

Scenariusz dla odbiorców w wieku 14-18 lat Szkolna Akademia Cyberbezpieczeństwa 2.0

Czas trwania: 5h

Czas trwania można dostosować do potrzeb, w zależności od możliwości czasowych realizować wybrane zadania.

Liczba uczestników: około 20 osób

Warsztaty składają się z 3 części:

1. Teoretyczne wprowadzenie do cyberzagrożeń: dyskusja i teoretyczne wprowadzenie w oparciu o prezentację.
2. Praktyczne zastosowanie wiedzy: prezentacja aplikacji Glide, wykonywanie ćwiczeń, dyskusje w grupach.
3. Projektowanie kampanii profilaktycznej: część aktywizująca, podczas której uczniowie będą zaangażowani w praktyczne działania poprzez tworzenie kampanii profilaktycznych.

Potrzebne materiały:

- sala ze stołami i krzesłami ustawiona w grupy
- rzutnik
- nagłośnienie
- duże kartki a3 dla każdej grupy

Struktura lekcji

1. Przywitanie i wprowadzenie: zacznij od przywitania uczestników i przedstawienia siebie jako nauczyciela oraz celów kursu. To ułatwi uczniom poczucie zaangażowania i komfortu.
2. Interaktywna prezentacja: użyj prezentacji multimedialnej do wprowadzenia podstawowych koncepcji. Włącz w prezentację krótkie filmy i case study, aby uczynić lekcję bardziej angażującą. Prezentacja do pobrania na stronie: <https://www.cyberbezpieczni.eu/>
3. Dyskusja z uczestnikami: rozpocznij dyskusję, zadając pytania, takie jak „Czym jest cyberprzemoc?” lub „Czy mieliście do czynienia z jakąś formą cyberprzemocy?”. Pozwoli to uczestnikom na refleksję i podzielenie się własnymi doświadczeniami.
4. Zastosowanie aplikacji padlet: zachęć uczestników do wysłania swoich odpowiedzi na pytania dyskusyjne za pomocą aplikacji Padlet. Ułatwi to zbieranie i organizację odpowiedzi, jak również pozwoli na anonimowe udział w dyskusji.

5. Analiza i omówienie odpowiedzi: po zebraniu odpowiedzi, przeczytaj je na głos i odnieś się do każdej z nich. Zapewni to uczestnikom indywidualną uwagę i pozwoli na głębszą analizę poruszanych zagadnień.
6. Podsumowanie: na koniec, podsumuj dyskusję, podkreślając najważniejsze wnioski i zachęcając uczniów do dalszej refleksji na temat omawianych zagrożeń.

Przebieg:

CZĘŚĆ 1

TEORETYCZNE WPROWADZENIE DO TEMATU CYBERZAGROŻEŃ

WPROWADZENIE DO TEMATU CYBERBEZPIECZEŃSTWA

Opis glide:

W pierwszej części kursu znajdziesz teoretyczne zagadnienia z zakresu cyberzagrożeń, zebrane w prezentacji z opisami, filmami, case study. Jako uczestnik dowiesz się w jaki sposób rozpoznać zjawiska takie jak cyberbullying, sexting, cyberprzemoc czy sharenting, a także będziesz miał okazję wypowiedzieć się w dyskusji z wykorzystaniem aplikacji padlet.

1. Przywitanie uczestników, przedstawienie trenera i projektu
2. Na rozpoczęcie warsztatów prowadzimy dyskusję z uczestnikami za pośrednictwem aplikacji Padlet.

Pytania do dyskusji: Czym jest cyberprzemoc, czy spotkaliście się z jakimś rodzajem cyberprzemocy?

Uczestnicy otrzymują link i wysyłają swoją odpowiedź na przedstawione zagadnienie, następnie prowadzący czyta odpowiedzi i odnosi się do każdej z nich.

