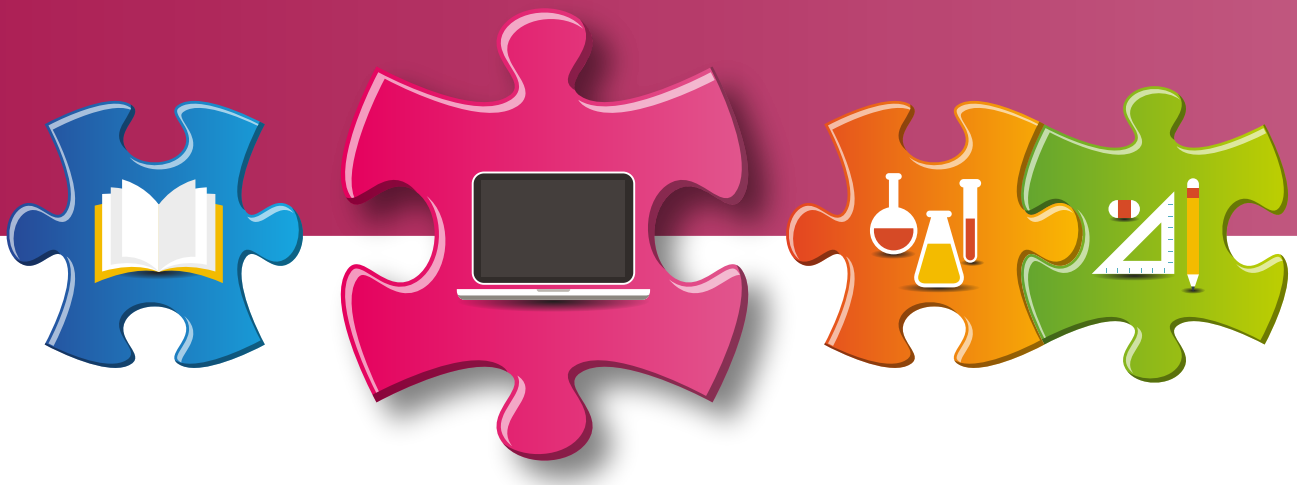
Zestaw 10

Zeszyt 2

Monika Spławska-Murmyło
Anna Wawryszuk

Bezpieczeństwo w użytkowaniu technologii informacyjno-komunikacyjnych

- Zagrożenia wynikające z użytkowania narzędzi TIK
- Wskazówki metodyczne



Redakcja językowa i korekta
Monika Lipińska-Pawełek

Projekt graficzny, projekt okładki
Wojciech Romerowicz, ORE

Skład i redakcja techniczna
Grzegorz Dębiński

Projekt motywu graficznego „Szkoły ćwiczeń”
Aneta Witecka

ISBN 978-83-65890-47-4 (Zestawy materiałów dla nauczycieli szkół ćwiczeń – informatyka)
ISBN 978-83-65890-86-3 (Zestaw 10. Aspekty prawne i kompetencje miękkie w edukacji informatycznej w klasach IV–VIII szkoły podstawowej i szkole ponadpodstawowej)
ISBN 978-83-65890-91-7 (Zeszyt 2. Bezpieczeństwo w użytkowaniu technologii informacyjno-komunikacyjnych)

Warszawa 2017
Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-478 Warszawa
www.ore.edu.pl

Fundusze Europejskie Wiedza Edukacja Rozwój
ORE Ośrodek Rozwoju Edukacji
Unia Europejska Europejski Fundusz Społeczny

Spis treści

Wstęp

Rozwój technologii informacyjno-komunikacyjnych w ciągu ostatnich kilkunastu lat bezpowrotnie zmienił takie aspekty życia ludzi, jak praca, dostęp do informacji, komunikowanie się, edukacja i relacje społeczne. Swobodny dostęp do internetu stwarza nam możliwości stałego i szybkiego pozyskiwania wiadomości, dostarcza narzędzia pomocne w pracy, nauce, komunikacji czy też służące rozrywce. Jednak mimo że sieć stała się ważnym środkiem wspierającym proces kształcenia, niesie ona również zagrożenia.

Bezpieczeństwo w internecie oraz odpowiedzialne korzystanie z mediów społecznościowych jest jednym z podstawowych kierunków realizacji polityki oświatowej państwa w roku szkolnym 2017/2018. Zagadnienia bezpieczeństwa w użytkowaniu narzędzia TIK zawierają się również w wytycznych dotyczących wzmacniania wychowawczej roli szkoły.

Przestrzeganie prawa i zasad bezpieczeństwa jest jednym z głównych celów edukacji zdefiniowanych w nowej podstawie programowej z informatyki dla szkół podstawowych, w której czytamy o jego składowych:

„Uczeń:

1. Rozumie, że niewłaściwe postępowanie w posługiwaniu się technologią i informacją rodzi negatywne konsekwencje.

2. Uznaje i respektuje prawo do prywatności danych i informacji oraz prawo do własności intelektualnej.

3. Zauważa zagrożenia związane z powszechnym dostępem do technologii oraz do informacji i wystrzega się ich.

4. Rozumie znaczenie profilaktyki antywirusowej i konieczność ochrony przed innymi zagrożeniami dla komputerów i informacji” (Podstawa…, b.r.: 7).

