na bezpečné návyky a základní orientaci, zatímco u dospívajících pracuje více s tématy identity, vztahů, kritického myšlení a odpovědnosti online. Zároveň program zapojuje nejen samotné žáky, ale i pedagogy a rodiče, aby kolem dítěte vzniklo srozumitelné a podpůrné prostředí. Díky tomu nejde jen o jednorázovou aktivitu, ale o dlouhodobou podporu digitální odolnosti a bezpečného fungování v online světě.

Principy programu Snooper

Principy programu Snooper vychází z etických aspektů, které kladou důraz na psychické bezpečí žáků a studentů, respektující přístup a profesionální vedení intervence. Tyto zásady určují způsob práce s kolektivem, nastavení role lektorů i následnou podporu všech zúčastněných. Díky jejich důslednému uplatňování program nepředstavuje pouze předávání informací, ale vytváří bezpečný a podpůrný prostor pro otevřený dialog o digitálním životě. Respektující přístup, zapojení peer prvků a důraz na spolupráci přispívají k tomu, že účastníci mohou sdílet své zkušenosti bez obav z

hodnocení, lépe porozumět rizikům a postupně rozvíjet zdravé a bezpečné návyky v online prostředí.

A. Respektující a nehodnotící přístup: program staví na bezpodmínečném respektu k účastníkům a jejich zkušenostem. Digitální pochybení nejsou vnímána jako selhání, ale jako příležitost k učení a společné reflexi. Snooper vytváří bezpečný prostor, ve kterém mohou děti a mladí lidé mluvit o svých zkušenostech bez obav z moralizování nebo sankcí. Součástí přístupu je také důraz na inkluzivitu, citlivou komunikaci a respekt k různorodosti účastníků.

B. Důstojnost a podpora individuální odlišnosti: program respektuje jedinečnost každého účastníka bez ohledu na jeho digitální návyky, zkušenosti či sociální zázemí. Cílem je prostředí, které umožňuje otevřenou sebereflexi a podporuje hledání funkčních strategií místo hodnocení nebo nálepkování. Pracujeme s principem „bezpečného selhání" – digitální incidenty chápeme jako situace vyžadující podporu a společné hledání řešení.

C. Důvěrnost a bezpečná práce s informacemi: psychologické bezpečí je podpořeno jasně komunikovanými pravidly důvěrnosti. Účastníci mají možnost sdílet zkušenosti anonymně, například prostřednictvím nástroje SnoopBox, což usnadňuje otevírání citlivých témat. Lektorský tým dodržuje mlčenlivost v rozsahu daném profesní etikou a právními normami; výjimkou jsou pouze situace ohrožení zdraví či bezpečí, o nichž jsou účastníci předem informováni.

D. Podpora odolnosti a práce se zdroji: Snooper nevychází z deficitního modelu, ale zaměřuje se na posilování schopností a zdrojů účastníků. Náročné digitální zkušenosti mohou být využity jako podnět k rozvoji digitální odolnosti a bezpečnějších strategií chování. Každý blok proto nabízí konkrétní možnosti podpory a navazující pomoci, včetně kontaktů na specializované služby.

E. Multidisciplinární spolupráce a péče o tým: program je realizován v tandemovém modelu, který propojuje odborné vedení s perspektivou peer pracovníků. Tato kombinace přispívá k odbornosti i přirozené komunikaci s cílovou skupinou. Součástí metodiky je také systém pravidelné reflexe a supervizní podpory, který pomáhá udržovat kvalitu práce a zároveň chrání realizátory před přetížením.

Struktura programu

A. Třífázový model intervence

Program Snooper je koncipován jako opakující se model, nikoliv jako izolovaný informační vstup. Struktura je rozdělena do tří fází, které na sebe logicky navazují v rámci formování digitální imunity.

1. Fáze: Deskripce a sebereflexe (Blok 1) – Žák identifikuje a mapuje vlastního digitálního prostředí. V této fázi dochází k vytvoření protektivního prostředí a navázání expertního spojenectví. Eliminace obav z normativního hodnocení a stimulace autentické sebereflexe, která je nezbytná pro další práci se změnou postojů.
2. Fáze: Analýza a souvislosti (Blok 2) – Studium hloubkové architektury technologií (algoritmická determinace, psychologické aspekty digitální ekonomiky a vlivové mechanismy sociálních médií). Žák identifikuje kauzální vazby mezi architekturou platformy a svými vlastními rozhodovacími procesy, čímž dochází k posílení mediální gramotnosti.
3. Fáze: Kompetence a ochrana (Blok 3) – Budování komplexní digitální imunity. Tato sekce je orientována na praktickou aplikaci technických i psychologických bariér proti manipulaci, kybernetické agresi a sociálnímu inženýrství.Žák si osvojuje funkční algoritmy chování (tzv. "digitální brnění"), které mu umožňují aktivně chránit svou integritu v kyberprostoru.

B. Metodické pilíře práce ve třídě

Každé setkání v rámci koncepce Snooper kombinuje čtyři základní prvky:

Interaktivita (SnoopBox): Implementace anonymizačních technologií vytváří bezpečný komunikační kanál, který eliminuje identifikaci jednotlivce a podporuje autentické vyjádření postojů bez vnějších bariér. Tento mechanismus efektivně eliminuje fenomén sociální desirability (tendence k sebeprezentaci v souladu s očekáváním okolí), čímž facilituje získávání objektivních dat a autentických výpovědí o reálném digitálním chování cílové skupiny.

Zkušenostní učení (Storytelling): Teoretické rámce jsou kontextualizovaný pomocí strukturovaných narativů. Využití expertně konzultovaných kazuistik (např. z oblasti kybernetické agresivity a stalkingu) umožňuje emocionální ukotvení látky a přenos abstraktních rizik do sféry konkrétní žité reality.

Peer-to-peer dynamika: Zapojení peer-průvodce plní funkci expertního validátoru. Zatímco lektor garantuje odbornou integritu (vertikální rovina), peer-průvodce zajišťuje komunikační relevanci a autenticitu (horizontální rovina). Tato synergie zvyšuje míru identifikace adolescentů s tématem a podporuje internalizaci preventivních postojů.

Reflektivní smyčka: Každá sekvenční jednotka je uzavřena procesem formativní evaluace (metoda *exit ticket*). Tato zpětnovazební struktura umožňuje lektorovi provádět průběžnou diagnostiku dynamiky skupiny a provádět kurikulární modifikace v souladu s aktuálními potřebami a psychosociálním stavem konkrétního kolektivu.

C. Časový rámec a kontinuita

Metodika programu Snooper fixuje optimální časovou prodlevu mezi jednotlivými moduly v rozmezí 4–8 týdnů. Tato periodizace je strategicky zvolena pro zajištění maximální efektivity učebního procesu a stability postojových změn.

Prostor pro dozrání tématu: Časový odstup mezi jednotlivými setkáními umožňuje účastníkům lépe vstřebat nové informace a promyslet je ve vztahu k vlastnímu chování v online prostředí. Postupně tak dochází k většímu uvědomění si vlastních návyků a emocí spojených s digitálním světem.

Uplatnění v praxi: Mezifáze mezi bloky slouží k tomu, aby si žáci mohli nové strategie vyzkoušet v běžném životě – například upravit nastavení soukromí nebo zavést drobné prvky digitální hygieny. Získané poznatky se tak postupně proměňují v konkrétní dovednosti.

Budování důvěry a kontinuity: Opakovaná přítomnost stejného lektorského tandemu (lektor a peer-průvodce) podporuje pocit bezpečí a důvěry. Díky tomu se skupina může postupně otevírat i náročnějším tématům, která vyžadují větší osobní sdílení.

D. Širší dopady

Design programu Snooper je koncipován jako víceúrovňová intervence, jejíž dopad přesahuje samotnou práci se skupinou a zasahuje i širší sociální prostředí účastníků. Edukační materiály a výstupy podporují přenos témat do rodin a otevírají dialog mezi dětmi a jejich zákonnými zástupci, čímž posilují preventivní roli rodiny v digitální oblasti. Současně program poskytuje školním metodikům prevence anonymizované a agregované výstupy z diagnostických nástrojů, které pomáhají lépe porozumět dynamice kolektivu v online prostoru a slouží jako podklad pro další práci se třídou v rámci školního preventivního programu.

Přehled tematických bloků

Jednotlivé tematické moduly jsou navržené tak, aby mohly fungovat samostatně, ale zároveň na sebe přirozeně navazují a vycházejí z toho, co už žáci znají a sami zažívají v digitálním světě. Obsah je vždy přizpůsoben věku a úrovni porozumění skupiny – jinak je pojat pro žáky základních škol a jinak pro středoškoláky, aby byl srozumitelný, smysluplný a skutečně využitelný v praxi.

BLOK 1: Online svět a já

Úvodní část bloku slouží k naladění skupiny a zjištění, jak žáci digitální svět sami vnímají a používají. Místo strašení riziky pracujeme s pozitivním přístupem – společně mapujeme, co jim technologie přinášejí, jaké mají zkušenosti a kde sami vidí výhody i limity. Tento způsob práce podporuje otevřenost, buduje důvěru a snižuje přirozený odpor k preventivním tématům.