3. Prezentacja o cyberbezpieczeństwie.

CZĘŚĆ 2

PREZENTACJA APLIKACJI GLIDE ĆWICZENIA I DYSKUSJE W GRUPACH

CYBERPRZESTĘPSTWA

Opis glide:

W drugiej części kursu znajdziesz filmy z praktycznym przedstawieniem wcześniej opisanych zagrożeń, odpowiesz na pytania, zrealizujesz zadania, a także weźmiesz udział w ciekawych dyskusjach grupowych. Po realizacji kursu będziesz wiedział jak praktycznie radzić sobie z zagrożeniami, gdzie szukać pomocy, jakie konsekwencje mogą mieć zachowania takie jak internet challenge czy cyberstalking zarówno dla Ciebie jak i dla Twoich rówieśników.

1. Przedstawianie aplikacji + rejestracja wszystkich uczestników
2. Realizacja zadań w glide. Każdy uczestnik ogląda film i realizuje zadanie w aplikacji, następnie odbywa się dyskusja w grupie, po której uczestnicy muszą wpisać wniosek w przygotowane do tego miejsce w aplikacji.

LEKCJA 1: CYBERPRZEMOC

Opis glide:

Cyberprzemoc to forma agresji, która manifestuje się poprzez użycie technologii informacyjno-komunikacyjnych, takich jak internet czy telefonia komórkowa, w celu zastraszania, poniżania, nękania lub ośmieszania innych osób.

Lekcja koncentruje się na świadomości cyfrowej, rozpoznawaniu określonych zagrożeń takich jak cyberstalking, troll parenting czy pro-ana, a także sposobach radzenia sobie z zagrożeniami online i osobach lub instytucjach do których można zgłaszać problem.

Case study:

<https://youtu.be/hvzDY4ijows>

Zadanie do Glide:

Przeczytaj opisy cyberprzestępstw i przyporządkuj odpowiednią nazwę: troll parenting, internet challenge, cyberstalking i pro-ana.

- a) Cyberstalking: Kamil, zazdrosny o Adama za jego sukcesy na boisku piłkarskim, zaczął intensywnie go nękać w sieci, wysyłając obraźliwe wiadomości i przerobione zdjęcia. Adam zaczął unikać treningów i szkoły z powodu rosnącego strachu przed spotkaniami z Kamilem. Zachowanie Kamila zepsuło atmosferę w drużynie, prowadząc do braku zwycięstw i spadku zaangażowania pozostałych graczy.
- b) Trollparenting: Mama Kasi regularnie publikuje w mediach społecznościowych zdjęcia dziewczynki w kompromitujących lub niezręcznych sytuacjach, często z "zabawnymi" komentarzami. Podczas wyjazdu do Torunia, po tym jak Kasia oblała się wodą, jej matka sfotografowała ją i opublikowała zdjęcie z dopiskiem "mój mały bejbik". Kasia jest niezadowolona z tego, że jej matka dzieli się takimi momentami bez jej zgody.
- c) Internet challenge: Maciek, zainspirowany przez swoich rówieśników, postanowił podjąć się wyzwania polegającego na połknięciu jak największej ilości kolorowych cukierków. Nie znalazłszy w domu cukierków, zastąpił je kolorowymi tabletkami należącymi do jego matki, co doprowadziło do utraty przez niego przytomności. Rodzice zastali go nieprzytomnego i musiał zostać przewieziony do szpitala.
- d) Pro-Ana: Julka, będąc celem drwin i wyzwisk ze strony koleżanek, zaczęła szukać w Internecie sposobów na szybkie schudnięcie i natrafiła na blogi propagujące ekstremalne ograniczenie jedzenia jako sposób na osiągnięcie "idealnej" sylwetki. Zaczęła drastycznie ograniczać spożywane posiłki, co nie tylko nie poprawiło jej samopoczucia, ale również miało negatywny wpływ na jej zdrowie i energię. Mimo to, kontynuowała to zachowanie, bojąc się przybrać na wadze, a jej relacje z rówieśnikami nie uległy poprawie.