Dodatkowo w opisie szczegółowych wymagań dla klas VI–VIII czytamy:

„Uczeń:

1. Opisuje kwestie etyczne związane z wykorzystaniem komputerów i sieci komputerowych, takie jak: bezpieczeństwo, cyfrowa tożsamość, prywatność, własność intelektualna, równy dostęp do informacji i dzielenie się informacją”.

Wyniki badań społecznych dowodzą, że dzieci i młodzież spędza w internecie coraz więcej czasu, nie zawsze mając świadomość konsekwencji ujawniania swoich danych osobowych czy dostosowując ustawienia prywatności swojego profilu na portalach społecznościowych (*Postrzeganie zagadnień…*, b.r.). Dlatego też konieczna jest edukacja dzieci i młodzieży mająca

na celu uświadomienie zagrożeń, a tym samym przekazanie zasad bezpiecznego korzystania z internetu oraz narzędzi TIK.

Przyczyny zagrożeń wynikających z użytkowania narzędzi TIK

Jeśli rodzice wspierają dzieci w informatyczno-komunikacyjnych poszukiwaniach, interesują się tym, co dzieci robią w sieci i czego szukają, jest szansa na rozwój prawidłowych zachowań i ustrzeżenie się przed zagrożeniami. Duża w tym rola nauczycieli, którzy jako przewodnicy po świecie technologii powinni kierunkować zainteresowania swoich uczniów i uczyć ich, jak korzystać z narzędzi TIK w sposób bezpieczny. Nie zawsze jednak osoby z otoczenia społecznego młodego człowieka są na tyle kompetentne, żeby towarzyszyć mu w wystarczający i odpowiadający jego potrzebom sposób.

Według wyników badań Diagnozy Społecznej (Diagnoza…, 2014: 357) nierzadko obecność dzieci w gospodarstwie domowym ma decydujące znaczenie dla posiadania komputera z dostępem do internetu. To jednak niekoniecznie wiąże się z większymi kompetencjami u dorosłych. Oznacza to, że dorośli w takich wypadkach zostawiają korzystanie z nowych technologii dzieciom, nie interesując się, co tak naprawdę one robią.

Nic więc dziwnego, że młodzi ludzie są często narażeni na zagrożenia w zakresie korzystania z narzędzi TIK. Najczęściej wymienia się następujące obszary zagrożeń (na podst. Prujszczyk, Śliwowski, 2010):

a) dziecko jako odbiorca treści:

- ekspozycja na reklamę i zagrożenie komercjalizacją,
- ekspozycja na reklamę produktów niedostosowanych do wieku (np. alkohol, papierosy),
- ekspozycja na treści z lokowaniem produktu,
- ekspozycja na treści pełne agresji, mające charakter erotyczny lub pornograficzny, pochwalające przemoc lub inne zachowania antyspołeczne,

b) dziecko jako uczestnik kontaktu:

- ryzyko nawiązania kontaktu przez osoby o złych zamiarach dzięki aplikacjom służącym do komunikacji (np. podających się za rówieśników),
- ryzyko podania przez dziecko danych osobowych obcej osobie,
- ekspozycja na treści wysyłane przez obcą osobę o złych zamiarach (np. pornograficzne),
- ekspozycja na zjawisko sekstingu,
- wysokie ryzyko manipulacji przez obce osoby,
- ryzyko wyłudzania pieniędzy za połączenia komórkowe lub wiadomości SMS,

c) dziecko jako sprawca niewłaściwego zachowania:

- cyberbullying,
- mowa nienawiści,
- wykradanie haseł do kont,
- naruszenie praw autorskich (kradzież zdjęć, tekstów itp.),
- rozsyłanie spamu (łańcuszki),
- piractwo (ściąganie muzyki, filmów, e-booków).

Uzależnienie od internetu i telefonów komórkowych

Dzieci i młodzież są coraz częściej narażone na uzależnienie od nowych technologii. Zjawisko to jest coraz bardziej powszechne i dość szeroko opisane w literaturze psychologicznej. Funkcjonuje ono pod następującymi terminami: siecioholizm, sieciozależność, cyberzależność, cybernałóg, internetoholizm, uzależnienie od internetu, uzależnienie komputerowe, infoholizm, infozależność. Naukowcy zainteresowali się tym problemem już w połowie lat 90. XX wieku, kiedy to amerykańska psycholog Kimberly Young zaczęła badania nad uzależnieniem od zapośredniczonych kontaktów społecznych, sieci komputerowej oraz pobierania informacji, porównując te sytuacje do uzależnienia od hazardu.

