

ДИГИТАЛНИТЕ ДЕЦА В МРЕЖАТА:

ПРЕДИЗВИКАТЕЛСТВА И ВЪЗМОЖНОСТИ

МЕТОДИЧЕСКО
РЪКОВОДСТВО
ЗА РАБОТА
С ДЕЦА
ЗА БЕЗОПАСНО
ПОВЕДЕНИЕ
В ИНТЕРНЕТ







ДИГИТАЛНИТЕ ДЕЦА В МРЕЖАТА:

ПРЕДИЗВИКАТЕЛСТВА И ВЪЗМОЖНОСТИ

Методическо ръководство за работа с деца
за безопасно поведение в Интернет

Настоящото ръководство е разработено от екип на Националния център за безопасен интернет, който се управлява от Асоциация „Родители“, в консорциум с Българска асоциация по семейно планиране и сексуално здраве (БАСП) и Национална мрежа за децата (НМД). Ръководството е второ преработено издание по проект „Дигитални деца 2“. Запазени са методическата логика, интерактивният подход и основните теми, като са актуализирани разделите за уязвимост, лични данни, сигурност, секстинг, сексторшън и изкуствен интелект. Добавени са нови части за онлайн радикализация, реакция при нови онлайн рискове и допълнителни инструменти за работа с деца.

С финансовата подкрепа на Европейския съюз по програма „Дигитална Европа“ (Project: 101266231 – DC2 – DIGITAL-2025-BESTUSE-08). Изразените възгледи и мнения са само на авторите и не отразяват непременно тези на Европейския съюз или Европейската изпълнителна агенция за здравеопазването и цифровизацията (HaDEA). Нито Европейският съюз, нито HaDEA могат да носят отговорност за тях.

Октомври 2026

**ДИГИТАЛНИ
ДЕЦА**
by sofennet.bg



Съфинансирано от
Европейския съюз

СЪДЪРЖАНИЕ

1. Въведение.....	5
2. Методология и цели	6
3. Обща методика на урочната единица.....	6
4. Фокус върху уязвимостта	9
5. Теми	
5.1. Нетикет.....	12
5.2. Комуникация онлайн и офлайн.....	13
5.3. Лични данни.....	15
5.4. Дигитален имидж	17
5.5. Вредно онлайн съдържание	19
5.6. Сигурност в мрежата	21
5.7. Онлайн тормоз	24
5.8. Секстинг	27
5.9. Непознатите в мрежата и рискът от сексторшън.....	31
5.10. Изкуствен интелект	35
5.11. Онлайн радикализация и екстремистко съдържание	38
6. Инструменти.....	42
7. Какво да направите, ако... ..	76
8. Развитие в юношеска възраст.....	81
9. Заключителна част	83

Днес е трудно да си представим ежедневието без интернет и дигитални технологии. За децата те са естествена част от живота още от най-ранна възраст – използват ги за игри и забавление, за общуване, учене, творчество и откриване на света.

Дигиталната среда предлага огромни възможности, но създава и редица рискове – кибертормоз, онлайн сексуална експлоатация и насилие, неподходящо или вредно съдържание, дезинформация, измами и злоупотреба с лични данни. Бързото развитие на технологиите и изкуствения интелект води и до появата на нови форми на онлайн заплахи, които изискват постоянно актуализиране на знанията и уменията за безопасно поведение в интернет.

Проектът „Дигитални деца 2“ е насочен към укрепване на безопасността на децата в дигиталната среда и към повишаване на тяхната дигитална и медийна грамотност. Проектът подкрепя работата на Националния център за безопасен интернет (НЦБИ), включително функционирането на Консултативната линия за онлайн безопасност (Helpline) и Горещата линия за сигнали за онлайн престъпления срещу деца (Hotline).

В рамките на проекта се реализират обучения, семинари и кампании за деца и младежи, учители, родители и професионалисти, работещи с деца. Особено внимание се отделя на уязвимите групи и на необходимостта всяко дете да има достъп до знания и подкрепа, които да му помогнат да разпознава рисковете, да се защитава и да търси помощ при проблем онлайн.

Освен образователните инициативи, проектът има стратегическа роля в застъпничеството за по-добри политики за онлайн безопасност, в съответствие с приоритетите на ЕС. Целта е да се подобри правната рамка, да се засили прилагането на мерки за защита и да се изгради политически ангажимент за борба с онлайн престъпления и неправомерни действия, извършвани от и срещу деца.

Настоящият наръчник е създаден в отговор на тези нужди и в рамките на проект „Дигитални деца 2“, финансиран по програма „Дигитална Европа“ (Project 101266231 – DC2). Той е предназначен за младежи, учители и професионалисти, работещи с деца в прогимназиална и гимназиална възраст, и предлага практически насоки и инструменти за разговори и работа по темите на дигиталната сигурност.

Надяваме се наръчникът да бъде полезен ресурс в ежедневната работа с децата и да допринесе за изграждането на по-информирани, уверени и отговорни дигитални граждани.

Пожелаваме ви успешна и вдъхновяваща работа!

Използваната методология се основава на личностно центрираното интерактивно обучение и се различава от класическия класно-урочен модел. Наръчникът обхваща 11 теми, като всеки урок има цели, необходими материали, въвеждаща част, основна и заключителна част, които са необходими за провеждането му. Целите на урока са свързани с това какво се очаква да могат да правят учениците след приключването на всеки урок. Необходимите материали са описани подробно, за да може всеки обучител/учител да подготви часа си предварително. Преди всеки час съветваме водещия да подрежда столовете в кръг и да заеме своето място в него, защото така се стимулират доверителните отношения и споделянето.

Цели на методологията:

- ▶ Учим децата да се държат отговорно и позитивно в интернет.
- ▶ Разпознаваме заедно рискови ситуации онлайн.
- ▶ Идентифицираме собствените ни уязвимости и овладяваме стратегии за справяне/отрабатване.
- ▶ Придобиваме знания и умения за справяне, стратегии и от кого търсим помощ, докладваме и блокираме.

Методологията на урока представлява устойчив и интерактивен модел за преподаване на уменията на 21. век и в контекста на споделената представа за общите ценности на позитивното възпитание и образование на децата. Тя се базира на личностно центрираното интерактивно обучение, подпомагано от съвременните технологии. Целите на урока са свързани с овладяване на определени знания, компетентности и умения, независимо коя тема сте избрали, за да работите с учениците.

Урокът е разделен на три части/дейности, като времето за всяка дейност е разписано подробно, така че учителят/обучителят да може да добие ясна представа за протичането на часа и неговото структуриране:

- 1. Въвеждаща дейност.** Това е бърза задача (например брейнсторминг), която има за цел да въведе темата на урока и да провери нагласите на учениците спрямо нея, базирани на личния им опит. Също така, те се настройват за същинската работа чрез създаването на добра работна атмосфера.

2. Основна дейност. Основната дейност е най-дълга като времетраене и обикновено включва 1-2 упражнения (инструменти), които засягат същността на темата. Упражненията са интерактивни и винаги ангажират пряко учениците. Използваните упражнения, които можете да намерите в този наръчник и да приложите, са:

Брейнсторминг. Мозъчната атака е стимулиращ и освобождаващ инструмент, в тази дейност децата са провокирани да изразят свободно какво мислят или знаят по дадената тема, като ключовото тук е, че няма вярно и грешно в това, което казват. Този вид упражнение подпомага мисленето, стимулира изразяването на мнение без притеснение и дава на учителя обратна връзка какво мислят децата, какви са нагласите, заблудите и къде липсват знания и умения.

Дискусия. При тази дейност учениците са насърчавани да мислят и да изразят своето мнение по определена тема. Ролята на учителя тук е много важна – той създава и поддържа позитивна атмосфера, в която всеки се чувства свободен да сподели какво мисли и да се аргументира. Важно е по време на дискусията всеки, който желае, да получи възможност да изрази своето мнение.

Групова работа. При тази дейност учениците развиват своите умения за работа в екип, докато едновременно работят и по темата на урока. Всеки участник в групата има своя роля – лидер/фасилитатор, човек, който води записки, човек, който следи времето, презентатор и т.н. Това помага на учениците да овладеят умения като комуникация, сътрудничество, решаване на проблеми, гъвкавост, наред с доверие, отговорност, уважение към съотборниците.

Викторина. Това упражнение, обикновено е вид игра, която стимулира развиване на определени умения като критично мислене, умения за комуникация, разрешаване на конфликти и разпознаване на рискови ситуации.

3. Заключителна дейност. Тя се използва, за да се обобщят новите знания и да се изследва мнението на учениците. Също така, по време на заключителната дейност те имат възможност да споделят емоциите от преживяното с другите, а водещият получава обратна връзка.

Всяка тема в наръчника включва интерактивни техники, тъй като при тях учениците си взаимодействат активно и случващото се може да бъде обсъдено. Предимството на интерактивните методи е, че чрез тях учениците не само получават знания, но преди всичко формират умения, изграждат нагласи и позитивно мислене, което способства за личностното им израстване. При този подход доминира дейността на ученика, неговото личностно развитие и утвърждаване, а учителят/обучителят играе по-скоро ролята на ментор, който насочва и подкрепя ученика в процеса през въпроси и поощрения.

Въвеждаща дейност: 7 - 10 минути	
Водещ	Ученици
Въвежда дейността, като обяснява каква е целта на урока и за какво ще говорим. Използва се, по избор, един от инструментите за въвеждаща дейност в съответната тема.	Учениците се включват във въвеждащата дейност и задават въпроси, ако имат.
Основна дейност: 20-25 минути	
Водещ	Ученици
Водещият избира един инструмент от упражненията за основна дейност от съответната тема, обяснява я добре на учениците/децата и се уверява, че всички са разбрали задачата. При избор на инструмент дискусия е важно водещият да следи всеки който иска, да има пространство да сподели мнението и да модерира дискусията така, че евентуално възникнал спор да не прерасне в конфликт.	Учениците се включват в дейността активно. Ако работят по групи, всяка група си избира говорител, който представя работата на групата. Ако дейността е дискусия – е важно всеки, който иска да вземе участие и да има пространство да сподели какво мисли.
Заклучителна дейност (обобщение на часа): 3-5 минути	
Водещ	Ученици
Водещият обобщава часа като задава въпроси на учениците: „Какво правихме през този час?“, „Какво беше полезно/ценно за вас?“.	Споделят своите наблюдения за това как е протекъл часът.

Всяка тема от наръчника предлага инструменти, които могат да се използват при провеждането на уроците. Обучителят/учителят има свобода да избира кой инструмент да приложи, включително и такива, които не са дадени в наръчника.

Дигиталната среда е естествена част от ежедневието на децата. Тя им дава достъп до знания, общуване, забавление, подкрепа и възможности за участие. В същото време онлайн пространството може да засили вече съществуващи неравенства и да изложи някои деца на по-висок риск от злоупотреби, манипулация, онлайн тормоз, експлоатация, дезинформация, вредно съдържание и реч на омразата.

Уязвимостта не е характеристика на самото дете. Тя възниква от средата, в която детето живее, от достъпа му до подкрепа, информация, образование, сигурни възрастни и подходящи услуги. Едно дете може да бъде много уверено в използването на телефон, социални мрежи или игри, но това не означава, че има достатъчно умения да разпознава риск, манипулация, фалшив профил, измама, натиск от връстници или вредно онлайн съдържание, нито да има идея или да разбира напълно защо точно някой може да е злонамерен в определена ситуация и какви могат да бъдат неговите лични мотиви за това. Затова в работата с децата е важно да не приемаме техническите умения за равни на дигитална грамотност.

Проектът „Дигитални деца 2“ поставя специален фокус върху децата, които поради социални, икономически, образователни, семейни или други фактори имат по-ограничен достъп до информация, подкрепа и безопасна среда. Това могат да бъдат деца от бедни семейства, деца от малцинствени общности, деца, живеещи в малки населени места или изолирани квартали, деца с ниска училищна ангажираност, деца, чиито родители имат ограничена дигитална грамотност, деца в риск от отпадане от училище, деца мигранти или бежанци, деца с езикова бариера, деца с увреждания, деца, преживели насилие, пренебрегване, загуба, семейна раздяла или други травматични събития.

Важно е този фокус да не води до поставяне на етикети. Не всяко дете от уязвима общност е непременно в риск, както и не всяко дете от привидно стабилна среда е защитено. Онлайн рисковете могат да засегнат всяко дете. Разликата е, че някои деца имат по-малко ресурси да разпознаят опасността, да потърсят помощ навреме или да бъдат подкрепени от възрастен, когато нещо се обърка.

Децата от уязвими общности често са изложени на няколко риска едновременно. Те могат да имат по-ограничени знания за настройките за сигурност и поверителност, по-малко опит в проверка на информация, по-слаба подкрепа от възрастни и по-силен натиск от групата на връстниците. Понякога родителите не разполагат с нужната информация, за да насочват децата си в онлайн пространството, а в други случаи самите родители са обект на дезинформация, измами или манипулативни кампании.

В България особено важен е фокусът върху деца от ромски общности и други групи, които често са обект на дискриминация, стереотипи и социално изключване. Фалшивите новини, речта на омразата, системните усилия за радикализиране на младежи в определени групи и медийните манипулации могат да задълбочат предразсъдъците към тях, но могат и да се разпространяват вътре в

самите общности, като предизвикват страх, недоверие и отказ от полезни услуги. Показателен пример е разпространението на слухове и конспиративни твърдения по време на COVID-19, както и случаи, при които фалшива информация е довела до паника сред родители и масово изтегляне на деца от училище.

Дезинформацията е особено силна, когато стъпва върху вече съществуващи страхове. Ако една общност има натрупан опит на бедност, изолация, дискриминация или недоверие към институциите, фалшивите новини могат да изглеждат по-убедителни. Затова противодействието на дезинформацията не може да се изчерпи само с казването „това не е вярно“. Нужно е да се работи с причините, поради които дадено послание изглежда достоверно: страх, липса на информация, недостъпни институции, лош предишен опит, ниска грамотност или липса на доверен посредник.

Уязвимостта в онлайн среда може да се прояви по различни начини:

- по-лесно приемане на покани за приятелство от непознати;
- споделяне на лични данни, снимки, адрес, училище или местоположение;
- участие в рискови онлайн предизвикателства;
- доверяване на фалшиви профили;
- попадане в измами, свързани с игри, награди, пари или профили;
- трудно разпознаване на фишинг съобщения;
- по-голяма податливост към онлайн тормоз и изнудване;
- по-трудно търсене на помощ поради срам, страх от наказание или липса на доверен възрастен;
- попадане в затворени групи, които по привлекателен за младежите начин разпространяват омраза, конспиративни теории, вредно съдържание или крайни идеи.

Особено внимание трябва да се обърне на децата, които се чувстват самотни, отхвърлени, унижени или несправедливо третирани. Онлайн групите понякога предлагат бързо усещане за принадлежност и признание. Това може да бъде положително, когато групата е подкрепяща и безопасна. Но може да бъде и рисково, когато групата изгражда мислене „ние срещу тях“, подхранва гняв към определени хора, насърчава омраза или представя насилието като оправдано. В такива случаи уязвимостта на детето може да бъде използвана от други хора.

Поради това работата с уязвимостта трябва да бъде внимателна, ненасилствена и подкрепяща. Децата не трябва да бъдат плашени, обвинявани или засрамвани. Когато едно дете е споделило лична информация, попаднало е на вредно съдържание, било е измамено или е общувало с рисков човек онлайн, първата реакция на възрастния е решаваща. Ако детето бъде наказано или осмяно, то вероятно ще се затвори и следващия път няма да потърси помощ. Ако бъде изслушано спокойно, шансът да се прекъсне рисковата ситуация е много по-голям.

При работа с деца от уязвими общности е важно да се използват ясни, достъпни и конкретни послания. Абстрактни понятия като „лични данни“, „поверителност“, „манипулация“, „алгоритъм“ или „дигитален отпечатък“ трябва да се обясняват чрез примери от ежедневието: телефон, снимка, чат, профил, игра,

училище, квартал, семейство, приятели. Добре работят казуси, ролеви игри, дискусии и упражнения, в които децата сами достигат до правилата за безопасност.

Особено полезно е включването на доверени посредници – учители, здравни медиатори, образователни медиатори, социални работници, училищни психолози, младежки работници, педагогически съветници, местни лидери и родители. Те могат да помогнат посланията да бъдат разбрани и приети, особено когато има ниско доверие към институциите. Работата с родителите е също толкова важна, колкото и работата с децата. Родителите не трябва да бъдат обвинявани, че „не разбират от технологии“. По-полезно е да бъдат подкрепени с кратки и практични насоки: как да говорят с детето, какво да наблюдават, кога да реагират, как да докладват и към кого да се обърнат.

Водещият трябва да помни, че дигиталната безопасност е свързана с доверие. Децата трябва да чуят ясно, че ако нещо ги притеснява онлайн, ако някой ги заплашва, изнудва, кара ги да пазят тайна, иска снимки, пари или лична информация, те имат право да потърсят помощ. Това не ги прави виновни. Виновен е човекът, който злоупотребява, заплашва, манипулира или наранява.

Работата с уязвимостта има три основни цели:

1. Да повиши знанията и уменията на децата за безопасно поведение онлайн.
2. Да намали риска децата да бъдат въввлечени в злоупотреби, манипулация, дезинформация, тормоз, експлоатация или крайни онлайн групи.
3. Да изгради мост между децата, родителите, училището, общността и професионалистите, така че помощта да бъде достъпна, навременна и не-накърняваща достойнството на детето.

Ключови насоки за водещия:

- Не поставяйте етикети на децата и общностите.
- Говорете за ситуации и поведения, а не за „лоши“ групи.
- Използвайте реалистични примери от онлайн живота на децата.
- Избягвайте език, който може да засрами участниците.
- Насърчавайте въпроси и споделяне, без принуда.
- Обяснявайте, че техническите умения не са същото като безопасност.
- Включвайте родителите и доверените възрастни, когато е възможно.
- Подчертавайте, че търсенето на помощ е правилна и смела реакция.
- При сериозен риск за дете следвайте процедурите за закрила и сигнализиране.
- При онлайн проблеми насочвайте към Националния център за безопасен интернет, Консултативната линия 124 123 и чата на www.safenet.bg.

Този подход позволява темата за уязвимостта да бъде разглеждана не като слабост на детето или общността, а като отговорност на възрастните и институциите да осигурят знания, подкрепа, доверие и безопасна среда.

5.1.

НЕТИКЕТ – ПРАВИЛАТА ЗА ПОЗИТИВНА КОМУНИКАЦИЯ В ИНТЕРНЕТ

Цели на урока: Участниците да познават правата си и ги прилагат. Изработват правила за комуникация онлайн, съобразени с правата и отговорностите на всеки участник.

**Обща информация**

Всяка среда, група и общество имат своите гласни и негласни норми и правила за етично поведение. За интернет тези норми и правила са познати под събирателното понятие Нетикет, съкратено от интернет етикет (Netiquette = Internet Etiquette). Нетикетът е набор от правила за спазване на добро поведение при изпращане на имейли, за общуване в социалните мрежи, в различни форуми и онлайн игри.

Интернет е социална среда за децата и затова е много важно преди започване на разговора за рисковете и възможностите на Мрежата – да обясним на децата какъв е етикетът на комуникация в онлайн пространството и да направим връзка с офлайн света. Защото на практика, правилата за позитивна и ненараняваща комуникация важат както офлайн, така и онлайн.

Важно е да се въведат правила (ако такива няма в групата/класа) заедно с децата. Чрез дискутирането и диференцирането на понятията „правила“, „права“ и „отговорности“ в основното упражнение в урока децата развиват чувствителност към правилата на етично поведение в Мрежата и когато ги създаваме заедно с тях, те са по-склонни да ги спазват. Допълнително, стават по-чувствителни към зачитането на правата на околните.

Тази тема поставя основата за по-нататъшна работа с наръчника и е препоръчително учителят/обучителят да започне с нея. Въвеждането на правила или припомнянето им при началото на всеки от уроците е необходимо условие за настрояване на групата за работа и напомняне на важните принципи в общуването.

Насоки при въвеждането на правила:

- ▶ Важно е правилата да изхождат от самите ученици – водещият ги приканва да дават предложения.
- ▶ Приемането на дадено правило става след кратко обсъждане/коментар с групата защо то е важно и след като е постигнато съгласие от всички.
- ▶ Правилата трябва да се изпишат на видно място, за да може да служат за пример и позоваване при нужда.
- ▶ Правилата трябва да са кратки, ясни и недвусмислени.

- ▶ Важно е правилата да са позитивно формулирани, за да формират позитивно мислене. Например – вместо предложеното „Да не говорим всички и да не вдигаме шум“, водещият може да помогне за преформулиране като „Да говорим един по един и да се изслушваме“.
- ▶ При затруднение водещият дава едно-две примерни правила, като ги обосновава.
- ▶ При необходимост в процеса на занятието може да се въведе ново правило, което да подобрява взаимодействието.

Учейки за правата си, децата разбират и как да се отнасят с другите, както и че правата са универсални и сме отговорни за зачитането им. Темата позволява дискутиране и формиране на собствено мнение и изграждане на ценности. Придобитите знания намират и практическо приложение в ежедневието при сблъскване със ситуации от различно естество, в които осъзнаването на собствените и чуждите права би спомогнало за по-толерантна и ефективна комуникация.



*Инструменти, които можете да ползвате, описани в раздел 6:
Инструменти 1, 9, 24*

5.2. КОМУНИКАЦИЯ ОНЛАЙН И ОФЛАЙН



Цел на урока: Участниците познават и прилагат принципите на ненасилствената комуникация в онлайн и офлайн контекст.

Уменията за ефективно общуване са сред най-ценените в съвременния свят – както офлайн, така и онлайн. Децата ги усвояват от най-ранна възраст от примерите на по-възрастните около тях. Училището също е изключително подходяща среда за развиване на уменията за общуване (не само яснотата на посланието, но и способността да слушаш и да откликваш с емпатия на отсрещната страна). Голяма част от конфликтите в ежедневието ни са породени именно от недоразуменията в общуването.

Д-р Маршал Розенберг е основател на подхода на ненасилствената комуникация (ННК), с която цели да предостави модел за разрешаване на межличностни конфликти. Този модел се основава на емпатия и честност, които за Розенберг са в основата на ефективната комуникация с околните. Той вярва, че моделът на ненасилствена комуникация има приложение и в училищната среда и говори за т. нар. обогатяващо живота образование: „образование, което подготвя учениците да учат през целия си живот, да се отнасят с разбиране към себе си и другите, да бъдат креативни, гъвкави и инициативни, както и да бъдат състрадателни не само към най-близките си, но и към целия свят“.



Ключови принципи на ненасилствената комуникация:

- 1. Наблюдение.** В различни ситуации, особено в конфликтните, е важно да можем да наблюдаваме, без да оценяваме или тълкуваме случващото се. Много често недоразуменията възникват, когато смесваме наблюденията с личните ни оценки. Особено важно е на този първи етап да се избягват директните критики и упреци, тъй като те провокират защитно поведение, блокират способността за изслушване и водене на конструктивен разговор и карат отсрещната страна да атакува на свой ред, вместо да сътрудничи.
- 2. Чувства.** Ненасилствената комуникация не изключва споделянето на чувства и емоциите, свързани с дадена ситуация. Изразяването на чувства обаче не е толкова лесно – те трябва да бъдат отделени от мислите и човек трябва да разполага с достатъчно богат речник, за да може да опише това, което чувства. Изказвания от типа „Чувствам се добре/зле“ са твърде неопределени. Ясното вербализиране на чувства е основна част от емоционалната интелигентност, която следва да бъде развивана у децата. Ключов елемент тук е, че чувствата не са пряко свързани с поведението на другия, а с нуждите, които то (поведението) провокира у нас.
- 3. Нужди.** Когато осъзнаем, че чувствата ни са пряко свързани с нашите собствени нужди, а не с това какво казват и правят другите, другите ще започнат по-лесно да ни разбират и съдействат. Ако не сме наясно с потребностите си, то тогава би било по-лесно да критикуваме и оценяваме една ситуация, вместо да спомогнем за разрешаването ѝ.
- 4. Молба.** Осъзнаването на нуждите ни помага да ги вербализираме ясно. Едва когато знаем какво искаме, можем да го поискаме от другите по ненасилствен начин. Важно е молбата да бъде формулирана по позитивен начин – какво искаме да се случи, а не какво не искаме (това би спестило объркване у другата страна). Колкото по-ясно формулираме молбата си, толкова по-голяма е вероятността другият да ни разбере правилно и да се отзове.



