Temat: Cyberbezpieczeństwo

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 zarządzaniem zasobami 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 jakimi może się wiązać korzystanie z internetu. Warto ugruntować wiedzę z tego zakresu, zwracając szczególną uwagę na sposoby radzenia sobie z tymi 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

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;
- pełni rolę lidera w zespole;
- 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.

Metody/techniki pracy

- prezentacja;
- dyskusja;
- metoda problemowa;
- metoda praktyczna;
- praca z komputerem, tabletem/smatfonem.

Formy pracy

- indywidualna;
- grupowa.

Środki dydaktyczne

- komputery z dostępem do internetu lub laptopy/tablety;
- karteczki samoprzylepne,
- prezentacja multimedialna „Zagrożenia w sieci”,
- karta pracy „Jak dbać o bezpieczeństwo w sieci” (różne rodzaje)
- przykłady kart pracy
- aplikacje internetowe do tworzenia testów/quizów, np. Learning Apps, Kahoot, Quzzlet

– smartfony.

Opis przebiegu zajęć/lekcji

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. 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

1. Nauczyciel dzieli uczniów na grupy. Zachęca ich, aby zastanowili się, czy w internecie można natknąć się na zagrożenia. Uczniowie na kartkach dokonują próby stworzenia definicji zagrożeń internetowych.

2. Nauczyciel omawia zagrożenia internetowe, korzystając z prezentacji multimedialnej o tej tematyce. Przykładowe zagadnienia:

a. Slajd 1. 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.

b. Slajd 2. 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.

c. Slajd 3. Kradzież danych osobowych.

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

d. Slajd 4. Wyłudzenia finansowe.

Internet jest dla współczesnej młodzieży m.in. miejscem rozrywki i zabawy. Dla relaksu uczniowie często grają w multimedialne gry – darmowe lub świadomie zakupione. Może tak się jednak zdarzyć, że nastolatek padnie ofiarą wyłudzenia finansowego, np. w przypadku nieświadomości zakupu cyklicznego, kiedy opłata pobierana jest wielokrotnie zamiast jednorazowo.

e. Slajd 5. Niebezpieczne znajomości.

Korzystając z internetu, możemy spotkać się ze zjawiskiem groomingu, czyli uwodzeniem w sieci w celu nawiązania więzi emocjonalnej i późniejszego wykorzystania seksualnego.

f. Slajd 6. 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.

g. Slajd 7. Sexting.

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

h. Slajd 8. 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.

i.Slajd 9. 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.

j. Slajd 10. Vishing.

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

k. Slajd 11. 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 lub SMS. 3.

Po omówieniu zagadnień nauczyciel rozdaje uczniom karty pracy „Jak dbać o bezpieczeństwo w sieci”. Każda grupa pracuje nad jednym przykładowym zagrożeniu: np. Cyberprzemoc; Naruszenie praw autorskich; Kradzież danych finansowych; Wyłudzenia finansowe; Niebezpieczne znajomości; Piractwo, Sexting; Uzależnienie od internetu. Propozycje odpowiedzi uczniów:

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

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

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

d. Wyłudzenia finansowe: uważne czytanie regulaminu zakupu, niepodawanie w sieci numerów kont bankowych, stosowanie zapór internetowych (ogniowych).

e. Niebezpieczne znajomości: świadomość anonimowości osoby z kontaktu internetowego. f. Piractwo: słuchanie muzyki online, oglądanie filmów w streamingu, ponoszenie opłat.

g. Sexting: niewysyłanie nagich zdjęć, niepublikowanie nagich zdjęć.

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

Po zakończonej pracy jeden uczeń z grupy omawia wykonane zadanie. Uczniowie z pozostałych grup ewentualnie uzupełniają odpowiedzi.

4. Nauczyciel prezentuje infografikę pokazującą zgłaszanie nielegalnych i szkodliwych treści – „Nielegalne i szkodliwe treści”.

Podsumowanie

„Bezpieczny internet” – praca w grupach. Uczniowie rozwiązują quiz/test zawierający pytania jednokrotnego wyboru, wykorzystując wiadomości nabyte podczas lekcji.