CYBERLEKCJE 3.0

Scenariusz lekcji

Zagrożenia w sieci

NASK

cyber profilaktyka NASK

Ministerstwo Cyfryzacji

Zagrożenia w sieci

Scenariusz lekcji dla szkół ponadpodstawowych

Scenariusz opracowany w ramach projektu „Działania wspierające nauczanie o cyberbezpieczeństwie"

Autorka scenariusza: Agata Arkabus, Bernardetta Czerkawska

Redakcja merytoryczna: Cyberprofilaktyka NASK (Dział Profilaktyki Cyberzagrożeń), Dział Budowania Świadomości Cyberbezpieczeństwa

Redakcja językowa, dostępność (WCAG): Emilia Troszczyńska-Roszczyk, Katarzyna Gańko, Marta Danowska

NASK – Państwowy Instytut Badawczy
ul. Kolska 12
01-045 Warszawa

Spis treści

Temat: **Zagrożenia w sieci**

Etap: **szkoła ponadpodstawowa**

Czas realizacji: **2 x 45 minut**

Warto wiedzieć – wprowadzenie do zajęć

Internet jest dla współczesnej młodzieży miejscem spotkań towarzyskich, rozrywki i nauki. Korzystanie z sieci niesie jednak za sobą również zagrożenia. Nastolatkom czasem trudno jest określić granice bezpieczeństwa. Wiążą się one również z wykorzystywaniem zasobów sieci, takimi jak muzyka czy zdjęcia. Młodzi ludzie nie zawsze wiedzą, jak korzystać z tych materiałów zgodnie z prawem.

Rolą nauczyciela jest wskazanie i uświadomienie młodemu człowiekowi ryzyka, z jakim może się wiązać korzystanie z Internetu. Warto ugruntować wiedzę z tego zakresu, zwracając szczególną uwagę na sposoby radzenia sobie z zagrożeniami. Z pomocą przychodzą nam tutaj otwarte zasoby edukacyjne, możliwość zgłaszania nieodpowiednich zachowań administratorom, dbanie o prywatność kont internetowych czy też uważne czytanie regulaminów sklepów sieciowych.

Informacje na temat zajęć

Cele ogólne powiązane z podstawą programową

Informatyka

IV. Rozwijanie kompetencji społecznych, takich jak: komunikacja i współpraca w grupie, w tym w środowiskach wirtualnych, udział w projektach zespołowych oraz zarządzanie projektami.

V. Przestrzeganie prawa i zasad bezpieczeństwa. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

IV. Rozwijanie kompetencji społecznych. Zakres podstawowy - uczeń:

1. aktywnie uczestniczy w realizacji projektów informatycznych rozwiązujących problemy z różnych dziedzin, przyjmuje przy tym różne role w zespole realizującym projekt i prezentuje efekty wspólnej pracy;

2. podaje przykłady wpływu informatyki i technologii komputerowej na najważniejsze sfery życia osobistego i zawodowego; korzysta z wybranych e-usług; przedstawia wpływ technologii na dobrobyt społeczeństw i komunikację społeczną.

Etyka

II. Wybrane zagadnienia etyki szczegółowej (praktycznej, stosowanej, zawodowej).

4. Etyka a nauka i technika. Uczeń:

1) podaje przykłady właściwego i niewłaściwego wykorzystywania nowych technologii, w szczególności technologii informatycznych.

Cele szczegółowe powiązane z podstawą programową

Uczeń:

- zna zagrożenia związane z korzystaniem z Internetu;
- wykorzystuje aplikacje komputerowe w celu poszerzania wiedzy;
- zna sposoby zapobiegania zagrożeniom internetowym.

Kompetencje kluczowe

- kompetencje w zakresie rozumienia i tworzenia informacji;
- kompetencje językowe;
- kompetencje cyfrowe;
- kompetencje osobiste, społeczne i w zakresie uczenia się.

Cele zajęć w języku ucznia:

1. Wyjaśnię, na czym polegają zagrożenia w Internecie.
2. Poznam pięć sposobów dbania o bezpieczeństwo w Internecie.

Kryteria sukcesu dla ucznia/uczennicy:

1. Wyjaśnię na przykładach, na czym polega niebezpieczeństwo trzech z poznanych zagrożeń w Internecie.
2. Omówię skuteczność pięciu sposobów dbania o bezpieczeństwo w Internecie.