SMART cíle:

- Žák dokáže pojmenovat přínosy i rizika internetu ve vztahu k vlastnímu životu a bezpečí.
- Na základě videoukázek rozpozná motivy jednání aktérů a navrhne vhodné způsoby obrany proti online rizikům.
- Uvede alespoň dva zdroje krizové pomoci (např. Linka bezpečí) a rozumí tomu, jak fungují.
- Umí se základně orientovat ve svém digitálním otisku a uvědomuje si, jaké informace o sobě online zanechává.
- Rozpozná roli technologických firem, algoritmů a vliv umělé inteligence na online prostředí a rozhodování uživatelů.

Klíčová témata: digitální rovnováha, online agrese, digitální hygiena, algoritmy a data, digitální stopa, krizová pomoc.

Metodika a SnoopBox: nástroj SnoopBox slouží jako anonymní způsob sběru odpovědí a názorů žáků. Pomáhá lektorům lépe porozumět tomu, jak se třída v online prostoru cítí a s čím se setkává, a umožňuje přizpůsobit další práci aktuálním potřebám skupiny.

Výstup pro žáka: Žák lépe rozumí své digitální zkušenosti, dokáže ji zasadit do kontextu vrstevníků a ví, kde hledat podporu, pokud se v online prostředí dostane do náročné situace.

BLOK 2: Jak se chováme na sítích

Tento modul se zaměřuje na to, jak digitální prostředí ovlivňuje naše vnímání, emoce i chování – často způsobem, který si ani neuvědomujeme. Žáci se seznamují s tím, jak fungují algoritmy, personalizace obsahu nebo online marketing, a učí se rozpoznávat situace, kdy s nimi digitální prostředí cíleně pracuje, například prostřednictvím reklamy, influencerů nebo manipulativního obsahu.

SMART cíle:

- Žák rozumí tomu, co je digitální otisk, a dokáže vysvětlit, jak může současná online aktivita

ovlivnit jeho budoucí studijní nebo pracovní příležitosti.
- Rozpozná manipulativní prvky v online obsahu, včetně klamavé reklamy a problematických forem influencerského marketingu.
- Chápe, jak algoritmy vybírají obsah, a dokáže kriticky uvažovat o fenoménu informačních bublin a personalizace na základě uživatelských dat.

Klíčová témata: digitální identita, dezinformace a hoaxy, manipulativní obsah, algoritmy a personalizace.

Metodika a SnoopBox: v rámci aktivity je do skupiny cíleně zařazen simulovaný hoax, který slouží jako modelová situace pro sledování toho, jak se informace šíří a jak na ni žáci reagují. Prostřednictvím anonymního hlasování v nástroji SnoopBox se sbírá zpětná vazba, která následně slouží k společné reflexi, ověřování informací a rozpoznávání emocionálních apelů v textu.

Výstup pro žáka: žák dokáže využít základní principy ověřování faktů a kriticky posuzovat důvěryhodnost informací, zejména v situacích, kdy se obsah rychle šíří online.

BLOK 3: Kyberbezpečnost

Tento blok navazuje na předchozí témata a zaměřuje se na praktickou digitální sebeobranu. Žáci se učí, jak rozpoznat nejčastější online hrozby a jak kombinovat technická opatření s kritickým přemýšlením o vlastním chování. Důraz je kladen na to, že bezpečnost v online prostředí nestojí jen na technologiích, ale i na schopnosti uživatele včas odhalit manipulaci nebo podezřelé situace.

SMART cíle:

- Žák rozpozná typické znaky phishingových zpráv, jako je časový nátlak, neobvyklý jazyk nebo podezřelé odkazy.
- Umí vytvořit bezpečné a zapamatovatelné heslo a rozumí principům dvoufázovému ověřování.
- Rozlišuje základní typy škodlivého softwaru (malware, spyware, ransomware) a chápe jejich možné dopady.

Klíčová témata: phishing a další formy sociotechnických útoků, bezpečná autentizace, digitální hygiena, práce s rizikem a online toxicitou.

Metodika a SnoopBox: aktivita probíhá formou interaktivní simulace, ve které žáci analyzují ukázky SMS a emailů a hledají varovné signály možného útoku. Pomocí anonymního hlasování v nástroji SnoopBox lze sledovat, jak si třída vede, a okamžitě společně reflektovat správná řešení.

Výstup pro žáka: Žák dokáže využít základní strategie digitální sebeobrany – kombinuje bezpečné technické nastavení s kritickým uvažováním a lépe rozpoznává situace, které mohou ohrozit jeho bezpečí online.

Propojení bloků a vazba na RVP

Třífázový model programu Snooper navazuje na rozvoj digitálních kompetencí definovaných v revidovaném RVP. Prostřednictvím praktických aktivit podporuje informatické myšlení, bezpečné chování online i etickou práci s digitálním obsahem.

Práce s technologiemi a systémy:
Žáci se učí základním principům bezpečného používání digitálních nástrojů a porozumění tomu, jak technologie fungují v každodenním životě.

Kritická práce s informacemi a daty:
Program rozvíjí schopnost ověřovat informace, rozpoznávat dezinformace a chápat, jak algoritmy ovlivňují to, jaký obsah se k uživatelům dostává. Žáci si osvojují analytické přístupy, které jim pomáhají lépe se orientovat v online prostoru.

Etika a autorská práva:
Součástí je reflexe odpovědného sdílení obsahu, respekt k duševnímu vlastnictví a porozumění tomu, jaké dopady může mít digitální stopa na budoucnost jednotlivce.

Digitální wellbeing a ochrana identity:
Program podporuje strategie, které pomáhají udržovat rovnováhu mezi online a offline světem, chránit osobní údaje a předcházet přetížení nebo manipulativním vlivům digitálního prostředí.

Doporučený postup realizace

Efektivita programu Snooper je založena na důsledném plánování před samotnou realizací a zajištění bezpečného vzdělávacího prostředí, které podporuje otevřenou interakci. Metodický protokol realizace je strukturován do čtyř sekvenčních fází.

Fáze realizace programu Snooper

1. Fáze: Příprava před vstupem do třídy

Tato fáze probíhá ještě před samotnou realizací programu a zaměřuje se na organizační a metodickou přípravu. Lektorský tým tvoří odborný garant a peer-průvodce, kteří si předem vyjasňují své role a způsob spolupráce. Součástí je kontrola techniky (funkčnost SnoopBoxu, audiovizuální materiály) a seznámení se s prostředím školy. Ve spolupráci s pedagogy probíhá také základní orientace v dynamice třídy a případných rizicích, aby bylo možné přizpůsobit obsah aktuální situaci.

2. Fáze: Úvod a nastavení bezpečného rámce

Na začátku programu je cílem vytvořit bezpečné a otevřené prostředí. Peer-průvodce pomáhá navázat partnerský kontakt a snižuje odstup mezi lektorem a žáky. Společně se nastavují pravidla komunikace – respekt, důvěrnost sdílení, dobrovolnost zapojení a možnost říct „stop“. Žáci jsou také seznámeni s fungováním nástroje SnoopBox a s principem anonymity, která podporuje otevřené vyjadřování.

3. Fáze: Práce s tématy a modelové situace

Hlavní část programu kombinuje krátké informační vstupy s aktivními metodami práce. Lektoři využívají videa, diskusi i anonymní hlasování přes SnoopBox, aby mohli průběžně reagovat na potřeby skupiny. Žáci pracují s modelovými situacemi z online prostředí (např. kyberšikana, manipulace nebo phishing), hledají řešení a společně reflektují jejich dopady. Lektor a peer-průvodce doplňují odborný kontext a praktické tipy pro bezpečné chování.

4. Fáze: Uzavření a navazující podpora

Závěr programu slouží k reflexi a ukotvení toho, co si žáci odnášejí. Účastníci mají prostor pojmenovat nové poznatky a strategie, které chtějí vyzkoušet v praxi. Lektoři reagují na případné dotazy a v případě potřeby nabízejí individuální podporu. Součástí je také předání kontaktů na krizové a poradenské služby. Po skončení probíhá krátká interní reflexe lektorského tandemu, která pomáhá průběžně zlepšovat kvalitu programu.

Možnosti adaptace programu: Program Snooper je navržen jako modulární systém, který lze přizpůsobit věku, zkušenostem i aktuálním potřebám konkrétní skupiny. Flexibilita programu je možná vždy při zachování jeho základních etických a preventivních cílů.

Popis jednotlivých bloků

Blok 1: Online svět a já

Obsahová náplň bloku je orientována na introspekci vzorců chování v kyberprostoru a na rozvoj schopnosti včasné detekce vztahových a bezpečnostních rizik v digitálním prostředí.

Základní přehled

- **Cílová skupina:** ZŠ (adaptovatelné pro 1. i 2. stupeň) a SŠ.
- **Časová dotace:** 90 minut (2 vyučovací hodiny).
- **Klíčové pojmy:** digitální stopa, algoritmy sociálních sítí,kyberšikana, hater, stalker, harasser, pomoc.

Harmonogram bloku (90 min)

1. Úvod a nastavení (10 min)

- Představení lektorského týmu (včetně role peera).
- Nastavení pravidel bezpečného prostoru (mlčenlivost, stop karta).
- Instruktáž k anonymnímu hlasování přes SnoopBox.