Temat do dyskusji: Omów w grupie z jakimi wyżej wymienionymi zagrożeniami najczęściej się spotykaliście i jak sobie radziście. Dodaj wniosek z przeprowadzonej dyskusji.

Propozycje nowych tematów:

1. Która z wyżej wymienionych sytuacji jest waszym zdaniem najgroźniejsza dla młodych ludzi i dlaczego? Przedstaw zagadnienie w formie graficznej.
2. Czy Waszym zdaniem ktoś jest bardziej podatny na zostanie ofiarą cyberprzemocy czy dotyczy to każdego w takim samym stopniu? Wyjaśnijcie swoje zdanie.

LEKCJA 2: CYBERSTALKING

Opis glide:

Cyberstalking to specyficzna forma cyberprzemocy, polegająca na uporczywym i niechcianym śledzeniu, nękanie lub zastraszaniu jednostki przez różne platformy cyfrowe, takie jak media społecznościowe, e-mail czy komunikatory internetowe. Działania te mają na celu wywołanie strachu, dyskomfortu lub zagrożenia dla ofiary.

Lekcja koncentruje się na konsekwencjach nękania w internecie, formach cyberstalkingu oraz sposobach identyfikacji zagrożenia. Podczas ćwiczeń i dyskusji będziesz miał okazję zastanowić się i przeanalizować własne zachowanie w sieci, a także jego wpływ na Ciebie i rówieśników.

Materiały edukacyjne: wykorzystaj dostępne case study oraz filmy edukacyjne, aby pokazać realne przykłady cyberstalkingu. Materiały te powinny pomóc uczniom zrozumieć konsekwencje tego typu zachowań.

Case study:

<https://www.youtube.com/watch?v=fdYMGkoarOQ>

Zadanie do Glide: Przeczytaj poniższą historię i napisz co powinna zrobić Anna? Jakie są sposoby na obronę przed cyberstalkingiem?

"Cyberstalking w Sieci Społecznościowej: Przypadek Anny"

Anna to 17-letnia uczennica, która rozpoczęła naukę w nowej klasie. Niestety, szybko stała się celem cyberstalkingu ze strony swoich rówieśników. Kilku z nich utworzyło fałszywe konta na mediach społecznościowych, udając innych uczniów. Na tych kontach publikowali obraźliwe treści oraz manipulowali innymi uczniami, twierdząc, że Anna jest autorką tych wpisów. Dziewczyna otrzymywała również ciągłe wiadomości tekstowe z groźbami od nieznanego numeru telefonów. Rówieśnicy rozpowszechniali dezinformację o Annie w całej szkole, robili jej zdjęcia w kompromitujących sytuacjach i udostępniali je w Internecie, a następnie komentowali.

Temat do dyskusji: Przedyskutuj w grupie czy któreś z Was udostępniło wstydlive czy obraźliwe informacje o którymś z rówieśników. Z jakimi zagrożeniami może się to wiązać?

Analiza i refleksja: zachęć uczniów do analizy własnego zachowania w sieci i jego wpływu na nich samych oraz na innych. Podkreśl znaczenie rozpoznawania cyberstalkingu i umiejętności reagowania na takie sytuacje.

LEKCJA 3: SHARENTING

Opis glide:

Sharenting to praktyka, w której rodzice aktywnie dzielą się zdjęciami, filmami oraz informacjami o swoich dzieciach w mediach społecznościowych lub innych platformach online. Takie działania mogą narazić dziecko na różnego rodzaju ryzyka, takie jak naruszenie prywatności, cyberprzemoc czy potencjalne wykorzystanie tych materiałów w nieodpowiedni sposób.

