РП2 – ПРИШИЛА – ЕДУКАТИВНА ПРОГРАМА ЗА МЛАДИ СО ИНТЕЛЕКТУАЛНА ПОПРЕЧЕНОСТ

МОДУЛ 3: ПОТЕНЦИЈАЛНИ РИЗИЦИ ПРИ КОРИСТЕЊЕ НА СОЦИЈАЛНИ МРЕЖИ

Автор на документот: ИНТРАС

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

ПРИШИЛА–ЕДУКАТИВНА ПРОГРАМА ЗА МЛАДИ СО ИНТЕЛЕКТУАЛНА ПОПРЕЧЕНОСТ

Модул 3: Потенцијални ризици при користење на социјалните мрежи

Преглед на модулот	Во овој модул, ќе научите за ризиците кои можат да се појават при користењето на социјалните мрежи. Овие ризици вклучуваат **онлајн малтретирање** (сајбер-булинг), кога луѓето се однесуваат злобно кон вас во дигитални средини), **намамување** (груминг)–кога возрасна личност се претставува како некој на ваша возраст и ве измамува да споделувате слики или да се вклучите во интимни активности) и **лажно претставување** (фишинг) –кога некој се обидува да го украде вашиот идентитет или лозинки. Ќе научите и како да ги препознаете овие ризици и како да останете безбедни додека користите социјални медиуми. Ризици можат да се појават и во онлајн игри. Во видео игрите, луѓето можат да разговараат со вас и понекогаш да побараат лични информации или да кажат несоодветни работи. Истите правила за безбедност важат и тука.
Цели на модулот	До крајот на овој модул вие ќе можете: • Да разберете што е сајбер-булинг, груминг и фишинг на социјалните мрежи. • Да ги препознаете ситуациите во кои вакви ризици можат да се случат. • Да примените совети и соодветни постапки за да ги избегнете овие ризици.
Применети едукативни принципи	Овој модул е дизајниран за да ви помогне во: • Преземање на позитивни ризици преку безбедно користење на социјалните мрежи. • Чувството дека вие ја имате контролата за вашите дејствија онлајн. • Да ја зајакнете вашата независност при користењето на социјалните мрежи. • Да донесувате безбедни одлуки со самодоверба.

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

Содржина на модулот

Во претходните модули, научивме дека социјалните мрежи се свет полн со можности. Тоа е место каде можеме да дознаеме интересни информации, да ги споделиме нашите размислувања и чувства на различни теми и да се поврземе со луѓе кои ги делат нашите интереси.
Сепак, важно е да се запамети дека виртуелниот свет исто така носи одредени ризици. За безбедно да ги користиме социјалните мрежи, потребно е да ги осознаеме овие ризици и да научиме како да се заштитиме од нив. На овој начин, можеме да ги ползуваме нашите онлајн искуства и притоа да останеме безбедни.

Ајде да ги разгледаме најчестите ризици: онлајн малтретирање, намамување и лажно претставување.

Што е онлајн малтретирање или сајбер-булинг?

Онлајн малтретирањето се случува кога луѓето користат социјални мрежи или онлајн платформи за да испраќаат непристојни пораки, да објавуваат несоодветни навредливи коментари или да шират гласини. Сајбер-насилниците најчесто се кријат преку лажни профили.

Примери на онлајн малтретирање:

- Некој коментира на твојата слика: "Изгледаш многу чудно, никој не те сака."
- Група на луѓе ти испраќаат навредливи пораки во групен разговор и прават да се чувствуваш исклучено или вознемирено. Пример: "Ајде да ја игнорираме и да не дозволиме повеќе да биде дел од нашата група."
- Некој ти испраќа приватна порака која гласи: "Многу си глупав. Прекини да објавуваш онлајн."