2. Moje digitální stopa a sebereflexe – Ice-breaker

Sběr dat prostřednictvím anonymizovaného rozhraní SnoopBox se zaměřením na ranní digitální rituály a celkovou časovou dotaci strávenou v online prostředí. Cíl: Objektivizace individuálního digitálního habitu participantů při zachování plné anonymity. Peer-průvodce následně realizuje subjektivní korelaci s fyziologickými dopady (narušení cirkadiánního rytmu), čímž téma demystifikuje a přibližuje žité realitě cílové skupiny.

- **Aktivita:** Žáci na SnoopBoxu odpovídají na otázky typu: „Co jsi udělal jako první věc po probuzení?“ nebo „Kolik hodin denně jsi online?“.
- **Cíl:** Zviditelnit téma bez nutnosti veřejného přiznání. Peer doplňuje svou zkušenost s tím, jak digitální svět ovlivňuje jeho biorytmus.
- Temporální dotace 15 minut

3. Pozitiva vs. Negativa online světa

- **Skupinová práce:** Žáci dělí pojmy do dvou sloupců.
- **Pozitiva:** Komunikace, vzdělávání, podpora, zábava.
- **Negativa:** Kyberkriminalita, ztráta soukromí, srovnávání se, dezinformace.
- **Reflexe:** Diskuze o tom, jak proměnit negativa v bezpečnější zkušenost.
- Temporální dotace 15 minut

4. Haters vs. Stalkers – Práce s videem (25 min)

- **Projekce:** Pustíme dvě zásadní videa připravená pro Snooper.

- **Analýza:** Společné hledání rozdílů.
    - *Hater:* Agresivní komentování, snaha ponížit, často veřejné.
    - *Stalker:* Pronásledování, slídění, neustálý kontakt, narušování soukromí.
- **Role peera:** Peer sdílí, jak se s podobným chováním setkal a jaký to mělo dopad na jeho psychiku.

5. Co dělat, když... (15 min)

- Modelové situace: „Někdo mi vyhrožuje“, „Někdo po mně chce peníze“, „Někdo sdílí mou fotku bez souhlasu“.
- Lektor učí konkrétní kroky: **Stop – PrintScreen – Blokovat – Nahlásit – Svěřit se.**

6. Závěr a zdroje pomoci (5 min)

- Představení kontaktů: Linka bezpečí (116 111), E-bezpečí, Nepanikař.
- Zodpovězení anonymních dotazů z „klobouku“.

Výstupy a materiály pro 1. blok

- **Pracovní list:** Tabulka Pozitiva/Negativa a seznam „Co dělám, když jsem venku vs. online“.
- **Kvíz pro SnoopBox:** 5 otázek na téma rozpoznání rizikového chování.
- **Podklad pro rodiče:** Shrnutí tématu kyberšikany a tipy, jak reagovat, když se dítě doma svěří s negativní online zkušeností.

Blok 2: Jak se chováme na sítích

Tento blok je zaměřen na rozvoj pokročilé digitální a mediální gramotnosti. Kritické myšlení, pochopení principů sociálních sítí a uvědomění si právních a sociálních dopadů našeho chování.

Základní přehled

- **Cílová skupina:** 2. stupeň ZŠ a SŠ (přizpůsobení hloubky diskuse).
- **Časová dotace:** 90 minut (2 vyučovací hodiny).
- **Klíčové pojmy:** Digitální stopa, algoritmy, sociální bubliny, dezinformace, klamavá reklama, falešné profily.

Harmonogram bloku (90 min)

1. Rekapitulace a naladění (10 min)

- Krátké ohlédnutí za 1. blokem: „Změnil někdo z vás něco ve svém online nastavení?“
- Aktivace přes SnoopBox: „Kterou sociální síť jsi dnes otevřel jako první?“

2. Digitální stopa a identita (20 min)

- **Výklad:** Vysvětlení, že internet nezapomíná. Vše, co lajkujeme, sdílíme nebo komentujeme, o nás vytváří obraz pro budoucí zaměstnavatele, školy i algoritmy.
- **Aktivita:** „Vygooglete si svého oblíbeného influencera/celebritu – co o něm víme jen z

internetu? Co byste o sobě nechtěli najít za 10 let?“

- **Role peera:** Sdílí příklad (vlastní nebo ze svého okolí), kdy starý komentář nebo fotka způsobily komplikace v reálném životě.

3. Mechanismus sítí: Algoritmy a bubliny (20 min)

- **Teorie:** Proč vidíme jiný obsah než náš soused v lavici? Vysvětlení principu potvrzovacího zkreslení (confirmation bias).
- **Diskuse:** Jak sítě vydělávají na naší pozornosti? (Dopaminové smyčky).
- **Cíl:** Pochopení, že obsah na sítích není objektivní realita, ale personalizovaný výběr.

4. Pravda nebo Fake? (20 min)

- **Práce s příklady (dle podkladů Jana Šalomouna):** Analýza konkrétních zpráv (např. o očkování, prezidentovi či událostech v ČR).
- **Interaktivní kvíz:** Žáci na SnoopBoxu určují, zda je zobrazený post:
  - **Hoax:** Podvodná, poplašná zpráva.
  - **Dezinformace:** Záměrně šířená lež.
  - **Klamavá reklama:** Snaha prodat produkt skrytě.
- **Metoda ověřování:** Ukázka, jak si informaci prověřit (reverzní vyhledávání obrázků, ověření zdroje).

5. Právní rámec a etika (15 min)

- **Teorie:** Co už není „jen legrace“? Pomluva, neoprávněné nakládání s osobními údaji, schvalování trestného činu.
- **Modelové situace:** Sdílení fotky spolužáka bez souhlasu, vytvoření falešného profilu učitele.
- **Cíl:** Uvědomění si, že za obrazovkou platí stejné zákony jako v reálném světě.

6. Reflexe a Exit Ticket (5 min)

- Otázka na závěr: „Jedna věc, na kterou si od teď dám na sítích pozor?“
- Rozdání informačních materiálů.

Výstupy a materiály pro 2. blok

- **Pracovní list:** Seznam otázek pro kritické hodnocení příspěvku (Kdo to napsal? Proč? Má to zdroj?).
- **Kvíz pro SnoopBox:** „Najdi 3 chyby v tomto příspěvku“ (zaměřeno na manipulativní techniky).
- **Podklad pro rodiče:** Téma: „Jak mluvit s dětmi o tom, co vidí na sítích“ a vysvětlení pojmu digitální stopa.

Blok 3: Kyberbezpečnost

Tento blok se zaměřuje na rozpoznávání moderních forem kybernetických útoků a na praktické kroky, jak jim předcházet. Pracuje s konceptem, že digitální budoucnost znamená větší zodpovědnost za vlastní zabezpečení.

Základní přehled

- **Cílová skupina:** ZŠ i SŠ (pro SŠ kladen větší důraz na bankovní podvody a malware).
- **Časová dotace:** 90 minut (2 vyučovací hodiny).
- **Klíčové pojmy:** Phishing, Smishing, Vishing, Malware, Dvoufázové ověření (2FA), Digitální hygiena, Netolismus.

Harmonogram bloku (90 min)

1. Budoucnost a digitalizace (10 min)

- Úvodní úvaha: „Všechno kolem nás se digitalizuje – peníze, doklady, známky ve škole. Co se stane, když k těmto datům získá přístup někdo cizí?“
- **Cíl:** Motivace žáků k ochraně svých účtů jako k ochraně vlastního majetku.

2. Anatomie útoku: Phishing, Smishing, Vishing (25 min)

- **Výklad:** Vysvětlení rozdílů (E-mail vs. SMS vs. Telefonát).
- **Interaktivní cvičení:** Ukázky reálných podvodných zpráv (např. falešná Česká pošta, přeplatky na daních, zablokovaný bankovní účet).
- **Práce se SnoopBoxem:** Žáci identifikují „podezřelé znaky“ v ukázkách:
    - Divná URL adresa (např. ceskaposta-kos.top).
    - Časový nátlak („Udělej to do 12 hodin, jinak...“).
    - Špatná čeština nebo neobvyklé oslovení.

3. Malware a nebezpečné výzvy (15 min)

- **Teorie:** Co jsou viry, spyware a ransomware (zašifrování dat za výkupné).
- **Diskuse:** Nebezpečné výzvy (challenges) na TikToku a jiných sítích – jak rozpoznat, kdy jde o zdraví.
- **Role peera:** Sdílení zkušenosti s „kliknutím na špatný odkaz“ a následky, které to mělo (např. ztráta herního účtu).

4. Workshop: Desatero bezpečného chování (25 min) Společné procházení a praktické zkoušení 12 bodů desatera Snooper:

1. **Silná hesla:** Jak vytvořit heslo, které si pamatuji, ale hacker ho neuhodne (metoda vět).
2. **Dvoufázové ověření (2FA):** Proč je kód v SMS nebo aplikaci nejdůležitější zámek.
3. **Sdílení citlivých údajů:** Co nikdy neposílat (fotky dokladů, platební karty).
4. **Aktualizace:** Proč neodkládat aktualizaci telefonu a aplikací.