**Инструменти, които можете да ползвате, описани в раздел 6:
Инструменти 2, 11, 26**

5.3. ЛИЧНИ ДАННИ



Цели на урока: Участниците разпознават кои данни са лични и защо трябва да бъдат защитавани. Разбират какво е дигитален отпечатък и как личната информация може да бъде използвана за злоупотреба, измама, изнудване или създаване на фалшив профил. Участниците използват стратегии за ограничаване на видимостта на личната си информация онлайн и знаят кога и към кого да се обърнат за помощ.



Обща информация

Когато използваме интернет, социални мрежи, онлайн игри, приложения за чат, образователни платформи или сайтове за пазаруване, ние оставяме следи. Част от тях са видими – снимки, коментари, харесвания, публикации, потребителски имена, сторита, видеа, местоположение. Друга част остават по-малко видими за нас – история на търсене, IP адрес, идентификатори на устройство, бисквитки, данни за поведението ни в приложенията, информация за това с кого общуваме и колко време прекарваме в дадено съдържание.

Всички тези следи изграждат нашия дигитален отпечатък. Той може да бъде активен – когато сами публикуваме нещо, и пасивен – когато дадена платформа събира информация за нас, докато я използваме. Децата често разбират добре как да използват дадено приложение, но не винаги си дават сметка каква информация оставят след себе си и кой може да я види, запази или използва.

Лични данни са всяка информация, чрез която един човек може да бъде разпознат пряко или косвено. Това включва трите имена, снимка, телефонен номер, имейл, домашен адрес, училище, клас, ЕГН, номер на документ за самоличност, потребителско име, местоположение, IP адрес, глас, лице, здравна информация, семейна информация, данни за приятели и роднини. Понякога една отделна информация не изглежда опасна, но когато се събере с други данни, може да разкрие много за детето – къде живее, кога е само, в кое училище учи, с кого общува и какви са интересите му.

За децата защитата на личните данни е особено важна, защото те могат по-лесно да бъдат подвеждани да споделят информация, от която след това някой да се възползва по недобросъвестен и недобронамерен начин. Това може да се случи чрез игра, награда, фалшив профил, приятелско съобщение, анкета, тест „кой герой си“, линк към „безплатни награди“ или „безплатни монети“ в игра, фалшива техническа поддръжка, онлайн предизвикателство или натиск от връстници.

Личните данни могат да бъдат използвани по различни начини. С тях може да бъде създаден фалшив профил, да бъде откраднат акаунт, да се изпращат съобщения от името на детето, да се извърши измама, да се упражни натиск или изнудване, да се разпространят снимки без съгласие, да се проследи местоположение или да се събере информация за семейството. Понякога злоупотребата започва с нещо малко – например изпратена снимка или споделена парола – но може бързо да прерасне в сериозен проблем.

Важно е учениците да разберат, че личните данни не са само „тайни“ или „много важни документи“. Дори обикновена снимка може да съдържа информация: училищна униформа, табела на улица, номер на автомобил, лице на приятел, интериор на дома, екран с отворен чат, билет за пътуване, QR код или местоположение. Затова преди публикуване е полезно да се създаде рефлексът: „Какво се вижда на тази снимка?“, „Кой може да я види?“, „Има ли информация за мен или за друг човек?“, „Ще ми бъде ли неприятно, ако тази снимка бъде препратена?“.

Особено рисково е споделянето на пароли. Паролата не е доказателство за доверие и не трябва да се дава на приятели, гадже, съученици или хора, които се представят за служители на платформа. Децата трябва да знаят, че истинските платформи не искат паролата им в чат. Ако някой настоява за парола, код за вход, код от SMS, снимка на личен документ или достъп до профил, това е предупредителен знак.

Местоположението също е лична информация. Много приложения искат достъп до локация, дори когато това не е необходимо. Споделянето на местоположение в реално време, отбелязването от дома, училището или мястото, където детето тренира, може да създаде риск. Добра практика е локацията да се споделя само когато има ясна причина и само с хора, на които детето и семейството имат доверие.

Изследване на Центъра за безопасен интернет (2025) и директният опит за работа с деца показват, че младежите масово са с публичен профил. Публичните профили увеличават риска. Когато профилът е публичен, публикациите могат да бъдат видени, запазени, коментирани и препратени от непознати. Това не означава, че всяко дете трябва да бъде изключено от социалните мрежи, а че трябва да знае как да управлява видимостта си. Настройките за поверителност трябва редовно да се преглеждат, защото приложенията се променят. Добре е профилите на деца и тийнейджъри да бъдат ограничени така, че съдържанието да се вижда само от хора, които те познават и приемат да са сред тези, с които са приятели и могат да виждат какво публикуват.

При работа с учениците е полезно да се обсъдят следните правила:

1. Не споделяме пароли, кодове за вход и кодове за възстановяване.
2. Не изпращаме снимки на лични документи, банкови карти, билети, QR кодове или други чувствителни данни.
3. Не публикуваме адрес, училище, клас, телефонен номер или местоположение в реално време.
4. Проверяваме кой може да вижда публикациите, сторитата и списъка ни с приятели.
5. Приемаме покани само от хора, които наистина познаваме.
6. Мислим преди да публикуваме снимка – какво се вижда и кой друг е на нея.
7. Не тагваме други хора без съгласие и изключваме възможността да бъдем тагвани без изрично съгласие.
8. Ако получим странен линк, не въвеждаме парола или лични данни.

9. Ако някой ни заплашва, изнудва или иска лична информация, не отговаряме сами, а търсим помощ.
10. Ако сме сгрешили и сме споделили нещо, не се крием – казваме на доверен възрастен възможно най-рано.

Важно е да се подчертае, че търсенето на помощ не означава, че детето е виновно. Децата често се страхуват, че ще бъдат наказани, ако признаят, че са дали парола, изпратили са снимка или са кликнули на линк. Това мълчание може да направи ситуацията по-опасна. Водещият трябва ясно да каже, че всеки може да бъде подведен онлайн, а най-важното е да се реагира навреме.

Урокът трябва да развива не само знания, но и нагласи. Добре е участниците да упражнят проверка на настройките за поверителност, да обсъдят примери за рискови публикации, да разпознават фалшиви съобщения и да формулират лични правила за споделяне. Използвайте упражненията, за да развиете уменията им за критично мислене и да им създадете рефлекс да мислят, преди да публикуват нещо в социалните мрежи, дали да отбележат локацията си в публикацията, както и рефлекс/инстинкт за самосъхранение преди да кликнат върху даден линк, тъй като фишингът като начин за кражба на лични данни има застрашителни размери.



Инструменти, които можете да ползвате, описани в раздел 6:
Инструменти 4, 10, 13, 25, 26, 27, 28, 37

5.4. ДИГИТАЛЕН ИМИДЖ



Цели на урока: Да информира участниците за значението на дигиталния имидж и как той влияе на личната репутация, като подчертае важността на внимателното споделяне на информация, съвпадението между онлайн и офлайн поведение и защитата на личните данни.



Обща информация

Дигиталният имидж представлява общото впечатление, което оставяме в интернет чрез информацията, която споделяме, и поведението, което демонстрираме в дигиталното пространство. Това включва всичко – от публикации, снимки и видеоклипове, до коментари, харесвания и дори търсения. Тази съвкупност от информация формира виртуален образ, чрез който ни възприемат хората – приятели, колеги, работодатели и дори непознати. В днешно време дигиталният имидж е почти толкова важен, колкото личната репутация извън интернет.

Изграждането на дигитален имидж може да бъде както съзнателно, така и несъзнателно, а двата процеса често се преплитат. Съзнателно изграждаме дигиталния си имидж, когато планираме какво съдържание искаме да представим за себе си. Например, много хора подбират внимателно какви снимки

да публикуват или какви мнения да изразят, така че да проектират позитивен, професионален или вдъхновяващ образ. Когато публикуваме статии, свързани с нашата работа, или изразяваме мнение по социални и екологични въпроси, ние контролираме какви качества и ценности искаме другите да свързват с нас. В дигиталното пространство правим доста неща, които не обмисляме задълбочено, но които също допринасят към нашия дигитален имидж несъзнателно. Случайни коментари, безразборно „харесване“ на съдържание или споделяне на новини без проверка на източника са примери за това как неволни действия могат да оставят траен отпечатък. Дори малките „дигитални следи“, като групите, в които членуваме, или рекламите, на които реагираме, формират част от начина, по който сме възприемани онлайн.

Защо е важно да знаем как изграждаме дигиталния си имидж?

Траен отпечатък: Всичко, което публикуваме онлайн, може да остане за дълго време и е възможно да бъде достъпно за широк кръг от хора. Това означава, че трябва да внимаваме с информацията, която споделяме, защото тя може да ни влияе дълго след като сме забравили за нея. Един недобре обмислен пост може да се окаже решаващ в даден момент – например, ако бъде видян от потенциален работодател.

Консистентност между онлайн и офлайн поведение: Един успешен дигитален имидж е този, който е автентичен и съответства на истинските ни качества. Когато онлайн образът ни не отговаря на реалната ни същност, това може да създаде неразбирателства и разочарования, както и да навреди на взаимоотношенията ни. Важно е да се стремим дигиталният имидж да отразява искрено нашите ценности и качества.

Личност и сигурност: Критичното изграждане на дигиталния имидж означава и да се замисляме кои части от информацията за нас са достъпни за другите. Съществуват настройки за поверителност в социалните мрежи, които помагат да ограничим видимостта на лична информация и да избегнем споделянето на съдържание с хора, които нямаме интерес да знаят повече за нас. Освен това, критичният подход към споделянето ни защитава от възможни негативни влияния върху репутацията и личната сигурност.

Дигиталният имидж е нашият виртуален „аз“, който влияе на начина, по който ни възприемат в обществото. Той може да играе роля при приемането ни в университет, в професионалното развитие или в създаването на нови контакти. Съзнателното изграждане на този имидж ни помага да комуникираме по-ясно кои сме, докато защитаваме своята лична сигурност и репутация. Важно е да бъдем осъзнати за дигиталния си отпечатък и да поддържаме последователност между това, което показваме онлайн, и нашите реални качества.



**Инструменти, които можете да ползвате, описани в раздел 6:
Инструменти 1, 4, 12, 14, 15, 26**

5.5. ВРЕДНО ОНЛАЙН СЪДЪРЖАНИЕ



Цели на урока: Участниците разпознават вредното онлайн съдържание. Разпознават и назовават емоциите, които провокира в тях различното съдържание онлайн. Осъзнават последствията от прекомерното излагане на съдържание с насилие. Използват стратегии за справяне с вредното онлайн съдържание.



Обща информация

Наред с възможностите за създаване и откриване на позитивно и полезно съдържание, социалните мрежи и медиите често стават пространство, в което се споделя и разпространява вредно онлайн съдържание. Децата и тийнейджърите са активни потребители на интернет и това ги прави потенциални жертви на вредното онлайн съдържание. В някои случаи попадането на такова съдържание може сериозно да повлияе на младия човек, затова е добре той да знае какво трябва да направи и към кого да се обърне.

Вредното онлайн съдържание може да бъде уебсайт, публикация или група за пропаганда на анорексия или булимия, на наркотични вещества, подтикване към самоубийство, саморазправа или друг вид вредно за здравето и безопасността на децата поведение. В последните години към това съдържание спадат и популярните онлайн предизвикателства (напр. правене на рискови селфита или видеа, поглъщане на опасни субстанции и т.н.). Част от това съдържание, например популяризирането на хранителни разстройства или онлайн предизвикателствата, могат да бъдат открити сравнително лесно в социалните мрежи в страници или открити групи. Друго съдържание (напр. популяризирането на зависимости) се споделя предимно в скрити (тайни) групи, които не могат да бъдат намерени от човек, който не е техен член.

Друг важен въпрос, който поставя тази тема, е за прекомерното излагане на съдържание с насилие, което в дългосрочен план може да има множество негативни последици. Когато един човек често става свидетел на насилие, независимо реално или виртуално, то е по-вероятно самият той да стане по-агресивен и да упражнява насилие. Механизмът, по който се случва това, е т. нар. десенситизация – колкото повече се сблъскваме с даден стимул, толкова по-малко ни влияе той. В случая с насилието става въпрос за емоционална десенситизация, която е намален емоционален отговор при натъкване на случаи, картини, видеа и т.н., съдържащи насилие.

Интересен аспект на емоционалната десенситизация е, че тя може да се пренесе в различен контекст. Ако някой често става свидетел на насилие в интернет, то е по-вероятно да спре да забелязва насилието в реалния живот, и обратното. Също така, ако някой често става свидетел на физическо насилие например, то по-вероятно е да спре да забелязва вербалното насилие като заплахите, обидите и т.н. Увеличеното излагане на насилие води до намаляване на емпатия към жертвите, както и на опитите да им се помогне. Важно е да се отбележи, че насилието онлайн е по-вероятно да доведе до намаляване на общата чувствителност, тъй като реалното насилие обикновено е по-интензивно от това в интернет и е по-трудно да се привикне към него толкова лесно. В този смисъл е от

значение децата да могат да разпознават формите на онлайн насилие и да знаят по какъв начин могат да се справят и да се предпазят от негативните последици, които това би могло да има върху психическото им и емоционално съзряване.

Друг вид опасност за младите хора в интернет е радикализацията – процес, обусловен от различни фактори. В този процес значение има и интернет, тъй като създава привидното усещане за анонимност¹. В националната Стратегия за противодействие на радикализацията и тероризма (2026-2030 г.) *„радикализацията се характеризира с решителна готовност за налагане на собствените възгледи и принципи над тези на останалата част от обществото, чрез отхвърляне на конституционните устои на демокрацията и непризнаване на фундаменталните права на човека. Много често води до споделяне на идеологията на насилието.“*

В зависимост от склонността към насилие, радикализацията може да бъде насилствена (или водеща до насилие) или когнитивна (не пряко свързана с насилствени действия). Тя може да има политически или религиозен характер, като началните прояви не винаги включват сериозни нарушения на обществения ред. Въпреки това, тези прояви често ескалират, прераствайки в по-сериозни противообществени действия, като палежи, нанасяне на средни и тежки телесни повреди или дори убийства.

Радикализацията е сложен процес, при който личностни качества на индивида се преплитат с политически и социални фактори. Това означава, че при едни и същи условия един човек може да не се радикализира, докато друг може да се превърне в терорист дори под по-слабо външно въздействие. Уязвимостите на личността често се изострят от усещането за заплаха, насочена към него самия или към групата, с която се идентифицира. Ключов етап в процеса е промяната в начина, по който индивидът тълкува различни житейски събития, като започва да ги възприема през призмата на определена идеология.

Онлайн пространството също играе роля, предоставяйки платформа за скрити групи от хора със сходни политически или религиозни убеждения. В тези групи често се споделят непроверени или умишлено манипулирани новини, които целенасочено усилват радикализацията. Членовете на подобни групи създават и използват символи, жестове и други знаци, които подчертават тяхната принадлежност и съпричастност към идеите на групата.

Причината за попадането в такива среди винаги е комплексна – от лош късмет и случайност, до целенасочено вербуване или провокирано от конкретно събитие, което е травматично или събужда определен интерес. Структурни фактори като бедност, ниво на образование и културни влияния се преплитат с външни въздействия, създавайки процеси на индивидуално, групово и обществено ниво.

Националният център за безопасен интернет приема сигнали за вредно онлайн съдържание. Децата (или техните родители) могат да се свържат с Консултативната линия за онлайн безопасност 124 123 (директно набиране от всеки мобилен оператор) и да споделят къде са попаднали на вредно съдържание и

¹ „Превенция и разкриване на радикализация, насилствен екстремизъм, реч на омразата и полицейска дейност в ромските общности“- наръчник на обучители, София 2023, издание на МВР в рамките на НМФ.

какво е това. След това със съдействието на консултант могат да подадат сигнал на Горещата линия към Центъра за безопасен интернет.



Инструменти, които можете да ползвате, описани в раздел 6:
Инструменти 5, 23, 29, 36, 37

5.6. СИГУРНОСТ В МРЕЖАТА



Цели на урока: Участниците правят сравнение между сигурността онлайн и офлайн. Познават основните рискове за профилите, устройствата и личната информация. Създават по-сигурни пароли, използват двуфакторна защита, разпознават фишинг и измамни съобщения, и знаят как да реагират при съмнение за компрометиран профил или устройство.



Обща информация

Сигурността в мрежата означава да пазим профилите, устройствата, личните си данни и комуникацията си така, както пазим личните си вещи в реалния свят. Не оставяме отключена входната врата, не даваме ключовете си на непознати и не оставяме лични документи на публично място. По същия начин не трябва да оставяме профилите си незащитени, да споделяме пароли, да кликаме на съмнителни линкове или да даваме лична информация на хора, които не познаваме.

Децата често използват много профили едновременно – социални мрежи, игри, училищни платформи, имейл, приложения за чат, видео платформи. За тях някои от тези профили имат огромна стойност: акаунт в игра с натрупани предмети, профил с много последователи, чатове с приятели, снимки и спомени. Затова кражбата на профил може да бъде преживяна много тежко и да доведе до срам, страх, изнудване, загуба на контакти или злоупотреба с името на детето.

Най-честите рискове за сигурността са слаби пароли, използване на една и съща парола на много места, споделяне на пароли с приятели, липса на двуфакторна защита, кликуване върху фишинг линкове, инсталиране на съмнителни приложения, използване на публични Wi-Fi мрежи за чувствителни действия, фалшиви профили за техническа поддръжка и измами, свързани с онлайн игри.

ПАРОЛИТЕ

Силната парола е първата защита на профила. Тя не трябва да бъде име, рожден ден, име на домашен любимец, любим отбор, последователност от цифри или дума, която лесно може да бъде позната. Добра практика е да се използва дълга парола или паролна фраза – няколко думи, които са лесни за запомняне, но трудни за отгатване. Още по-добре е всяка регистрация да има различна парола.

Използването на една и съща парола навсякъде е опасно. Ако една платформа бъде пробита или някой научи паролата от един профил, той може да опита

същата парола и в други профили – имейл, социална мрежа, игра, училищна платформа. Затова учениците трябва да разберат, че повторението на пароли е като да имаш един ключ за дома, училището, велосипеда и банковата карта.

При по-големи ученици може да се обсъди използването на мениджър на пароли с подкрепата на родител или настойник. При по-малки деца е важно да се изгради основният навик: паролата е лична и не се споделя.

ДВУФАКТОРНА ЗАЩИТА

Двуфакторната защита добавя втори слой сигурност. Това означава, че освен парола, при влизане в профила се изисква още едно потвърждение – например код от приложение, код от SMS, известие на устройство или друг метод. Така, дори ако някой научи паролата, няма автоматично да получи достъп до профила.

Важно е учениците да знаят, че кодовете за вход също не се споделят. Ако някой пише „прати ми кода, за да ти помогна“, „ще ти върна профила“, „трябва ми кодът, за да получиш награда“ или „аз съм от поддръжката“, това най-вероятно е измама. Кодът за вход е като временен ключ и трябва да остане само при собственика на профила.

ФИШИНГ И ИЗМАМИ

Фишингът е опит някой да ни подведе да дадем парола, код, лични данни или достъп до профил. Това може да стане чрез имейл, SMS, съобщение във Viber, WhatsApp, Messenger, Instagram, TikTok, Discord, Telegram, училищна платформа или чат в игра. Фишингът често изглежда спешен: „Профилът ти ще бъде изтрит“, „Нарушил си правилата“, „Спечели награда“, „Потвърди веднага“, „Някой се опитва да влезе“, „Вземи безплатни скинове“, „Гласувай за мен в конкурс“.

Основни признаци на фишинг:

- съобщението създава паника или силно изкушение;
- иска бърза реакция;
- съдържа линк към страница за вход;
- иска парола, код, лични данни или снимка на документ;
- подателят изглежда странно или имитира позната платформа;
- има правописни грешки, необичаен език или лош превод;
- обещава награда, пари, последователи, предмети в игра или възстановяване на профил;
- идва от човек, който твърди, че е „поддръжка“, но пише през личен профил.

Добро правило е: ако съобщението те кара да бързаш, спри и провери. Не се влиза в профил през линк от съобщение. По-безопасно е приложението или сайтът да се отвори директно, както обикновено, и там да се провери дали има реално известие.

ОНЛАЙН ИГРИ И ПЛАТФОРМИ ЗА ОБЩУВАНЕ

Гейминг средата е важна част от живота на много деца. Там те общуват, създават приятелства и изграждат принадлежност. Но в игрите също има рискове: измами за предмети, валута или акаунти; фалшиви „админи“; линкове към външни сайтове; натиск за споделяне на профил; обиден език; контакт с непознати; покани за частни чатове в други приложения.

Учениците трябва да знаят, че правилата за сигурност важат и в игрите. Не се споделя парола. Не се влиза в сайт за „безплатни“ награди. Не се изпращат снимки или лична информация на хора, познати само от игра. Ако разговорът стане неприятен, заплашителен, сексуален или изисква тайна от възрастните, детето трябва да прекъсне контакта и да потърси помощ.

УСТРОЙСТВА И ПРИЛОЖЕНИЯ

Сигурността не се отнася само до профилите, но и до устройствата. Телефонът, таблетът и компютърът трябва да имат заключване – PIN, парола, пръстов отпечатък или лицево разпознаване, според възрастта и устройството. Приложенията трябва да се свалят от официални магазини, а не от случайни линкове. Добре е операционната система и приложенията да се обновяват редовно, защото обновяванията често поправят пропуски в сигурността.

Публичните Wi-Fi мрежи могат да бъдат удобни, но не са подходящи за чувствителни действия като онлайн банкиране, въвеждане на важни пароли или изпращане на лични документи. При деца основното правило е да не въвеждат пароли и лични данни в непознати мрежи и да се консултират с възрастен, когато имат съмнение.

КАК ДА РАЗБЕРЕМ, ЧЕ ПРОФИЛЪТ МОЖЕ ДА Е КОМПРОМЕТИРАН?

Възможни признаци са:

- паролата вече не работи;
- имейлът или телефонът за възстановяване са променени;
- приятели получават странни съобщения от профила;
- има публикации, които детето не е качвало;
- профилът следва непознати страници или хора;
- има известия за вход от непознато място или устройство;
- липсват снимки, съобщения или настройки са променени;
- някой иска пари или снимки, за да „върне“ профила.

КАКВО ДА НАПРАВИМ ПРИ СЪМНЕНИЕ ЗА ПРОБИТ ПРОФИЛ?

1. Да не се паникьосваме.
2. Да кажем на доверен възрастен.
3. Да сменим паролата от сигурно устройство, ако все още имаме достъп.
4. Да излезем от всички устройства чрез настройките за сигурност.
5. Да включим двуфакторна защита.
6. Да проверим имейла и телефона за възстановяване.
7. Да предупредим приятелите да не отварят странни линкове, изпратени от профила.

8. Да докладваме проблема към платформата.
9. Да пазим доказателства – скрийншоти, съобщения, имейли.
10. При изнудване, заплахи или сериозен риск да потърсим помощ от възрастни, НЦБИ или компетентните органи.

КАК ДА ГОВОРИМ С УЧЕНИЦИТЕ ЗА СИГУРНОСТ?

Темата не трябва да се представя като списък със забрани. По-добре е да се покаже връзката между сигурността и свободата: когато профилът е защитен, детето има повече контрол, повече спокойствие и по-малък риск някой да злоупотреби с него. Добре е да се използват реалистични казуси: фалшива награда в игра, съобщение от „поддръжка“, приятел, който иска парола, линк за гласуване, публичен Wi-Fi, изгубен телефон, хакнат профил.

Основното послание към учениците е: „Не е нужно да се справяш сам.“ Ако нещо изглежда съмнително, ако си кликнул на линк, ако си дал парола, ако някой те заплашва или ако профилът ти е откраднат, най-важното е да кажеш навреме на възрастен, на когото имаш доверие. Колкото по-рано се реагира, толкова по-лесно може да се ограничи вредата.