Практични совети за да се избегнеш онлајн малтретирање

1. **Не одговарај.** Доколку некој ти испраќа злобни и омаловажувачки пораки, немој да одговараш на нив.
2. **Сочувај ги доказите.** Зачувај екрански слики на кои се гледаат злобните пораки или коментари за да можеш да ги покажеш на возрасен на кого му веруваш.
3. **Блокирај и пријавувај.** Користи ги алатките што ти се на располагање на платформата за да го блокираш насилникот и да го пријавиш неговото однесување.

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

4. **Зборувај со некој на кому му веруваш.** Сподели ги своите чувства со родител, учител или пријател.
5. **Биди љубезен онлајн**. Однесувај се кон другите со почит за да креираш позитивна онлајн средина.

Што е намамување или груминг?

Намамување се случува кога некој од возрасните го искористува интернетот со цел да заведе и манипулира млада личност да сподели свои лични информации , да испрати приватни фотографии, или да се впушти во небезбедни практики. Намамувачите често се претставуваат како ваши пријатели, како индивидуи на ваша возраст или како некој што ве разбира, со цел да ја придобијат вашата доверба.

Примери за намамување:

1. Онлајн профил ви испраќа пријателски пораки и комплименти, но истовремено поставува лични прашања од типот на "Каде живееш?" или "Можеш да ми испратиш слика од себе?"
2. Некој ви пишува: "Многу ми се допаѓа твојот изглед. Ти си прекрасен/а. Мојот вујко е сопственик на агенција за модели и ние можеме да те направиме славен/а доколку ми испратиш неколку фотографии од себе."

Практични совети за да избегнете груминг

1. **Не споделувајте лични информации.** Никогаш не ја споделувај својата адреса, телефонски број, име на вашето училиште, или лозинки.

2. **Биди внимателен со фотографии.** Не испраќај фотографии на некој што не го познаваш.

3. **Верувај му на твоите чувства.** Доколку некои личности онлајн прават да се чувствуваш непријатно, прекини да зборуваш со нив.

4. **Зборувај со возрасен на кому му веруваш.** Доколку се чувствуваш неодлучно во однос на некој контакт

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

онлајн, сподели го тоа со родител, учител, или старател.

5. **Блокирај и пријавувај.** Употреби ги можностите за нагодување на платформата што ја користиш за да ги блокираш профилите и да го пријавиш нивното однесување.

Што е лажно претставување или фишинг?

Фишинг е кога некој се претставува како личност од доверба или компанија, со цел да ги украде твоите информации како лозинка, податоци за твојата банковна сметка, или пари. Ваквите измамници често користат лажни е-пошти, пораки на социјалните медиуми, или веб страници за да те измамат.

Примери за фишинг:

- Добиваш е-пошта која изгледа како да е испратена од твојата банка, и гласи "Се појави проблем со твојата банковна сметка. Ве молиме притиснете тука за да се логирате."
- Добивате порака која гласи: "Вие добивте награда! Кликнете тука за да преземете."

Практични совети за да избегнете фишинг

1. **Не отворајте непознати линкови.** Ако добиете порака или е-пошта од некој на кого не му верувате, игнорирајте ја и не кликајте на линковите што ги содржи.
2. **Проверете го испраќачот.** Внимателно погледнете ја е-поштата или корисничкото име на испраќачот. Лажните пораки често имаат мали правописни грешки.
3. **Зачувајте ја безбедноста на вашите лозинки.** Никогаш не споделувајте ги вашите лозинки со никого.

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

4. **Бидете внимателни со награди.** Ако некој ви каже дека сте освоиле нешто, но никаде не сте се пријавиле за награда, и објавата изгледа чудно или премногу добро за да биде вистинито, веројатно е измама.

5. **Користете безбедни веб-страници.** Осигурете се дека името на веб-страницата започнува со „https://“ и прикажува симбол на катанец.

Анализа на случаи

Вовед

Објаснете им на учесниците дека тие ќе слушнат и прочитаат три различни приказни од кои секоја ќе раскажува за ситуација што се случила онлајн. Овие приказни се креирани со цел да им се помогне на младите луѓе да ги сфатат некои од ризиците со кои можат да се соочат додека ги користат социјалните мрежи и интернетот.