5. Co dělat při úspěšném útoku? (10 min)

- Okamžité kroky: Změna hesel, odhlášení zařízení, kontaktování banky/policie/rodičů.
- **Cíl:** Snížit pocit studu – „Každý dělá chyby, důležité je jednat rychle.“

6. Reflexe a závěr celého cyklu (5 min)

- Krátké video „Jak mluvit na internetu“.
- Finální anonymní dotazník přes SnoopBox.

Výstupy a materiály pro 3. blok

- **Pracovní list:** Tahák „Poznej podvodníka“ a prostor pro návrh vlastního bezpečného hesla (bez jeho zapsání).
- **Kvíz pro SnoopBox:** „Kyber-detektiv“ – série 5 zpráv, u kterých Žáci určují, zda jsou bezpečné.
- **Podklad pro rodiče:** „Digitální bezpečí rodiny“ – jak si nastavit dvoufázové ověření v rodinných účtech a na co si dát pozor při online nákupech.

Blok 1: Online svět a já

Cíl: Přechod od "vím, že tam jsem moc" k "vím, jak si nastavit hranice".

Praktické úpravy:

- Místo teorie o dopadech (bod 2): Peer ukáže přímo v nastavení telefonu položku "Čas u obrazovky" / "Digitální rovnováha". Žáci se dívají na své nejčastější aplikace a "počet odemknutí".
- Praktická rada "Spánková hygiena": Konkrétní tip – nastavení automatického filtru modrého světla (Night Shift) 2 hodiny před spaním a pravidlo "nabíječka v předsíni, ne u postele".
- Aktivita v bodě 5 (Jak reagovat): Nejen říct "nahlásit", ale ukázat Live demo: Kde přesně je v aplikaci Instagram/TikTok tlačítko "Nahlásit" a co se stane poté (ukázka, že je to anonymní).

Blok 2: Jak se chováme na sítích

Cíl: Od "pozor na fotky" k "ovládám svůj algoritmus".

Praktické rady:

- Hacking algoritmu (bod 3): Praktický návod, jak "převychovat" svůj TikTok/Reels. Pokud mi padá toxický obsah, musím: 1. Dlouze podržet video -> "Nezajímá mě". 2. Vyhledat 5 videí s tématem, které mě baví (hobby, sport), a dokoukat je do konce. Tím aktivně měním, co mi sítě servírují.
- Digitální stopa v praxi (bod 2): "Test babičkou/šéfem". Předtím, než něco nasdílím, položím si otázku: *„Chtěl bych, aby tohle viděla moje babička nebo budoucí zaměstnavatel na pohovoru?“* Pokud ne, post nepatří ven.

- Ověřování (bod 4): Praktický trik SIFT:
    1. Stop (Zastav se).
    2. Investigate the source (Prověř zdroj – má web sekci "O nás"?).
    3. Find better coverage (Najdi zprávu jinde – píší o tom i velká média?).
    4. Trace back to context (Najdi původní fotku přes Google Lens).

Blok 3: Kyberbezpečnost

Cíl: Od "neklikejte na odkazy" k "mám neprůstřelný digitální hrad".

Praktické rady:

- Tvorba hesla (bod 4): Zapomeňte na "heslo123". Použijeme metodu "Věta do mlejnce".
    1. Věta: *„Můj pes Alík žere granule 2x denně.“* -> Heslo: `MpAzg2xd!` (Extrémně silné, snadno zapamatovatelné).
- 2FA (Dvoufázové ověření): Praktický úkol – kdo nemá zapnuté 2FA na svém zařízení nebo aplikacích, zkusí si ho pod vedením lektora zapnout. Vysvětlení, proč je autentizační aplikace (Google/Microsoft Authenticator) lepší než SMS.
- Kontrola úniků: Ukázka webu `haveibeenpwned.com`. Žáci si mohou (dobrovolně) zadat svůj e-mail a zjistit, zda jim někdy v minulosti uniklo heslo. To je největší "eye-opener".
- Phishingový detektor (bod 2): Tři zlatá pravidla:
    1. Stresuje mě ta zpráva? (Časový nátlak).
    2. Chce po mně údaje/peníze?
    3. Je odkaz podezřelý? (Najedu na něj myší/podržím prst, abych viděl skutečnou adresu).

Doplněné výstupy pro rodiče

Místo obecného shrnutí jim dejte "Patero pro klidný spánek":

1. Nainstalujte si domů správce hesel (např. Bitwarden).
2. Nastavte dětem na YouTube "Omezený režim".
3. Domluvte si "Digitální blackout" (např. neděle bez mobilů pro celou rodinu).
4. Reagujte na chybu dítěte (např. kliknutí na link) s klidem: *„Děkuju, že jsi mi to řekl, vyřešíme to spolu.“* (Strach z trestu je hlavní důvod, proč děti problémy v kyberprostoru tají)

Peer průvodce je definován jako rovnocenný partner v multidisciplinárním týmu, jehož expertní vědomosti jsou ukotveny v autentické prožité zkušenosti. Nejedná se o pouhého vrstevníka, ale o specialistu na proces zotavení, který vykazuje vysokou míru sebereflexe a schopnost řízeného sdílení. Jeho role spočívá v destigmatizaci nepříznivých životních osudů a v poskytování naděje skrze modelování úspěšné adaptace.

Koncepční vymezení role peer průvodce

- Základním nástrojem peer pracovníka je jeho vlastní příběh. Namísto teoretických rad používá sdílení osobní zkušenosti k navázání autentického kontaktu. Tím se eliminuje přirozený odpor ke „všemocným" autoritám a vytváří se bezpečné prostředí pro spolupráci. Důvěra se zde nestaví na titulu, ale na společné zkušenosti.
- Svojí přítomností v kolektivu zosobňuje koncept pozitivního vzoru. Demonstruje, že krizové situace v digitálním prostoru jsou řešitelné a nemusí mít fatální dopad na integritu jedince. Působí jako živý důkaz funkčních mechanismů, čímž u žáků posiluje individuální i skupinovou odolnost vůči kybernetickým rizikům.
- Představuje komunikační uzel, jenž zasazuje odborná doporučení do reálného prostředí a kultury současné generace. Technické a bezpečnostní postupy (např. kybernetickou hygienu) interpretuje skrze optiku reálných potřeb a digitálního chování mládeže. Díky znalosti specifického slangu a dynamiky online prostředí zajišťuje vysokou míru srozumitelnosti a přijatelnosti preventivních opatření.

Klíčové charakteristiky peera

1. Autenticita: Peer nemluví v naučených frázích. Jeho nejsilnějším nástrojem je upřímnost a schopnost říct: „Tohle jsem zažil taky a takhle jsem se u toho cítil."
2. Nosič naděje: Svou přítomností ve třídě vysílá signál, že online chyby nejsou konečné a že existuje cesta k nápravě a bezpečí.
3. Most mezi světy: Dokáže přeložit odborná doporučení (např. o zabezpečení účtů) do jazyka, kterému žáci věří, protože vychází z reálných potřeb jejich generace.

Role peera v metodice Snooper

1. Mechanismy zapojení peera (Peer-to-Peer edukace)

V odborném kontextu peer nevypráví pouze „příběhy", ale využívá metodu storytellingu jako nástroje pro budování kognitivní empatie. Jeho role se v jednotlivých blocích transformuje následovně:

- Blok: Online svět a já
  - Lektor: Definuje digitální identitu a mechanismy algoritmů.
  - Peer: Skrze sebereflektivní narativ popisuje proces utváření vlastního digitálního obrazu. Zaměřuje se na psychologické aspekty, jako je FOMO (*Fear of Missing Out*)

nebo tlak na sebeprezentaci, čímž teoretický koncept „identity“ ukotvuje v žité realitě.

- Blok: Jak se chováme na sítích
  - Lektor: Klasifikuje formy kyberagrese a netikety.
  - Peer: Působí jako moderátor postojů. Sdílením osobní zkušenosti s dynamikou sociálních skupin v online prostoru pomáhá cílové skupině dekódovat jemné nuance mezi humorem a kyberšikanou.
- Blok: Kyberbezpečnost
  - Lektor: Vysvětluje technické principy hrozeb (např. sociální inženýrství, phishing).
  - Peer: Realizuje tzv. viktimologickou sondu. Popisuje subjektivní prožívání v krizové situaci (stres, pocit selhání) a demonstruje copingové strategie (strategie zvládání) – tedy konkrétní kroky k eliminaci následků a obnovení digitálního bezpečí.

2. Didaktické přínosy synergie lektora a peera

- Integrace kognitivní a afektivní složky: Propojení faktických informací (lektor) s prací s postoji a emocemi (peer) vytváří komplexní učební prožitek.
- Katalyzátor identifikace: Díky věkové blízkosti peer odbourává komunikační bariéry a zvyšuje důvěryhodnost sdělovaného obsahu.
- Narativní ukotvení: Využití storytellingu zasazuje abstraktní technické pojmy do reálného sociokulturního kontextu cílové skupiny.
- Zvýšení retence informací: Propojení expertního výkladu s autentickou prožitkovou reflexí vede k hlubšímu a trvalejšímu osvojení znalostí.
- Aktivizace postojů: Model neslouží pouze k předání dat, ale motivuje k reálné změně vzorců chování v digitálním prostředí.