Lekcja koncentruje się na zwiększeniu świadomości na temat ryzyk związanych z dzieleniem się informacjami osobistymi i zdjęciami w mediach społecznościowych przez Ciebie, jak również Twoich rodziców. Podczas zajęć omówione zostaną kwestie prywatności, bezpieczeństwa i potencjalnych konsekwencji sharentingu.

Materiały edukacyjne: wykorzystaj dostępne case study oraz filmy edukacyjne, aby pokazać realne przykłady i konsekwencje sharentingu. Materiały te powinny pomóc uczniom zrozumieć skomplikowane aspekty tej praktyki.

Case study:

https://www.youtube.com/watch?v=_Xy6fd-fUK0

Zadanie do Glide: Przeczytaj poniższe scenariusze i określ czy to jest sharenting, wpisując TAK/NIE.

- a. Scenariusz 1: Rodzic postuje zdjęcie swojego 7-letniego dziecka w mundurku szkolnym przed szkołą, tagując lokalizację i używając hashtagów związanych z pierwszym dniem w szkole.
- b. Scenariusz 2: Rodzic dzieli się filmem, na którym jego 12-letnia córka zdobywa bramkę w meczu piłki nożnej. Film jest udostępniony publicznie i zawiera informacje o drużynie i lokalizacji meczu.
- c. Scenariusz 3: Rodzic postuje zdjęcie swojego 4-letniego dziecka w szpitalu z opisem opowiadającym o trudnej sytuacji zdrowotnej, apelując o wsparcie i modlitwy.
- d. Scenariusz 4: Rodzic tworzy publiczny album na Facebooku, w którym regularnie dzieli się zdjęciami swoich dzieci od ich narodzin do chwili obecnej, dokumentując każdy ich krok i osiągnięcie.
- e. Scenariusz 5: Rodzic zamieszcza na Twitterze zdjęcie swojego 5-letniego dziecka, które właśnie skończyło pracę plastyczną w przedszkolu, razem z podziękowaniem dla przedszkolanki za inspirację.
- f. Scenariusz 6: Rodzic tworzy publiczny album na Facebooku, w którym regularnie dzieli się zdjęciami swoich dzieci od ich narodzin do chwili obecnej, dokumentując każdy ich krok i osiągnięcie.

Temat do dyskusji: Omów w grupie czy ktoś z Was spotkał się z przykładami sharentingu. Podajcie przykłady z Waszego otoczenia.

Propozycje dodatkowych tematów:

1. Czy Waszym zdaniem możemy publikować w Internecie zdjęcia innych osób, także dzieci bez ich zgody?
2. Czy Waszym zdaniem zdjęcia dzieci publikowane przez rodziców mogą zostać w przyszłości wykorzystane przez ich rówieśników do ośmieszania lub szantażowania? Jeżeli tak, jak temu zapobiec? Przedstawcie odpowiedź w formie graficznej.

Analiza i refleksja: zachęć uczniów do refleksji nad własnymi postawami wobec publikowania zdjęć w Internecie, zwłaszcza zdjęć innych osób, w tym dzieci. Podkreśl znaczenie zgody i prywatności.

LEKCJA 4: INTERNET CHALLENGE

Opis glide:

Internet Challenge to rodzaj ryzykownego wyzwania, często propagowanego w mediach społecznościowych, w którym uczestnicy są zachęceni do wykonywania niebezpiecznych lub nieodpowiedzialnych czynności i publikowania ich w formie wideo lub zdjęć online.

Lekcja koncentruje się na przedstawieniu negatywnych skutków brania udziału w internetowych wyzwaniach, przedstawieniu popularnych, ale ryzykownych wyzwań, jakie krążą w mediach społecznościowych, oraz omówieniu konsekwencji dla zdrowia i bezpieczeństwa.

Materiały edukacyjne: użyj dostępnych grafik oraz case study, aby zilustrować realne skutki uczestnictwa w tych wyzwaniach. Przykłady mogą zawierać nagłówki dotyczące skutków zdrowotnych lub nawet śmiertelnych przypadków związanych z internetowymi wyzwaniami.