По читањето на секоја приказна, фасилитаторот води дискусија со учесниците преку поставување на специфични прашања. Овие прашања имаат за цел да ги поттикнат учесниците да размислуваат на тема како најдобро и најбезбедно да се однесуваат во вакви ситуации.

Целта на оваа активност е да им се помогне на младите да ги препознаат опасностите онлајн и да развијат стратегии за да се заштитат себе.

Анализа на случај 1

Случајот на Луција

Луција е 19 годишна девојка која сака да црта. Таа често ги споделува своите уметнички творби на социјалните медиуми. Еден ден, некој од профилите што ја следат на социјалните мрежи и испрати порака што гласи: “Здраво!, Ги обожавам твоите цртежи. Многу си талентирана! Може да бидеме пријатели?” Луција се чувствува среќно и одговара: “Фала ти! Секако!.” По неколку дена, личноста почнува да комуницира со Луција поставувајќи лични прашања од типот

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

на: “Каде живееш?” и “Дали можеш да ми испратиш слика од тебе?” Личноста исто така и напоменува на Луција: “Не кажувај никому за нашиот разговор—тоа ќе биде наша тајна.”

1. Што може да се случи ако Луција сподели лични информации со некој што не го познава онлајн?

а) Личноста може да ги употреби овие информации за да ја измами или повреди Луција.

б) Тие можат да станат најдобри пријатели.

в) Ништо; Споделувањето на лични информации е секогаш добра идеја.

2. Како треба Луција да постапи кога личноста бара од неа да и испрати слика од себе?

а) Да ја испрати за кратко време за да биде љубезна.

б) Да рече не и да го блокира профилот.

в) Да ја праша личноста за која намена и треба нејзината слика.

3. Доколку Луција не е сигурна како треба да постапи во оваа ситуација, кој е најдобриот чекор што може да го преземи?

а) Да зборува за пораките со возрасен на кому му верува.

б) Да ги игнорира сопствените чувства и да продолжи да пишува со личноста.

в) Да ги запраша нејзините пријатели дали е добро да го направи тоа што го бара личноста.

Анализа на случај 2

Случајот на Лука

Лука споделува смешна слика од себе на социјалните медиуми. Некој коментира: “Изгледаш многу глупаво!”

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

Веднаш други личности се вклучуваат, почнуваат да се смејат и да пишуваат навредувачки коментари за него. Лука се чувствува многу вознемирено и не знае што да прави. Тој се запрашува дали треба да го избрише својот профил или со лутина да возврати на коментарите.

1. **Кој треба да биде првиот чекор на Лука во однос на злобните коментари?**

а) Да ги игнорира коментарите и да направи слики од екранот за доказ.

б) Да возврати на коментарите со иста мерка, да напише злобни работи за секој што го навреди.

в) Веднаш да си а си го избрише профилот.

2. **Со кој треба Лука да зборува ако се чувствува повреден од коментарите?**

а) Возрасен на кого му верува, учител, родител, или старател.

б) Со оние што ги објавија коментарите

в) Никого, се што има да каже треба да си го чува за себе.

3. **Кој е најдобриот начин за Лука да се справи со онлајн насилство во иднина?**

а) Да избегнува споделување на било што во иднина.

б) Да ги блокира и пријави луѓето кои се однесуваа злобно кон него онлајн.

в) Да напише долга објава која објаснува колку повредено се почувствувал.

Анализа на случај 3

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

PR.I.S.C.I.LLA

Случајот на Ана

Ана добива е-пошта што изгледа како да поаѓа од нејзината омилена онлајн продавница. На пораката пишува: "Честитки! Добивте 50 € ваучер во форма на картичка-подарок! Кликнете тука за да ја добиете вашата награда." Ана е возбудена, меѓутоа не е сигурна дали понудата е реална. Таа забележува дека адресата на е-поштата изгледа чудно, и дека адресата во линкот не соодветствува со интернет страницата на продавницата.

1. Што треба да направи Ана пред да кликне на линкот?