Polski psychiatra B. Woronowicz zaproponował następujący opis objawów uzależnienia od internetu (za: Bezpieczeństwo informacyjne…):

Muszą występować co najmniej trzy z sześciu objawów w okresie 12 miesięcy:

I. Tolerancja, rozumiana jako:

1. potrzeba coraz dłuższego czasowego korzystania z internetu w celu uzyskania zadowolenia i/lub

2. wyraźny, stopniowy spadek satysfakcji osiąganej przez tę samą ilość czasu przebywania w sieci.

II. Objawy odstawienia manifestujące się:

1. zespołem abstynencyjnym wyrażającym się w formie co najmniej dwóch z następujących objawów, występujących w okresie od kilku dni do miesiąca po zaprzestaniu lub ograniczeniu korzystania z internetu:

- pobudzenie psychoruchowe,
- niepokój lub lęk,
- wyraźne obniżenie nastroju,
- obsesyjne myślenie o tym, co się dzieje w sieci,
- fantazje i marzenia senne na temat internetu,

- celowe lub mimowolne poruszanie palcami w sposób charakterystyczny dla pisania na klawiaturze,

2. korzystaniem z sieci w celu uniknięcia przykrych objawów abstynencyjnych po „odstawieniu" internetu.

III. Częste przekraczanie planowanego wcześniej czasu korzystania z internetu.

IV. Utrwalona potrzeba lub nieudane próby ograniczania lub zaprzestania korzystania z internetu.

V. Poświęcanie dużej ilości czasu na wykonywanie czynności związanych z internetem (np. kupowanie książek na temat sieci, testowanie nowych przeglądarek stron WWW, porządkowanie ściągniętych z internetu materiałów, plików, programów itp.

VI. Zmniejszanie lub rezygnowanie z aktywności społecznej, zawodowej lub rekreacyjnej na rzecz internetu.

VII. Korzystanie z internetu pomimo świadomości doświadczania trwałych bądź narastających problemów somatycznych (fizycznych), psychologicznych lub społecznych, spowodowanych lub nasilających się w związku z korzystaniem z sieci (np. ograniczenie czasu snu, występowanie problemów rodzinnych, spóźnianie się do pracy i na spotkania, zaniedbywanie obowiązków, rezygnacja z innych istotnych działań).

W ostatnich latach uzależnienie od internetu ma coraz ściślejszy związek z uzależnieniem od telefonów komórkowych (fonoholizm). Według raportu zamieszczonego na stronie Uzależnienia behawioralne „na pytanie »Czy jesteś osobą uzależnioną od telefonu komórkowego?« co piąty uczeń (20,8%) odpowiada w sposób twierdzący, prawie co dziesiąty zaznacza odpowiedź »trudno powiedzieć«. Takie wnioski płyną z ogólnopolskich badań przeprowadzonych wśród 3471 nauczycieli i 22 086 osób między 12 a 18 rokiem życia, eksperymentu społecznego pt. „POZ@ SIECIĄ" oraz badań jakościowych z lat 2015–2016. (...) Problem szeroko rozumianego problemu e-uzależnień zauważają także badani nauczyciele, których zdaniem w ciągu ostatnich 5 lat problem nałogowego i niekontrolowanego korzystania z mediów cyfrowych wśród uczniów zdecydowanie się nasilił. Przekonani są o tym również rodzice. Prowadzone badania wykazały, że część z nich wskazuje na własne uzależnienie od korzystania z cyfrowych narzędzi komunikacji".

Psychologowie podkreślają, że tendencje do intensywnego korzystania z internetu/telefonów komórkowych są powiązane z określonymi stylami radzenia sobie ze stresem, zwłaszcza skoncentrowanego na emocjach i polegającego na unikaniu stresu. Wydaje się, że u takich osób stres może stanowić czynnik indukujący uzależnienie.

Zagrożenia wynikające z użytkowania narzędzi TIK

Jak już zaznaczyliśmy, samo używanie narzędzi TIK nie stanowi zagrożenia dla dzieci i młodzieży. Ryzyko pojawia się dopiero w określonym kontekście postępowania ich użytkowników. Chodzi tu zarówno o ich kompetencje medialne, jak i fakt towarzyszenia im ze strony dorosłych. Wszelkie działania profilaktyczne muszą zatem odnosić się nie tylko do samych instrumentów TIK, ale i do kompetencji uczniów oraz ich otoczenia społecznego (rodziców, nauczycieli). Dlatego w dalszej części niniejszego zeszytu przedstawimy potencjalne zagrożenia czyhające na użytkowników wybranych narzędzi TIK, pokażemy ich społeczny kontekst oraz zaprezentujemy strategie nauczania o bezpieczeństwie w sieci.