Zadanie do Glide: Wymyśl edukacyjny internet challenge, który przyniesie korzyści w Twoim otoczeniu.

Temat do dyskusji: Omów w grupie czy ktoś z Was brał udział w jakimś wyzwaniu i z jakimi wiązało się to konsekwencjami.

Propozycje dodatkowych tematów:

1. Co Waszym zdaniem powoduje, że młodzi ludzie tak chętnie angażują się w wyzwania internetowe, nawet bardzo niebezpieczne?

Analiza i refleksja: zachęć uczniów do refleksji nad tym, co powoduje, że młodzi ludzie angażują się w niebezpieczne wyzwania internetowe. Zadaj pytania, które pomogą uczniom zastanowić się nad psychologicznymi i społecznymi aspektami tych działań.

LEKCJA 5: SEXTING

Opis glide:

Sexting to wysyłanie, odbieranie lub udostępnianie treści o charakterze seksualnym, takich jak zdjęcia czy wiadomości tekstowe, za pomocą środków elektronicznych, najczęściej telefonów komórkowych.

Lekcja koncentruje się na podniesieniu świadomości na temat ryzyk i konsekwencji związanych z udostępnianiem zdjęć, filmów i innych materiałów o charakterze seksualnym w przestrzeni internetowej. Dowiesz się jakie są prawne i etyczne aspekty sextingu, a także sposoby ochrony prywatności i bezpieczeństwa w kontekście tej praktyki.

Materiały edukacyjne: wykorzystaj dostępne case study oraz filmy edukacyjne, aby pokazać realne konsekwencje sextingu. Przedstaw przykłady i omów skutki, zarówno pozytywne, jak i negatywne.

Case study: <https://www.youtube.com/watch?v=2ysEpl0sdZ0>

Zadanie do Glide: Przeczytaj poniższą historię i odpowiedz na pytania.

Anna i Kamil są w związku od dwóch lat i uważają swoją relację za stabilną i zaufaną. Oboje są dorosłymi i świadomymi osobami. Pewnego wieczoru, będąc w różnych miastach z powodu obowiązków zawodowych, zaczynają rozmowę przez komunikator internetowy. W pewnym momencie Anna prosi Kamila o przesłanie jej kompromitującego zdjęcia, zapewniając, że nikt poza nią tego nie zobaczy. Kamil się zgadza i wysyła zdjęcie.

Co by się stało, gdyby relacja między Anną a Kamilem się zakończyła? Jakie są ryzyka związane z przechowywaniem takich materiałów?

Jakie środki ostrożności można by zastosować w takiej sytuacji?

Temat do dyskusji: Czy w zaufanej relacji, wysłanie takich zdjęć jest akceptowalne? Jakie są potencjalne ryzyka, nawet jeśli obie strony są dorosłe i wyrażają zgodę?

Analiza i refleksja: poproś uczniów o refleksję nad odpowiedzialnością, jaką niesie za sobą sexting, oraz nad sposobami ochrony swojej prywatności i bezpieczeństwa online.

LEKCJA 6: SEXTORTION

Sextortion to sytuacja, w której ktoś grozi komuś innemu, że ujawni jego intymne zdjęcia, filmy lub informacje, jeśli ta osoba nie zrobi czegoś, czego żąda szantażysta. To poważne naruszenie prywatności i nielegalne zachowanie online. Ważne jest, aby być ostrożnym i nie udostępniać intymnych treści innym osobom oraz zgłaszać tego rodzaju działania odpowiednim służbom.

Lekcja koncentruje się na przedstawieniu zjawiska sextortion i jego konsekwencji dla młodych ludzi, a także możliwościach uzyskania pomocy.

Materiały edukacyjne: wykorzystaj dostępne case study oraz filmy edukacyjne, aby pokazać realne przykłady sextortion i jego wpływu na ofiary. Przedstawienie realnych historii pomoże uczniom zrozumieć powagę tego zjawiska.