Едни от основните инструменти, с които възрастните разполагат в този случай, са дискусиите и откритото обсъждане на тези въпроси. Този урок помага за развиването на чувствителността на тийнейджърите към личните им данни онлайн. Тази чувствителност и изграждането на умения за защита на личните данни от възможно най-ранна възраст са в основата на едно добро и активно дигитално гражданство в бъдеще. Урокът полага основите на сигурността в социалните мрежи - създаването на защитен профил и засилването на чувствителността към споделянето на лична информация онлайн, което е добра отправна точка за по-нататъшно обсъждане на въпроса какъв дигитален отпечатък оставяме.



*Инструменти, които можете да ползвате, описани в раздел 6:
Инструменти 4, 19, 28, 37*

5.7. ОНЛАЙН ТОРМОЗ (Тормоз в училище и онлайн)



Цели на урока: Участниците дефинират онлайн тормоз и разграничават училищния от онлайн тормоза, и ролите в тормоза. Учениците развиват умения да формулират и прилагат стратегии за справяне с онлайн тормоз и умения за работа в екип.



Обща информация

Колкото повече порастват децата, толкова по-сложни стават отношенията им. Групата на връстниците включва хора, които са близки по интереси, разбирания, социален статус и т.н. Те прекарват много време заедно (най-вече в училище) и в тази група търсят подкрепа, разбиране и одобрение, които често не

получават в пълна степен от възрастните. В този етап от техния живот за тях е важно да „проиграят“ и усвоят умения за общуване, да натрупат социален опит и да получат информация и знания по различни теми.

Някои от децата обаче не преминават през този период толкова леко и без проблемно. Конфликтите, споровете, разрушените приятелства са често срещани. „Грозното лице“ на отношенията сред децата на тази възраст обаче е тормозът – умишленото използване на сила и власт, за да бъде сплашен някой по-уязвим ученик. Ако конфликтите и скарванията между доскорошни приятели са малко или много обичайни и обикновено се случват между равни, то тормозът може да приеме много крайни форми и обикновено е системен и насочен към по-беззащитни и уязвими връстници (или по-малки деца). До голяма степен това отличава тормоза от насилието, което може да бъде и еднократен акт.

От значение е учениците да са запознати с формите на тормоза в училище и да знаят, че всяка от тях е неприемлива:

- ▶ **Физически** – удряне, блъскане, ритане, щипане, спъване, плюене, замеряне с различни предмети, задържане чрез физически контакт и др.;
- ▶ **Вербален** – заплашване, дразнене, обиждане, подигравки, изнудване, наричане с обидни имена, разпространяване на лъжи и слухове и др.;
- ▶ **Емоционален/психически** – избягване, игнориране, преднамерено изключване от група или занимание, манипулиране, осмиване и др.;
- ▶ **Сексуален** – сексуализирани прякори, словесни коментари, бележки и надписи със сексуално съдържание, показване на неприлични жестове и действия, разпространение на истории и изображения със сексуален подтекст, сексуално докосване, показване на порнографски материали, показване на интимни части на тялото и сваляне на дрехи, подтикване или принуждаване към сексуални действия, заснемане в сексуални пози.

Тормозът в училище може да се случи на много места – класната стая, тоалетните, коридора, двора. Това означава, че много често присъстват и свидетели на случващото се между извършителя и жертвата. Извършителят може да е мотивиран от желанието си да бъде популярен и харесван от своите връстници, както и да все у тях страх и респект. От огромно значение е да се помни, че децата, които упражняват тормоз в училище, е много вероятно да са жертва на насилие в собствените си домове или на друго място. За тях това е заучен модел на поведение, начин на справяне и взаимодействие с околните. Това е важно да се има предвид при справянето в подобни ситуации – насилникът също има нужда от подкрепа и помощ.

Около извършителя нерядко има и малка група от деца, които активно го подкрепят, но без да вземат лидерската роля. Възможно е те също да бъдат извършители (напр. също да обиждат, удрят, бутат и т.н.) или да подкрепят чрез одобрение, смях, поддържане на вниманието към случващото се. Тормозът има и пасивни наблюдатели – такива, които не взимат никакво отношение към случващото се (нито подкрепят тормоза, нито се противопоставят). В повечето случаи те са ключът към това тормозът да бъде прекратен. Когато децата имат изградена нагласа, че тормозът е нещо неприемливо, е по-вероятно да подкрепят жертвата и да се обърнат за помощ към някой по-възрастен. Тормозът сам по

себе си спира само когато децата си тръгнат от училище, но тогава спира само физическият тормоз.

Интернет позволява реалните конфликти да бъдат пренесени онлайн, а децата се възползват от тази възможност. Онлайн тормозът е използването на интернет за нанасяне на емоционална вреда на други хора. Това е и най-често срещаният онлайн риск за децата в България. Онлайн тормозът често се корени във взаимоотношенията в реалността (най-вече в училище), но това, което го прави особено нараняващ, е, че се случва в интернет, т.е. той може да бъде непрекъснат и може да бъдат видян от много хора (напр. сбиването между двама ученици може да има няколко непосредствени свидетели, но обиден коментар в интернет може да бъде видян от стотици хора).

Днешните деца са много уверени в начина, по който използват интернет мобилните технологии, и често пъти не осъзнават потенциалните рискове – както за себе си, така и за това какво могат да причинят на другите в интернет. Не е изключено обидите и коментарите, както и кражбите на профили например, да се правят на шега. Също така, първоначално тормозът може да започне като форма на отмъщение от наранено бивше гадже или пък като опит за унижаване от страна на оскърбен съперник/съперничка. Друга възможна причина за възникването на тормоз може да бъде затруднението на момичето/момчето да се впише в средата си, срещането на агресивно или враждебно поведение от страна на другите, ниско самочувствие или притеснения, които го спират да общува свободно с околните.

Има различни признаци, че едно дете преминава през някакъв труден период, като това може да включва и онлайн тормоз. Важно е учителят да подходи внимателно към ситуацията, за да определи какви трудности изпитва ученикът и каква намеса би била най-подходяща в случая.

Признаци:

- Изолиране от групата на връстниците;
- Честа смяна на настроеността;
- Повишен стрес;
- Проява на агресия;
- Депресивна симптоматика;
- Отсъствия от училище;
- Загуба на интерес към училищните дейности;
- Спад в успеха;
- Самонараняване;
- Промяна на приятелския кръг;
- Прекомерна употреба на мобилно устройство или пълен отказ да бъде използвано такова.

Много е трудно ситуацията на онлайн тормоз да бъдат прекъснати веднага. Онлайн тормозът се случва 24 часа в денонощието и е вероятно да ангажира вниманието на много хора. Също така възможно е определено съдържание да бъде разпространено на различни места (напр. обидна страница, фалшив про-

фил, груби коментари под различни снимки) и да е трудно да бъде премахнато на момента. Към това се прибавя и притеснението на децата да споделят за случващото се, в резултат на което остават прекалено дълго време в дадената ситуация, която може и да се усложни.

Ако онлайн тормозът се извършва от дете в същото училище, добре е да се говори с двете деца поотделно, за да не нараства напрежението между тях и за да може професионалистът, водещ разговора, да не заема несъзнавано ролята на защитник/обвинител спрямо някоя от страните. Важно е в такъв момент да бъдат отразени преживяванията на жертвата, за да може тя да почувства подкрепа и да се увери, че има кой да ѝ помогне за справянето с този проблем. Тъй като онлайн тормозът има множество свидетели, чувствата на срам и тъга у жертвата могат да са дори още по-засилени. След овладяването на първоначалните емоции се преминава към възможни стратегии за справяне според потребностите на ученика, които той може да заяви в поверителен разговор.

От друга страна, подходът към тормозещия също следва да бъде възможно най-щадящ – такива деца често се ангажират с модели на поведение, които са усвоили на по-ранен етап. Възможно е самите те също да са жертва на насилие, което да ги кара да се държат по този начин. Важно е да се стигне до дълбочината на проблема, за да може той да бъде разрешен по ефективен начин. Често е необходима по-дългосрочна работа с деца, които извършват насилие и тормозят други деца.

Ако се сблъскате със случай на онлайн тормоз, може да се свържете с Консултативната линия за онлайн безопасност на Националния център за безопасен интернет на тел. 124 123 или през чата на www.safenet.bg за съвет от обучен консултант.

Препоръчваме ви също да се запознаете с Механизма за противодействие на тормоза и насилието в образователните институции, разработен от Министерството на образованието и науката, който включва насоки за превенция и интервенция при случаи на тормоз, включително онлайн.



*Инструменти, които можете да ползвате, описани в раздел 6:
Инструменти 6, 9, 16, 30, 37*

5.8. СЕКСТИНГ



Цели на урока: Участниците дефинират „секстинг“ и разбират защо размяната на интимни съобщения, снимки или видеа може да носи сериозни рискове. Разграничават доверие, натиск, манипулация и принуда в интимното онлайн общуване. Познават възможните емоционални, социални и правни последствия от разпространението на интимно съдържание. Развиват умения да поставят граници, да казват „не“, да търсят помощ и да реагират без срам и самообвинение, ако попаднат в рискова ситуация..



Обща информация

Дигиталните технологии са част от начина, по който децата и младежите общуват, флиртуват, изграждат приятелства и първи интимни отношения. За много тийнейджъри телефонът е основно средство за поддържане на близост – чрез чатове, снимки, видеа, сторита, реакции и лични съобщения. Това прави онлайн общуването важно пространство за разговори за доверие, граници, уважение и безопасност.

Секстингът представлява размяна на съобщения, снимки или видеа със сексуално съдържание. Най-често се случва между хора, които се харесват, флиртуват или са във връзка. Понякога може да изглежда като израз на доверие и близост, но може да бъде и резултат от натиск, страх да не загубиш връзка, желание за одобрение, подражание на връстници или опит да се докаже любов.

Важно е участниците да разберат, че не всяка ситуация, която изглежда „доброволна“, е наистина свободен избор. Ако някой настоява, притиска, заплашва, обижда, казва „ако ме обичаш, ще го направиш“, „всички го правят“, „няма страшно“, „само аз ще го видя“ или „ще ти се разсърдя, ако не ми пратиш“, това вече е натиск. В такава ситуация детето или младежът има право да откаже, без да се чувства виновен.

Секстингът крие риск, защото след изпращане на снимка, видео или съобщение контролът върху него се губи. Дори когато е изпратено в личен чат, другият човек може да направи екранна снимка, да запише екрана, да го препрати, да го качи в група или да го използва по-късно за натиск. Някои приложения съобщават за скрийншот, но това не е пълна защита. Възможно е съдържанието да бъде заснето с друго устройство или запазено по друг начин.

Разпространението на интимно съдържание може да доведе до онлайн тормоз, подигравки, изолация, чувство на срам, вина, страх, предателство и загуба на доверие. При децата и младежите тези последствия могат да бъдат много тежки, защото групата на връстниците има голямо значение, а публичното унижение може да се преживее като „край на света“. Затова е важно възрастните да реагират спокойно, подкрепящо и без обвиняване.

Основното послание към учениците трябва да бъде ясно: ако интимна снимка или видео бъде разпространено без съгласие, отговорността е на човека, който го е разпространил или използвал за натиск, а не на детето, което е било убедено, подведено, притиснато или е проявило доверие. Засрамването на потърпевшото дете може да задълбочи вредата и да го откаже да търси помощ.

ПРАВЕН АСПЕКТ

Важно е да се обясни на достъпен език, че интимни изображения на лица под 18 години са изключително чувствителна и рискована категория съдържание. Създаването, притежаването и разпространяването на сексуализирани изображения или видеа на непълнолетни може да има сериозни правни последствия. Дори когато снимката е изпратена между връстници, нейното препращане, публикуване или използване за подигравка и натиск може да бъде престъпление и трябва да се приема сериозно.

Този правен аспект трябва да бъде представен не с цел плашене, а като защита на децата. Учениците трябва да разберат, че чуждата интимност не е съдържание за шега, споделяне или отмъщение. Ако някой получи такава снимка, правилната реакция не е да я препрати, а да не участва в разпространението и да потърси помощ от възрастен.

AI И НОВИТЕ РИСКОВЕ

В последните години рискът се увеличава и заради инструменти с изкуствен интелект. Вече е възможно да се създават фалшиви интимни изображения или видеа, които изглеждат реалистично, без човекът никога да е правил такава снимка. Това може да се случи чрез обработка на обикновена снимка от социална мрежа или чрез поставяне на лице върху чуждо тяло. Такива изображения често се наричат *deepfake* или генерирано интимно съдържание.

За децата е важно да знаят две неща. Първо, създаването или разпространението на такива изображения е форма на злоупотреба и може да има сериозни последици. Второ, ако някой ги заплашва с фалшива интимна снимка, те не са виновни и трябва веднага да потърсят помощ. Дори когато изображението е „фалшиво“, преживяването за детето може да бъде напълно реално – страх, срам, паника, унижение и усещане за загуба на контрол.

ЗАЩО ТИЙНЕЙДЖЪРИТЕ СА УЯЗВИМИ?

В юношеска възраст младите хора търсят близост, приемане, самостоятелност и признание. Понякога те трудно различават истинското доверие от манипулацията. Могат да изпратят снимка, защото се страхуват да не бъдат изоставени, защото искат да се почувстват харесвани, защото вярват, че „това е нормално“, или защото някой ги убеждава, че отказът означава липса на любов.

Натискът може да идва от партньор, човек, когото детето харесва, връстници, онлайн познат или непознат профил. При някои момичета натискът може да бъде свързан с това да изглеждат привлекателни и „достатъчно смели“. При някои момчета може да има натиск да доказват мъжественост, опит или популярност. И в двата случая възрастните трябва да избягват стереотипи и обвинения. Темата трябва да се постави през уважение, граници и право на отказ.

КАКВО ТРЯБВА ДА ЗНАЯТ УЧЕНИЦИТЕ?

1. Никой няма право да изисква интимна снимка или видео като доказателство за любов, доверие или вярност.
2. Отказът е право. Не е нужно да се обясняваш дълго, за да кажеш „не“.
3. След изпращане на съдържание контролът върху него може да бъде загубен.
4. „Изчезващи“ съобщения и снимки не са пълна защита.
5. Не трябва да се препраща интимно съдържание на други хора.
6. Ако получиш интимна снимка на друг ученик, не я разпространявай и не я показвай.
7. Ако някой те притиска, заплашва или изнудва, потърси помощ.
8. Ако вече си изпратил/а снимка и се притесняваш, пак можеш да получиш помощ.

9. Ако някой създаде фалшива интимна снимка с AI, това е злоупотреба, а не твоя вина.

10. Най-важното е да не оставаш сам/а в ситуацията.

СТРАТЕГИИ ЗА ОТКАЗ

Добре е учениците да упражнят конкретни фрази, защото в реална ситуация често е трудно да се реагира спокойно. Примерни отговори:

- „Не искам да изпращам такива снимки.“
- „Ако ме уважаваш, няма да настояваш.“
- „Не ми е комфортно с това.“
- „Не доказвам доверие със снимки.“
- „Не. Това е мое решение.“
- „Спирам този разговор.“
- „Ще говоря с възрастен, ако продължиш да настояваш.“

При нужда детето може да прекъсне разговора, да блокира профила и да запази доказателства. Не е нужно да убеждава другия човек дълго. Поставянето на граница е достатъчна причина.

КАКВО ДА НАПРАВИМ, АКО ИНТИМНО СЪДЪРЖАНИЕ ВЕЧЕ Е ИЗПРАТЕНО?

1. Да не се изпраща повече съдържание.
2. Да не се отговаря на натиск с нови снимки или видеа.
3. Да се запазят доказателства – съобщения, профили, линкове, скрийншоти.
4. Да се блокира човекът, ако няма непосредствена нужда да се запази комуникация за доказателства.
5. Да се докладва профилът или съдържанието в платформата.
6. Да се говори с доверен възрастен възможно най-рано.
7. Да се потърси помощ от Националния център за безопасен интернет чрез 124 123 или www.safenet.bg.
8. При заплахи, изнудване или риск за безопасността да се потърси съдействие от компетентните органи.

КАК ДА РЕАГИРА ВЪЗРАСТНИЯТ?

Първата реакция на възрастния е решаваща. Полезни реакции са: „Радвам се, че ми каза“, „Ще ти помогна“, „Не си сам/а“, „Ще действаме спокойно“, „Вината е на този, който злоупотребява“. Неподходящи реакции са: „Как можа?“, „Сам/а си си виновен/виновна“, „Забранявам ти телефона“, „Ще кажа на всички“, „Това е срам“. Такива реакции могат да задълбочат травмата и да попречат на детето да съдейства.

Целта на урока не е да създаде страх от интимните отношения, а да помогне на младите хора да изграждат отношения, основани на уважение, съгласие и лични граници. Секстингът трябва да бъде обсъждан не само като „онлайн риск“, а и като тема за доверие, натиск, самоуважение и правото на всеки човек да контролира собственото си тяло и образ.



**Инструменти, които можете да ползвате, описани в раздел 6:
Инструменти 7, 17, 18, 31, 32, 33, 37**

5.9. НЕПОЗНАТИ В МРЕЖАТА И РИСКЪТ ОТ СЕКСТОРШЪН



Цели на урока: Участниците разпознават рисковете при общуване с непознати онлайн, включително фалшиви профили, манипулация, изграждане на доверие и сексуално изнудване. Разбират какво е сексторшън и какви стратегии използват извършителите. Развиват умения да прекъсват рискова комуникация, да пазят доказателства, да не се поддават на изнудване, да докладват и да търсят помощ от доверен възрастен или компетентна служба.



Обща информация

Социалните мрежи, онлайн игрите, приложенията за чат и видеоплатформите позволяват бързо и лесно общуване. Децата могат да се свързват с връстници, да намират хора със сходни интереси, да играят, да създават съдържание и да участват в общности. В същото време тези пространства могат да бъдат използвани от хора, които се представят за други, изграждат доверие и след това злоупотребяват с детето.

Сексторшънът е форма на сексуално изнудване. Най-често извършителят получава или твърди, че има интимна снимка, видео или друго сексуализирано съдържание, и заплашва, че ще го разпространи, ако детето не изпълни исканията му. Исканията могат да бъдат за още снимки и видеа, за пари, за среща на живо, за достъп до профили, за включване в нови чатове или за извършване на други действия.

Сексторшънът може да започне по различни начини. Понякога извършителят се представя за връстник и започва приятелски разговор. Друг път се представя за привлекателен човек, който проявява романтичен или сексуален интерес. В някои случаи започва с фалшива награда, предложение за популярност, покана за участие в група, игра или „частен чат“. Може да се случи в Instagram, TikTok, Snapchat, Facebook, Discord, Telegram, WhatsApp, Viber, онлайн игри, форуми или други платформи.

ГРУМИНГ И ИЗГРАЖДАНЕ НА ДОВЕРИЕ

Преди да започне изнудването, извършителят често се опитва да изгради доверие. Това може да стане чрез комплименти, внимание, подкрепа, слушане на проблемите на детето, споделяне на „тайни“, обещания за връзка или приятелство. Той може да казва на детето, че го разбира по-добре от родителите и приятелите му, че то е специално, красиво, зряло или различно от останалите.

Постепенно разговорът може да стане по-личен. Извършителят може да поиска снимка, да изпрати уж своя снимка, да предложи „игра“, да настоява за видеоразговор, да премести комуникацията в друго приложение, където има по-малко контрол, или да поиска разговорът да остане тайна. Тайните от възрастните са един от най-сериозните предупредителни знаци.

Важно е децата да разберат, че човекът отсреща може да не е този, за когото се представя. Профилът може да използва чужди снимки, генерирани с AI изображения, фалшиво име, измислена възраст, фалшиво училище и дори инфор-

мация, която изглежда истинска. Някои извършители предварително събират данни от публичните профили на детето, за да изглеждат по-убедителни – например знаят училището, квартала, любимия отбор, приятелите или интересите му.

AI И ФАЛШИВИ ИЗОБРАЖЕНИЯ

Изкуственият интелект прави фалшивите профили и сексуалното изнудване по-трудни за разпознаване. Вече могат да се създават реалистични лица, снимки, гласове, съобщения и дори фалшиви интимни изображения. Извършителят може да твърди, че има интимна снимка на детето, дори такава снимка никога да не е изпращана. Може да използва обикновена снимка от профила и да създаде фалшиво изображение, с което да заплашва детето.

Това трябва да бъде казано ясно: дори когато изображението е фалшиво, заплахата и изнудването са реален проблем. Детето не трябва да доказва само, че изображението е фалшиво. Не трябва да се поддава на натиск, да плаща, да изпраща още снимки или да се опитва да преговаря само с извършителя. Трябва да потърси помощ веднага.

ФИНАНСОВ СЕКТОРШЪН

Все по-често секторшънът включва искане на пари. Това може да засегне както момичета, така и момчета. При някои случаи извършителят много бързо насочва разговора към интимно съдържание, получава снимка или запис, а след това заплашва, че ще го изпрати на родители, приятели, съученици или последователи, ако не получи пари. Понякога заплахата е придружена със списък с контакти на детето, за да изглежда по-страшна.

При финансов секторшън основното правило е: не плащай. Плащането не гарантира, че съдържанието ще бъде изтрито. Често след първото плащане следват нови искания. Същото важи и за изпращането на нови снимки – това не спира изнудването, а го засилва.

КАКВИ СТРАТЕГИИ ИЗПОЛЗВАТ ИЗВЪРШИТЕЛИТЕ?

- представят се за връстник или привлекателен човек;
- използват фалшиви или откраднати снимки;
- дават много внимание и комплименти;
- бързо създават усещане за близост;
- искат разговорът да остане тайна;
- преместват комуникацията в друго приложение;
- изпращат или обещават да изпратят интимно съдържание първи;
- настояват за снимка, видео или видеоразговор;
- използват натиск: „ако ми вярваш“, „ако ме харесваш“, „само веднъж“;
- заплашват с разпространение;
- твърдят, че имат контактите на детето;
- искат пари, още снимки или среща;
- създават паника и чувство, че трябва да се реагира веднага.

КАК ДА РАЗПОЗНАЕМ ФАЛШИВ ИЛИ РИСКОВ ПРОФИЛ?

Няма напълно сигурен признак, но няколко сигнала заедно трябва да повишат вниманието:

- профилът е нов или има малко реални публикации;
- снимките изглеждат прекалено „перфектни“ или са малко на брой;
- няма нормална активност с приятели и роднини;
- човекът избягва реална проверка на самоличността;
- твърди, че учи в същото училище, но никой не го познава;
- бързо започва личен или интимен разговор;
- иска тайна;
- настоява за снимки;
- предлага подаръци, пари, последователи или помощ;
- кара детето да премине в друг чат;
- реагира агресивно при отказ.

Важно е учениците да знаят, че дори профилът да изглежда истински, това не означава, че ситуацията е безопасна. Риск може да има и когато човекът е познат, връстник, съученик, бивш партньор или приятел на приятел.

КАКВО ДА НАПРАВИМ ПРИ СЕКСТОРШЪН?

Това трябва да бъде представено много ясно и практично:

1. Спри комуникацията, доколкото е безопасно.
2. Не изпращай повече снимки или видеа.
3. Не плащай.
4. Не обещавай среща.
5. Не се опитвай да „се разбереш“ сам/а с извършителя.
6. Запази доказателства – скрийншоти, профил, линкове, потребителско име, съобщения, искания за пари.
7. Блокирай и докладвай профила в платформата.
8. Кажете веднага на доверен възрастен.
9. Потърси помощ от Националния център за безопасен интернет на 124 123 или през www.safenet.bg.
10. При непосредствена заплаха, риск от среща, заплахи за живота или сериозно изнудване се търси помощ от компетентните органи и 112.

Деца трябва да чуят, че сексторшънът е ситуация, в която не бива да остават сами. Страхът и срамът са част от начина, по който извършителят ги контролира. Когато детето каже на възрастен, контролът започва да се връща обратно при него.

КАК ДА РЕАГИРАТ НАБЛЮДАТЕЛИТЕ?