Rozpracuji podrobně kapitolu 5.2 Role peerů v programu Snooper. Text je koncipován tak, aby přesně definoval, jakým způsobem peer průvodce vstupuje do interakce s žáky a jak doplňuje odbornou část lektora.

5.2 Role peerů v programu Snooper

Role peera v projektu Snooper není pomocná, nýbrž klíčová pro dosažení autenticity a důvěryhodnosti celého programu. Peer průvodce plní čtyři základní funkce, které se prolínají všemi třemi bloky metodiky.

1. Sdílení příběhu (Storytelling)

Sdílení vlastního příběhu je nejsilnějším nástrojem peera. Nejde o pouhé vyprávění historie, ale o cílený metodický vstup:

- Autenticita: Peer popisuje reálné situace (např. ztrátu kontroly nad časem na sítích nebo reakci na kyberšikanu). Tím zhmotňuje teoretická rizika do podoby skutečného lidského prožitku.

- Struktura vstupu: Příběh má vždy tři části: popis problému – emoce s ním spojené – cesta k řešení (zotavení). Tento model ukazuje žákům, že z každé situace existuje východisko.
- Hranice: Peer je vycvičen sdílet jen tolik, aby to pomohlo preventivnímu účelu, ale zároveň aby si zachoval své bezpečí a soukromí.

2. Validace pocitů žáků

V digitálním stresu žák podléhá zkreslení situací. Peer metodicky postupuje tak, že mění tragické příběhy na řešitelný technický problém. Peer zde působí jako emoční stabilizátor:

- Normalizace: Když žák skrze SnoopBox přizná, že naletěl na podvod, peer reaguje první: „Chápu tě, mně se stalo něco podobného a cítil jsem se tehdy podvedený a hloupý. Je důležité vědět, že to není tvoje vina, ale vina útočníka."
- Snížení bariér: Díky peerovi žáci vidí, že i dospělý/starší člověk může udělat chybu, což jim dodává odvahu o svých problémech mluvit otevřeně.

3. Demonstrace nástrojů

Teoretické rady o bezpečnosti získávají na váze, pokud je žáci vidí v praxi u někoho, koho respektují jako vrstevnickou autoritu:

- Praktické ukázky: Peer ukazuje, jak má on sám nastavené soukromí na Instagramu nebo jakou aplikaci používá pro dvoufázové ověření.
- Živý příklad: Pokud lektor mluví o digitálním wellbeingu, peer může demonstrovat, jak si v telefonu nastavit limity pro konkrétní aplikace a proč to dělá (např. „aby se ráno necítil unavený").

4. Bezpečný kontakt

Role peer-průvodce je v programu Snooper definována jako specifický mediální a vztahový most, který optimalizuje informační tok mezi cílovou skupinou a odborným zázemím programu.

- Využití neformální chronologie: Peer v těchto momentech (přestávky) plní roli kontaktního bodu první linie, který umožňuje individuální dotazování v neformálním rámci, čímž saturuje potřebu okamžité emoční podpory či rady bez nutnosti oficiální expozice před kolektivem.
- Redukce bariér skrze sociální blízkost: Peer-průvodce funguje jako neformální komunikační kanál, jenž dekonstruuje komunikační bariéry vůči vertikálním autoritám. Díky principu věkové a zkušenostní homofilie (sociální blízkosti) vytváří bezpečný diskurzivní prostor. V tomto prostředí edukanti projevují vyšší míru openness (otevřenosti) při sdílení obav a dotazů, které by v rámci formální pedagogické interakce zůstaly z důvodu strachu z normativního posouzení latentní.
- Navigační kompetence: Působí jako facilitátor přístupu k pomoci, kdy skrze vybudovanou důvěru citlivě naviguje ohroženého jedince k odbornému lektorovi či do sítě indikované prevence (Linka bezpečí, E-bezpečí). Tímto procesem dochází k zásadní redukci prahu pro vyhledání pomoci a zmírnění úzkosti z následné intervence.

Souhrn role v rámci multidisciplinárního týmu

Peer průvodce tvoří s lektorem tandem. Zatímco lektor zodpovídá za metodický rámec, strukturu a bezpečí skupiny, peer dodává emoční hloubku, dynamiku a propojení s realitou cílové skupiny. Tato synergie je tím, co dělá projekt Snooper unikátním a účinným.

Rozpracuji podrobně kapitolu **5.3 Výběr peerů**. Tento text definuje proces identifikace, oslovení a prověření vhodných kandidátů tak, aby byla zajištěna odborná kvalita i bezpečnost všech zúčastněných stran.

5.3 Výběr peerů

Proces výběru peer průvodců je v projektu Snooper klíčový. Vzhledem k tomu, že peer pracuje s citlivými tématy (kyberšikana, ohrožení dětí) a sdílí svůj osobní příběh, musí být proces výběru strukturovaný a vícefázový.

1. Profil ideálního kandidáta

Při výběru se zaměřujeme na tři základní oblasti:

- **Zkušenostní expertíza:** Kandidát musí mít autentickou zkušenost s tématy online světa (pozitivní i negativní). Nejde jen o to „být na internetu“, ale rozumět dynamice sociálních sítí a rizikům, o kterých program mluví.
- **Fáze zotavení (Stability check):** Kandidát musí vykazovat vysokou míru náhledu na svou minulou zkušenost. Musí být schopen o negativních událostech mluvit bez emočního zahlcení, které by mohlo vést k jeho vlastní retraumatizaci nebo k ohrožení bezpečí skupiny.
- **Osobnostní předpoklady:** Empatie, schopnost naslouchat, respekt k odlišným názorům a schopnost dodržovat profesionální hranice (etiku).

2. Zdroje náboru

Kde Snooper hledá své peer průvodce:

- **Vlastní sítě organizace:** Absolventi jiných programů organizace Prostor plus o.p.s., kteří projevili zájem o další rozvoj.
- **Akademická půda:** Studenti sociálních, pedagogických či psychologických oborů, kteří mají osobní zkušenost s online riziky a chtějí ji metodicky využít.
- **Komunitní sítě:** Oslovování skrze online platformy, kde se pohybují lidé se zájmem o digitální wellbeing a prevenci.

3. Fáze výběrového řízení

A. První kontakt a dotazník Zájemce vyplňuje vstupní formulář, kde definuje svou motivaci a stručně nastiňuje své zkušenosti.

B. Osobní pohovor s multidisciplinárním týmem Pohovoru se účastní odborný vedoucí projektu a zkušený lektor. Zaměřujeme se na:

- **Motivaci:** Proč chce kandidát svou zkušenost sdílet? (Hledáme altruistickou motivaci, nikoli potřebu si „veřejně léčit rány“).
- **Reflexi:** Jak kandidát hodnotí své minulé chyby v online světě a co mu pomohlo je vyřešit?
- **Etiku:** Testování reakcí na modelové situace týkající se mlčenlivosti a hranic vztahu s žáky.

C. Praktická zkouška (Modelový vstup) Kandidát dostane za úkol připravit si 5–10minutový vstup na konkrétní téma (např. „Můj digitální wellbeing“). Sledujeme:

- Schopnost srozumitelného projevu.
- Míru autenticity vs. přílišnou intimitou (tzv. oversharing).
- Schopnost reagovat na doplňující otázky lektora (simulace otázek od žáků).

4. Vstupní vzdělávání a zkušební doba

Vybraný kandidát se stává peerem v terénu až po absolvování:

- **Metodické minimum:** Školení v ovládání SnoopBoxu a struktuře všech 3 bloků.
- **Etické minimum:** Podpis a podrobný rozbor Etického kodexu peer průvodce Snooper.
- **Hospitační fáze:** První dva workshopy ve škole peer pouze sleduje nebo se účastní jen drobných aktivit pod přímým vedením zkušeného kolegy.

5. Formální náležitosti

Každý participující peer-průvodce je povinen před zahájením terénní intervence doložit kompletní dokumentaci, která garantuje jeho bezúhonnost a profesní připravenost. Tato dokumentace zahrnuje:

- Písemné prohlášení o mlčenlivosti, kterým se pracovník zavazuje k dodržování informační integrity a ochraně senzitivních dat v souladu s GDPR a etickým kodexem programu.
- Zákonná garance (u nezletilých peerů): V případě peer-průvodců mladších 18 let je vyžadován písemný souhlas zákonného zástupce. Tento dokument validuje účast na veškerých projektových aktivitách, včetně terénních výjezdů a supervizních setkání, a stvrzuje převzetí odpovědnosti v rámci sjednaného časového harmonogramu.
- Realizace aktivit je podmíněna uzavřením trojstranné či vícestranné Dohody o spolupráci mezi zastřešující organizací, kmenovou školou peer-průvodce a cílovým školským zařízením. Tato smlouva upravuje právní postavení peera, podmínky jeho uvolnění z výuky a metodické krytí během výkonu preventivní činnosti.

5.4 Příprava a spolupráce s peery

Efektivita programu Snooper spočívá v synergii mezi odborností lektora a autenticitou peera. Aby tato spolupráce fungovala, musí být jasně nastavena pravidla komunikace, rozdělení rolí a proces společné přípravy.