Case study: <https://www.youtube.com/watch?v=NzKLcvUQAqA>

Zadanie do Glide: Gdzie zwrócić się o pomoc w przypadku zjawiska sextingu?

Temat do dyskusji: Omów w grupie aktualny temat "Pandora Gate". Czy uważacie, że ofiary mogły w jakiś sposób uniknąć tej sytuacji?

Analiza i refleksja: zachęć uczniów do refleksji nad ważnością ochrony własnej prywatności i bezpieczeństwa w Internecie oraz nad odpowiedzialnym zachowaniem w cyfrowym świecie.

CZĘŚĆ 3 SPOTY PROFILAKTYCZNE

KAMPANIA PROFILAKTYCZNA

Opis glide:

W trzeciej części kursu sprawdzisz się podczas pracy grupowej w której razem z rówieśnikami zaprojektujesz swoją własną kampanię profilaktyczną na jeden z wylosowanych tematów: cyberstalking, sharenting, sextorion, Internet Challenge, zjawisko FOMO, cyberbullying. W ramach kampanii stworzycie hasło, grafikę lub plakat profilaktyczny, spot, a także opis wydarzenia profilaktycznego w swojej szkole.

W JAKI SPOSÓB TWORZYĆ KAMPANIE PROFILAKTYCZNE

Wprowadzenie do kampanii: https://youtu.be/JiOXP8B8nYA?si=IY4F0OSxayu_zT6W

Przykłady kampanii profilaktycznych:

Uczestnicy w grupach pracują nad przygotowaniem spotu profilaktycznego na wylosowany temat:

1. **Cyberstalking** - wielokrotne wysyłanie komuś w internecie lub przy użyciu telefonu niechcianych informacji, zdjęć, bardzo częste wysyłanie e-maili i informacji za pomocą komunikatorów czy czatów mimo braku zgody odbiorcy.
2. **Sharenting** - regularne zamieszczanie przez rodziców w internecie, głównie na portalach społecznościowych, blogach, forach dyskusyjnych, szczegółowych informacji, zdjęć i filmów z życia dzieci.
3. **Sextorion** - polega na pozyskaniu od ofiary materiałów o charakterze seksualnym, następnie wymuszeniu okupu (pieniędzy lub kolejnych treści pod groźbą ich opublikowania lub dalszego rozpowszechniania)
4. **Internet Challenge** - internetowe wyzwanie do wykonania niebezpiecznego zadania.
5. **Zjawisko FOMO** - strach przed tym co nas omija w odniesieniu do ciągłego korzystania z telefonu i mediów społecznościowych.
6. **Spoofing** - rodzaj ataku, w którym przestępcy podszywają się pod banki, instytucje i urzędy państwowe, firmy, a nawet osoby fizyczne w celu wyłudzenia od swoich ofiar danych lub pieniędzy.

7. **Cyberbullying** - nękanie online, która może przybierać różne formy, takie jak obraźliwe wiadomości, wyśmiewanie, groźby lub rozpowszechnianie obraźliwych treści wobec innych osób.

Zadania:

1. Wymyśl hasło profilaktyczne ostrzegające Twoich rówieśników przed wylosowanym cyberprzestępstwem.
2. Stwórz plakat lub grafikę profilaktyczną. Możesz to zrobić na stronie www.canva.com
3. Nagraj 30 sekundowe wideo, w którym wykorzystasz wymyślone hasło kampanii profilaktycznej.
4. Omów w grupie jak dotrzeć do swoich rówieśników i wymyśl wydarzenie, jakie moglibyście zorganizować w swojej szkole dotyczące zapobiegania wylosowanej cyberprzemocy.

Przygotowane filmy, grafiki i opisy każda z grup dodaje do aplikacji glide w sekcji KAMPANIA PROFILAKTYCZNA.