Понякога интимно съдържание или заплахи се разпространяват в групови чатове. Учениците трябва да знаят, че препращането, показването и коментирането на такова съдържание увеличава вредата. Правилната реакция е:

- не препращай;
- не се подигравай;
- не обвинявай потърпевшия;
- направи скрийншот само ако е нужно като доказателство и го покажи на възрастен;
- докладвай съдържанието;
- подкрепи човека, който е потърпевш;
- кажи на доверен възрастен.

КАК ДА РЕАГИРА ВЪЗРАСТНИЯТ?

Възрастният трябва да запази спокойствие. Детето вероятно е уплашено и може да очаква наказание. Първите думи са важни: „Добре, че ми каза“, „Не си виновен/виновна за изнудването“, „Ще действаме стъпка по стъпка“, „Няма да те оставя сам/а“. След това трябва да се запазят доказателствата, да се ограничи контактът с извършителя, да се подаде сигнал и при нужда да се потърси психологическа подкрепа.

Не е подходящо възрастният да отнема веднага телефона като наказание. Това може да накара детето да се почувства още по-безпомощно и следващия път да не сподели. По-полезно е устройството да се използва за запазване на доказателства и за докладване, като детето бъде подкрепено в процеса.

ПРЕВЕНЦИЯ

Превенцията на сексторшъна започва преди конкретната опасна ситуация. Децата трябва да знаят как изглежда здравословното общуване: никой няма право да ги притиска, да изисква тайни, да настоява за снимки, да заплашва или да ги кара да се чувстват виновни. Урокът трябва да развива умения за разпознаване на манипулация, поставяне на граници, проверка на профили и търсене на помощ.

Добре е темата да се свърже с други уроци от наръчника – лични данни, сигурност в мрежата, онлайн тормоз, вредно съдържание, дигитален имидж и изкуствен интелект. Сексторшънът не е изолиран риск, а пресечна точка между доверие, интимност, лични данни, фалшиви профили, натиск и злоупотреба.

Основното послание към учениците е: ако някой те заплашва с интимна снимка, видео или фалшиво изображение, не си сам/а и има помощ. Не плащай. Не изпращай още. Запази доказателства. Потърси възрастен. Докладвай.



**Инструменти, които можете да ползвате, описани в раздел 6:
Инструменти 8, 20, 32, 33, 37**

5.10. ИЗКУСТВЕН ИНТЕЛЕКТ – възможности и рискове



Цели на урока: Участниците разбират какво е изкуствен интелект (ИИ) и къде го срещат в ежедневието си. Разпознават основните ползи и рискове при използването му, включително рисковете за личните данни, достоверността на информацията, дигиталния имидж и безопасността на децата. Участниците развиват критично мислене и умения за отговорно използване на ИИ в училище, общуването и свободното време.



Обща информация

Изкуственият интелект вече е част от ежедневието на децата, често без те да го назовават по този начин. Той присъства в търсачките, автоматичните преводачи, навигацията, препоръките за видеа и музика, филтрите в социалните мрежи, онлайн игрите, чатботовете, приложенията за учене и инструментите за създаване на изображения, текст, звук и видео. Затова темата за ИИ не трябва да се представя само като технологична тема, а като част от дигиталната грамотност и безопасното поведение в интернет.

Най-общо, ИИ е система, която обработва големи количества информация, открива модели в нея и на тази основа прави предложения или генерира съдържание. За разлика от обикновената компютърна програма, която изпълнява предварително зададени инструкции, много системи с ИИ могат да се „обучават“ от данни и да подобряват работата си според примери. Това не означава, че ИИ мисли и чувства като човек. Той може да имитира човешка реч, да отговаря убедително, да създава текстове, снимки или видео, но няма личен опит, съзнание, емпатия и морална отговорност.

Особено бързо се развиват т.нар. генеративни системи с ИИ. Те могат да създават ново съдържание – текст, изображения, музика, код, презентации, видео или глас. За учениците това може да бъде полезно: ИИ може да обясни трудна тема с по-прости думи, да предложи структура за есе, да помогне при превод, да даде идеи за проект, да създаде примерни въпроси за подготовка или да подкрепи деца със специални образователни потребности. В този смисъл ИИ може да разшири достъпа до знание и да направи ученето по-персонализирано.

В същото време ИИ крие специфични рискове, които трябва да бъдат обсъждани с децата спокойно, конкретно и без плашене.

1. Риск, свързан с достоверността на информацията. Чатботовете и генеративните системи могат да дават грешни, непълни или подвеждащи отговори, но да ги представят уверено т.е. да „халюцинира“. Затова е важно учениците да знаят, че отговорът на ИИ не е непременно верен. Той трябва да се проверява чрез надеждни източници, особено когато става дума за здраве, безопасност, права, история, новини или лични решения.
2. Риск, свързан с личните данни и поверителността. Децата не бива да въвеждат в инструменти с ИИ свои лични данни, адрес, телефон, училище, пароли, снимки на документи, интимна информация, данни за приятели или семейство. Веднъж въведена в дадена услуга, информацията може да бъде съхранена, анализирана или използвана по начин, който потребителят не разбира напълно. Това е особено важно при безплатни приложения и непознати сайтове, които обещават бързи резултати, „магически“ снимки или лесно създаване на съдържание.

3. Риск, свързан с дигиталния имидж и злоупотребата със снимки и видео. С помощта на ИИ вече е възможно лесно да се създават фалшиви изображения, фалшиви профили, подправени гласове и видеа, в които изглежда, че реален човек казва или прави нещо, което никога не се е случвало. Това се нарича *deepfake*. Особено опасни са случаите на създаване на сексуализирани или унизителни изображения на деца чрез ИИ. Дори когато подобно съдържание е „фалшиво“, последиците за детето могат да бъдат реални – срам, страх, изолация, онлайн тормоз, изнудване и загуба на доверие. Важно е децата да знаят, че създаването, разпространението или запазването на сексуализирани изображения на непълнолетни е сериозна злоупотреба и трябва незабавно да се търси помощ от възрастен и да се подаде сигнал.
4. Риск, свързан с манипулацията и измамите. ИИ може да бъде използван за създаване на много убедителни фишинг съобщения, фалшиви реклами, измамни профили, гласови съобщения или „персонализирани“ опити за изнудване. Децата трябва да бъдат насърчавани да се съмняват в прекалено добри предложения, неочаквани линкове, искания за снимки, пари, кодове, пароли или лична информация. Ако съобщението предизвиква силен страх, срам, спешност или обещава бърза награда, това е сигнал за внимание.
5. Риск, свързан с прекомерното доверяване на ИИ. Ако ученикът използва ИИ, за да решава всички задачи вместо него, той може да загуби възможност да развива собствени умения – четене с разбиране, писане, аргументация, смятане, творчество и критично мислене. Затова в образователна среда е важно ИИ да бъде представян като помощник, а не като заместител на ученето. Добър принцип е: „ИИ може да помогне да мисля по-добре, но не трябва да мисли вместо мен.“
6. Риск, свързан с пристрастията и дискриминацията. ИИ се обучава върху данни, създадени от хора, а в тези данни може да има стереотипи, предразсъдъци и неравенства. Затова системите с ИИ могат да възпроизвеждат несправедливи или обидни внушения за пол, етнос, религия, социален статус, увреждане или други лични характеристики. Това е особено важно при работа с уязвими групи, защото технологиите могат неусетно да засилят вече съществуващи форми на изключване и стигматизация.

В Европейския съюз темата за ИИ вече е част от по-широката рамка за защита на правата, безопасността и достъпа до надеждна информация в дигиталната среда. Европейският акт за изкуствения интелект въвежда подход, основан на риска, и поставя акцент върху човешкия контрол, прозрачността и защитата на основните права. От 2025 г. в ЕС се прилагат и изисквания, свързани с грамотността по ИИ – хората, които използват или внедряват системи с ИИ, трябва да имат достатъчно знания и умения, за да разбират възможностите, ограниченията и рисковете им. Това е особено важно за училищата, защото учениците имат нужда не само да използват нови инструменти, но и да разбират как те влияят върху тяхното учене, общуване и сигурност.

При работа с деца е полезно темата да се води през практически въпроси:

- Къде вече използвам ИИ, без да се замислям?
- Как ИИ може да ми помогне да уча?
- Какво не бива да споделям с ИИ?
- Как проверявам дали отговорът е верен?

- Как разпознавам фалшиво изображение, видео или профил?
- Какво правя, ако някой използва ИИ, за да ме унижи, измами или изнудва?
- Кога използването на ИИ е помощ, и кога е преписване?

Водещият трябва да насърчава балансиран подход. Не е необходимо ИИ да бъде представян нито като заплаха, която трябва изцяло да се избягва, нито като чудодееен инструмент, който решава всички проблеми. Най-важното послание към децата е, че човекът остава отговорен за решенията си. ИИ може да предложи идея, текст, изображение или отговор, но ученикът трябва да мисли критично, да проверява, да пази личните си данни, да уважава другите и да търси помощ при риск.

Практически правила за учениците при използване на ИИ:

1. Не споделям лични данни, пароли, адрес, училище, телефон, снимки на документи или интимна информация.
2. Не качвам снимки на други хора в инструмент с ИИ без тяхното съгласие.
3. Проверявам важната информация в първичния/официалния източник.
4. Не приемам отговора на ИИ като окончателна истина.
5. Използвам ИИ, за да уча и да развивам идеи, а не за да представям чужда работа като своя.
6. Не създавам и не разпространявам унижително, фалшиво или сексуализирано съдържание за друг човек.
7. Ако видя deepfake, фалшив профил, заплаха, изнудване или злоупотреба със снимка, правя скрийншот, не отговарям на натиска и търся помощ от доверен възрастен.
8. При сериозен проблем се обръщам към Националния център за безопасен интернет чрез www.safenet.bg или на телефон 124 123.

Възможно е темата за ИИ да се свърже и с други уроци от наръчника: лични данни, дигитален имидж, вредно онлайн съдържание, онлайн тормоз, секстинг, непознати в мрежата и фишинг. Това ще помогне на учениците да разберат, че ИИ не е отделен от останалите рискове в интернет, а често ги усилва, ускорява или прави по-трудни за разпознаване.



**Инструменти, които можете да ползвате, описани в раздел 6:
Инструменти 1, 22, 34, 35**

Източници за актуализиране на информацията:

1. Министерство на образованието и науката, „Насоки за използване на изкуствения интелект в образователната система“, 2024.
2. Европейска комисия, „Етични насоки за преподавателите относно използването на изкуствен интелект (ИИ) и на данни при преподаване и учене“.
3. Европейски акт за изкуствения интелект, Регламент (ЕС) 2024/1689; чл. 4 въвежда задължение за грамотност по ИИ.
4. UNESCO, [Guidance for generative AI in education and research](#).
5. Европейска стратегия за по-добър интернет за децата (BIK+).
6. Европейска комисия, „Насоки за преподавателите и образователните специалисти за противодействие на дезинформацията и насърчаване на цифровата грамотност чрез образование и обучение“, актуализирано издание, 2026 г.;
7. UNICEF Innocenti, [Guidance on AI and Children](#), Version 3.0, 2025 г.
8. Европейска комисия, [Насоки относно мерки за гарантиране на високо равнище на неприкосновеност на личния живот, безопасност и сигурност на малолетните и непълнолетните лица онлайн съгласно Регламент \(ЕС\) 2022/2065 \(Акт за цифровите услуги\)](#), 2025 г.
9. Council of Europe, [Digital Citizenship Education Handbook](#), 2022 г.
10. OECD, [Digital Education Outlook](#), 2026 г.



Цели на урока: Участниците разбират какво означава радикализация, на кого и за какво може да служи, и как онлайн средата може да улесни разпространението на крайни идеи, реч на омразата и насилствени послания. Разпознават рискови онлайн ситуации, свързани с манипулация, пропаганда, конспиративни теории, дехуманизиране на хора и групи и призови към насилие. Развиват умения за критична оценка на съдържание, за безопасно поведение онлайн, за докладване и за търсене на помощ от доверен възрастен или компетентна институция.



Обща информация

Радикализацията е процес, при който човек постепенно започва да възприема все по-крайни възгледи, да отхвърля различното мнение и да приема, че определена група хора е „враг“, „заплаха“ или „по-малко ценна“. Радикалните идеи сами по себе си не винаги водят до насилие. Проблем възниква, когато към тях се добавят омраза, дехуманизиране на други хора, оправдаване на насилие или готовност за участие в действия, които застрашават другите и нарушават човешките права.

Важно е още в началото да се направи ясно разграничение: радикализацията не е свързана с конкретна религия, етнос, националност или социална група. Тя може да има различни форми – политическа, религиозна, етнонационалистическа, расистка, антисемитска, ксенофобска, мизогинна или свързана с една конкретна кауза. Общото между тези форми е не самата тема, а начинът, по който се изгражда мисленето „ние срещу тях“, отхвърля се диалогът и се оправдава вреда спрямо други хора.

За децата и младежите темата е особено важна, защото юношеството е период на търсене на идентичност, принадлежност, смисъл, справедливост и признание. В този възраст младите хора често търсят група, в която да бъдат приети, и модели, които да им дадат усещане за сила, яснота и значимост. Това е нормална част от развитието. Рискът възниква, когато такава потребност бъде използвана от хора или групи, които предлагат много прости обяснения за сложни проблеми, насочват гнева към „виновна“ група и представят омразата като смелост, а насилието като справедливост.

Онлайн средата може да ускори този процес. Социалните мрежи, видеоплатформите, приложенията за чат, форумите, гейминг платформите и групите в затворени канали позволяват бързо разпространение на крайни послания. Понякога радикализиращото съдържание не изглежда открито опасно. То може да бъде поднесено като шега, мем, „истинска история“, конспиративна теория, клип с „разобличение“, патриотично послание, религиозно обяснение, мотивационен текст или разговор в игрови чат. Именно това го прави трудно за разпознаване.

Много често процесът започва с обикновено съдържание, което буди силни емоции – гняв, страх, възмущение, чувство за несправедливост или унижение.

След това алгоритмите могат да препоръчат още подобни публикации, видеа или групи. Така детето може постепенно да попадне в информационна среда, в която вижда само едни и същи послания. Това създава усещане, че „всички мислят така“, че определена група е виновна за личните или обществени проблеми, и че насилието или унижението спрямо нея е допустимо.

Онлайн радикализацията рядко се случва само чрез един клип или една публикация. По-често тя е процес на натрупване. Детето първо проявява интерес, после започва да следва страници, канали или инфлуенсъри с крайни послания, влиза в чатове или групи, споделя съдържание, използва нови изрази и символи, а постепенно може да започне да се дистанцира от хора, които не споделят същите възгледи. В някои случаи то може да бъде насърчавано да пази тайна, да не вярва на родители, учители, медии или институции, и да приема само информацията от групата като „истинска“.

Затова една от най-важните задачи на възрастните не е да наказват или засрамват децата при първи контакт с такова съдържание, а да говорят с тях спокойно и открито. Ако детето бъде директно обвинено, то може да се затвори, да изтрие следите и да продължи да общува в по-скрити канали. Много по-полезно е да се изследва какво го е привлякло: чувство за несправедливост, преживян тормоз, самота, нужда от група, интерес към история, политика, религия, спортна агитка, войни, конспирации или желание да изглежда „силно“ пред връстниците си.

КАКВО ПРАВИ ОНЛАЙН СРЕДАТА РИСКОВА?

Интернет дава бърз достъп до съдържание, което може да е манипулативно, агресивно или незаконно. Платформите често показват още от същото съдържание, защото то задържа вниманието. В онлайн групите децата могат да получат бързо одобрение за крайни мнения, което им създава чувство за принадлежност. Анонимността или псевдонимите намаляват усещането за отговорност. Шегите, меметата и игровият език могат да прикриват сериозни послания на омраза.

Особен риск представляват пространства, в които има постоянна подигравка с определени групи, използване на обидни прякори, символи и кодови думи, призови към „прочистване“, „отмъщение“, „защита“ чрез насилие, или съдържание, което представя някои хора като заплахата за нацията, религията, семейството, мъжете, жените или „нормалните хора“. Такива послания могат да се появят и в контекст на конспиративни теории – например, че „тайна група“ управлява света, че определено малцинство е виновно за всички проблеми, или че медиите и институциите винаги лъжат.

При по-малките деца и в прогимназиална възраст рисковете често са свързани с повторение на език и символи, които те не разбират напълно. Дете може да използва расистка, антисемитска, религиозно омразна или друг вид обидна фраза „на шега“, защото я е видяло в клип или игра. Това не означава автоматично, че детето е радикализирано. Означава, че има нужда от разговор за смисъла на думите, за последствията от тях и за това как онлайн шегите могат да нараняват реални хора.

При по-големите ученици рискът може да бъде по-свързан с търсене на идеология, идентичност и принадлежност. Част от тях могат да попаднат в групи, които използват език на „пробуждане“, „истина“, „братство“, „чистота“, „спасение“, „война“ или „предателство“. Такива групи често предлагат ясен враг и много прост отговор на сложни лични и обществени проблеми. Важно е участниците да разберат, че когато една група изисква пълно съгласие, забранява съмненията, кара членовете си да крият общуването и оправдава насилие, това е сериозен предупредителен знак.

ПРИЗНАЦИ, ЗА КОИТО ДА ВНИМАВАМЕ

Няма един-единствен признак, който да доказва радикализация. Промени в поведението могат да се дължат на много други причини – тормоз, проблеми в семейството, депресивни преживявания, загуба, зависимост, конфликт с връстници или нормално юношеско търсене. Затова признаците винаги трябва да се разглеждат заедно, внимателно и в контекст.

Възможни предупредителни знаци са: внезапно силно отдръпване от приятели и семейство; рязка промяна в онлайн интересите; често споделяне на съдържание, което унижава или дехуманизира други групи; използване на нови символи, кодови думи или лозунги, свързани с омраза; оправдаване на насилие като „необходимо“; отхвърляне на всички източници на информация извън конкретна група; участие в затворени чатове, в които се говори за „врагове“ и „отмъщение“; възхвала на хора или групи, извършили насилие; рязка нетърпимост към различно мнение; изрази от типа „те не са хора“, „трябва да бъдат премахнати“, „няма друг начин“.

За водещия е важно да подчертае, че целта не е учениците да се превърнат в „наблюдатели“ или „доносници“ един срещу друг. Целта е да разпознават кога дадено съдържание или група може да навреди – на тях, на техния приятел или на други хора – и да знаят как да потърсят помощ навреме.

КАК ДА ГОВОРИМ С ДЕЦАТА ПО ТЕМАТА?

Разговорът за радикализация не трябва да започва със страх. По-подходящо е да се започне от теми, които учениците вече познават: фалшиви новини, манипулация, онлайн тормоз, реч на омразата, групов натиск, инфлуенсъри, алгоритми, мемета и гейминг общности. Водещият може да задава въпроси, които развиват критично мислене: „Кой печели, ако повярваме на това?“, „Какво чувство се опитва да предизвика тази публикация?“, „Кой е представен като враг?“, „Има ли доказателства?“, „Има ли друг прочит?“, „Как бихме се почувствали, ако така говорят за нас или за нашето семейство?“.

Много важно е да се избягва стигматизиране на конкретни общности. Ако урокът бъде воден така, че определена религия, етнос или група да изглежда „по-опасна“ от останалите, това може да произведе обратен ефект: да засили предразсъдъци, да нарани деца от уязвими групи и да създаде ново чувство за несправедливост. Подходът трябва да бъде основан на човешките права, уважението, достойнството и безопасността.

КАКВО МОГАТ ДА НАПРАВЯТ УЧЕНИЦИТЕ?

Когато попаднат на съдържание, което насърчава омраза или насилие, учениците могат да предприемат няколко стъпки. Важно е да не го споделят, дори „за да го покажат колко е абсурдно“, защото по този начин допринасят за разпространението му, а това се отразява и върху видимостта му – колкото повече се споделя дадено съдържание, толкова повече го „избутват“ алгоритмичните системи.

Друга важна стъпка е да направят екранна снимка, ако има заплаха, тормоз или призив към насилие, за да запазят доказателство. Да докладват съдържанието в платформата и да блокират профили, които ги притесняват или ги въвличат в рискови разговори. Трябва да знаят, че определени категории съдържание, което отговаря на определението за език на омраза, е незаконно. Важно е да говорят с доверен възрастен – родител, учител, училищен психолог, педагогически съветник, медиатор или друг професионалист.

Ако съдържанието е свързано с непосредствена заплаха за нечия безопасност, не трябва да се чака. В такъв случай е необходимо да се потърси помощ от възрастен и да се подаде сигнал към компетентните органи. При риск за живота и сигурността на хора се звъни на 112. При онлайн проблеми, вредно съдържание, тормоз, изнудване или нужда от консултация учениците и възрастните могат да се обърнат към Националния център за безопасен интернет чрез Консултативната линия 124 123 или през сайта www.safenet.bg.

ПРЕВЕНЦИЯ

Най-добрата превенция срещу онлайн радикализацията не е забраната на интернет, а изграждането на критично мислене, емоционална устойчивост, умения за общуване и чувство за принадлежност към позитивна общност. Децата имат нужда да знаят, че могат да задават трудни въпроси, да спорят, да се съмняват, да търсят справедливост и да защитават каузи, без да мразят и без да нараняват други хора.

Важно е да се различава наличието на крайни или непопулярни възгледи от процеса на насилствена радикализация, при който се стига до демонизация на индивиди или обществени групи, както и до оправдаване, подкрепа или подготовка на насилие.

Училището може да бъде защитна среда, когато насърчава диалог, уважение към различието, медийна грамотност, участие на учениците и реални възможности за изразяване. За уязвимите деца това е още по-важно. Ако едно дете преживява изолация, дискриминация, бедност, тормоз или липса на признание, то може да бъде по-податливо на групи, които му обещават сила, принадлежност и ясни отговори. В този смисъл превенцията на радикализацията е свързана и с превенцията на тормоза, речта на омразата, социалното изключване и дезинформацията.



Инструменти, които можете да ползвате, описани в раздел 6:

Инструменти 3, 5, 11, 23, 24, 29, 36, 37

ИНСТРУМЕНТИ ЗА ВЪВЕЖДАЩАТА ЧАСТ



Инструмент 1: Мозъчна атака



Цел: да изведе „права и отговорности/правила“ като верен отговор.

Правата са нещо, което хората притежават и което не бива да им се отнема. Отговорността е способността да проявяваме грижа, да взимаме решения и приемаме последствията от тях. Но можем ли лесно да правим разлика между правата и отговорностите? Нека се упражним.

Кои от следните твърдения са „ПРАВА“ или „ОТГОВОРНОСТИ“. На флипчарт или дъска се написват ПРАВА и ОТГОВОРНОСТИ, като учениците казват, което според тях е право, кое отговорност и учителят/обучителят ги разпределя в едно от двете полета.

1. Да бъда в безопасност – (верен отговор: право)
2. Да пиша редовно домашните си – (верен отговор: отговорност)
3. Да ходя на училище – (верен отговор: право)
4. Да си подреждам стаята – (верен отговор: отговорност)
5. Да се отнасят справедливо с мен – (верен отговор: право)
6. Да изразявам мнението си – (верен отговор: право)
7. Да бъда внимателен и учтив към околните – (верен отговор: отговорност)



Инструмент 2: Игра-демонстрация и мозъчна атака

Водещият казва, че има нужда от двама доброволци за първото упражнение.

След като ги избере, моли ги да застанат един срещу друг пред групата и им дава инструкции:

„Нека единият от вас бъде със стиснат юмрук, а другият да се опита да открие начин да го накара да разтвори юмрука си.“

Ако ученикът не успее да накара другия да разтвори юмрука си, водещият може да му подсказва да му подаде ръка за здрависване или да го помоли да разтвори ръката си.