1. Model tandemu: Lektor a Peer

V rámci metodiky Snooper funguje vztah lektora a peera jako rovnocenné partnerství, nikoli jako hierarchie nadřízeného a podřízeného.

- **Lektor:** Zodpovídá za metodickou strukturu, časový harmonogram, odbornou správnost informací a bezpečí skupiny (řešení krizových situací).
- **Peer:** Zodpovídá za vnášení perspektivy „žité zkušenosti“, emocionalitu tématu a autentické propojení s cílovou skupinou.

2. Proces společné přípravy

Před každým vstupem do třídy (nebo před zahájením nového cyklu) probíhá povinná přípravná fáze:

- Lektor a peer procházejí konkrétní složení třídy a specifika školy. Vyjasňují si, které pasáže metodiky budou v daný den akcentovat (např. pokud se ve třídě řeší negativní komentáře, posílí se tato část).
- Peer s lektorem konzultuje svůj příběh. Lektor pomáhá peerovi vybrat ty části zkušenosti, které nejlépe ilustrují probírané téma (např. phishing), a hlídá, aby sdílení nebylo příliš intimní nebo zraňující.
- Společná kontrola SnoopBoxu a prezentace. Rozdělení úkolů, kdo bude obsluhovat techniku v konkrétních pasážích.

3. Komunikace během workshopu

Během samotné realizace využívá tandem naučené signály a postupy:

- **Předávání slova:** Lektor a peer mají dohodnuté přechody (např. „A teď by mě zajímalo, jak jsi to v praxi vnímal ty...“).
- **Vzájemná podpora:** Pokud se peer dostane do úzkých při dotazu žáka, lektor do diskuse vstupuje a nabízí odborný rámec. Naopak peer může lektorův výklad „zlidštit“, pokud vidí, že třída přestává rozumět odborným pojmům.
- **Krizové situace:** Pokud se během workshopu otevře téma vyžadující okamžitou odbornou pomoc, lektor přebírá vedení a peer se soustředí na udržení klidné atmosféry ve zbytku třídy.

4. Reflexe

Bezprostředně po odchodu ze třídy probíhá krátká reflexe (15–20 min):

- **Hodnocení dynamiky:** Jak třída reagovala? Které aktivity fungovaly a které ne?
- **Psychohygiena peera:** Lektor se zajímá o to, jak se peer po sdílení svého příběhu cítí. Je to

prevence vyhoření a emočního vyčerpání.

- **Zápis:** Společné doplnění poznámek do lektorské evaluační tabulky, které poslouží jako podklad pro další blok (po 1–3 měsících).

5. Multidisciplinární tým a supervize

Součinnost přesahuje rámec úzké tandemové kooperace a je plně integrovaná do širší struktury multidisciplinárního týmu organizace.

- Peer pracovník je aktivní součástí týmů Snooper. V rámci pravidelných porad dochází k výměně odborného know-how a ke sdílení zkušeností z intervenční činnosti na jednotlivých školských zařízeních.
- V souladu s Etickým kodexem je peer pracovník povinen se účastnit na případové supervizi. Tento proces, vedený externím supervizorem, slouží k odborné reflexi náročných situací, prevenci syndromu vyhoření a k precizování profesních hranic. Role lektora je v tomto kontextu definována jako mentorská podpora, která usnadňuje profesní růst a ukotvení peera v týmu.

Bezpečnostní aspekty práce

Práce v programu Snooper s sebou nese specifická rizika vyplývající z povahy peer práce a citlivosti probíraných témat (kyberšikana, obtěžování, závislosti). Bezpečnostní rámec je rozdělen do dvou hlavních rovin: ochrana žáků a ochrana samotného peera.

1. Ochrana žáků a etické hranice

Bezpečí cílové skupiny je nadřazeno všem ostatním zájmům.

- **Prevence nevhodného vzoru:** Peer je instruován, aby při sdílení svého příběhu nepoužíval popisy, které by mohly sloužit jako návod (např. konkrétní postupy, jak někoho sledovat nebo jak obcházet technické blokace). Cílem je prevence, nikoli edukace v rizikovém chování.
- **Jasná ohlašovací povinnost:** Peer musí být srozuměn s tím, že mlčenlivost končí tam, kde začíná zákonná ohlašovací povinnost. Pokud se mu žák svěří s trestným činem nebo situací ohrožující život (např. myšlenky na sebepoškozování), peer musí tuto informaci okamžitě předat odbornému lektorovi.
- **Profesionální odstup:** Přestože peer buduje vztah na bázi rovnosti, musí zachovávat profesionální hranice. Je nepřípustné navazovat se žáky soukromé kontakty na sociálních sítích mimo oficiální komunikační kanály projektu Snooper.

2. Ochrana a psychohygiena peera

Sdílení vlastního zranitelného příběhu může být pro peera emočně náročné. Metodika proto obsahuje „záchrannou síť“:

- **Hranice sdílení:** Peer má právo i povinnost chránit své soukromí. Sdílí pouze ty části příběhu, které má zpracované. Lektor v průběhu bloku sleduje emoce peera a v případě potřeby diskuzi usměrní, aby peera ochránil před přílišným tlakem skupiny.
- **Stop karta peera:** Stejně jako žáci, i peer má právo na „stop kartu“. Pokud padne dotaz, který zasahuje příliš hluboko do jeho soukromí nebo mu je nepříjemný, může jej s odkazem na své hranice odmítnout odpovědět.
- **Supervize jako standard:** Účast na supervizích není pro peera volitelná, ale povinná. Slouží k „odložení“ emocí, které si peer může ze tříd odnášet, a k prevenci retraumatizace.

3. Technická a organizační bezpečnost

- **Vždy v týmu:** Peer nikdy nepůsobí ve třídě sám. Přítomnost odborného lektora zaručuje, že v případě vyostřené dynamiky ve třídě nebo krizového vývoje bude situace profesionálně zvládnout.
- **Anonymizace dat:** Veškeré informace získané skrze SnoopBox jsou zpracovávány anonymně. Peer ani lektor nesmí vynášet konkrétní jména žáků v souvislosti s jejich odpověďmi v dotaznících.
- **Právní krytí:** Každý peer je smluvně vázán mlčenlivostí a je pojištěn pro případ odpovědnosti v rámci činnosti organizace Prostor plus o.p.s.

4. Bezpečné ukončení kontaktu

Ukončení workshopu je kritickým momentem. Peer musí být schopen se od skupiny emočně odpojit:

- **Rituál ukončení:** Každý blok končí společným shrnutím a „předáním odpovědnosti“ zpět do rukou lektora/učitele.
- **Jasné nasměrování:** Žáci musí vědět, že peer není jejich osobní mentor, ale že pro další podporu mají využít oficiální platformy (Linka bezpečí, poradna Snooper).

Nástroj Snoopbox

Zařízení SnoopBox představuje zakázkově vyvinutý technologický přístroj, sestávající z optimalizované hardwarové vrstvy a dedikovaného softwarového vybavení. Systém byl navržen jako integrované komunikační médium, které zajišťuje digitální interakci a datový přenos v rámci metodických aktivit projektu Snooper, čímž eliminuje limity standardizovaných komerčních produktů.

Technická podstata a fungování

SnoopBox funguje jako lokální mikrosíť (hotspot).

Síťová nezávislost: Systém vykazuje plnou technologickou soběstačnost a je nezávislý na externí síťové infrastruktuře (školní Wi-Fi či mobilní datové sítě). SnoopBox generuje proprietární uzavřenou síť (intranet). Přístup koncových uživatelů (žáků) je realizován prostřednictvím mobilních terminálů skrze dynamický QR kód nebo specifickou URL adresu, což zajišťuje okamžitou konektivitu v rámci daného lokálního segmentu.

Bezpečné uživatelské rozhraní: Interaktivní vrstva je založena na technologii webového rozhraní (Web-based Interface). Tento přístup nevyžaduje instalaci klientských aplikací (Zero-Install přístup) ani proces registrace. Architektura systému je navržena s prioritou na ochranu soukromí a anonymizaci dat, díky čemuž nedochází k retenci osobních údajů (e-mailové adresy, identifikační metadata) ani k monitoringu identity uživatelů.

Klíčové funkce SnoopBoxu

Zařízení v rámci workshopu plní tři hlavní funkce:

Agregovaná anonymní reflexe a kvantitativní sběr dat. Modul umožňuje realizaci anket a hlasování. Lektorský tým prostřednictvím cílených dotazů stimuluje participaci žáků, přičemž výstupy jsou v reálném čase zpracovávány a vizualizovány v agregované podobě na projekční ploše. Tento mechanismus zajišťuje bezpečné prostředí pro sdílení citlivých zkušeností bez rizika demaskování jednotlivce.

Žáci mají k dispozici diskrétní kanál pro formulaci dotazů v průběhu celého metodického bloku. Tento modul slouží jako digitální sběrné místo, ke kterému se lektor vrací v rámci dedikované reflexe. Tento přístup eliminuje bariéry spojené s obavou z veřejného dotazování a umožňuje strukturované uzavření probíraných témat.