Szyfrowanie SSL

Wszelkie dane, które przesyłamy w sieci, niezależnie od tego, czy chodzi o treść wiadomości e-mail, posty na portalach społecznościowych czy prywatne zdjęcia umieszczane w chmurach, jeśli ich nie zaszyfrujemy, są potencjalnie dostępne dla osób trzecich. Co to oznacza? Otóż, jak piszą Grzegorz Prujszczyk i Kamil Śliwowski w swoim raporcie „Bezpieczeństwo informacyjne w serwisach Web 2.0” (2010: 3), „oznacza to, że osoby postronne mogą przeczytać to, co czytamy i piszemy w sposób niezauważalny dla nas. Jest to możliwe, ponieważ komunikacja z serwerem serwisu, z którego korzystamy, prowadzona jest w formie standardowych pakietów informacji, które muszą przebyć drogę od naszego komputera do serwera, po drodze przechodząc przez naszą sieć lokalną do routera, potem do dostawcy internetu i poprzez kolejne punkty przesyłowe. Ponieważ pakiety mają określony format, mogą bez trudu zostać rozpoznane przez oprogramowanie do analizy ruchu, np. program Wireshark, i przedstawione w formie pozwalającej na wygodne odczytanie treści. Wszelka niezaszyfrowana komunikacja bez problemu może paść ofiarą takiej analizy sieci i osoba »uzbrojona« w taki program może czytać nasze czaty czy przechwycić prywatne zdjęcia”.

Sposoby ochrony:

- korzystanie z szyfrowania SSL (uwaga, w szczególnych przypadkach i ono może zostać złamane); szyfrowanie poczty umożliwia np. wtyczka Enigmail do Thundebirda;
- używanie otwartoźródłowego narzędzia VeraCrypt pozwalającego na szyfrowanie całych dysków, partycji, przenośnych dysków USB oraz tworzenie wirtualnych zaszyfrowanych dysków;
- używanie alternatywnych sieci, np. TOR (ang. The Onion Router), wirtualnej sieci komputerowej zapobiegającej analizie ruchu sieciowego, co zapewnia niemal anonimowe korzystanie z internetu;
- uważne korzystanie z przeglądarki internetowej: nie używajmy opcji zapamiętywania haseł do żadnych kont i serwisów;
- bezdyskusyjnie największą ochronę prywatności zapewnia szyfrowanie poczty; z mechanizmu szyfrowania i podpisywania poczty, nazywanego PGP lub GPG (Pretty Good Privacy lub GNU Privacy Guard), możemy skorzystać, np. instalując wtyczkę Enigmail do Thundebirda. Dostępna jest też wtyczka do przeglądarek Mailvelope.

Geolokalizacja

Wielu użytkowników portali społecznościowych korzysta z możliwości „meldowania się" w różnych miejscach, w których aktualnie przebywają, np. w barze, kinie, bibliotece, galerii itp. Taką możliwość dają m.in. popularne serwisy, np. Facebook, Twitter, Snapchat i Instagram. Podobnie działają aplikacje śledzące nasz ruch, jak Google Maps, lub monitorujące np. nasze dokonania sportowe, jak Endomondo. Warto się zastanowić, czy ujawnienie dokładnych współrzędnych GPS miejsca, w którym się znajdujemy, to naprawdę dobry pomysł.

Po pierwsze, serwisy mające dostęp do naszej lokalizacji i udostępniające nasze miejsce pobytu zdradzają nasze miejsce zamieszkania, co jest szczególnie niebezpieczne w wypadku dzieci nawiązujących kontakty z obcymi ludźmi przez internet. Po drugie, jeśli za pomocą portalu społecznościowego „meldujemy się" w danym miejscu innym niż nasz dom (niektórzy udostępniają nawet fakt wyjazdu na wakacje), niesie to ze sobą ryzyko wykorzystania tej informacji przez potencjalnych złodziei. Po trzecie, jeśli do informacji o miejscu przebywania dodamy pokusę pochwalenia się nowym nabytkiem, może to dodatkowo zachęcić złodziei do odwiedzenia naszego mieszkania.

Jaki korzystać z aplikacji umożliwiających „meldowanie się"?

- Jeżeli już musisz, melduj się tylko za pomocą serwisów udostępniających informacje jedynie niewielkiemu i zamkniętemu gronu znajomych.

- Nie włączaj funkcji geolokalizacyjnych dostępnych w serwisach Facebook, Instagram, Twitter i Snapchat.
- Nie informuj innych o dłuższych wyjazdach, np. na wakacje.

Udostępnianie danych

Czy tego chcemy, czy nie, jedną z głównych funkcji TIK, w tym sieci internetowej, jest przetwarzanie ogromnej ilości danych. Każdy z nas może zadbać o to, by poprawić ochronę swojej prywatności i własnych danych osobowych.