Стартира кратка мозъчна атака с цел извличане темата на урока: „Какво наблюдавахме?“, „Какво накара Х (името на доброволеца) да разтвори юмрука си?“, „Това какво ви кара да мислите?“, „Влияят ли поведението и думите ни върху другите?“

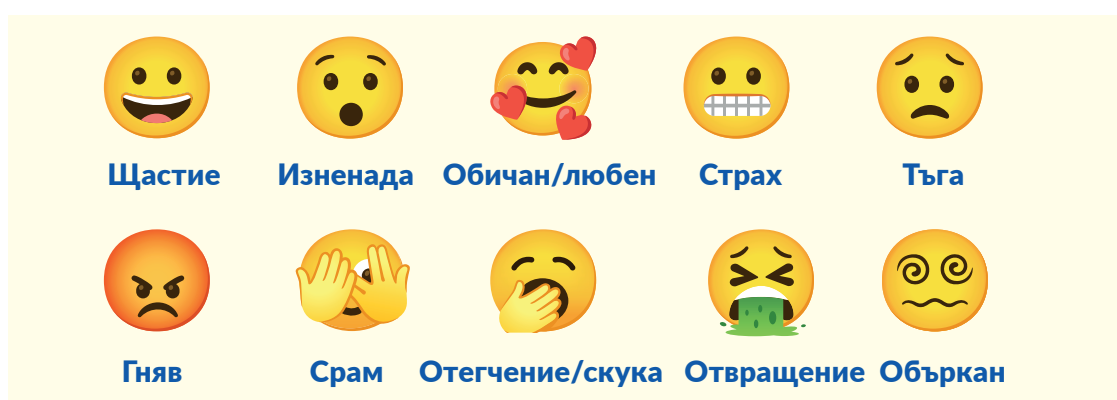
Обобщава, че темата на днешното занятие е ненасилствената комуникация.

Инструмент 3: Дискусия

Всеки от нас използва интернет и устройствата за различни дейности – за училище, за разговори с хора, за правене на снимки, за гледане на клипчета, за играене на игри и още много други! Когато сме в интернет, попадаме на различни видове съдържание, което може да ни накара да се чувстваме по определен начин – понякога тези чувства могат да са много приятни, но друг път не чак толкова.

Нека първо да проверим колко добре разпознавате емоциите, като на помощ ще извикаме любимите ни емотикони! Нека да се опитаме да назовем емоцията, която всеки емотикон изразява.

На екрана се прожектират един след друг различни емотикони, всеки от които изразява определена емоция от списъка по-долу. Учениците се опитват да назоват емоцията:



Инструмент 4: Мозъчна атака

Водещият стартира мозъчната атака, с която да въведе участниците в темата на урока:

„Знаете ли какво са лични данни? Дайте примери!“, „Кои от тези лични данни споделяме в интернет?“

Водещият обобщава, че темата на днешния час са личните данни в интернет и как да ги пазим.

Участват в дискусията и дават примери за лични данни:

Лични данни са информацията, чрез която едно лице може да бъде разпознато. Личните данни могат да бъдат:

- Собствено име и фамилия;
- Домашен адрес;
- ЕГН;
- Имейл адрес;
- Номер на лична карта;
- Данни за местоположение;
- Адрес на интернет протокол (IP);
- Идентификационен номер на „бисквитка“² и др.
- Телефонен номер.

² „Бисквитка“ е малък текст, който се изпраща до браузъра след посещение в определен сайт. Бисквитките дават информация за предпочитанията на потребителя като език, настройки, реклами и т.н.

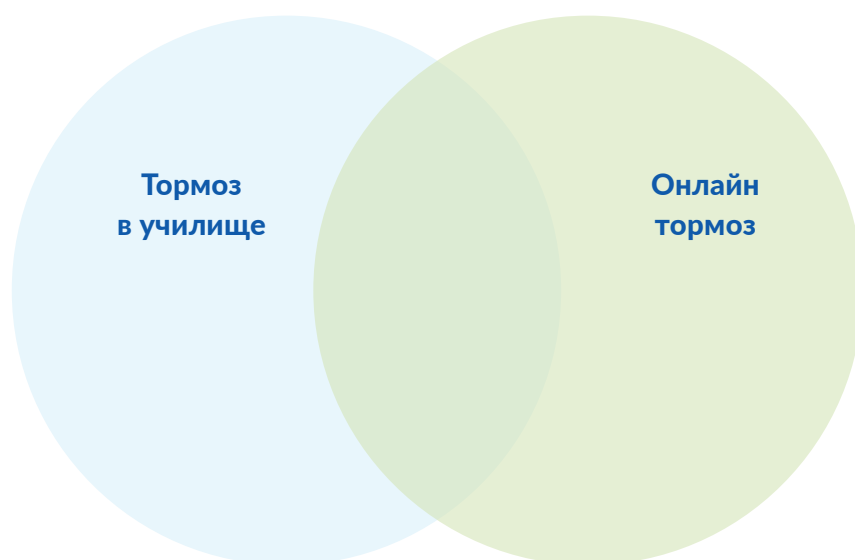
Инструмент 5: Дискусия (Вредно съдържание)

Водещият открива с кратка дискусия през следните въпроси: „Какво най-често търсите в интернет?“, „Споделете нещо любопитно/интересно, което сте прочели в интернет!“, „Случвало ли ви се е да търсите едно, а да попаднете на друго?“, „Някой иска ли да даде пример?“, „Защо според вас понякога в интернет попадаме на нещо, което не сме търсили?“, „Може ли понякога да бъдем неприятно изненадани/уплашени/разстроени от намереното?“

Водещият обяснява, че днес ще говорят за вредното онлайн съдържание, как ни влияе то и какво можем да направим, ако попаднем на такава.

Инструмент 6: Брейнсторминг

Обучителят въвежда темата, като обяснява, че в рамките на следващия час ще обсъдят проблемите с онлайн тормоз. Представя се Вен диаграма, в която на лявото кръгче е изписано като заглавие „Тормоз в училище“, а на дясното - „Онлайн тормоз“. Отдолу са изписани поредица от думи и изрази.



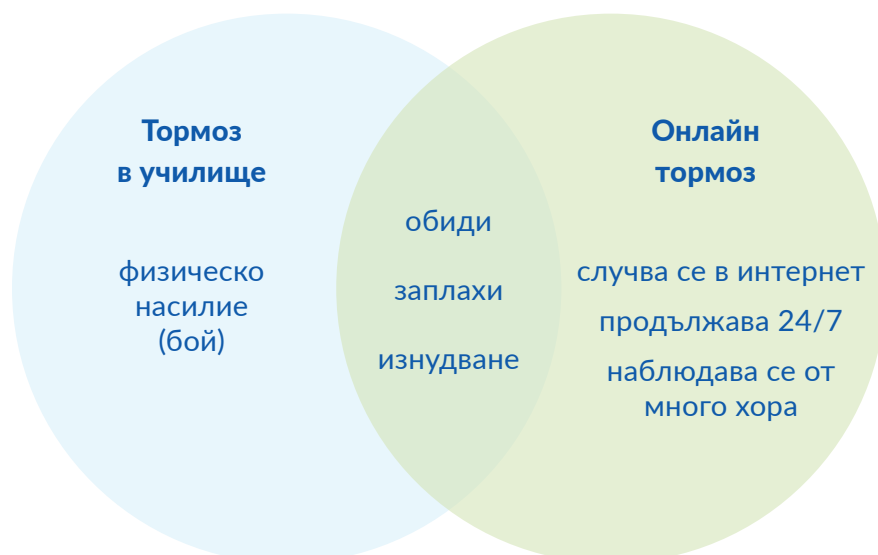
физическо насилие (бой), психически тормоз, обиди, заплахи, изнудване, наблюдава се от много хора, продължава 24/7, случва се в интернет...

Обучителят пита учениците дали се досещат каква е идеята на двете преплетени кръгчета и респективно каква ще бъде задачата им. Ако не се досетят, им помага - в лявото кръгче ще разположат думите и изразите, които се отнасят за тормоза в училище, вдясно - тези, които са характеристики на онлайн тормоза, а по средата - тези, които се отнасят и за двата вида тормоз.

Примерни правилни отговори от учениците: „Показват кое е общото и кое е различното между онлайн тормоза и тормоза в училище“, „Трябва да сложим думите и изразите в съответното кръгче, за което се отнасят или по средата“.

Моли учениците с вдигане на ръка да предполагат коя дума/израз къде трябва да се разположи.

Правилно решена задача:



На тази база се извежда определението за онлайн тормоз чрез характерните му признаци (в дясната част на вен-диаграмата. Търсен отговор: „Онлайн тормозът са обиди, подигравки и заплахи към едно дете/човек, които се случват в интернет, продължително време, през деня и през нощта (24/7) и може да бъде видяно от много хора“.



Инструмент 7: Брейнсторминг (Секстинг)

Групата се подрежда в кръг и прави брейнсторминг по два въпроса: *Какво е флирт? Какво правим/казваме на някого, когато флиртуваме? Възможен ли е онлайн флирт?*



Инструмент 8: Викторина (Непознатите в Мрежата и рискът от сексторшън)

Водещият моли участниците да прочетат следващите твърдения и да отговорят според тях истина или мит са.

- Съобщенията и снимките в Snapchat изчезват, затова е напълно безопасно да пращаме, каквото си искаме. (Верен отговор: мит)
- Всички стриймъри в Twitch са проверени от платформата и затова са безопасни. (Верен отговор: мит)
- Всеки във Facebook може да ви изпрати съобщение. (Верен отговор: истина)
- Discord се използва само за гейминг, затова непознатите не са риск. (Верен отговор: мит)
- Ако от известно време си пишете с непознат в Instagram, няма проблем да се видите на живо. (Верен отговор: мит)

ИНСТРУМЕНТИ ЗА ОСНОВНАТА ТЕМА



Инструмент 9: Групова работа

За да сме сигурни, че правата на хората се спазват, имаме нужда от отговорности и правила. Сега, след като можем да правим разлика между тях, нека се разделим на отбори за следващото упражнение!

Учениците се разделят на отбори от по 5-6 деца, които сядат заедно. За разделянето на учениците може да използвате методи като броене, теглене на номера/цветове и други подобни (Приложение 2).

Сега ще изгледаме кратко видео, в което ще видите историята на Николай, който е ученик в девети клас. Гледайте внимателно видеото, защото задачата ви ще бъде свързана с него.

Изчита се долния казус или се избира материал от следния сайт:

<https://bg.izzi.digital/DOS/710078/710089.html>

Николай е ученик в пети клас и много обича да играе на Minecraft. Един ден решава да си направи YouTube канал, като любимите си геймъри, и да качва клипчета на това как играе играта. Изведнъж започва да получава много и различни коментари: в някои от тях го обиждат и го наричат слабак, други го питат къде да живее и искат да се срещнат с него, трети го питат дали може да сподели паролата си за профила си в Minecraft с тях, за да могат и те да играят? Николай е толкова объркан и притеснен!

След това учителят поставя задачата:

Задачата на всяка група е да състави правила, които Николай и всички деца трябва да спазват, когато са онлайн. Групата трябва да запише правилата на лист хартия и да избере отговорник, който да ги прочете след това и отговорник, който да следи за времето. Учениците имат 5 минути за работа.

Когато времето изтича, всяка група се редува и прочита по едно от правилата, които е съставила. Учителят ги записва на дъската/в платформата.

Примерен списък:

1. Държим се учтиво и уважително с другите.
2. Пазим личната си информация (три имена, адрес, училище, пароли).
3. Докладваме вредно или обидно съдържание.
4. Не приемаме покани за запознанства с непознати онлайн.
5. Ако нещо ни притеснява в интернет, можем да споделим с родителите си.

След всяко правило има кратко обсъждане защо е важно и с какво е полезно. Добре е правилата да са формулирани по позитивен начин. Учителят си служи с насочващи въпроси, за да изведе допълнителни правила, ако посочените от учениците са твърде малко или се повтарят. Учителят въвежда идеята, че списъкът остава „отворен“, тъй като правилата могат да се променят във времето.



Инструмент 10: Групова работа

Водещият разделя групата на отбори от по 3-4 ученици с цел максимално участие на всички присъстващи. След това стартира играта „Митове и факти“. Разделените на отбори деца дискутират и отговарят на въпросите. Целта на играта е да провокира дискусията относно най-честите митове, свързани с поверителността в интернет и това как управляваме информацията за себе си. Отборите се редуват да отговарят дали дадено твърдение е мит, или истина. След това целият клас/група се ангажира в кратка дискусия с цел изясняване на твърдението. При някои от въпросите могат да се изведат конкретни стъпки за защита на личните ни данни в интернет (подчертани са) – водещият може да ги запише на дъската или на флипчарт лист.

Можете да подготвите презентация с митовете, така че поднасянето им да е по-атрактивно. Другият вариант е да четете твърденията на всеки отбор и той да дава своя отговор. След всеки мит са посочени примерни въпроси, които можете да използвате в дискусията, както и примерни отговори.

МИТ ИЛИ ФАКТ?

1. Потребителите в интернет са анонимни – (верен отговор: мит)

Въпроси за дискусия: „Защо е мит, че потребителите в интернет са анонимни?“, „Дайте примери за начини, по които може да бъде установена вашата самоличност в интернет!“, „Какво можем да направим, ако не искаме наша лична информация да бъде качена онлайн?“

Примерни отговори: „Може да бъде използван IP-адресът, можем да сме обект на разследване... Не качваме своя интимна информация онлайн.“

2. Трябва да ни е грижа за онлайн поверителността само ако имаме какво да крием – (верен отговор: мит)

Въпроси за дискусия: „Защо е важна онлайн поверителността?“, „Как бихте се чувствали, ако знаете, че всеки има достъп до личните ви разговори?“, „Каква друга информация споделяме онлайн, която не бихме искали другите да знаят?“

Примерни отговори: „Всеки има право на своето лично пространство и своята лична информация – дори онлайн. Затова имаме пароли, кодове и т.н. В интернет споделяме информация за себе си, използваме кредитни/дебитни карти, ползваме различни услуги...“

3. Името, профилната снимка, полът и мрежите (работа, училище...) са винаги публични във Facebook – (верен отговор: факт)

Въпроси за дискусия: „Защо според вас тази информация е публична?“, „Какво можем да направим, ако не искаме тя да достига до другите?“

Примерни отговори: „Тази информация е публична, за да прави свързването с другите по-лесно. Може да изберем да не публикуваме част от нея – например в кое училище учим, къде работим, коя година сме родени... Ако не я публикуваме, другите няма как да я знаят.“

4. Когато изтрия нещо от интернет, то изчезва завинаги – верен отговор: мит

Въпроси за дискусия: „Защо нещата не изчезват от интернет?“, „Какво можем да направим, за да се предпазим от това?“

Примерни отговори: „Някой може да направи скрийншот (екранна снимка), информацията да бъде споделена, да остане на някой сървър... Винаги трябва да обмисляме добре нещата, които споделяме в интернет.“

5. Когато кача нещо в интернет, аз нямам вече контрол върху него – верен отговор: факт

Въпроси за дискусия: „Какво се случва, когато качим нещо онлайн?“, „Възможно ли е наши приятели и познати да злоупотребят с наша информация – дори ако е изпратена на лично съобщение?“, „Какво можем да направим?“

Примерни отговори: „Когато качим нещо онлайн, то става видимо за много хора и всеки може да съхрани информацията по някакъв начин или да я използва. За да се предпазим, трябва добре да помислим, преди да качим нещо, както и да внимаваме с кого я споделяме – дори наши приятели биха могли да се възползват от нещо, което сме качили онлайн или което сме им изпратили.“

6. Режим „Инкогнито“ в браузъра не ни прави анонимни – верен отговор: факт

Въпроси за дискусия: „За какво служи режим „Инкогнито“?“, „Той осигурява ли ни пълна анонимност и сигурност?“, „За кого продължава да е видима информацията?“

Примерни отговори: „Режим „Инкогнито“ крие историята на посещенията на нашето устройство и не запазва пароли. Той не ни осигурява пълна анонимност, защото цялата информация продължава да е видима за интернет доставчика ни например.“

7. Използването на публичен Wi-Fi е безопасно – верен отговор: мит

Въпроси за дискусия: „Телефонът ви автоматично ли се свързва със свободните Wi-Fi мрежи?“, „Това може ли да бъде опасно? Защо?“, „Какво можете да направите?“

Примерни отговори: „Свободно достъпните мрежи са уязвими и нямат достатъчно защити. Техните собственици имат достъп до информацията ни и могат да я използват за различни цели. Ако имаме възможност, използваме мобилни данни или мрежи, на които имаме доверие.“

8. Използването на една и съща парола навсякъде крие рискове – верен отговор: факт

Въпроси за дискусия: „Използвате ли една и съща парола за всичките си регистрации?“, „Защо това може да бъде опасно?“, „Какви са признаците на една силна парола?“, „Споделяме ли паролите си с други хора?“

Примерни отговори: „Разбиването на паролата в една регистрация може да доведе до разгадаването ѝ на други места – по този начин други хора имат достъп до наша лична информация и данни. Задължително използваме силни пароли и никога една и съща парола за всичките ни профили. Силната парола съдържа минимум 8 знака, малки и големи букви, цифри и специални знаци и символи. Никога не казваме паролата си на други хора.“

9. Игрите и приложенията, които ползвам във Facebook, нямат достъп до информацията в профила ми – верен отговор: мит

Въпроси за дискусия: „Преди да ползвате дадено приложение, то иска ли достъп до информацията ви?“, „До каква информация имат достъп тези приложения?“, „За какво им е необходима тя?“

Примерни отговори: „Приложенията имат достъп до публичната информация, която сме споделили, както и до списъка с приятели, пола, възрастта, говоримите езици и местоживееенето. Приложенията използват тази информация за създаване на собствен профил, реклама, персонализиране на съдържанието, помощ в откриването на приятели и т.н.“

10. Свляянето на файлове от интернет може да бъде опасно – верен отговор: факт

Въпроси за дискусия: „Какви файлове свляяме от интернет?“, „Как могат да бъдат опасни те?“, „Какво можем да направим, за да се предпазим?“

Примерни отговори: „Свляяме музика, картинки, филми, документи, програми и т.н. Част от тях могат да съдържат вируси, които да заразят устройството ни. За да се предпазим, можем да инсталираме антивирусна програма на устройството си и да сканираме новите файлове, които свляяме.“



Инструмент 11: Групова работа (Комуникация онлайн и офлайн)

Водещият започва основната дейност, като използва въвеждащата игра: „Понякога безсилието може да ни накара да прибегнем до физическа сила, както видяхме преди малко (ако ученикът не се е опитал насила да разтвори юмрука на съученика си, водещият може да промени изказа – „Възможно бе едн-кой си дори да използва физическа сила в опит да постигне целта си...“). Какво друго може да ни накара да бъдем груби с околните и да прибегнем до насилие? Дайте примери.“

Записва думите на дъската.

Продължава със следното кратко обобщение: „Както виждате, понякога се държим лошо с другите и ги нараняваме, защото се чувстваме уплашени, безпомощни, ядосани, несигурни и т.н. и не знаем по какъв друг начин да постъпим.“
(5 минути)

Водещият въвежда следващото упражнение: „Сега ще се опитаме да открием начини, по които да общуваме с околните, без да използваме насилие – нито физическо, нито вербално. За тази цел трябва да се разделим на групи.“

Разделя класа на 4 групи, раздава им принтиран казус и инструкции за работа:

„Пред вас имате казус и задачата ви е да измислите отговор или реакция, които не нараняват другия и не включват насилие. Старайте се да давате максимално конкретни предложения – напишете точните думи, които бихте използвали.“

Казуси:

Ситуация 1

Иван учи много старателно за контролното си по география, но не е удовлетворен от оценката, която получава, и решава да говори с преподавателя.

Ситуация 2

Петя качва свое селфи в Instagram, но нейна съученичка пише обидни коментари под снимката. Петя решава да пише на лично съобщение на момичето и да поговори с нея.

Ситуация 3

Гергана чака с нетърпение рождения ден на своята най-добра приятелка, но родителите ѝ в последния момент не ѝ позволяват да отиде, тъй като на следващия ден трябва да пътуват рано сутринта. Гергана решава да се опита да поговори с тях.

Ситуация 4

Мариела разбира, че ѝ е направен фалшив профил във Facebook, от който се пишат неприлични съобщения на нейни приятели. Тя подозира, че фалшивият профил е направен от Нели – момиче от съседния клас, с което са се карали преди. Мариела решава да поговори с Нели.

(Дайте 10 минути за работата по групи и обсъждане на казусите)

След това водещият стартира дискусия, чиято цел е да изведе основни принципи на ненасилствената комуникация.

Примерни въпроси: „След като чухме всички отговори, можете ли да откриете нещо общо между тях?“, „Какво ви прави впечатление?“, „Какво е характерно за тези отговори?“

„Кое би имало повече успех – да говорим от собствено име или от името на всички?“, „Какъв е най-подходящият изказ?“, „Важно ли е да заявим от какво имаме нужда/как се чувстваме/какво ни се иска да се случи?“, „Можем ли да направим това, без да засегнем другия? Как?“

„Според вас кое изречение би имало по-голям ефект – „Ти си страшно несебриозен!“ или „Разочарован/а съм от поведението ти“?“

„Има ли значение дали разговаряме във формална, или неформална ситуация? Ако говорите на „ти“ на учител, това може ли да бъде обидно, или неуместно?“

„Някои от вас имаха случки в интернет. Какво е особеното там?“, „Могат ли тези принципи да се приложат в онлайн общуването? Как?“, „Онлайн можем ли просто да игнорираме човека?“, „Можем ли да направим това в реалността?“

(13 минути)

Водещият записва принципите и ценните отговори на флипчарт лист, който да може да бъде използван и по-късно.

Примерни отговори, към които се стремим:

1. Говорим от собствено име.
2. Не обиждаме и не нагрубяваме събеседника.
3. Говорим ясно, конкретно и искрено.
4. Изслушваме мнението на събеседника.
5. Други



Инструмент 12: Рефлексия: Дигитален имидж

Водещият моли участниците да помислят за следните въпроси и да запишат отговорите си:

- Какъв искам да бъда онлайн? Как искам да ме виждат другите?
- Какви качества, умения и интереси искам да покажа?
- Какво съдържание искам да споделям? (Снимки, статии, видеа и т.н.)
- Каква аудитория искам да привлека?



Инструмент 13: Групова работа

Водещият разделя на 3 отбора учениците/групата, като всеки отбор получава казус с въпроси към него, на които трябва да отговори. Казусите се отнасят до общуване в определени социални мрежи, затова е важно във всеки отбор да има поне един човек, който използва даденото приложение. Отборите изчитат казусите. Дават се **10 минути**. След като 10-те минути изтекат, водещият задава въпроси (които могат и предварително да се раздадат по отборите) на всеки отбор (въпросите са под всеки казус по-долу) и участниците трябва да направят екипен отговор. Водещият е добре да напомни, че е важно всички да се изслушват, защото другите отбори могат да задават въпроси и да дават предложения. Тази част от инструмента отнема около 25 минути.

Казус 1. Facebook

Качвате ваши снимки на стената си във Facebook и пишете статуси, но много непознати хора започват да коментират. Част от коментарите под вашите публикации са доста обидни. Непознати, които са коментирали, започват да ви пращат покани за приятелство, да ви пишат лични съобщения, както и да ви отбелязват в различни публикации.

Кои настройки трябва да промените в профила си, за да се справите със ситуацията? Използвайте вашите реални профили, за да ги откриете и запишете:

Примерни верни отговори:

1. Review posts that you're tagged in before the posts appear on your timeline?
Settings -> Privacy -> Timeline and tagging -> Review -> Review posts that you're tagged in before the posts appear on your timeline? -> On
2. Who can post on your timeline?
Settings -> Privacy -> Timeline and tagging -> Timeline -> Who can post on your timeline? - Only me
3. Who can see your future posts?
Settings -> Privacy -> Privacy settings -> Your activity -> Who can see your future posts? -> Friends (You decide who can see your posts each time you create a new post)
4. Who can send you friend requests?
Settings -> Privacy -> Privacy settings -> How people can find and contact you -> Who can send you friend requests? -> Friends of friends
5. Do you want search engines outside of Facebook to link to your profile?

Settings -> Privacy -> Privacy settings -> How people can find and contact you -> Do you want search engines outside of Facebook to link to your profile?