а) Да провери дали адресата од е-поштата и линкот изгледаат веродостојно и дали соодветствуваат со веб страницата на продавницата.
б) Брзо да кликне додека наградата е достапна.
в) Да одговори на е-поштата со прашања за повеќе детали.

2. Кој е потенцијалниот знак дека оваа е-поштата е лажна?

а) Е-поштата бара лична информација од Ана.
б) Е-поштата е напишана на пријателски начин.
в) Е-поштата го вклучува името на продавницата.

3. Доколку Ана верува дека оваа е-поштата е сомнителна, што треба да направи?

а) Да ја пријави е-поштата како фишинг или лажно претставување и да ја избрише.
б) Да ја препрати е-поштата до нејзините пријатели, за тие да проверат дали е реална.
в) Да ја игнорира е-поштата но да ја задржи во своето поштенско сандаче (инбокс).

Дополнителни материјали

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

Користена литература	
	Активност 1 на модулот
Наслов на активноста	**Препознавање на ризици**
Цели	Во оваа активност ќе вежбате препознавање на потенцијални ризици во различни онлајн ситуации и ќе дискутирате за соодветните акции што треба да ги преземеме за да останеме безбедни.
Методологија	Учење преку практично работење, практични вежби и интерактивни активности.
Времетраење на активноста	30 минути
Потребни материјали	1. Картички со сценарија. 2. Бели листови и пенкала доколку некој сака да си го напише својот одговор.
Инструкции	Во оваа активност, ќе видите слики или ќе слушнете кратки приказни за нешта што може да се случат онлајн. Вашата задача е: 1. Да одлучите дали ситуацијата е ризична или безбедна. 2. Да кажете зошто мислите дека е ризична. 3. Да објасните што би направиле за да останете безбедни. **Примери** Да започнеме со едноставен пример за да ви помогнеме да разберете како функционира активноста: Странец ви испраќа порака со текст: „Ти си супер! Можеме ли да се сретнеме?“ Поставете си прашања: - Дали ова е ризично?

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

- Зошто би можело да биде ризично?
- Што треба да направам во оваа ситуација?

Одговор:

Да, ова е ризична ситуација бидејќи не го познавате лицето. Тоа може да биде некој што се претставува лажно. Треба да ја игнорирате пораката, да ја блокирате личноста или да кажете на некој возрасен од доверба.

Сега, ќе разгледаме различни онлајн ситуации. За секоја од нив размислете внимателно и одговорете на следните прашања:

- Дали е ризично или безбедно?
- Зошто мислите дека е ризично или безбедно?
- Што ќе направите за да останете безбедни?

Сценарио 1:

"Лице од онлајн профил онлајн ви пишува: „Можам да ви помогнам да придобиете многу следбеници ако ми ја испратите вашата лозинка."

Сценарио 2:

"Пријател објавува смешна фотографија од вас без да ве праша за одобрување."

Сценарио 3:

"Некој коментира на вашата објава: „Многу си грд/а, сите те мразат."

Сценарио 4:

"Добивте е-пошта со текст: „Честитки! Освоивте 1 000€! Кликнете овде за да ја подигнете вашата награда."

Сценарио 5:

"Член сте во онлајн групен разговор за вашата омилена видео игра. Некој во прашува: „Кога е твојот роденден? Сакаме да го прославиме со тебе!"

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

Сценарио 6:

"Добивате порака од непознат профил која гласи: „Бараме луѓе за работа од дома. Испратете ни го вашето име, адреса и податоци од вашата банковна сметка за да започнете!"

Сценарио 7:

"Правите групна фотографија со вашите пријатели во парк и сакате да ја објавите на социјалните медиуми. Еден од вашите пријатели вели дека не сака неговата/нејзината слика да биде објавена."

Сценарио 8:

"Непознат профил ви испраќа порака со текст: „Ти си толку супер и убава! Би сакал да разговараме повеќе. Можеш ли да ми кажеш нешто повеќе за себе?"