Wiele podmiotów i instytucji prowadzi różne działania edukacyjne, informacyjne i szkoleniowe w zakresie bezpiecznego korzystania z internetu, mimo to, według badań Biura Generalnego Inspektora Ochrony Danych Osobowych (GIODO), zaledwie niecała połowa spośród wszystkich badanych uczniów (45%) słyszała o tym, w jaki sposób chronić swoje dane osobowe i prywatność w internecie. Większość z nich dowiedziała się o tym na zajęciach w szkole od nauczycieli informatyki, wychowawców, pedagogów szkolnych lub osób z zewnątrz przeprowadzających szkolenia. Drugim źródłem informacji o zabezpieczaniu danych osobistych byli rodzice. Nieliczne osoby wskazywały również inne źródła pozyskiwania wiedzy i informacji, np. artykuły w internecie oraz w innych środkach przekazu.

Jak chronić swoją prywatność i dane osobowe?

1. **Przeglądanie stron internetowych**

   Wśród najpopularniejszych przeglądarek: Mozilla Firefox, Google Chrome, Internet Explorer, Safari i Opera. Największą gwarancję prywatności daje Firefox. Trudno „przemycić" w nim dodatki śledzące użytkowników. Oprócz wyboru przeglądarki w zabezpieczeniu naszej prywatności pomoże dostosowanie ustawień przeglądarki. Nawet te mniej przyjazne dla prywatności umożliwiają np. zmianę ustawień związanych z instalacją ciasteczek. Następnym krokiem jest zainstalowanie wtyczek do przeglądarki (np. AdBlock Plus – odpowiada za blokowanie reklam, Ghostery – pokazuje i blokuje skrypty śledzące funkcjonujące na danej stronie internetowej, Flashblock – pomaga kontrolować odpalanie dodatków typu flash, i in.)

   „Ustawienie w przeglądarce blokowania wszystkich ciasteczek spowoduje utrudnienia w korzystaniu z niektórych stron internetowych, zwłaszcza wymagających logowania (np. poczta, bank). Warto zatem skorzystać z możliwości dodania wybranych adresów do wyjątków. Witryny będą wtedy mogły zapisywać ciasteczka na danym urządzeniu" (Prywatność…, b.r.).

2. **Wyszukiwanie informacji w internecie**

   Wyszukiwarki takie jak Google Search i Bing (Microsoft), mimo że najpopularniejsze na świecie, a może właśnie dlatego, wcale nie gwarantują ochrony prywatności. Zbierają dane na podstawie historii wyszukiwania. Z jednej strony może to być wygodne,

bo otrzymujemy wyniki dopasowane do naszych preferencji, z drugiej jednak takie filtrowanie ogranicza dostęp do wiedzy i kultury, a nawet prowadzi do dyskryminacji w dostępie do usług.

Wyjściem z tej sytuacji jest zmiana przeglądarki, np. na DuckDuckGo. Nie przechowuje ona żadnych informacji o swoich użytkownikach i nie przekazuje informacji o wyszukiwanych frazach podmiotom trzecim. Podobnie działa StartPage, która bazuje na mechanizmie wyszukiwania Google, ale nie przekazuje danych dalej.

3. **Poczta elektroniczna**

Korzystamy z niej przez przeglądarkę internetową oraz przez klienta pocztowego (wyższy poziom ochrony). Pierwszy sposób wymaga odpowiedniego wyboru i konfiguracji przeglądarki internetowej (patrz pkt 1). Jednak najistotniejszy jest „wybór dostawcy poczty – należy szukać takiego, który szanuje prywatność swoich użytkowników. Najwyższy stopień ochrony zapewnia jednak szyfrowanie poczty" (Prywatność…, b.r.).

4. **Rozmowy przez internet**

W dzisiejszym świecie e-mail powoli jest wypierany przez szybszą formę komunikacji – czat. Popularny Skype czy Google Talk nie zapewniają nam żadnej ochrony danych. Natomiast Jabber w połączeniu z protokołem kryptograficznym OTR daje wystarczającą ochronę prywatności. Aby móc z niego korzystać, trzeba „zainstalować jedną z aplikacji, które go obsługują, np. Pidgin, Adium, Xabber. Do obsługi wideoczatów można wykorzystać aplikację Jitsi.

5. **Wysyłanie SMS-ów**

Aplikacja TextSecure pozwala na szyfrowanie treści przesyłanych wiadomości tekstowych. Jest dostępna dla użytkowników smartfonów. Jednak właściciele zwykłych telefonów komórkowych również bez tej aplikacji mogą czuć się bardziej bezpieczni – ponoszą znacznie mniejsze straty w prywatności niż użytkownicy smartfonów.

Dostęp do treści zawierających przemoc i seks

Wśród jednych z najpoważniejszych zagrożeń, jakie internet niesie młodym ludziom, jest ekspozycja na szkodliwe treści. Internet jest pełen materiałów nieodpowiednich dla dzieci i młodzieży. Przemoc, pornografia, wulgaryzacja treści oraz akty pełne nienawiści i agresji pozostają dostępne dla wszystkich użytkowników, a nawet jeśli na stronach internetowych pojawiają się jakieś obostrzenia, to z łatwością można je obejść. Niebezpieczne są również treści promujące zachowania autodestrukcyjne, takie jak samookaleczenia, anoreksja, oraz przedstawiające różne zachowania antyspołeczne w pozytywnym świetle.