Водещият насочва дискусията с помощта на различни въпроси:

„Защо е добре да решаваме кои публикации искаме на стената си?“, „Възможно ли е дори приятел да ни отбележи в нещо, в което не искаме?“, „Какво се случва, когато публикациите ни са публични? Това може ли да бъде опасно?“, „А ако всеки може да ни изпраща покани за приятелство?“, „Как хората намират профила ни?“, „Могат ли просто да напишат името ни в Google? Така колко хора могат да открият нашия профил?“

Водещият може да зададе няколко допълнителни въпроса към отбора и целия клас:

„Познати ли ви бяха тези настройки?“, „Променихте ли някои в своите профили?“, „След като разбрахте колко са важни те, ще ги промените ли?“, „Смятате ли, че имате контрол върху информацията във вашите профили във Facebook?“

Бонус въпрос: „Как можем да въведем всички тези настройки само с една промяна?“

Казус 2. Instagram

Ученик от съседен клас ви следва в Instagram и редовно спама с коментари всички нови снимки, които качвате. Много често реагира с коментари и на историите ви, които са ви досадни, а понякога са и малко обидни.

Кои настройки трябва да промените в профила си, за да се справите със ситуацията? Използвайте вашите реални профили, за да ги откриете и запишете:

Примерни верни отговори:

1. Private Account

Settings -> Privacy and Security -> Privacy -> Account Privacy -> Private Account -> On

2. Add automatically photos and videos of you (Как да активирам опцията за ръчно избиране на снимки, които да се показват в профила ми?)

Settings -> Privacy and Security -> Privacy -> Photos and Videos of You -> Add automatically -> Off

3. Block Comments From Settings -> Privacy and Security -> Privacy -> Comment Controls -> Controls -> Block Comments From -> Add people

4. Hide Story From Settings -> Privacy and Security -> Privacy -> Hide Story From -> Choose people

5. Remove Follower - Profile -> Followers -> Choose follower you want to remove -> Select the tree dots -> Select Remove

Водещият насочва дискусията с помощта на различни въпроси:

„Какво се случва, когато профилът ни в Instagram е поверителен?“, „Кой може да ни следва тогава? А кой може да ни отбелязва в снимки и видеа?“, „Можете ли да скриете някои от тях? Как?“, „Ако нечий коментари са ви неприятни, как

можете да ги ограничите?“, „Случвало ли ви се е да искате да си публикувате история, но да не искате определен човек да я вижда? Какво можете да направите тогава?“, „А ако не искате някой да ви следва?“

Водещият може да зададе няколко допълнителни въпроса към отбора и целия клас:

„Познати ли ви бяха тези настройки?“, „Променихте ли някои в своите профили?“, „След като разбрахте колко са важни те, ще ги промените ли?“, „Смятате ли, че имате контрол върху информацията във вашите профили в Instagram?“

Казус 3: Snapchat

Непознат ви добавя в Snapchat, където започва да ви пише и да ви гледа историите. Понякога му отговаряте, но понякога не. Един ден сте излезли в парка с приятели и сте качили история за това. Скоро се появява непознат човек, който ви нарича с името ви в Snapchat и иска да се присъедини към компанията ви.

Кои настройки трябва да промените в профила си, за да се справите със ситуацията? Използвайте вашите реални профили, за да ги откриете и запишете:

Примерни верни отговори:

1. Who can contact me: Profile screen -> Settings (the ⚙️ button) -> Who can... -> Who can contact me -> My Friends
2. Who can view my story: Profile screen -> Settings (the ⚙️ button) -> Who can... -> Who can view my story -> My Friends
3. Who can see my location on Snap Map: Profile screen -> Settings (the ⚙️ button) -> Who can... -> Who can see my location -> Ghost Mode
4. Block a friend: Friends screen -> Tap and hold on a friend's name -> More -> Block
5. Who can see me in Quick Add: Profile screen -> Settings (the ⚙️ button) -> Who can... -> Who can see me in Quick Add -> Off

Водещият насочва дискусията с различни въпроси:

„Защо не бихте искали всеки да може да се свързва с вас в Snapchat?“, „Защо не бихте искали всеки да вижда къде сте на картата?“, „Може ли да бъде опасно това? По какъв начин?“, „Можете ли да бъдете 100% сигурни, че снимките изчезват, след като ги изпратите?“

Водещият може да зададе няколко допълнителни въпроса към отбора и целия клас:

„Познати ли ви бяха тези настройки?“, „Променихте ли някои в своите профили?“, „След като разбрахте колко са важни те, ще ги промените ли?“, „Смятате ли, че имате контрол върху информацията във вашите профили в Snapchat?“



Инструмент 14: **Дигитален имидж: Огледало на профила**



Цел: Учениците да осъзнаят каква информация за тях е видима онлайн и как тя влияе на дигиталния имидж.

Подготовка:

- ▶ Подгответе презентация или табло със следните въпроси:
 - Какво казва за вас профилната снимка?
 - Какви публични публикации или коментари сте споделили?
 - Каква информация за вас е видима без влизане в профила (напр. име, училище, местоположение)?

Инструкции за учениците:

1. Разделете учениците на двойки или ги оставете да работят индивидуално.
2. Накарайте ги да разгледат своите профили в социалните мрежи (например Instagram, Facebook, TikTok) или да помислят за поведението си в онлайн игрите и други платформи.
3. Учениците трябва да си запишат следното:
 - Три положителни неща, които техният профил показва за тях.
 - Едно нещо, което би могло да остави лошо впечатление.
4. След анализа, обсъдете в клас:
 - Какви първи впечатления създават техните профили?
 - Как могат да подобрят своето онлайн присъствие?

Времетраене: ~15 минути

Допълнение: Ако устройствата не са позволени, учениците могат да опишат профила си по спомени.



Инструмент 15: **Работа по групи: Създай перфектния дигитален имидж**



Цел: Учениците да упражнят създаването на съдържание, което изгражда положителен дигитален имидж.

Подготовка:

- ▶ Донесете шаблони за профили (може да са нарисувани на хартия или създадени в Canva).
- ▶ Подгответе примери за добри постове: вдъхновяващи цитати, снимки на успехи, участие в проекти.

Инструкции за учениците:

1. Разделете класа на групи от 3-4 ученика.
2. Задайте задачата:
 - „Вашата група трябва да създаде профил на измислен герой – ученик, който поддържа положителен дигитален имидж.“

- Героят трябва да е вдъхновяващ и да показва личностни качества като отговорност, креативност и добри взаимоотношения.
- 3. Елементите на профила трябва да включват:
 - Профилна снимка и биография (например: „Любител на науката | Капитан на училищния отбор | Харесвам доброволчество“).
 - Две публикации – например снимка от училищен проект с кратък текст или цитат за успеха.
- 4. След като приключат, всяка група представя профила си пред класа.

Дискусия след активността:

- Как създадените профили изглеждат на пръв поглед?
- Какво са научили за изразяването на себе си онлайн?

Допълнение: Ако има технически възможности, групите могат да използват онлайн инструменти като Canva, за да създадат дигитална версия на профила.



Инструмент 16: Групова работа: Онлайн тормоз

Казус

Марияна е ученичка в 6-ти клас, която планира да празнува рождения си ден с приятелките си. Родителите обаче не ѝ позволяват да кани повече от 6 деца, така че тя не успява да събере всичките си приятели на празника си. Две момичета от класа ѝ – Ана и Стефания разбират, че не са поканени и решават да направят профил в Инстаграм, озаглавен „Смотаната Марияна“. Там качват компрометиращи снимки и колажи с Мариана, придружени с подигравателни и обидни постове по неин адрес. Казват на всички приятели на Марияна, че не трябва да ходят на рождения ѝ ден и ги поканват да последват профила, който са направили срещу нея.

За кратко време профилът добива много последователи – както познати на Марияна, така обаче и непознати за нея хора. Някои от тях оставят груби шеги, подигравки и обидни коментари по адрес на Мария, но други само наблюдават пасивно профила, без да го следват или да коментират.

След няколко дни Марияна разбира за профила и го посещава. Ужасена е да види, че всеки ден и по всяко време на денонощието се появяват нови гадни коментари по неин адрес. Усеща болки в стомаха, преставя и да ходи на училище, защото се опасява, че и там ще се сблъска с подигравки и обиди.

След като прочете/покаже казуса, учителят разделя класа/групата на 4 или 5 групи, като всяка има за задача да помисли върху въпросите към казуса. Когато групите са готови всяка изчита поред отговорите на всеки въпросите към казуса, които виждат прожектирани на мултимедията. После всяка група по ред предлага своя отговор на всеки от въпросите като се стреми да допълва предходната или да коригира отговора ѝ, ако смята, че има нужда.

Въпроси по казуса: (въпросите се разпечатват за участниците)

1. Това ситуация на онлайн тормоз ли е? Защо/Защо не? (припомнете си характеристиките на онлайн тормоза)

.....

2. Кой/Кои са извършителите на онлайн тормоза?

.....

3. Кой е потърпевш от онлайн тормоза?

.....

4. Как мислите се е почувствал/а?

.....

5. Освен извършителят и потърпевшата, има ли други участници в онлайн тормоза? Кой са те и как бихте определили тяхната роля?

.....

6. Какви съвети бихте дали на потърпевшата, за да се справи с проблема?

.....

7. Какви съвети бихте дали на другите участници? Как бихте ги убедили да ви послушат?

.....

Отговори на въпросите към казуса:

1. Това ситуация на онлайн тормоз ли е? Защо/Защо не? (припомнете си характеристиките на онлайн тормоза)

Да, защото се случва в интернет, може да продължи много дълго (24/7) и да се наблюдава от много хора“.

2. Кой/Кои са извършителите на онлайн тормоза?

Анна и Стефания (бившите приятелки на Марияна). Също и останалите последователи и хора, които пишат обидни коментари, които са съучастници.

3. Кой е потърпевшият от онлайн тормоза?

Марияна.

4. Как мислите се е почувствала потърпевшата?

Обидена, натъжена, разочарована, засрамена, притеснена, уплашена/ ужасена, усеща и физически болки (в стомаха).

5. Освен извършителят и потърпевшата, има ли други участници в онлайн тормоза? Кой са те и как бихте определили тяхната роля?

Да, хората, които само наблюдават, но не са последвали профила и не коментират. Можем да ги определим като „наблюдатели“ или „свидетели“.

6. Какви съвети бихте дали на потърпевшата, за да се справи с проблема?

Да опита да поговори с извършителите, да обясни ситуацията, заради която са ѝ сърдити и да им каже как се чувства от постъпката ѝ и да поиска да престанат (без да ги обижда, но категорично).

Ако не престанат:

- ▶ Да сподели случилото се с родителите си и/или с доверен възрастен (друг роднина, учител, училищен психолог, педагогически съветник.
- ▶ Да направи екранна снимка (скрийншот) на профила срещу нея за доказателство.
- ▶ Да докладва профила в Инстаграм.
- ▶ Да блокира профилите на Анна и Стефания.
- ▶ Да се обърне за съвет на Консултативната линия на Центъра за безопасен интернет на телефон 124 123 или в чат-модула на сайта www.safenet.bg

7. Какви съвети бихте дали на другите участници? Как бихте ги убедили да ви послушат?

- ▶ Да подкрепят морално Марияна, така че да ѝ помогнат да се успокои и да се почувства по-добре.
- ▶ Ако познават или са приятели с извършителите (Анна и Стефания) да опитат да поговорят с тях и да ги убедят да престанат с онлайн тормоза над Марияна.
- ▶ Да сподели случилото се с учител, училищен психолог, педагогически съветник.
- ▶ Да направят екранна снимка (скрийншот) на профила срещу нея за доказателство.
- ▶ Да докладват също профила в Инстаграм.
- ▶ Да се обърнат за съвет на Консултативната линия на Центъра за безопасен интернет на телефон 124 123 или в чат-модула на сайта www.safenet.bg



Инструмент 17: Дискусия: Секстинг, доверие и лични граници



Цел: Участниците да изведат дефиниция за секстинг, да различават доверие от натиск и да разберат, че всеки има право да поставя граници в интимното онлайн общуване.



Времетраене: 10-15 минути

Водещият започва с кратка дискусия:

„Когато хората се харесват или са във връзка, как общуват онлайн?“

„Какво означава доверие в една връзка?“

„Може ли някой да поиска нещо, което другият не иска да направи?“

„Как разбираме дали нещо е свободен избор, или натиск?“

След първите отговори водещият въвежда понятието „секстинг“:

Секстинг е размяна на съобщения, снимки или видеа със сексуално съдържание. Това може да се случи между хора, които се харесват, флиртуват или са във връзка. Понякога изглежда като израз на доверие, но може да бъде и резултат от натиск, страх, срам, желание за одобрение или манипулация.

След това водещият записва на дъската две колони:

Участниците дават примери, които водещият разпределя в двете колони.

ДОВЕРИЕ	НАТИСК
Примерни отговори за „доверие“: • Човекът приема отказ. • Не настоява. • Не заплашва. • Не кара другия да пази тайна от възрастни. • Уважава границите. • Не използва снимки или съобщения срещу другия.	Примерни отговори за „натиск“: • „Ако ме обичаш, ще ми пратиш.“ • „Всички го правят.“ • „Само аз ще го видя.“ • „Ще ти се разсърдя.“ • „Ще скъсам с теб.“ • „Ще покажа на другите какъв/каква си.“ • „Прати още, иначе ще разпространя това, което вече имам.“

Водещият обобщава:

„Доверието не се доказва със снимки. Ако някой настоява, заплашва, обижда или кара другия да се чувства виновен, това вече не е доверие, а натиск. Всеки има право да каже „не“ и не е длъжен да изпраща интимно съдържание, за да докаже любов, близост или вяност.“



Инструмент 18: Групова работа по казус: „Само за нас двамата“



Цел: Участниците да разберат последствията от разпространение на интимна снимка и да упражнят подкрепящ, а не обвиняващ подход към потърпевшото дете.



Времетраене: 20-25 минути

Водещият разделя участниците на 3-4 групи и раздава казуса.

Казус:

Дани и Алекс са в един клас и от известно време си пишат всеки ден. Алекс казва на Дани, че много го/я харесва и че иска да имат „нещо специално, което да е само между тях“. След няколко дни започва да настоява Дани да изпрати интимна снимка. Дани първоначално отказва, но Алекс казва: „Ако ми имаш доверие, ще го направиш. Няма да я показвам на никого.“

Дани изпраща снимката. След седмица двамата се скарват. Алекс изпраща снимката в групов чат на няколко съученици. Част от тях започват да се подиграват, други препращат снимката, а трети само гледат и мълчат. Дани спира да идва на училище и не казва на никого какво се е случило.

Въпроси за работа по групи:

1. Какво се случва в този казус?
2. Имало ли е натиск? По какво разбираме?
3. Кой носи отговорност за разпространението на снимката?
4. Как според вас се чувства Дани?

5. Какво не трябва да правят съучениците, които са получили снимката?
6. Какво могат да направят наблюдателите, за да помогнат?
7. Какво трябва да направи Дани?
8. Как трябва да реагира възрастният, ако Дани сподели?

След работата по групи всяка група представя отговорите си.

Търсени изводи:

- Натиск има, защото снимката е поискана като „доказателство за доверие“.
- Отговорност за разпространението носи човекът, който е препратил снимката.
- Потърпевшият не трябва да бъде обвиняван или засрамван.
- Получилите снимката не трябва да я препращат, показват или коментират.
- Наблюдателите могат да подкрепят потърпевшия, да не участват в подигравките, да докладват и да кажат на доверен възрастен.
- Дани трябва да запази доказателства, да потърси възрастен и да получи подкрепа.
- Възрастният трябва да реагира спокойно: „Добре, че ми каза. Ще ти помогна. Не си сам/а.“

Водещият обобщава:

„Когато интимна снимка бъде разпространена без съгласие, това е злоупотреба. Най-важното е да се спре разпространението, да се запазят доказателства и потърпевшото дете да получи подкрепа, а не обвинения.“



Инструмент 19: Практическо упражнение за включване на двуфакторната верификация

Да научим участниците в групата как да настроят и използват двуфакторна верификация, за да повишат сигурността на своите акаунти.

Стъпки:

1. **Въведение в темата:** Обяснете какво е двуфакторна верификация и защо е важна. Споделете, че това е допълнителен слой на защита, който затруднява неотризиран достъп до акаунтите на потребителите.

Двуфакторната верификация е важна, защото дава допълнителна защита към акаунтите и имейлите ни. Дори ако някой научи паролата ни, той няма да има достъп до имейла/акаунта ни, без втория фактор – код, изпратен на телефона ни или генериран от приложение. Това значително намалява риска от неотризиран достъп и защитава личните ни данни и онлайн профили.

2. **Избор на платформа:** Помолете всеки участник да избере социална мрежа или онлайн услуга, която използва (например Instagram, Gmail, Facebook или друга, която поддържа двуфакторна верификация).
3. **Инструкции за активиране на двуфакторна верификация:** покажете на ек-

ран инструкциите за активиране на двуфакторна верификация за различни платформи. Ако всички са с еднакво устройство (например Android или iOS), може да демонстрирате процеса стъпка по стъпка.

4. **Сваляне на приложение за верификация:** Ако платформата изисква приложение за генериране на кодове (например Google Authenticator или Authy), обяснете как да го инсталират и свържат с акаунта си.
5. **Практическо изпълнение:** Помолете участниците да настроят двуфакторна верификация на акаунта, който са избрали. Подпомагайте процеса и отговаряйте на въпросите им.
6. **Тест за сигурност:** След като настроят двуфакторна верификация, помолете ги да излязат от акаунта си и след това да влязат отново, използвайки новите настройки. Обсъдете какво се случва, когато добавят втория фактор, и как това подобрява сигурността им.



Инструмент 20: **Непознатите в мрежата, груминг и сексторшън**



Цел: участниците да разпознават стратегии за манипулация от непознати онлайн, фалшиви профили и ранни признаци на сексуално изнудване.



Времетраене: 25-30 минути

Водещият разделя участниците на три групи. Всяка група получава един казус и въпроси към него.

Казус 1: „Новият приятел в Snapchat“

Непознат профил започва да пише на Мира. Профилът изглежда на момче на нейната възраст. Той е мил, пита я как е минал денят ѝ, прави ѝ комплименти и казва, че я разбира по-добре от хората в класа ѝ. След няколко дни започва да ѝ пише, че е красива и че иска да види „по-лична снимка“. Казва: „Няма да я показвам. Нали си имаме доверие?“

Въпроси:

1. Какво се случва в този казус?
2. Как човекът отсреща изгражда доверие?
3. Кои са предупредителните знаци?
4. Какво може да направи Мира?
5. Към кого може да се обърне?

Казус 2: „Профилът от същото училище“

Профил в Instagram пише на Виктор, че е ученик от съседен клас. Профилът знае името на училището му, любимия му отбор и имената на двама негови приятели. Виктор не го разпознава, но човекът казва, че просто не са се засичали. След няколко разговора предлага да преминат в Telegram, защото „там е по-лично“. После започва да иска снимки и настоява разговорът да остане тайна.

Въпроси:

1. Защо профилът изглежда убедителен?
2. Откъде може да знае информация за Виктор?
3. Какви са рисковете при преминаване в друг чат?
4. Как Виктор може да провери дали човекът е реален?
5. Каква е безопасната реакция?

Казус 3: „Безплатни скинове“

В онлайн игра Ники получава съобщение от играч, който му обещава безплатни скинове и валута в играта. За целта Ники трябва да влезе в линк и да потвърди профила си. След като го прави, профилът му е откраднат. После същият човек му пише, че ще върне профила само ако Ники изпрати снимка или плати с ваучер.

Въпроси:

1. Каква измама се случва първо?
2. Как измамата преминава в изнудване?
3. Какво не трябва да прави Ники?
4. Какви доказателства трябва да запази?
5. Към кого може да се обърне?

След представянето на групите водещият извежда общите стратегии на извършителите:

- представят се за връстник;
- използват комплименти;
- създават усещане за тайна и специална връзка;
- използват информация от публични профили;
- местят разговора в друг канал;
- искат снимки, пари, кодове или пароли;
- заплашват и създават паника.

Обобщение:

„Ако някой иска тайна, снимки, кодове, пари или разговор в друг чат, това е знак да спрем и да потърсим помощ. Не е нужно да доказваме нищо на човек, когото познаваме само онлайн.“



Инструмент 21: Дискусия: Дискусия по видео или казус: „Кажу НЕ на изнудването“



Цел: участниците да разберат как се развива сексторшънът и какви са правилните първи стъпки за реакция.



Времетраене: 15-20 минути

Водещият може да използва подходящо видео по темата, ако има проверен и възрастово подходящ материал. Ако няма такова видео, използва следния кратък казус.

Казус:

Иво си пише с момиче, с което се е запознал в социална мрежа. След кратък флирт тя му изпраща снимка и го кара и той да изпрати своя. Малко след това профилът му пише: „Имам снимката ти и списъка с приятелите ти. Ако не платиш до 30 минути, ще я изпратя на всички.“

Въпроси за дискусия:

1. Какво се случва?
2. Защо извършителят поставя кратък срок?
3. Какви чувства може да изпита Иво?
4. Какво не трябва да прави?
5. Какво трябва да направи първо?
6. Защо плащането не решава проблема?
7. Как могат да помогнат възрастните?

Търсени отговори:

- Това е сексторшън – сексуално изнудване.
- Краткият срок създава паника и пречи на детето да мисли спокойно.
- Иво може да се чувства уплашен, засрамен, виновен, отчаян.
- Не трябва да плаща, да изпраща още снимки или да се опитва да решава сам.
- Трябва да запази доказателства и да каже на доверен възрастен.
- Плащането често води до нови искания.
- Възрастните могат да помогнат с докладване, ограничаване на вредата и търсене на подкрепа.

Водещият записва на дъската:

- ▶ **НЕ ПЛАЩАЙ.**
- ▶ **НЕ ПРАЩАЙ ОЩЕ.**
- ▶ **ПАЗИ ДОКАЗАТЕЛСТВА.**
- ▶ **КАЖИ НА ВЪЗРАСТЕН.**
- ▶ **ДОКЛАДВАЙ.**

Обобщение:

„Сексторшънът разчита на страх и срам. Когато детето каже на възрастен, извършителят губи част от контрола.“

Инструмент 22: Дискусия: Изкуствен интелект



Цел: е участниците да помислят и да дискутират ролята на изкуствения интелект в различни области, предимства и недостатъци.



Времетраене: 15-20 минути

Разделете участниците на групи по 4-5, според общия брой. Подгответе флипчарт и напишете няколко области, в които ИИ има определено влияние, например „ИИ в здравеопазването“, „ИИ в образованието“, „ИИ в науката и технологиите“, и др. Под заглавието на всяка област разделете флипчарта на две „Предимства на ИИ“ и „Недостатъци на ИИ“.

Всяка група получава по една област да помисли за предимствата и недостатъците. Дайте им 10 мин. След това в общата група дискутирайте отговорите. Упражнението има за цел да ги накара да мислят и да разсъждават, да обменят мисли с останалите, в случая не търсим верни или грешни отговори. В таблицата по-долу са дадени примерни предимства и недостатъци на ИИ за сравнение.

Предимства на ИИ	Недостатъци на ИИ
1. Намаляване на случаите на човешка грешка Едно от най-големите предимства на ИИ е, че може значително да намали грешките и да увеличи точността и прецизността. Решенията, взети от ИИ във всяка стъпка от процеса, се основават на предварително събрана информация и определен набор от алгоритми. При правилно програмиране, тези грешки могат да бъдат намалени до нула.	1. Творчество ИИ няма присъщата креативност на хората, която произтича от емоционалната дълбочина, способността за абстрактно мислене и въображаеми процеси. ИИ може да имитира творчество, но не притежава истинска оригиналност. Резултатите на ИИ са всъщност рекомбинация на съществуващи данни.
2. Вземане на решения ИИ подобрява вземането на решения, защото използва огромни масиви от данни, като идентифицира модели и тенденции, често неосъзнати от хората. ИИ може да обработи голям обем от информация за много кратко време, което дава предимство в динамична среда.	2. Безработица По замисъл ИИ има за цел да замени човека в редица дейности, което само по себе си е предпоставка за увеличаване на човешката безработица. В същото време създаваните нови възможности на ИИ създават нови професии.
3. Нулеви рискове Машините с ИИ могат да намалят или премахнат рискове за хората, когато е необходимо действие в опасна среда. Това може да означава изследване на океанските дълбини или работа в космоса – така хора няма да бъдат изложени на риск.	3. Емоционална интелигентност Системите на ИИ нямат емоционална интелигентност или способността да разбират, интерпретират и реагират на човешки емоции по нюансиран и съпричастен начин. Емоционалната интелигентност означава също и разпознаване и управление на собствените емоции, както и съпричастност към другите и емпатично справяне с междуличностните отношения.
4. Може да се разчита винаги За разлика от човека, машините с ИИ могат да работят почти безкрайно. Могат да изпълняват дълго досадни и повтарящи се задачи с помощта на създадени алгоритми.	4. Рискове за сигурността Системите с ИИ могат да представляват значителни рискове за сигурността, особено в критични инфраструктури като финанси, здравеопазване и национална сигурност. Те могат да бъдат уязвими за хакерство, нарушения на данните и злонамерени атаки. Гарантирането на сигурността изисква постоянна бдителност и усъвършенствани мерки за киберсигурност, които могат да бъдат както скъпи, така и технически предизвикателство.