SnoopBox disponuje modulem pro realizaci řízených simulací (např. detekce kybernetických hrozeb či phishingu) a soutěžních prvků. Využitím principů gamifikace dochází k výraznému zvýšení kognitivní angažovanosti cílové skupiny a k praktické verifikaci nabytých kompetencí v reálném čase.

Přidaná hodnota nástroje

Použití „krabičky“ je vhodné především díky:

Garance 100% anonymity: Žáci vědí, že jejich odpovědi nejsou spojeny s jejich osobou. To vede k mnohem vyšší upřímnosti u citlivých témat (např. u kyberšikany), kde by se při běžném zvedání ruky báli stigmatizace.

Práce s daty v reálném čase: Lektor může okamžitě reagovat na to, co se v dané třídě skutečně děje. Pokud 80 % třídy odpoví, že má zkušenost se stalkingem, lektor může tuto část metodiky operativně rozšířit.

Atraktivita pro digitální generaci: Zapojení vlastního telefonu jako „hlasovacího zařízení“ je pro žáky přirozené a zvyšuje jejich pozornost.

Bezpečnost dat

- Žádná data nejsou odesílána na externí servery (cloudy).
- Po ukončení workshopu a vypnutí zařízení se dočasná data o připojených klientech mažou.
- Zařízení nesbírá MAC adresy ani jiná identifikační metadata telefonů žáků.

Nastavení a příprava před hodinou

Aby SnoopBox plnil svou funkci, musí být jeho zprovoznění rychlé a spolehlivé. Lektorský tým by měl mít zařízení připravené k provozu ideálně 10–15 minut před začátkem bloku.

Hardwarová kontrola a napájení

Kontrola baterie: SnoopBox je vybaven interním akumulátorem, ale pro stabilitu během celého 90 minutového bloku se doporučuje připojení k síťovému adaptéru.
Zapnutí: Po stisknutí hlavního spínače lektor vyčká na indikační signál (LED dioda nebo náběh displeje), který potvrzuje, že lokální Wi-Fi hotspot je aktivní.
Propojení s notebookem: Lektor připojí svůj řídicí notebook k Wi-Fi síti SnoopBoxu. Tím získá přístup k administrátorskému rozhraní, odkud ovládá prezentaci a ankety.

Konfigurace softwarového rozhraní

Výběr metodického bloku: V administraci lektor zvolí, který ze tří bloků (1, 2, nebo 3) bude realizovat. Systém automaticky načte příslušné sady otázek a kvízů.
Test zobrazení: Lektor ověří, zda se výstupy ze SnoopBoxu správně zrcadlí na projektor či interaktivní tabuli školy. Výsledky hlasování musí být pro třídu dobře čitelné.
Reset dat: Před začátkem každé nové třídy musí lektor potvrdit vymazání dat z předchozího měření, aby nedošlo k míchání výsledků mezi různými kolektivy.

Příprava přístupových bodů pro žáky

Distribuce QR kódu: Lektor si připraví slide s unikátním QR kódem, který se zobrazí na začátku hodiny. Alternativně má připravenou krátkou URL adresu pro žáky, kteří nemají čtečku QR kódů.
Kontrola dosahu: Lektor se ujistí, že SnoopBox je umístěn na viditelném a centrálním místě (např. katedra), aby signál pokryl celou učebnu i v zadních lavicích.

Krizový plán „Co když to nefunguje“

Metodika definuje postupy pro případ technického selhání:

Výpadek Wi-Fi: Pokud se žáci nemohou připojit, lektor provede restart zařízení. Během restartu (cca 2 minuty) přebírá iniciativu peer se svým příběhem, aby nedošlo k proluce ve výuce.
Nedostatek telefonů: Pokud někteří žáci nemají chytrý telefon nebo data/nabití, lektor vyzve k vytvoření „hlasovacích dvojic“. V metodice Snooper je povoleno sdílet zařízení, pokud to nenarušuje anonymitu odpovědí (domluva ve dvojici).
Analogová záloha: Lektor má vždy v kufříku sadu barevných hlasovacích karet (A, B, C), které lze použít pro veřejné hlasování, pokud by SnoopBox selhal fatálně.

Práce s daty a interpretace výsledků

Hlavním smyslem SnoopBoxu není sběr statistik pro statistiku samotnou, ale vytvoření zrcadla třídy. Lektor musí umět v reálném čase interpretovat to, co se objeví na plátně, a citlivě na to reagovat.

Vizualizace odpovědí

Jakmile žáci odešlou své odpovědi, systém SnoopBox je zpracuje do vizuálně srozumitelných formátů:

Sloupcové/koláčové grafy: Používají se pro uzavřené otázky (např. „Ano/Ne“, „Kolik hodin trávíte na mobilu?“).
Slovní mrak (Word Cloud): Používá se pro otevřené asociace. Čím častěji žáci napíší stejné slovo (např. u otázky „Co je na internetu negativního?“), tím je toto slovo v mraku větší.
Seznam dotazů: Pro anonymní schránku dotazů, kde se otázky řadí pod sebe.

Metodický postup interpretace

Lektor by měl při zobrazení výsledků dodržovat tento postup:

1. **Co vidíme:** „Vidím, že v této třídě má polovina z vás zkušenost s tím, že mu někdo cizí napsal na Instagramu.“ (Objektivní konstatování bez hodnocení).
2. **Normalizace:** „To, co tady vidíme, je úplně přirozené. Podobné zkušenosti mají děti i v jiných třídách nebo školách. Rozhodně v tom nejste sami a neznamená to, že by s vámi bylo něco špatně – v online světě se do podobné situace dostane dříve nebo později skoro každý.“
3. **Výzva k peer reflexi:** V tuto chvíli vstupuje peer průvodce: „Taky jsem v tom grafu na té straně 'Ano'. Když se mi to stalo poprvé, nevěděl jsem, co s tím.“
4. **Hledání řešení:** „Když vidíme, že je nás tolik, pojďme si ukázat, jak na takovou zprávu reagovat bezpečným způsobem.“

Práce s jedinečnými situacemi a citlivými daty

Metodika programu počítá s výskytem tzv. red flags v anonymním sběru dat. V takových případech lektorský tým uplatňuje princip nekonfrontační reflexe. Extrémní vstupy jsou využity jako modelové příklady pro demonstraci odborné pomoci, čímž dochází k de-eskalaci napětí a k jasnému nasměrování žáka na odbornou síť (peer, lektor, Linka bezpečí) v bezpečném, privátním nastavení.

Práce s anonymní schránkou dotazů

Tato funkce je nejdůležitějším zdrojem pro lektora.

Průběžné sledování: Lektor nebo peer může na tabletu průběžně sledovat přicházející dotazy, zatímco probíhá jiná aktivita.
Třídění: Lektor nevybírá dotazy jen podle zajímavosti, ale provádí tzv. průběžnou diagnostiku. Lektor vybere ty nejvíce relevantní pro celou třídu.
Zodpovídání: V případě výskytu dotazů na téma intimity či vysokým rizikem traumatické zkušenosti, dotaz zodpoví v obecné rovině jako modelový příklad. V případě identifikace akutního ohrožení lektor aktivuje mechanismus individuální konzultace v bezpečném prostředí mimo kolektiv třídy. Pokud situace přesahuje kompetence lektorského týmu, je účastníkovi zprostředkován kontakt na specializovaná pracoviště nebo krizové linky.

Po skončení bloku lektor data ze SnoopBoxu vyexportuje (pokud je to součástí dohody se školou).

Anonymizovaný report: Škola (metodik prevence) dostane souhrnnou informaci: „Ve třídě 8.B má 40 % dětí zkušenost s kyberšikanou, doporučujeme se v třídnických hodinách zaměřit na klima třídy."
Evaluace programu: Data slouží organizaci Prostor plus o.p.s. k měření efektivity programu (posun v znalostech mezi 1. a 3. blokem).

Nejčastější problémy a jejich řešení

Práce s technologiemi ve třídě může přinášet různé situace, na které je vhodné být připraven. Důležité je reagovat klidně a s nadhledem, aby nebyla narušena atmosféra důvěry ani plynulost programu.

Problémy s připojením (konektivita)
Někdy se žáci nemohou připojit k Wi-Fi SnoopBoxu nebo se nenačítá stránka. Doporučuje se zkontrolovat vypnutá mobilní data, restartovat prohlížeč nebo zařízení. Pokud problém trvá, lektor může SnoopBox restartovat a peer mezitím vede krátkou diskusi. Pokud se připojení nepodaří do několika minut, žák se zapojí ve dvojici se spolužákem.

Nevhodné využití anonymity
Pokud se v anonymním chatu objeví vulgarismy nebo spam, lektor na ně zbytečně neupozorňuje. Nevhodný komentář jednoduše skryje nebo smaže. Pokud se situace opakuje, v klidu připomene dohodnutá pravidla nebo chat na chvíli pozastaví, aby se skupina mohla vrátit k tématu.

Absence zařízení nebo vybitá baterie
Program je navržen tak, aby se mohl zapojit úplně každý, i bez vlastního chytrého telefonu. Žáci

mohou spolupracovat ve dvojicích nebo využít klasické papírové karty. Technologie je pro nás jen nástroj – to nejdůležitější je názor a zapojení každého žáka.