Ryzyko mogą nieść również takie instrumenty TIK (w tym gry i aplikacje komputerowe i mobilne), które przedstawiają bohaterów mających atrybuty antyspołeczne, np. są

przemocowi, wulgarni lub stanowią w inny sposób negatywne wzorce. Szczególnie niebezpieczne są sytuacje, kiedy dziecko wciela się w rolę postaci tego typu i przejmuje jego cechy. Zagrożenia tworzą również takie narzędzia TIK, które zawierają treści nieprawdziwe, podtrzymujące szkodliwe stereotypy lub zachowania antyspołeczne.

Jak czytamy w materiałach zamieszczonych na stronie Cyfrowej Wyprawki, „szacuje się, że 30% treści dostępnych w internecie ma charakter pornograficzny. Oglądane są one nie tylko za pomocą komputerów, ale też np. smartfonów (ocenia się, że 1 na 5 tego rodzaju urządzeń wykorzystywane jest do takiego celu).

Treści pornograficzne są w dużej części tworzone i dystrybuowane zgodnie z polskim prawem i adresowane do osób pełnoletnich, ale jest to ograniczenie czysto teoretyczne. W praktyce niemal każdy – także poniżej tej granicy wieku – prędzej lub później, celowo czy przypadkiem, zetknie się z takimi treściami. Dotyczy to również młodzieży. Badania przeprowadzone przez Fundację Dzieci Niczyje na trzytysięcznej próbie nastolatków w wieku od 15 do 19 lat pokazują, że młodzi mają bardzo zróżnicowane doświadczenia i stosunek do pornografii. Różnice rysują się również między częstotliwością sięgania po pornografię przez chłopców i dziewczęta (przynajmniej według deklaracji). Wśród 67% badanych osób, które zetknęło się z pornografią, 20% dziewcząt i 66% chłopców sięgnęło po nią celowo w ciągu ostatnich 30 dni. Z tej liczby 14% chłopców oglądało treści pornograficzne powyżej 30 razy w ciągu jednego miesiąca”.

Jednym ze sposobów ograniczania dostępu młodych ludzi do treści zawierających przemoc i seks są rozwiązania techniczne polegające na filtrowaniu i blokowaniu treści na urządzeniach lub przez dostawców internetu. Niestety, nie ma wśród nich rozwiązań idealnych, każde ma w jakimś stopniu ograniczoną skuteczność. Mechanizmy te mogą działać wybiórczo lub nawet ograniczać dostęp do wielu innych stron, niekoniecznie zawierających niepożądane treści, ale np. omawiających wyniki badań lub prezentujących sposoby radzenia sobie z zagrożeniami. Dla mających nieco większą wiedzę nastolatków nie jest problemem ominięcie zabezpieczeń bądź też korzystanie z pornografii za pomocą innego, niezabezpieczonego sprzętu lub łącza internetowego.

Agresja online – cyberbullying

Cyberprzemoc (ang. *cyberbullying*) zdefiniować można najkrócej jako przemoc z użyciem TIK. Odnosi się on szczególnie do przemocy rówieśniczej z użyciem telefonów komórkowych lub internetu. Podstawowe formy cyberprzemocy to:

- nękanie, straszenie, szantażowanie z użyciem sieci,
- publikowanie w internecie lub rozsyłanie, np. przy użyciu telefonu komórkowego, ośmieszających, kompromitujących informacji, zdjęć, filmów,
- podszywanie się w sieci pod cudzą tożsamość.

Sprawcy cyberprzemocy wykorzystują m.in: pocztę elektroniczną, czaty, komunikatory, strony internetowe, blogi, serwisy społecznościowe, grupy dyskusyjne, telefony komórkowe,

serwisy SMS i MMS. Sprzyja temu poczucie wysokiego poziomu anonimowości w sieci. Poza tym w takich działaniach nie ma znaczenia siła fizyczna, a przewagę nad ofiarą daje biegłość, z jaką sprawca posługuje się nowoczesnymi technologiami komunikacyjnymi.

Charakterystyczna dla cyberbullingu jest również szybkość rozpowszechniania materiałów kierowanych przeciwko ofierze, ich powszechna dostępność w sieci, wielokrotnie powielanie oraz to,że ich całkowite usunięcie jest zazwyczaj niemożliwe. Ponieważ cyberprzemoc nie zostawia widocznych śladów, zjawisko to jest mniej kontrolowane przez rodziców lub nauczycieli w porównaniu z przemocą klasyczną. Przeszkodą w przeciwdziałaniu cyberprzemocy przez dorosłych może być również słaba znajomość specyfiki mediów elektronicznych oraz częste bagatelizowanie problemu (*Stop…*, 2012).