Предимства на ИИ	Недостатъци на ИИ
5. Дигитална помощ Въпреки някои несъвършенства, ИИ може да замести нуждата от човешки персонал в различни присъщи на хората дейности.	5. Високи разходи Създаването на машина, която да може да симулира човешки интелект е скъпо и трудоемко начинание.
6. Нови изобретения Големият набор от данни, с които работи ИИ може да даде нови насоки на хората за иновации. Това може да се отнася до ключови за човека области като медицина, химия, физика, които да дадат ново качество на живот.	6. Насърчаване на човешкия мързел Нарастващата зависимост от ИИ за задачи, вариращи от обикновени задължения до сложно вземане на решения, може да доведе до човешки мързел. Тъй като системите с ИИ поемат повече отговорности, хората могат да станат по-малко склонни да развиват своите умения и знания, разчитайки прекомерно на технологиите. Тази зависимост може да намали критичното мислене и способностите за решаване на проблеми.
7. Безпристрастни решения Липсата на емоционално влияние прави използването на ИИ много безпристрастен съветник. Разбира се, трябва да се доверим, че програмирането на ИИ се е случило без предразсъдъци.	7. Опасения за поверителността Системите на ИИ често изискват огромни количества данни, за да функционират ефективно, което може да доведе до значителни опасения за неприкосновеността на личния живот. Събирането, съхранението и анализът на лични данни могат да бъдат компрометирани. Съществува риск от нарушения и изтичане на данни, които могат да компрометират лична и финансова информация, което да доведе до кражба на самоличност и финансови злоупотреби.
8. Избягване на измами ИИ може да подобри откриването и предотвратяването на измами, като анализира моделите на финансови транзакции и идентифицира аномалии. Алгоритмите могат да открият необичайно поведение и да сигнализират за подозрителни действия в реално време, което да съкрати времето за реакция.	8. Пристрастия ИИ може да увеличи съществуващите отклонения в данните, на които е обучен. Тези пристрастия могат да се проявят по различни начини, като дискриминационни практики за наемане или неравен достъп до услуги. Тъй като ИИ се учи от исторически данни, той може непреднамерено, поради работата на алгоритмите, да засили стереотипите и дискриминационните модели.
9. Оптимизация на работни процеси ИИ може да анализира ефективността на работните процеси, изпълнявани от хора, и да предложи тяхното подобряване. Това например може да помогне на организациите да подобрят работния процес, да повишат производителността на служителите и да намалят оперативните разходи.	9. Проблеми с развитието на алгоритмите Бързото развитие на алгоритмите на ИИ поражда опасения относно темпа и посоката на технологичния напредък. Съществува риск алгоритмите да се разработват и внедряват по-бързо, отколкото регулаторните рамки и етичните насоки могат да се справят. Това може да доведе до нежелани последици, като например злоупотреба с технологии с ИИ, точна оценка на цялостно въздействие върху обществото.
10. Персонализирани препоръки ИИ може да подобри търсенето и намирането на различни стоки или услуги, като прави анализ на индивидуалните предпочитания и поведение. Това може да включва анализ на историята на потребителското поведение, история на търсенето, демографска информация. Това би дало профил на клиента и спомага за по-добро позициониране на фирмите, увеличавайки удовлетвореността и лоялността на клиентите.	10. Етични съображения ИИ повдига многобройни етични опасения, особено по отношение на процесите на вземане на решения и потенциала за злоупотреба. Проблеми като липсата на отчетност, прозрачността и потенциала на ИИ да бъде използван по вредни начини (например автономни оръжия или масово наблюдение) поставят значителни етични предизвикателства. Гарантирането, че системите с ИИ работят в рамките на етичните граници, изисква стабилни рамки за управление, ясни етични насоки и постоянен диалог между заинтересованите страни, включително технологи, политици и обществеността.

Предимства на ИИ	Недостатъци на ИИ
11. Сигурност ИИ може да подобри сигурността, като анализира огромни обеми от данни от различни източници. По този начин могат да се откриват необичайни дейности, да се разпознават лица и да се идентифицират потенциални заплахи за сигурността.	11. Липса на здрав разум Въпреки напредналите си възможности, системите на ИИ често се нуждаят от повече разумни разсъждения. Те могат да обработват и анализират огромни количества данни, но се нуждаят от помощ при разбирането на контекста, правенето на интуитивни преценки или адаптирането към нови и непредвидени ситуации. Това ограничение може да доведе до грешки или неподходящи действия в сценарии, които изискват нюансирано разбиране и гъвкавост. За разлика от хората, изкуственият интелект няма вродената способност да схваща и „разбира“ ежедневните промени и социални норми, които могат да доведат до логически правилни решения, но като резултат са практически погрешни или етично неиздържани.
12. Пристрастие и справедливост Възможно е ИИ да бъде използван по начин, така че да бъдат установени модели на пристрастия или влияния, които да са довели до неправилни решения. ИИ може да сведе до минимум такива отклонения и да подобри използването на обективни и безпристрастни критерии за оценка.	12. Екологични проблеми Разработването и внедряването на технологии на ИИ може да има значително въздействие върху околната среда. Обучението на големи модели на ИИ често изисква голяма изчислителна мощност, която изисква значителна консумация на енергия. Това може да допринесе за увеличаване на въглеродните емисии и да изостри изменението на климата. Центровете за данни, в които се помещава инфраструктурата за системи на ИИ, изискват постоянно охлаждане и поддръжка, което допълнително увеличава техния екологичен отпечатък. Тъй като технологията на ИИ расте, намирането на устойчиви и енергийно ефективни решения е от решаващо значение за смекчаване на въздействието върху околната среда.



Инструмент 23: Групова работа: Вредно онлайн съдържание

КАЗУСИ ЗА РАБОТАТА ПО ГРУПИ:

■ Казус 1

Камелия е ученичка в 9. клас, която, въпреки че е висока и тежи 47 кг, винаги се е смятала за пълна. Когато е споделяла със свои приятели притесненията си, те винаги са отвръщали със смях, казвали са ѝ, че няма реална преценка за себе си и да престане да си мисли глупости. Един ден, разглеждайки Facebook, Камелия попада на група, наречена „Ана и Мия – новите ти приятелки“, която е пълна със снимки на много слаби момичета и надписи, които насърчават отслабването и заявяват колко красиво е това. В коментарите Камелия открива други момичета, които се окуражават една друга да спазват диети, да не се хранят, да повръщат, след като са яли, споделят начини за броене на калории. В тази група Камелия открива подкрепа, която не получава на друго място, тъй като членовете ѝ споделят нейните собствени възгледи за това как би трябвало да изглежда.

Въпроси за дискусия:

1. Кой е главният герой в казуса?
2. Какво се случва с него?
3. Какво вредно онлайн съдържание откривате в казуса?
4. Защо е опасно то?
5. Какви мерки бихте предприели в този случай?

■ Казус 2

Пламен е ученик в 8. клас, който, както повечето си съученици и приятели, обича да играе различни игри и непрекъснато търси нови и различни занимания. Един ден, докато е във Facebook, попада на следното предизвикателство, споделено от непознато момче: от участника се иска през нощта да се покатери върху новострояща се сграда в града, където да си направи селфи и да го сподели публично в профила си с хаштага #topoftheworld. Условието обещава още, че притежателят на снимката, събрала най-много коментари, ще получи чисто нов смартфон като награда.

Въпроси за дискусия:

1. Кой е главният герой в казуса?
2. Какво се случва с него?
3. Какво вредно онлайн съдържание откривате в казуса?
4. Защо е опасно то?
5. Какви мерки бихте предприели в този случай?

■ Казус 3

Лора и Анелия са ученички в 7. клас в едно и също училище, но са от съседни паралелки. От няколко седмици Лора излиза с Георги, който е бивш приятел на Анелия. Постепенно между двете момичета почва да назряват конфликти – гледат се презрително, когато се разминат в училище, разпространяват фалшива информация една за друга, обиждат се във Facebook и Instagram. Цялото училище е наясно с драмата, докато един ден след училище, двете се сбиват в градинката до сградата на училището. Лора и Анелия си разменят удари, скубят се, ритат се. Никой не се намесва, а техен съученик прави видео на боя. Малко по-късно клипът е качен във Facebook, където за кратко време събира хиляди гледания и коментари от различни хора.

Въпроси за дискусия:

1. Кой са главните герои в казуса?
2. Какво се случва с тях?
3. Какво вредно съдържание откривате в казуса?
4. Защо е опасно то?
5. Какви мерки бихте предприели в този случай?

ИНСТРУМЕНТИ ЗА ЗАКЛЮЧИТЕЛНАТА ЧАСТ:



Инструмент 24: Дискусия

Обучителят задава насочващи въпроси, чрез които прави обобщение на урока.

Нека сега да си припомним най-важните неща, които научихме днес.

Каква е разликата между права и отговорности? Кои права запомнихте? Всички хора и деца ли имат права? А кои отговорности?

Припомнете основните правила за безопасно сърфиране в Интернет.

1. Държим се учтиво и уважително с другите.
2. Пазим личната си информация (три имена, адрес, училище, пароли).
3. Посещаваме само сайтове, които са подходящи за нашата възраст.
4. Докладваме вредно или обидно съдържание.
5. Не приемаме покани за запознанства с непознати онлайн.
6. Ако нещо ни притеснява в интернет, можем да споделим с родителите си.

Знаете ли към кого още можете да се обърнете при проблем в интернет? - Националната телефонна линия за онлайн безопасност на тел. 124 123 или в чата на www.safenet.bg. Там можете да зададете въпрос, да получите подкрепа и да докладвате за проблем в интернет.



Инструмент 25: Дискусия

Чрез насочващи въпроси и кратка дискусия водещият извежда основните изводи от работата през часа:

„Какво са лични данни?“, „Можем ли да контролираме информацията за нас в интернет и социалните мрежи? Как?“



Инструмент 26: Брейнсторминг с елемент на дискусия

С това упражнение създавате рефлекс „Мисли, преди да публикуваш“ у децата. Изберете публикация (своя или на някой друг и обсъдете с децата какво виждат и какво разбират от публикацията през въпроси като: „Какво искат да кажат с тази снимка според теб?“, „Какво е посланието на това видео?“, „Какъв е изводът в последната ти публикация, какво могат хората да научат за теб от това, което качваш в мрежата?“. Така ще ги наведете на мисълта, че е важно да помислят внимателно, преди да споделят нещо онлайн. Дискутирайте какво биха искали приятелите им и непознати хора онлайн да научават за тях и дали и как публикуваната информация ги прави уязвими. Наблегнете на факта, че веднъж публикувани, информация, снимка, видео, започват да водят свой собствен живот и дори да бъдат изтрети от профила, те може да продължат да циркулират из мрежата. Ако има хора, които свалят съдържанието или направят скриншот, то може да бъде видимо в интернет години наред.

Инструмент 27: Брейнсторминг

Направете брейнсторминг по темата „Какви са рисковете от споделяне на локация в социалните мрежи? Може ли да има негативни последствия и какви?“. Поговорете с децата дали е необходимо да се „отбелязват“ в социалните медии. Проверете чрез въпрос колко от тях са изключили автоматичното разрешаване на приложението или сайта да използва/отбелязва местоположението му. Попитайте ги дали искат разрешение от приятелите си, когато ги тагват.

Инструмент 28: Брейнсторминг (Фишинг)

Помолете участниците да си представят че както си скролват в Инстаграм им се появява реклама/предложение: „Ако искате да спечелите 50 евро за акаунта си в Steam или Roblox, кликнете тук?“. Направете брейнсторминг какво може да се случи, ако кликнат. Записвайте на дъската или на флипчарт всички предположения. След това ги попитайте знаят ли какво е фишинг и знаят ли каква е целта му? Покажете им, че фишингът може да се случи и през имейл и чрез смс/вайбър съобщение. Направете следното упражнение за разпознаване дали едно съобщение е истинско или фалшиво.

Насочвайте учениците да преглеждат внимателно подателя на имейли, да следят за лош правопис и съмнителни искания. Насърчете ги в началото винаги да се консултират, преди да кликнат върху линкове или да предприемат действия. Илюстрирайте риска с примери за деца и възрастни, които са загубили профилите си, след като са реагирали на фалшиви съобщения за нарушаване на правилата на социални мрежи. Подчертайте, че връщането на профил е сложен процес, а за тийнейджърите тези профили често са много ценни.

Инструмент 29: Дискусия: Вредно съдържание

Водещият започва дискусия, с която да обобщи урока, използвайки последния казус:

„Попадали ли сте в интернет/по телевизията на картинки, снимки, видеа, новини и т.н., изобразяващи насилие (може да се уточни, че не е задължително насилието да е само върху хора, но и върху животни например)?“, „Има ли желаещи, които да споделят как са се почувствали в подобна ситуация?“, „Според вас гледането на насилие влияе ли ни по някакъв начин?“, „Представете си, че попадате на видео, в което деца бият свой съученик. Как ще се почувствате първия път, когато го гледате?“, „Ще се чувствате ли по същия начин, ако гледате видеото пет пъти?“, „Ако често попадате на насилие, това може ли да ни направи по-малко чувствителни към него?“, „Какво трябва да направим, ако попаднем на такова съдържание в интернет?“

Децата извеждат стратегии за справяне със съдържанието с насилие и с вредното онлайн съдържание:

1. Можем да докладваме в самия сайт.
2. Можем да докладваме на Консултативната линия за онлайн безопасност 124 123.

Можем да поговорим с родител, учител, училищен психолог, ако сме разстроени от видяното.



Инструмент 30: Дискусия: Онлайн тормоз

Обучителят инициира дискусия, като задава насочващи въпроси като „Какво е характерно за онлайн тормоза?“, „Какви са основните роли във всяка ситуация на онлайн тормоз?“, „Какво бихте посъветвали потърпевшия?“, „А наблюдателите?“.

Търсени отговори: „Онлайн тормозът е вид тормоз, който се случва в интернет, може да продължи много дълго (24/7) и да се наблюдава от много хора“,

„Основните роли в такива ситуации са на извършител, потърпевш и наблюдатели/свидетели“, „Бихме посъветвали потърпевшия да опита да поговори с извършителите, да обясни ситуацията, заради която са й сърдити и да им каже как се чувства от постъпката им и да поиска да престанат и ако не престанат – да сподели случилото се с родителите си и/или с доверен възрастен, да направи екранна снимка (скрийншот) на профила срещу нея за доказателство, да докладва профила в съответната социална мрежа, да докладва и блокира профила на извършителя, да а се обърне за съвет на Консултативната линия на Центъра за безопасен интернет на телефон 124 123 или в чат-модула на сайта www.safenet.bg“, „Бихме посъветвали наблюдателите да подкрепят морално потърпевшия, ако познават или са приятели с извършителя да опитат да поговорят с него и да го убедят да престане с онлайн тормоза, да споделят случилото се с учител и/или друг доверен възрастен, да направят екранна снимка (скрийншот) на профила срещу нея за доказателство, също да докладват профила на извършителя в самата социална мрежа и също да се обърнат за съвет на Консултативната линия на Центъра за безопасен интернет на телефон 124 123 или в чат-модула на сайта www.safenet.bg“.



Инструмент 31: Заклучителна дискусия: Какво научихме за секстинга?



Цел: участниците да обобщят наученото и да формулират ясни правила за безопасно и уважително онлайн общуване.



Времетраене: 5-8 минути

Водещият задава въпроси:

„Какво е секстинг?“

„Кога една ситуация вече не е доверие, а натиск?“

„Какво означава да поставиш граница?“

„Какви могат да бъдат последствията от изпращането или разпространението на интимна снимка?“

„Кой носи отговорност, ако снимката бъде разпространена?“

„Какво можем да направим, ако сме притиснати да изпратим снимка?“

„Какво можем да направим, ако получим чужда интимна снимка?“

Търсени изводи:

- Секстингът е размяна на сексуализирани съобщения, снимки или видеа.
- Никой няма право да изисква интимно съдържание като доказателство за любов или доверие.
- Отказът е право.
- Разпространението на интимно съдържание без съгласие е злоупотреба.
- Потърпевшото дете не трябва да бъде обвинявано.
- Не препращаме чуждо интимно съдържание.
- При натиск, заплаха или разпространение търсим помощ.

Водещият завършва:

„Истинското доверие уважава отказа. Ако някой настоява, заплашва или изнудва, това не е любов и не е доверие.“



Инструмент 32: Брейнсторминг и ролеви отговори: Как да кажем „не“?



Цел: участниците да упражнят конкретни фрази за отказ при натиск за интимни снимки или видеа.



Времетраене: 10-15 минути

Водещият въвежда ситуацията:

„Представете си, че човек, когото харесвате, ви поиска интимна снимка. Вие не искате да изпращате такава снимка, но не искате и разговорът да се превърне в конфликт. Какво можете да кажете?“

Участниците дават предложения, които водещият записва. След това групата обсъжда кои отговори са най-ясни, спокойни и категорични.

Примерни отговори:

- „Не искам да изпращам такива снимки.“
- „Не ми е комфортно.“
- „Ако ме уважаваш, няма да настояваш.“
- „Не доказвам доверие със снимки.“
- „Не. Това е мое решение.“
- „Спирам този разговор.“
- „Ще говоря с възрастен, ако продължиш да настояваш.“
- „Не изпращам снимки, които не бих искал/а да бъдат препратени.“

След това водещият предлага работа по двойки. Единият участник чете натискаща фраза, а другият упражнява отказ.

Примерни натискащи фрази:

- „Ако ме обичаш, ще го направиш.“
- „Всички го правят.“
- „Само аз ще я видя.“

- „Няма да ти пиша повече.“
- „Не ми ли вярваш?“
- „Прати само една.“
- „Ако не пратиш, ще покажа какво вече имам.“

Важно е водещият предварително да уточнява, че упражнението е учебно и никой няма право да се подиграва на отговорите на другите.

Обобщение:

„Краткият и ясен отказ е достатъчен. Не сме длъжни да убеждаваме другия дълго, когато става дума за лични граници.“



Инструмент 33: Изработване на лична стратегия при натиск и изнудване



Цел: всеки участник да формулира личен план за действие при натиск за интимна снимка, разпространение на съдържание или сексторшън.



Времетраене: 8-10 минути

Водещият раздава листове или моли участниците да напишат в тетрадките си:

„Моят план, ако някой ме притиска или изнудва онлайн“

Участниците попълват следните изречения:

1. Ако някой ми поиска интимна снимка, аз ще...
2. Ако някой продължи да настоява, аз ще...
3. Ако вече съм изпратил/а снимка и ме е страх, аз ще...
4. Ако някой ме заплаши, че ще разпространи снимка, аз няма да...
5. Първият възрастен, към когото мога да се обърна, е...
6. Мога да потърся помощ и от...
7. Най-важното, което искам да запомня, е...

Водещият може да даде примерни попълвания:

- „ще кажа не“;
- „ще спра разговора“;
- „ще направя скрийншот“;
- „няма да плащам“;
- „няма да пращам още“;
- „ще кажа на родител/учител/психолог/медиатор“;
- „ще се свържа с 124 123 или www.safenet.bg“.

Участниците не са длъжни да споделят личните си отговори. Водещият може да покани желаещи да споделят само общи идеи.

Обобщение:

„Когато имаме план предварително, е по-лесно да реагираме спокойно в трудна ситуация.“



Инструмент 34: Брейнсторминг - Изкуствен интелект

Поканете участниците да помислят за 2 минути за всичко, което свързвате с изкуствения интелект и използвате в ежедневието си – приложения, устройства или услуги, които ви улесняват. Споделете примери, когато сте готови!“

Примерни насоки (ако участниците се затруднят):

- Гласови асистенти (Siri, Alexa).
- Препоръки за филми/музика (Netflix, Spotify).
- Навигация (Google Maps).
- Автоматични преводачи (Google Translate).
- Онлайн пазаруване (препоръки в Amazon).



Инструмент 35: Изкуствен интелект в училище „За“ или „Против“



Цел: да се развие критично мислене и аргументация. ИИ има както ползи, така и рискове. Важен е начинът на използване.

Разделете участниците на три групи:

1. Защитници на ИИ;
2. Критици на ИИ;
3. Жури

Поканете участниците да помислят за 2 минути над въпроса

„Трябва ли учениците свободно да използват ИИ за домашни работи?“

Групите имат 5 минути подготовка, след което представят аргументите си по 2-3 минути.

Журито избира най-убедителната позиция.



Инструмент 36: Разпознаване на манипулативни послания



Цел: участниците да разпознават признаци на манипулация, радикализация и реч на омразата.

Разделете участниците на малки групи. Раздайте им листчета зелено, жълто, червено.

Напишете изречения като например:

- „Само ние знаем истината.“
- „Не вярвай на никого извън нашата група.“
- „Те унищожават нашето общество.“
- „Патриотизмът означава да пазиш демокрацията, свободата и достойнството на хората.“

- „Всички медии лъжат, само ние казваме истината.“
- „Ако не си с нас, си срещу нас.“
- „Няма нужда от доказателства – всички знаят, че е така.“
- „Истинските патриоти трябва да действат.“
- „Сподели това веднага, преди да го изтрият.“
- „Тези хора са виновни за всички проблеми в държавата. Трябва да бъдат изолирани и изключени от обществото.“
- „Нека проверим информацията от няколко източника.“

Помолете участниците да маркират съдържанието с:

-  Безопасно съдържание
-  Съмнително съдържание
-  Червен флаг за манипулация или радикализация

Дискутирайте аргументите: Какво ги накара да изберат този цвят?

Кои думи или послания будят съмнение? „Кое от тези послания би било най-трудно да разпознаете като манипулация и защо?“

Радикализацията често започва с манипулативни послания, а не с директни призови към насилие.

Инструмент 37: Работа с помощните центрове на платформите и с техните AI асистенти

 **Цел:** децата да разберат как сами да намират актуални настройки, вместо да запомнят пътища в менюта, които платформите често променят, както и да имат безопасен модел за действие при нужда: търся → проверявам → докладвам/ограничавам/блокирам → казвам на възрастен.

С този инструмент учениците ще могат самостоятелно и безопасно да тестват официалните помощни центрове на социални мрежи, видео платформи и игрови среди, за да намерят как да:

- направят профила си по-поверителен;
- ограничат кой може да им пише, коментира, тагва или вижда местоположението им;
- докладват профил, коментар, публикация, чат, видео или група;
- блокират или ограничат нежелан контакт;
- реагират при фалшив/пробит профил, тормоз, измама или изнудване.

Подходящо за: 5.–12. клас, с адаптиране на казусите според възрастта. Учителят трябва да вземе предвид, че профилите в социалните мрежи не са разрешени под 14-годишна възраст.

По време на упражнението децата не публикуват, не изпращат сигнали по реални случаи и не споделят лични данни. Работи се с търсене в помощните центрове, демонстрационни екрани или предварително подготвени казуси.