Едноставни одговори

Одговори за сценарио 1

- Ова е ризично бидејќи тие можат да го користат твојот лозинка за да го преземат твојот профил.
- Никогаш не споделувај ги твоите лозинки со никого. Блокирај ја личноста и пријави ја.

Одговори за сценарио 2

- Ова може да биде ризично бидејќи фотографијата може да те изложи на срам или да сподели приватни информации.
- Треба да го замолиш твојот пријател да ја избрише фотографијата и да му објасниш зошто е важно да се побара дозвола.

Одговори за сценарио 3

- Ова е случај на онлајн малтретирање бидејќи коментарот е лош и може да ти ги повреди чувствата.

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

- Треба да направиш слика од екран, да ја блокираш личноста што тоа го направи и да се довериш кај возрасен на кому му веруваш.

Одговори за сценарио 4

- Ова е ризична ситуација, најверојатно станува збор за лажно претставување–измама која има за цел да ги украде твоите лични информации.
- Треба да ја избришеш пораката и да ја пријавиш како спам. Никогаш не кликај на линкови од слични пораки.

Одговори за сценарио 5

- Ова е ризично бидејќи споделувањето на твојот роденден во јавен разговор може да доведе до крадење идентитетот или непосакувани контакти.
- Треба да избегнуваш да даваш лични детали како целосниот датум на раѓање во јавни простори. Ако некој праша, љубезно кажи дека не споделуваш лични информации онлајн.

Одговори за сценарио 6

- Ова е ризична ситуација бидејќи веројатно е измама дизајнирана да украде твоите лични или финансиски информации.
- Треба да ја избришеш пораката веднаш и да го пријавиш испраќачот. Никогаш не споделувај чувствителни информации како адреса или податоци за банка со луѓе што не ги познаваш.

Одговори за сценарио 7

- Ова е безбедно само ако ги почитуваш желбите на твојот пријател и не ја објавуваш фотографијата. Игнорирањето на нивната молба не би било безбедно или љубезно.
- Треба да бидеш сигурен дека прашуваш секој на фотографијата за дозвола пред да ја објавиш онлајн. Ако некој каже не, избери друга фотографија или не објавувај воопшто.

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

Одговори за сценарио 8

- Ова е ризична ситуација бидејќи непознати кои даваат комплименти може да се обидуваат да те манипулираат или да ја стекнат твојата доверба за небезбедни цели.
- Не треба да одговараш на пораката. Блокирај ја личноста веднаш и кажи на возрасен од доверба што се случило.

Размислувања

По разгледувањето на сценаријата, размислете за она што го научивте.

Запрашајте се:

- Која ризична ситуација ве изненади најмногу?
- Како се чувствувавте кога одлучувавте што да направите во секоја ситуација?
- Што би направите поинаку следниот пат кога ќе бидете онлајн?

Разговарајте со групата или со вашиот учител за вашите одговори. Споделувањето на вашите размислувања може да ви помогне да се почувствувате самоуверено во тоа како да останете безбедни онлајн.

Заклучок

Завршивте одлична работа во препознавање на потенцијалните ризици и размислувањето како да останите безбедни на социјалните мрежи. Запомни:

- ✓ Ако за нешто на социјалните медиуми почувствувате дека не е како што треба, верувајте им на своите емоции.
- ✓ Не споделувајте лични информации лозинки со луѓе кои не ги познавате.
- ✓ Секогаш зборувате со некој на кому му верувате доколку не сте сигурни за некоја ситуација.