Formy cyberprzemocy

- nagrywanie, upublicznianie, rozsyłanie zdjęć, materiałów filmowych ośmieszających ofiarę, zawierających treści zarejestrowane wbrew jej woli, np. nagranie, na którym ktoś przebiera się w szatni przed zajęciami WF;

- wysyłanie ofierze wiadomości SMS, e-maili, wiadomości na czacie internetowym, na forum dyskusyjnym, przez komunikator internetowy zawierające wulgarne, złośliwe, obraźliwe, poniżające treści lub groźby;

- dodawanie wulgarnych, obraźliwych komentarzy pod materiałami zamieszczonymi przez ofiarę, np. na jej profilu na portalu społecznościowym (hejty);

- podawanie się za kogoś w internecie, rozsyłanie innym w czyimś imieniu złośliwych, obraźliwych wiadomości, tworzenie pod czyimś imieniem fałszywych profili na portalach społecznościowych, blogach i umieszczanie tam ośmieszających ofiarę treści;

- włamania na konta e-mailowe, profile na blogu, portalu społecznościowym, na konto w grze internetowej (stworzenie którego mogło wiązać się zainwestowaniem pewnej sumy realnych pieniędzy);

- wykluczenie danej osoby z grupy utworzonej w internecie, np. wyłącznie kogoś z grupy klasowej na portalu społecznościowym (Iwan, 2016: 10).

Jak już wspomnieliśmy, z powodu braku widocznych śladów cyberprzemocy trudno jest z nią walczyć. Niezwykle ważne jednak jest uświadamianie dzieci i młodzieży, że takie zachowanie w sieci krzywdzi innych. Może prowadzić do bardzo poważnych konsekwencji, nie tylko dla ofiary, ale również sprawcy, który nie jest bezkarny i można go wykryć. Należy jak najczęściej rozmawiać na ten temat z młodymi ludźmi, tworzyć atmosferę zaufania, tak żeby nie bali się prosić dorosłych o pomoc, jeśli staną się ofiarami cyberprzemocy. Powinni wiedzieć, że zawsze mogą też zadzwonić do telefonu zaufania dla dzieci i młodzieży 116 111 (połączenie bezpłatne) albo napisać wiadomość na stronie 116111.pl. Również rodzice i nauczyciele

mogą szukać pomocy specjalistów w sprawie bezpieczeństwa dzieci pod numerem telefonu 800 100 100.

Seksting

Terminem seksting (ang. sexting) powstałym z połączenia słów „sex" oraz „texting" określamy zjawisko przesyłania między użytkownikami telefonów komórkowych wiadomości tekstowych o charakterze seksualnym oraz zdjęć lub filmów przedstawiających nagie lub półnagie zdjęcia nadawców. Seksting nie dotyczy jedynie dzieci i młodzieży, jednak to w tej grupie wiekowej stanowi najpoważniejsze zagrożenie. Konsekwencją sekstingu bywa upublicznienie zdjęć i filmów bez zgody ich autorów, a prezentujące się na nich osoby stają się obiektem cyberprzemocy ze strony rówieśników.

Według badań przeprowadzonych we wrześniu 2014 przez agencję GfK Polonia na zlecenie Fundacji Dzieci Niczyje (metoda CAWI – wywiad internetowy, próba ogólnopolska, N=503, wiek 15-18 lat). Znacząca większość (58%) ankietowanych odpowiedziała twierdząco na pytanie: „Czy zdarza się, że twoi znajomi przesyłają sobie za pomocą telefonu lub internetu zdjęcia lub filmy przedstawiające ich nago lub prawie nago?". Ponad jedna trzecia (34%) przyznała, że otrzymała kiedykolwiek takie materiały. Natomiast 11% zadeklarowało, że wysyłało takie zdjęcia lub filmy samemu. Oznacza to, że zjawisko jest silnie obecne wśród młodych ludzi w Polsce.

O głośnych przypadkach sekstingu czytamy na stronie internetowej Fundacji Dzieci Niczyje poświęconej temu zjawisku:

> „Specyfikę sekstingu przybliżają m.in. doniesienia medialne. Spośród wielu innych przypadków sekstingu opisywanych przez prasę na całym świecie niewątpliwie najgłośniejsza jest historia Amandy Todd. Niespełna 16-letnia Kanadyjka poznała na wideoczacie mężczyznę, który namówił ją do pokazania przed kamerą piersi, a następnie szantażował i prześladował domagając się kolejnych pokazów. Gdy zdjęcia trafiły do sieci dziewczyna przeszła załamanie nerwowe i depresję. Po nieudanej próbie samobójczej opublikowała w serwisie YouTube dramatyczny film, w którym na kolejno pokazywanych kartkach opisała swoją historię, co tylko wzmogło ataki rówieśników pod jej adresem. Niedługo później Amanda Todd odebrała sobie życie.
>
> Polskie media w 2006 roku obiegła historia 14-letniej dziewczyny z podtoruńskiej Chełmży, która zrobiła sobie w domu nagie zdjęcia i wysłała je przez komunikator Gadu-Gadu do 22-letniego chłopaka z intencją zawarcia bliższej znajomości. Ten, wraz z kolegami, upublicznił zdjęcia, które po krótkim czasie krążyły między telefonami komórkowymi uczniów chełmżyńskich szkół. Sprawa zrobiła się głośna, kiedy trzech sprawców rozsyłania fotografii 14-latki skazano na kary pozbawienia wolności".