Wskazówki do przeprowadzenia zajęć:

- W czasie zajęć uczniowie pracują przy stoliczkach, które zmieniają co ok. 12 minut. Warto dokładnie omówić z nimi zasady pracy.
- ROZSZERZENIE: w czasie V i VI rundy pracy grupy uczniowie mogą wypracować ciekawe pomysły działań. Można zachęcić ich później do realizacji projektu społecznego np. z zwolnienizteorii.pl

Metody/techniki pracy

- dyskusja;
- metoda problemowa.

Formy pracy

- indywidualna;
- grupowa.

Środki dydaktyczne

- komputery z dostępem do Internetu lub laptopy/tablety;
- karteczki samoprzylepne;
- karta pracy „zagrożenia w sieci" – mapy myśli dla grup;
- smartfony.

Przebieg zajęć

Wprowadzenie

Nauczyciel rozdaje uczniom karteczki samoprzylepne. Prosi uczniów o napisanie na nich, z jakich treści/zasobów najczęściej korzystają w sieci. Następnie uczniowie przyklejają karteczki w wyznaczonym miejscu, np. na tablicy. Nauczyciel prosi o wzięcie pod uwagę różnych obszarów, np. uczenie się, rozwój pasji, blogi/vlogi, informacje itp.

Wybrani uczniowie grupują zapisane odpowiedzi, tworząc obszary treści czy zasobów, np. rozwój zainteresowań; edukacja i dokształcanie się; celebryci i influencerzy itp. Nauczyciel podsumowuje udzielone przez uczniów odpowiedzi. Zwraca uwagę, że niektóre z tych treści mogą należeć do tzw. treści szkodliwych i niebezpiecznych.

Część główna

Nauczyciel szykuje przestrzeń klasy do pracy: przygotowuje pięć stolików dla grup, grupy będą się przemieszczać po klasie.

Organizacja przestrzeni:

Na stolikach leżą mazaki i wydrukowane na A3 karty pracy dla każdej z grup, lub plakaty/szary papier, aby grupy przerysowały sobie schemat notatki.

Zasady pracy:

Praca w grupach odbywa się w 6. turach. Po każdej turze grupy zmieniają stolik do pracy. Plakaty zawsze zostają dla następnej grupy. Każda grupa wypowiada się na temat każdego zagrożenia. Na każda turę warto przeznaczyć ok. 12 minut, ale warto to monitorować. Notatki poszczególnych grup muszą być wyraźne, żeby nie było kłopotów z odczytaniem zapisów.

Przebieg pracy:

Nauczyciel łączy uczniów w 6 grup.

I tura – każda grupa wybiera sobie stolik. Na plakacie zapisane jest zagadnienie, które jest omawiane w tym miejscu.

- Zadaniem grupy jest napisanie w chmurze nr 1 definicji zagrożenia.

II tura – grupy zmieniają stoliki do pracy.

- Przeczytanie zapisków, które już są na plakacie.
- Dyskusja nad zapisami i dodanie swoich przemyśleń.
- Uzupełnienie chmury nr 2: jakie znacie przykłady takich zagrożeń?

III tura – grupy zmieniają stoliki do pracy.

- Przeczytanie zapisków, które już są na plakacie.
- Dyskusja nad zapisami i dodanie swoich przemyśleń.
- Uzupełnienie chmury nr 3: jakie są konsekwencje tego zagrożenia?

IV tura – grupy zmieniają stoliki do pracy.

- Przeczytanie zapisków, które już są na plakacie.
- Dyskusja nad zapisami i dodanie swoich przemyśleń.
- Uzupełnienie chmury nr 4: jak się chronić przed tym zagrożeniem?

V tura – grupy zmieniają stoliki do pracy.

- Przeczytanie zapisków, które już są na plakacie.
- Dyskusja nad zapisami i dodanie swoich przemyśleń.
- Uzupełnienie chmury nr 5: jak rozpowszechniać wiedzę o tym zagrożeniu?

VI tura – grupy zmieniają stoliki do pracy.

- Przeczytanie zapisków, które już są na plakacie.
- Dyskusja nad zapisami i dodanie swoich przemyśleń.
- Uzupełnienie chmury nr 6: które działania najszybciej i najskuteczniej trafią do młodzieży?

Przykładowe definicje:

Cyberprzemoc. Obecność młodzieży w sieci niesie za sobą ryzyko włamania się oszustów na konto (w celu kradzieży tożsamości i podszywania się) czy wzajemnego ośmieszania. Prześladowcami są zazwyczaj rówieśnicy. Rodzaje cyberprzemocy: cybermobbing, cyberbullying, trolling.