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

Име на активноста	**Игра на улоги**
Цели	Вежби за како да реагирате на различни онлајн ризици преку изведување ситуации во мали групи. Оваа активност ќе ви помогне да се почувствувате посамоуверени во тоа што треба да направите ако се соочите со овие ризици во реалниот живот. Ќе научите: ✓ Како да се справите со честите ризици онлајн. ✓ Како да донесете паметна и безбедна одлука кога нешто чувствувате како погрешно. ✓ Како да побарате помош кога ви е потребно.
Методологија	Игра на улоги
Времетраење на активноста	30-40 минути
Потребни материјали	• Картички со сценарија, или печатени листови со сценарија. • Безбедна простор за групирање во мали групи и игра на улоги.
Инструкции	Учесниците ќе работат во мали групи за да одиграат различните сценарија. Секоја група ќе добие сценарио за еден тип на ризична ситуација онлајн. Едно лице ќе биде во улога на лицето што се соочува со овој ризик, а другите ќе имаат различни улоги како пријател, непознатото лице или возрасен од доверба. По реализирањето на сценариото, ќе разговараме за она што се случи и како да се справиме со тоа. **Сценарио 1** **Ситуација**: Некој онлајн вели, „Ти си толку талентиран/а! Може ли да видам повеќе слики од тебе? Ти ветувам дека нема да ги споделам со никого.“ **Улоги:** • Лице од кое се бараат слики. • Непознато лице кое бара слики.

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

- Возрасен или пријател од доверба од кого лицето обично прифаќа совети.

Дејства:

- Одбивање да се испратат слики.
- Блокирање на непознатиот.
- Разговарање со пријателот или возрасниот од доверба за она што се случило.

Сценарио 2

Ситуација: Некој коментира на вашата објава, „Ова е толку глупаво. Зошто се трудиш воопшто?“ Други луѓе почнуваат да го лајкнуваат коментарот и исто така да пишуваат злобни работи.

Улоги:

- Лице кое е малтретирано.
- Насилник.
- Возрасен или пријател на кого лицето се доверува.

Дејства:

- Не одговарајте на злобните коментари.
- Сликајте го екранот како доказ.
- Блокирајте го и пријавете го насилникот.

Сценарио 3

Ситуација: Добивате е-пошта која гласи: „Честитки! Добивте нов телефон! Кликнете на овој линк за да ја потврдите вашата награда.“

Улоги:

- Лице кое ја добива е-поштата.
- Измамникот кој ја испратил е-поштата.
- Пријател или возрасен кој дава совети.

Дејства:

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

- Не кликајте на линкот.
- Избришете ја е-поштата и пријавете ја како спам.
- Разговарајте со возрасниот од доверба ако сте не сигурни.

Дискусија

Откако секоја група ќе го одигра своето сценарио, групирајте се во голема група и дискутирајте:

- Што е тоа што ја прави оваа ситуацијата ризична?
- Што направи лицето за да ја зачува својата безбедност?
- Како се чувствувавте кога ја игравте оваа ситуација?
- Што би направиле ако реално ви се случи ваква ситуација?

Заклучок

Одлично ги одигравте своите улоги во оваа вежба за справување со онлајн ризици! Запомнете:

- Секогаш верувајте во вашиот инстинкт - ако нешто изгледа погрешно, веројатно е.
- Блокирајте и пријавете луѓе кои ви прават да се чувствувате неудобно онлајн.
- Разговарајте со возрасен од доверба доколку не сте сигурни како да постапите.

Активност 3 на модулот	
Име на активноста	**Игра за сортирање на ризици**
Цели	Вежби за препознавање на безбедни и ризични онлајн однесувања преку сортирање на примери во категориите „Безбедно“ или „Ризично“
Методологија на учење	Практични вежби и интерактивни активности

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

Времетраење на активноста	20 минути
Потребни материјали	• Картички со онлајн активности • Два означени простора: "Безбедно" и "Ризично" (на табла или маса).
Инструкции	Ајде да го тестираме она што смее го научиле за онлајн ризиците! Во оваа активност, ќе разгледуваме примери за работи што луѓето можат да ги прават онлајн. Ваша задача е да одлучите за секој од примерите дали е „Безбеден“ или „Ризичен.” Ќе работите во двојки или мали групи. Секоја група ќе добие картички со примери од онлајн активности. Вашата задача е да ги поставите картичките со дејствијата во две категории „Безбедно“ или „Ризично“ на табла или масата. По сортирањето на картите, групно ќе ја продискутираме вашата одлука. Ајде да пробаме еден пример заедно: **Пример картичка со акција:** "Споделување на твоето полно име и адреса на твојот профил." Дали е безбедно или ризично? **Одговор:** Ризично. Споделувањето лични информации може да те направи подложен на измама. Сега си ти на ред! Сортирај ги следниве картички: • “Прифаќање на барање за пријателство од некој што не го познаваш.” • “Објавување фотографија што не содржи никаква друга информација освен како изгледа твојата омилена книга.” • “Кликнување на линк од порака која вели дека си добил награда." • “Блокирање на некој кој ти испраќа лоши пораки”