Selhání projekce nebo techniky
Pokud nefunguje projektor, lektor může výsledky interpretovat ústně nebo je peer zapisuje na tabuli. V případě většího výpadku lze přejít na alternativní aktivity, například „živé škály“ v prostoru třídy.

Ticho nebo nejistota po zobrazení citlivých výsledků
Silná témata mohou vést k momentu ticha. Peer může sdílením vlastní zkušenosti pomoci otevřít diskusi a lektor následně nabídne konkrétní a konstruktivní kroky, které pomohou situaci zpracovat.

Limity práce s technologiemi

Při práci s interaktivními nástroji je důležitá aktivní a citlivá moderace ze strany lektorského týmu. SnoopBox obsahuje základní filtry, které pomáhají omezovat nevhodné projevy, přesto je role lektora klíčová. Pokud se objeví nevhodné chování nebo pokusy obcházet pravidla, může lektor zasáhnout – například skrýt obsah nebo žáka dočasně vyřadit z aktivity. Veškeré výsledky slouží pouze ke společné reflexi práce třídy, nikoli k označování jednotlivců.

Etické využití nástrojů

Některé funkce SnoopBoxu (např. demonstrační nástroje BlackEye nebo Tshark) slouží výhradně k edukativním ukázkám. Jejich použití musí být transparentní a probíhat pouze ve školním prostředí s vědomím účastníků. Nástroje nejsou určeny k reálným útokům ani k získávání citlivých dat – slouží jen k bezpečné demonstraci rizik, například simulaci phishingu nebo vysvětlení principů fungování sítí.

Technická bezpečnost zařízení

Pro dlouhodobé a bezpečné fungování je důležité dodržovat základní pravidla zacházení se zařízením. Uživatelé by zařízení neměly rozebírat ani zasahovat do jeho vnitřní konstrukce, protože by tím mohli poškodit hardware a ztratit záruku. Zvláštní pozornost je třeba věnovat chlazení zařízení a nepřetěžovat systém neautorizovanými úpravami. Přístup k pokročilým nastavením je určen pouze pro servisní účely.

Metodika Snooper využívá tandemový model vedení, který kombinuje odbornou garanci lektora s přirozenou autoritou peer průvodce. Tato spolupráce umožňuje efektivněji předávat preventivní sdělení, protože peer průvodce slouží jako komunikační most k cílové skupině. Výsledkem je vyvážená intervence, která je věcně správná, a přitom maximálně relevantní pro aktuální potřeby žáků.

1. Odborný garant (lektor)

Lektor vystupuje jako procesní a odborný garant intervenčního bloku. Je odpovědný za metodickou integritu, didaktickou správnost a zajištění protektivního rámce v rámci skupinové dynamiky.

- **Vzdělání a praxe:**
  - Ukončené nebo probíhající vysokoškolské vzdělání v magisterském či bakalářském studijním programu (pedagogika, psychologie, sociální práce, adiktologie či jiné relevantní pomáhající profese).
  - Prokazatelná praxe v úseku všeobecné či selektivní primární prevence rizikového chování, případně v oblasti pedagogicko-psychologického poradenství a práce s cílovou skupinou dětí a adolescentů
- **Klíčové kompetence:**
  - Lektorská flexibilita: Schopnost dodržet stanovené cíle programu při zachování vysoké vnímavosti vůči dynamice skupiny. Lektor adaptuje hloubku a tempo témat podle toho, co třída v danou chvíli skutečně řeší.
  - Krizová intervence a diagnostika: Kompetence k včasné detekci indikátorů rizikového chování a patologických procesů v kolektivu. Lektor disponuje dovednostmi pro poskytnutí bazální krizové intervence a facilitaci následné indikované péče.
  - Technická a systémová gramotnost: Pokročilá administrace prostoru SnoopBox. Zahrnuje schopnost nativní správy síťové infrastruktury (konfigurace síťových rozhraní) a diagnostiku systémových procesů (např. správa portů a síťových služeb), zajišťující bezproblémovou technologickou kontinuitu programu.

2. Společné kompetence týmu

Síla programu Snooper spočívá v úzké spolupráci lektora a peer-průvodce. Jako sehraný tým se doplňují tak, aby zajistili odbornou správnost a zároveň blízkost k realitě žáků. Oba sdílejí tyto klíčové dovednosti:

- Neustálé sledování nových funkcí sociálních sítí, herních platforem a aktuálních triků v kyberkriminalitě.
- Schopnost identifikovat nebezpečné jevy (kyberšikana, grooming, dezinformace) a vyhodnotit jejich dopad na duševní pohodu žáků.
- Schopnost provádět průběžné revize upravovat parametry systému podle aktuální metodiky a dokumentace.
- Společné vnímání atmosféry ve třídě a schopnost reagovat na citlivá témata spojená s bezpečím v online prostoru.

3. Systém dalšího vzdělávání

Pracovníci programu Snooper jsou vázáni k soustavnému zvyšování odborné kvalifikace v následujících klíčových doménách:

- Socio-technologický monitoring a kybernetická bezpečnost: Sledování dynamického vývoje v oblasti digitálních platforem a aktuálních trendů v kybernetické kriminalitě. Důraz je kladen na hloubkovou analýzu rizikových fenoménů a jejich dopadů na psychosociální zdraví cílové populace.
- Správa a optimalizace technologického prostředí: Pravidelné ověřování dovedností v oblasti administrace a údržby hardwarové i softwarové vrstvy systému SnoopBox. Tato kompetence zahrnuje precizní implementaci standardizovaných napájecích protokolů (USB-C standardy) a pokročilou editaci konfiguračních skriptů (.local.php) v souladu se schválenou technickou dokumentací.
- Didaktika zážitkové pedagogiky a facilitační dovednosti: Prohlubování kompetencí v oblasti zážitkové pedagogiky a moderování skupinových procesů. Cílem je osvojení pokročilých technik facilitace diskusí, které stimulují kritickou reflexi a efektivní ukotvení preventivních narativů u participantů.

Etické aspekty práce

Realizace programu Snooper, zejména při práci s interaktivními simulacemi digitálních rizik, stojí na jasných etických principech. Ty slouží k ochraně žáků, k udržení profesionálních hranic a k bezpečnému fungování programu ve školním prostředí.

Respekt k soukromí a anonymita
Ochrana identity účastníků je základním pravidlem programu. SnoopBox nevyžaduje osobní údaje a odpovědi žáků zůstávají anonymní. Lektor ani peer nesmí usilovat o identifikaci autora konkrétního sdělení. Pokud se v anonymních dotazech objeví závažné téma (např. kyberšikana), cílem je nabídnout podporu celé skupině nebo odkázat na odbornou pomoc, nikoli pátrat po konkrétním jednotlivci.

Respekt k soukromí při dokumentaci

Během programu pořizujeme fotografie pouze tak, aby na nich nebyla rozpoznatelná identita žáků (např. záběry zezadu, detaily materiálů, skupinové fotky z dálky). Pokud škola nemá výslovný souhlas rodičů s focením, dbáme na to, aby dokumentace sloužila pouze k ilustraci atmosféry bez narušení anonymity dětí.

Etické využití demonstračních nástroj
Některé funkce SnoopBoxu slouží pouze k bezpečné demonstraci rizik. Nástroje pro simulaci phishingu či analýzu síťového provozu mohou být využívány výhradně pro vzdělávací účely a v uzavřeném prostředí. Žáci musí být vždy informováni, že jde o modelovou situaci, a je zakázáno jakékoliv reálné získávání dat nebo hesel.

Zodpovědnost za hardware a přístupy

Součástí etiky práce je i bezpečné zacházení s technikou. Zařízení by neměla být neautorizovaně upravována ani rozebírána. Lektor odpovídá za ochranu přístupových údajů a za to, aby zařízení bylo provozováno bezpečně a v souladu s technickými doporučeními.

Mlčenlivost a zákonná oznamovací povinnost

Lektoři pracují v souladu s vnitřními směrnicemi organizace Prostor plus, které striktně vyžadují ochranu osobních a citlivých údajů účastníků. Základní pravidlo důvěrnosti je však limitováno zákonem: v případech popsaných v trestním zákoníku (§ 367 a § 368 – nepřekažení a neoznámení trestného činu) jsou lektoři povinni informovat příslušné orgány. Systém je nastaven tak, aby chránil integritu žáka i zákonné normy.

Bezpečné nakládání s daty po ukončení programu

Po skončení bloku dochází k vymazání dočasných dat a ukončení všech běžících procesů tak, aby v prostředí školy nezůstaly žádné citlivé informace. Cílem je vrátit zařízení i síť do původního bezpečného stavu.

Sdělování informací o klientech

Veškeré detaily o průběhu lekcí zůstávají uvnitř odborného týmu (v rámci porad a supervizí), kde slouží výhradně ke zkvalitňování naší práce. Závěrečné zprávy pro školu neobsahují žádné jmenovité ani citlivé údaje o žácích – zaměřují se pouze na celkové hodnocení programu a atmosféry v kolektivu. Jedinou výjimkou jsou zákonem stanovené situace (ohrožení života nebo zdraví), kdy je naší povinností informovat policii či orgány sociálně-právní ochrany.