Naruszanie praw autorskich. Korzystanie z internetowych źródeł informacji jest powszechne. Młodzież na co dzień, np. przygotowując się do zajęć, korzysta z Internetu. Nie zawsze uczniowie są świadomi łamania praw autorskich.

Kradzież danych osobowych. Dane osobowe bardzo często są udostępniane przez uczniów w portalach społecznościowych czy komunikatorach. Dane mogą być również podstępnie wyłudzane przez przestępców.

Piractwo. W ramach rozrywki uczniowie często słuchają muzyki czy oglądają filmy z Internetu. Czasem materiały te zapisują na dysku komputera. Działanie to nie jest zgodne z prawem.

Sexting. To forma komunikacji elektronicznej, w której przekazem jest seksualnie sugestywny obraz lub treść.

Uzależnienie od Internetu. Korzystając z Internetu w domu, w szkole, podczas nauki i rozrywki, łatwo można się od niego uzależnić. Bardzo trudno zauważyć granicę bezpieczeństwa przy korzystaniu z sieci.

Phishing. To metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań.

Vishing. Oszustwo polegające na wyłudzaniu danych (ang. phishing) w wersji głosowej, w trakcie rozmowy telefonicznej.

Smishing. Rodzaj phishingu skierowanego na telefony komórkowe. Celem przestępcy jest zgromadzenie danych osobowych, takich jak np. numer ubezpieczenia społecznego lub numer karty kredytowej. Drogą ataku są wiadomości tekstowe (SMS).

Przykładowe pomysły jak się chronić:

Cyberprzemoc: brak reakcji na nękanie, zachowywanie dowodów, blokowanie nękającej osoby, zgłoszenie nieodpowiednich zachowań administratorowi strony, poinformowanie o przykrej sytuacji rodziców/nauczycieli.

Naruszenie praw autorskich: świadomość istnienia praw autorskich, otwarte zasoby edukacyjne, licencje Creative Commons, ochrona wizerunku.

Kradzież danych osobowych: dbanie o prywatność kont internetowych, nieujawnianie w Internecie danych osobowych, zakładanie odpowiednich haseł dostępu.

Piractwo: słuchanie muzyki online, oglądanie filmów w streamingu, ponoszenie opłat.

Sexting: niewysyłanie nagich zdjęć, niepublikowanie nagich zdjęć.

Uzależnienie od internetu: ograniczanie czasu spędzanego przed komputerem, kontakty „na żywo" z rówieśnikami, rozwijanie zainteresowań niezwiązanych z Internetem.

Po zakończonej pracy w grupach nauczyciel prosi przedstawicieli zespołów o odczytanie tylko 6., ostatniego punktu.

Podsumowanie

Nauczyciel zaprasza uczniów do dyskusji:

- Co było dla was nową wiedzą?
- Co myślicie o dzisiejszej tematyce zajęć? Jak duży jest to problem?
- Czy możemy coś zrobić, żeby świadomość użytkowników sieci na temat zagrożeń była większa?

Komentarz metodyczny

Sposoby oceniania

- aktywność;
- udział w dyskusji.

Praca z uczniem ze specjalnymi potrzebami edukacyjnymi (SPE)

Uczniowie zdolni mogą przygotować na zajęcia prezentację dotyczącą zagrożeń internetowych, którą omówią we współpracy z nauczycielem.

Konieczne jest zadbanie, aby w czasie pracy grup osoby mające trudności w przemieszczaniu się miały komfort pracy. W czasie zajęć jest sporo zmian miejsc - należy rozpoznać, czy w klasie jest uczeń z ADHD lub zespołem Aspergera i czy taki poziom zmian jest akceptowalny. Jeśli nie, ta osoba może pracować przy tym samym stoliku lub można zamieniać się plakatami, a nie stolikami.

Bibliografia/Netografia

- Borkowska A., (2019), „Cyberprzemoc włącz blokadę na nękanie", Warszawa: NASK – Państwowy Instytut Badawczy [online, dostęp z dn. 5.07.2023].
- Fundacja Dajemy Dzieciom Siłę, (2015), film „Seksting: rejestrowanie, wysyłanie, upublicznianie nagich zdjęć przez młodzież" [online, dostęp z dn. 5.07.2023].
- Infografika „Phishing"
- Minitest „Bezpieczny internet" – LearninApps [online, dostęp z dn. 5.07.2023].
- Zintegrowana Platforma Edukacyjna, „Bezpieczeństwo w sieci – rodzaje zagrożeń" [online, dostęp z dn. 5.07.2023].