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

- “Споделување на твојот телефонски број во јавна објава."
- “Добивате барање за пријателство од профил без профилна слика и без објави.“
- Непознато лице ти пишува "Испрати ми ја твојата локација за да се дружиме!"
- "Објавуваш слика од името на твоето училиште на социјалните медиуми."
- "Твој пријател ти кажува дека е малтретиран онлајн и ти го охрабруваш да разговара со возрасен од доверба."

Одговори:

- “Прифаќање на барање за пријателство од некој што не го познаваш.”

Одговор: Ризично. Прифаќањето на барања од луѓе кои не ги познаваш може да биде небезбедно, бидејќи тие можеби не се тоа што тврдат дека се. Осигурете се секогаш дека се поврзувате со луѓе на кои им верувате.

- “Објавување фотографија што не содржи никаква друга информација освен како изгледа твојата омилена книга.”

Одговор: Безбедно. Споделувањето на твоите интереси, како фотографија од твоето омилено хоби е сосема во ред, се додека истата не содржи приватни детали како што се твојата локација или името на твоето училиште.

- Кликнување на линк од порака која вели дека си добил награда."

Одговор: Ризично. Овдека најверојатно станува збор за фишинг. Кликнување на линкот може да им овозможи на измамниците да дојдат до твоите податоци или да го оштетат твојот уред. Избриши ја пораката и не кликај на линкот.

- “Блокирање на некој кој ти испраќа лоши пораки”

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

Одговор: Безбедно. Блокирањето на некој кој е груб кон тебе онлајн е добар начин да се запре негативност. Исто така, важно е да го пријавиш нивното однесување и за ова да известиш возрасен од доверба.

- “Споделување на твојот телефонски број во јавна објава."

Одговор: Ризично. Споделувањето на твојот телефонски број во јавна објава е небезбедно, бидејќи секој може да го искористи за да те контактира или да дознае лични детали. Зачувај го твојот телефонски број приватен и споделувај го само со луѓе на кои им веруваш директно.

- Непознато лице ти пишува " Испрати ми ја твојата локација за да се дружиме!"

Одговор: Ризично. Споделувањето на твојата локација со непознати може да биде опасно.

- "Објавуваш слика од името на твоето училиште на социјалните медиуми."

Одговор: Ризично. Споделувањето на името на твоето училиште може да им помогне на непознати лица да откријат каде можат да те најдат.

- "Твој пријател ти кажува дека е малтретиран онлајн и ти го охрабруваш да разговара со возрасен од доверба."

Одговор: Безбедно. Поддржувањето на пријателот и помагањето да побара помош е правилно дејствување.

Дискусија

По групирање на картите, разговарајте за вашите одговори со групата.

- Дали сите се согласија кои дејствија се ризични?
- Што ги направи некои дејствија побезбедни од другите?
- Како можете да се сетите да бидете безбедни во слични ситуации?

Заклучок

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union

Направивте одлична работа при сортирањето на акциите! Сега знаете како да ги препознаете безбедните од ризични однесувања онлајн. Запомнете, кога сте во дилема, секогаш побарајте помош од возрасен од доверба.

Број на проект: 2023-2-RO01-KA220-YOU-000174271

Финансирано од Европската Унија. Изразените ставови и мислења се на авторот(ите) и не ги одразуваат ставовите на Европската Унија или на Европската извршна агенција за образование и култура (EACEA). Ниту Европската Унија, ниту EACEA не сносат одговорност за истите.

Co-funded by the European Union