Може да представите на учениците следната информация: „Социалните мрежи и игрите често променят бутоните и менютата си. Затова не е необходимо да помним всяка стъпка наизуст. По-важно е да знаем къде да търсим официална помощ и как да зададем ясен въпрос.“

Когато не знаеш как да включиш настройка, да ограничиш контакт, да блокираш човек или да докладваш съдържание, първо отвори официалния помощен център на платформата. Ако платформата предлага AI помощник за поддръжка, можеш да го използваш, за да намериш точните стъпки. AI помощниците стават все по-добри и работят добре и на български език. Никога не въвеждай в AI чат пароли, кодове за вход, адрес, телефон, лични документи, интимни снимки, снимки на други хора или детайли, по които може да бъдеш разпознат/а.“

В таблицата по-долу са посочени линковете, които децата могат да тестват.

Платформа	Официален Help Center	AI помощник / как да се използва	Примерни въпроси
Facebook	https://www.facebook.com/help/	https://www.facebook.com/help/994963392422769	„Как да докладвам фалшив профил?“, „Как да блокирам човек?“, „Как да скрия публикациите си от непознати?“
Instagram	https://help.instagram.com/	https://help.instagram.com/2045270819367334/	„Как да направя профила си частен?“, „Как да ограничавам коментари?“, „Как да докладвам тормоз?“, „Как да премахна таг?“
Messenger	https://www.facebook.com/help/messenger-app/	https://www.facebook.com/help/messenger-app/671966618200379	„Как да блокирам или ограничавам човек?“, „Как да докладвам съобщение?“, „Как да спра непознати да ми пишат?“
Snapchat	https://help.snapchat.com/hc/en-us - позволява директно използване на български език	https://help.snapchat.com/hc/en-us/p/ai-search	„Как да включа Ghost Mode?“, „Как да блокирам човек?“, „Как да докладвам Снар или чат?“, „Кой може да ми пише?“
TikTok	https://www.tiktok.com/support	Няма публично потвърден универсален AI чат за потребителска поддръжка. Използват се търсачката в Support Center и „Report a problem“ в приложението.	„Как да докладвам видео?“, „Как да докладвам профил?“, „Как да направя профила частен?“, „Как да ограничавам коментарите?“

Платформа	Официален Help Center	AI помощник / как да се използва	Примерни въпроси
YouTube	https://support.google.com/youtube/	„Ask YouTube“ е AI функция за въпроси за видео, което в момента потребителят гледа. Функцията не е за поддръжка и сигнали. За безопасност, блокиране и докладване се използва Help Center.	„Как да докладвам видео?“, „Как да докладвам коментар?“, „Как да блокирам канал?“, „Как да подам сигнал за вредно съдържание?“
Discord	https://support.discord.com/hc/en-us - Официалният помощен център е на английски. Учениците могат да използват вграден превод в браузъра, но трябва да проверяват, че са на официалния адрес support.discord.com .	Деца трябва да се обръщат само към официалния Help Center и да не разчитат на неофициални Discord AI ботове.	How to block a user How to report a message How to report a server How to disable direct messages How to stay safe on Discord
Roblox	https://www.roblox.com/support	Деца трябва да използват официалната поддръжка и настройките в самата платформа. Към момента не се препоръчват външни/непотвърдени AI чатове.	„Как да докладвам играч?“, „Как да блокирам играч?“, „Как да настроя родителски контрол?“, „Как да защита профила си?“

Важно за възрастта:

Повечето социални мрежи и чат приложения, включително Facebook, Instagram, TikTok, Snapchat, WhatsApp и YouTube с личен профил, изискват потребителят да е поне на 13 години. Discord изисква потребителите в България да са поне на 14 години. Roblox допуска по-малки деца, но трябва да се използва с подходящи възрастови и родителски настройки. В учебна среда не е необходимо учениците да влизат в лични акаунти — могат да работят с официалните помощни центрове и примерни казуси.

УЧАСТНИК НЕ ЖЕЛАЕ ДА УЧАСТВА В ПРЕДЛОЖЕНАТА ДЕЙНОСТ?

Това е напълно възможна и естествена реакция. Някои дейности изискват споделяне на мисли и емоции по чувствителни теми и не всеки участник е готов да го направи. Не бива да се използва принуда. Важно е участникът да знае, че има право да не споделя и че, ако реши да се включи по-късно, ще получи необходимото пространство и подкрепа. Дори самото наблюдение на останалите може да бъде полезно и да насърчи участника да се включи в следваща дейност.

ДИСКУСИЯТА СЕ ОТКЛОНЯВА ОТ ТЕМАТА?

Водещият може спокойно да върне фокуса към основната тема чрез насочващ въпрос, подходящ пример или кратка задача. Ако отклонението е свързано с важен въпрос за участниците, то може да бъде отбелязано и обсъдено в подходящ момент или оставено за допълнителна дискусия.

В ХОДА НА УРОКА ВЪЗНИКВАТ СПОРОВЕ, ОБИДИ ИЛИ ВЕРБАЛНА АГРЕСИЯ?

Водещият трябва спокойно да прекрати обидите и агресивното поведение и да напомни за правилата на уважително общуване. В зависимост от ситуацията възникналият конфликт може да бъде използван като основа за дискусия и рефлексия – например как се чувстват участниците, какво е довело до конфликта и какви други начини за реакция са възможни.

Полезен подход е и смяната на перспективата – участниците могат да бъдат поканени да разгледат ситуацията от гледната точка на другия човек или да влязат в различна роля.

КЛАСЪТ СТАВА МНОГО ШУМЕН И ВСИЧКИ ГОВОРЯТ ЕДНОВРЕМЕННО?

Водещият може да използва предварително договорени сигнали и техники за привличане и задържане на вниманието. Например може да се използва предмет като символичен „микрофон“, като говори само участникът, който го държи. Друг вариант е предварително договорен сигнал – вдигане на ръка, пляскане с ръце или кратък звук, който означава, че всички спират разговора и насочват вниманието си към водещия.

КЛАСЪТ ГУБИ ИНТЕРЕС КЪМ ТЕМАТА И УЧАСТНИЦИТЕ СТАВАТ ОТЕГЧЕНИ ИЛИ НЕТЪРПЕЛИВИ?

Водещият може да направи кратка пауза или да включи кратка игра за раздвижване и възстановяване на вниманието. Може също да използва интересен факт, реална история, психологически експеримент или актуален пример, свързан с темата.

Подходящ е и методът на провокацията – въпрос, твърдение или кратка задача, които предизвикват участниците да заемат позиция, да изразят мнение или да направят избор.

ЧАСТ ОТ УЧАСТНИЦИТЕ ИСКАТ ПО-БЛИЗЪК КОНТАКТ С ВОДЕЩИЯ ИЛИ ПО-АКТИВНО УЧАСТИЕ?

Желанието за по-активно включване може да бъде насърчено чрез даване на подходящи роли – например наблюдател, говорител, помощник при раздаването на материали или записването на идеи.

Важно е водещият да спазва ясни професионални граници и да избягва близък физически контакт или поведение, което може да бъде възприето като специално отношение към конкретен участник. Това е важно както от гледна точка на етичните стандарти за работа с деца, така и за запазване на безопасна и професионална среда.

При силен интерес към темата водещият може да предложи допълнително занятие или да насочи участниците към подходящи курсове, обучения, книги и онлайн ресурси. При необходимост от подкрепа за разработване на допълнителни занятия по темите за дигиталната и медийната грамотност може да бъде потърсен Националният център за безопасен интернет.

КЛАСЪТ ИЛИ ОТДЕЛНИ УЧАСТНИЦИ ПРОВОКИРАТ ВОДЕЩИЯ?

Провокациите са възможни, особено при чувствителни теми. Водещият е добре да запази спокойствие и да не влиза в личен конфликт с участниците. Лични или обидни коментари, свързани с външен вид, пол, сексуалност или други лични характеристики, не е необходимо да бъдат обсъждани. Водещият може спокойно да покаже, че е чул коментара, но да постави граница и да върне разговора към темата.

Когато е подходящо, провокацията може да бъде превърната в повод за дискусия – например да се обсъди защо определено твърдение предизвиква реакция или как бихме могли да отговорим на него по конструктивен начин. Спокойният тон, чувството за хумор и уважителната реакция често помагат за разреждане на напрежението.

КЛАСЪТ СЕ ПРИТЕСНЯВА ДА ГОВОРИ ИЛИ СЕ СМУЩАВА ОТ ТЕМАТА?

Това е нормална реакция, особено когато темата е чувствителна и участниците не са свикнали да разговарят открито по нея. Водещият трябва да създаде спокойна и безопасна атмосфера и да напомни, че всеки има право на собствено мнение и че не е необходимо да споделя лична информация.

Подходящо е да се използват по-непреки и интерактивни дейности, които постепенно да насърчат участието. Водещият може да задава отворени въпроси, да приема различни гледни точки и да помага на учениците да формулират своите мисли и чувства.

УЧАСТНИК СПОДЕЛЯ ЛИЧНО ПРЕЖИВЯВАНЕ ИЛИ РЕАГИРА СИЛНО ЕМОЦИОНАЛНО?

При споделяне на лично преживяване водещият трябва да реагира спокойно и без оценка. Необходимо е да се избягва както омаловажаването на преживяното, така и насърчаването на участника да споделя повече лични подробности пред групата.

Водещият може да попита участника как се чувства и от каква подкрепа има нужда. Ако е необходимо, може да предложи разговор след занятието и да го насочи към училищния психолог, педагогическия съветник или друг доверен възрастен.

Ако споделената информация се отнася до насилие, сексуална експлоатация, заплахата или друг сериозен риск, водещият трябва да следва установените процедури за защита и да потърси съдействие от компетентните специалисти и институции. Важно е младежът да не бъде оставян сам с проблема и да получи необходимата подкрепа.

КАК ДА РАЗБЕРЕТЕ, ЧЕ УСТРОЙСТВОТО ВИ МОЖЕ ДА Е КОМПРОМЕТИРАНО?

Зловредният софтуер може да засегне компютри, телефони и други дигитални устройства. Той може да краде информация, да променя настройки, да използва ресурсите на устройството или да позволява неоторизиран достъп.

Не всеки необичаен проблем означава, че устройството е заразено, но някои признаци могат да са сигнал, че е необходима проверка.

ПРИЗНАЦИ ПРИ КОМПЮТЪР

1. Компютърът се рестартира сам

Ако компютърът се рестартира без предупреждение и това не е свързано с инсталиране на актуализация, причината може да е технически проблем или зловреден софтуер. Ако това се случва многократно, устройството трябва да бъде проверено.

2. Твърдият диск работи необичайно активно - „бръмчи“

При изпълнение на тежки задачи е нормално компютърът да използва повече ресурси. Ако обаче твърдият диск работи постоянно и необичайно активно дори при прости дейности, това може да е знак за програма, която работи във фонов режим.

3. Компютърът е значително по-бавен

Зловредният софтуер може да използва процесора, паметта и други ресурси на устройството. Ако компютърът внезапно започне да работи много по-бавно без видима причина, е добре да бъде проверен.

4. Програмите се стартират или затварят сами

Ако приложения или програми започнат да се отварят, затварят или държат по необичаен начин без действие от ваша страна, това може да е сигнал за проблем със сигурността.

5. Курсорът на мишката се движи сам

Самостоятелното движение на курсора може да има различни причини, но ако се случва без ваше действие, особено заедно с други необичайни признаци, е необходимо устройството да бъде проверено.

6. Появяват се необичайни изскачащи прозорци

Чести или странни изскачащи прозорци, фалшиви предупреждения за вируси и предложения за инсталиране на непознати програми могат да са свързани със зловреден или рекламен софтуер.

7. Променя се началната страница на браузъра

Ако началната страница или търсачката на браузъра се променят без ваше действие, това може да е знак, че нежелана програма е променила настройките. Понякога това се използва за пренасочване към фалшиви или опасни сайтове.

8. Софтуерът за сигурност е изключен

Ако антивирусната програма или друга защита на устройството е изключена, без вие да сте го направили, това е причина за внимание. Някои видове зловреден софтуер се опитват да деактивират защитните инструменти.

9. От профила ви се изпращат съобщения, които не сте изпращали

Проверявайте периодично изпратените съобщения и активността на своите профили. Ако откриете имейли или други съобщения, които не сте изпращали, е възможно профилът или устройството ви да са компрометирани.

10. Батерията се изтощава необичайно бързо

Необичайно бързото изтощаване на батерията може да има много причини. Една от тях е програма, която работи постоянно във фонов режим и използва ресурсите на устройството.

11. Устройството често замръзва или се срива

Неочакваното блокиране, забавяне или срив на системата може да е резултат от технически проблем, но понякога е свързано и със зловреден софтуер. Ако тези проблеми се появяват често и без видима причина, устройството трябва да бъде проверено.

12. Необяснимо намалява свободното пространство

Ако свободното пространство на устройството внезапно намалее без да сте добавяли големи файлове или приложения, причината може да е нежелан или зловреден софтуер.

ПРИЗНАЦИ ПРИ ТЕЛЕФОНИ С ANDROID

Самата операционна система Android не представлява заплаха за сигурността. Както при всяка дигитална платформа обаче, устройствата с Android могат да бъдат засегнати от зловреден софтуер. Рискът се увеличава при инсталиране на приложения от непознати източници, използване на остаряла версия на операционната система или посещаване на опасни сайтове.

Сред по-честите сигнали са:

1. Необичайно високо използване на мобилни данни

Зловредният софтуер често работи във фонов режим. Ако потреблението на мобилни данни внезапно се увеличи без видима причина, е възможно приложение да работи активно във фонов режим.

2. Появяват се приложения, които не сте инсталирали

Ако на телефона се появи непознато приложение, което не сте изтегляли сами, не го отваряйте, преди да проверите какво представлява. Някои зловредни приложения могат да получат достъп до лични данни, съобщения или други ресурси на устройството.

3. Появяват се непознати реклами и изскачащи прозорци

Ако започнете да виждате необичайно много реклами или изскачащи прозорци, особено когато не използвате конкретно приложение, това може да е знак за рекламен или друг нежелан софтуер.

4. Телефонът работи по-бавно от обичайното

Внезапното забавяне на телефона може да има различни причини, включително недостатъчно свободно пространство или остарял софтуер. В някои случаи обаче то може да бъде свързано и със зловреден софтуер.

Какво да направите, ако подозирате зловреден софтуер?

- Не игнорирайте проблема, особено ако се появяват няколко от описаните признаци едновременно.
- Не отваряйте подозрителни файлове и линкове и не инсталирайте непознати приложения.
- Проверете устройството със софтуер за сигурност от надежден източник.
- Деинсталирайте подозрителни приложения, ако знаете, че не сте ги инсталирали или не ги използвате.
- Актуализирайте операционната система и приложенията до последните налични версии.
- Проверете профилите си за необичайна активност и при необходимост сменете паролите си.
- Ако проблемът продължава, потърсете помощ от родител, учител, специалист или друг доверен възрастен.

В някои случаи може да се наложи възстановяване на фабричните настройки на устройството. Това трябва да бъде крайна мярка и да се предприема след архивиране на важната информация и, когато е възможно, след консултация със специалист.

Настоящият наръчник е предназначен за деца и младежи от 5. до 12. клас – възраст, която до голяма степен обхваща периода на юношеството. Това е важен етап от развитието, свързан с прехода от детството към зрелостта и с множество биологични, психологически и социални промени.

Основните задачи на юношеството са свързани с изграждането на собствена идентичност, постепенното придобиване на независимост и създаването на значими отношения с другите. През този период младият човек започва все по-активно да търси отговори на въпросите „Кой съм аз?“, „Какво е важно за мен?“ и „Какво е моето място сред другите?“. Тези процеси се развиват на фона на бързи промени в тялото, емоциите, начина на мислене и взаимоотношенията с околните.

Юношеството често се свързва с противопоставяне на авторитетите, промени в настроението, експериментирание, силна потребност от приемане от връстниците и стремеж към самостоятелност. Тези прояви обаче не бива да се възприемат единствено като проблемно поведение. В повечето случаи те са част от естествения процес на израстване и опознаване на себе си.

Особено важна през този период е връзката с връстниците. Младите хора търсят приемане, близост, доверие и разбиране и чрез общуването с другите изпробват различни роли и поведения. Те се срещат с различни гледни точки, формират свои убеждения и ценности и развиват умения за разбиране и съпричастност. Приемането от групата има важно значение за самочувствието и психичното благополучие, поради което начинът, по който младият човек се възприема и представя пред другите, често е особено значим.

През юношеството се променя и начинът на мислене. Младите хора постепенно развиват по-добра способност да мислят абстрактно, да разглеждат различни възможности, да правят хипотези и да анализират ситуации от различни гледни точки. Това им позволява да разсъждават по-задълбочено за себе си, другите и света.

В същото време способността за вземане на решения все още се развива. Юношите могат да бъдат по-импулсивни, да подценяват определени рискове или да не предвиждат всички възможни последствия от своите действия. Това е свързано и с факта, че мозъкът продължава да съзрява през юношеството, включително областите, свързани с планирането, самоконтрола и оценката на риска. Затова подкрепата от страна на възрастните е важна, но тя трябва да бъде основана на доверие и диалог, а не на назидание и морализиране.

ЮНОШЕСТВОТО В ДИГИТАЛНИЯ СВЯТ

Интернет и дигиталните технологии добавят ново измерение към развитието на младия човек. Днес юношите изграждат не само своята идентичност в реалния свят, но и своя дигитален образ – начина, по който се представят и възприемат онлайн.

Дигиталната среда има много положителни страни. Тя улеснява общуването с приятели, дава възможност за създаване на общности със сходни интереси, предоставя достъп до знания и информация и позволява на младите хора да изразяват своите идеи и творчество.

В същото време онлайн пространството може да засили някои от предизвикателствата на юношеството. Социалните мрежи предлагат множество модели за подражание, които невинаги са реалистични или позитивни. Външният вид, популярността, броят последователи и начинът, по който човек се представя пред другите, могат да се превърнат в източник на натиск и несигурност.

В интернет младите хора могат по-лесно да експериментират с начина, по който се представят, включително да създават различни версии на себе си. Това може да бъде възможност за себеизразяване, но понякога може да затрудни изграждането на устойчиво усещане за собствената идентичност. Затова е важно младите хора да развиват умения за критично мислене, позитивно себеизразяване, общуване и разпознаване на рисковете онлайн.

Целта на дигиталната безопасност не е младите хора да бъдат ограничавани или изолирани от интернет. По-важно е те да могат да използват неговите възможности уверено, критично и отговорно, като същевременно разпознават рисковете и знаят как да се защитят и към кого да се обърнат за помощ.

Именно затова настоящият наръчник съчетава темите за онлайн безопасността с развитието на социални и личностни умения. Умението да общуваме, да поставяме граници, да разпознаваме манипулация, да мислим критично и да уважаваме другите е също толкова важно за безопасността онлайн, колкото и познаването на техническите настройки за сигурност.

УЧЕНЕ ЧРЕЗ ОБЩУВАНЕ И ОПИТ

В юношеска възраст връстниците са важен източник на знания, подкрепа и обратна връзка. Обмяната на опит позволява на младите хора да чуят различни гледни точки, да сравнят собствените си преживявания с тези на другите и да търсят заедно решения.

Затова заниманията в настоящия наръчник са в голяма степен основани на групова работа, дискусии и активно участие. Те дават възможност на учениците не само да получат информация, но и да споделят собствен опит, да задават въпроси, да обсъждат реални ситуации и да се учат един от друг.

Този подход цели да подкрепи младите хора да се ориентират по-уверено в дигиталния свят – да се възползват от неговите възможности, да разпознават рисковете и да изграждат устойчиво усещане за това кои са, какво е важно за тях и как искат да присъстват както онлайн, така и офлайн.

Настоящото методическо ръководство е разработено като част от дейностите по проект „Дигитални деца 2“, финансиран по Програма „Дигитална Европа“ на Европейската изпълнителна агенция за здравеопазването и цифровизацията (HaDEA).

Националният център за безопасен интернет се представлява от консорциум от организации - Асоциация Родители, Българската асоциация по семейно планиране и сексуално здраве (БАСП) и Национална мрежа за децата (НМД).

НАЦИОНАЛНИЯ ЦЕНТЪР ЗА БЕЗОПАСЕН ИНТЕРНЕТ (НЦБИ)

НЦБИ (осн. 2005 г.) работи в подкрепа на сигурността и овластяването на децата онлайн вече над 20 години. Поддържа две важни услуги – Горещата линия за докладване на незаконно онлайн съдържание и Консултативната линия за онлайн безопасност за деца. 124 123 е телефонът, на който деца, родители и учители могат да потърсят помощ, информация и да подадат сигнал при онлайн проблем с дете. Освен по телефона, и родителите, и учителите, и самите деца могат да потърсят помощ и чрез чата на Консултативната линия на адрес [safenet.bg](https://www.safenet.bg).

Като единствена организация, защитаваща децата в онлайн пространството, Центърът вярва, че най-добрата превенция е развиването на техните цифрови умения и на медийната и информационната им грамотност, с което се изгражда тяхната устойчивост, увереност и способност да разпознават както рисковете, така и възможностите.

Уебсайт: www.safenet.bg

Facebook: <https://www.facebook.com/SafenetBG>

Instagram: <https://www.instagram.com/safenet.bg>

За контакт: info@safenet.bg; Иглика Иванова, iglika.ivanova@safenet.bg

АСОЦИАЦИЯ „РОДИТЕЛИ“

Асоциация „Родители“ е създадена през 2001 г. като неправителствена организация за осъществяване на общественополезна дейност. Основна мисия на организацията е гарантиране правото на всяко дете до равен достъп до съвременно и качествено образование. Голяма част от дейностите са с фокус върху образованието и доброто взаимодействие между училището, детската градина, яслата и родителя.

Асоциация Родители е член на Алианса за ранно детско развитие; работни групи към Националния съвет за закрила на детето; Консултативния съвет за безопасен интернет; Национална мрежа за децата и MenEngage Europe.

Уебсайт: www.roditeli.org

Facebook: <https://www.facebook.com/AsociaciaRoditeli>

За контакт: Яна Алексиева, office@roditeli.org

БЪЛГАРСКА АСОЦИАЦИЯ ПО СЕМЕЙНО ПЛАНИРАНЕ И СЕКСУАЛНО ЗДРАВЕ (БАСП)

БАСП е основана през 1992 г. Основните цели на организацията са насочени към насърчаване и предоставяне на адекватни услуги в областта на репродуктивното здраве, осигуряване на достъп до информация по различни аспекти на здравната превенция и сексуалното здраве, както и застъпничество за развитието на ефективни здравни политики и услуги, с особен фокус върху уязвимите групи.

БАСП има дългогодишен опит в работата с деца и млади хора и в разработването и реализирането на образователни инициативи, насочени към здравето, правата, личната безопасност и развитието на умения за вземане на информирани и отговорни решения. В работата си с младежи организацията прилага методи на неформалното образование, интерактивни подходи и активно участие на младите хора, като поставя специален акцент върху включването на уязвими групи и осигуряването на равен достъп до информация, образование и подкрепа. БАСП има свои центрове в София, Русе, Стара Загора и Плевен.

Уебсайт: www.bfpa.bg

Facebook: www.facebook.com/basp.bfpa

За контакт: Павлина Филипова, pfilipova@bfpa.bg

НАЦИОНАЛНА МРЕЖА ЗА ДЕЦАТА (НМД)

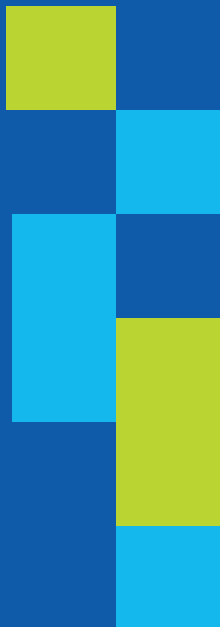
Национална мрежа за децата е най-голямото у нас обединение на близо 140 граждански организации и активисти, които работят в полза на децата и семействата в България. Ежегодно 10 000 професионалисти от организациите в Мрежата подкрепят над 150 000 деца и 20 000 семейства.

Уебсайт: <https://nmd.bg>

Facebook: <https://www.facebook.com/nmdbg>

LinkedIn: <https://www.linkedin.com/company/nmdbg>

За контакт: Георги Еленков georgi.elenkov@nmd.bg



Обади се на **124 123**
или пиши в чата на safenet.bg.

Безопасна, безплатна и поверителна услуга
в подкрепа на деца и младежи.