Symptomatyczne dla zjawiska sekstingu jest to, że młodzież nie ma większych oporów przed udostępnianiem innym osobom swoich intymnych zdjęć, traktując to jako sposób np. na nawiązanie nowej relacji. Przesłanie zdjęcia staje się często wstępnym warunkiem

do dalszych kontaktów, w tym ewentualnego spotkania. Należy pamiętać, że nierzadko przesyłanie materiałów o charakterze seksualnym jest jednak wymuszane przez odbiorcę i towarzyszy jej nękanie, prześladowanie oraz inne formy cyberprzemocy.

Spam, scam i phishing

Spam to niechciane wiadomości. Mimo że najczęściej kojarzy się z pocztą elektroniczną, jest nagminnym zjawiskiem również na portalach społecznościowych, a właściwie w każdym rodzaju komunikacji internetowej. Spam to nie tylko zapychanie skrzynek e-mailowych. Stanowi prawie 90% całej korespondencji w sieci, co prowadzi do olbrzymiego jej obciążenia. W interesie wszystkich internautów jest nie tylko obrona przed spamem własnej skrzynki, ale także minimalizowanie jego ilości.

Jak zabezpieczyć się przed spamem:

- Używaj niestandardowej nazwy użytkownika.
- Unikaj publikowania adresu e-mailowego w formie tekstowej.
- Jeżeli chcesz aby adres e-mailowy był upubliczniony, ukrywaj go przed robotami oraz zabezpieczaj.
- Do rejestracji w serwisach o wątpliwej reputacji lub w czasie zakupów internetowych użyj jednorazowych adresów e-mailowych (np. korzystając z Temp-Mail.org).
- Na własnych serwisach WWW podawaj tylko adresy zabezpieczone przed robotami kodem JavaScript.
- Nie klikaj w odnośniki w spamie, może spowodować to zapisanie adresu do jeszcze większej liczby list.
- Unikaj wchodzenia na niezaufane strony i podawania swojego adresu, jeżeli nie jest to koniecznie.
- Nie otwieraj podejrzanych załączników, wiadomości łańcuszków, reklam itp.

Scam to ogólnie naciąganie lub wyłudzenie. Najczęściej użytkownicy otrzymują wiadomość o otrzymaniu spadku lub nagrody pod warunkiem wpłacenia pewnej sumy. Mogą być to też próby oszustwa przy płatności za przedmioty na aukcjach. Na Facebooku może wyglądać to tak, że zainfekowane konto rozsyła automatycznie spam do znajomych z linkiem do strony, która będzie próbować wyłudzić nasz login i hasło (formularz logowania często jest bardzo podobny do prawdziwej strony Facebooka). Wiele tego typu oszustw obiecuje korzyści finansowe, obejrzenie kontrowersyjnych materiałów lub sugeruje, że np. nasze zdjęcia zostały umieszczone w sieci.

Phishing (spoofing) – metoda oszustwa, w której przestępca, podszywając się pod inną osobę lub instytucję, próbuje wyłudzić określone informacje lub nakłonić ofiarę do określonych działań. Jest to rodzaj ataku wykorzystujący naszą nieuwagę, zaufanie do danej instytucji i często odruchowe działania.

Jak chronić się przed phishingiem:

- Nie ufaj wiadomościom z prośbą o odwiedzenie i zalogowanie się na stronie internetowej. Zarówno banki, jak i instytucje finansowe nie wysyłają listów z prośbą o uzupełnienie danych.

- Nie otwieraj odnośników (hiperłączy) bezpośrednio z otrzymanej wiadomości e-mail. Linki mogą kierować do innej strony, niż to sugerują.

- Pamiętaj o regularnych aktualizacjach systemu i zainstalowanych na nim programach, szczególnie poczty e-mailowej oraz przeglądarek internetowych.

- Pod żadnym pozorem nie wolno przesyłać haseł i loginów, numerów kart kredytowych oraz innych danych. Wszelkie prośby o podanie danych należy traktować jako potencjalne zagrożenie i zgłosić odpowiednim osobom.

- Instytucje finansowe oraz banki stosują protokół HTTPS na każdej stronie wymagającej logowania. Jeśli strona logowania nie zawiera w adresie nazwy

protokołu HTTPS, powinno zgłosić się to pracownikom banku i w żadnym wypadku nie należy wypełniać formularza z danymi.

- Nie należy korzystać ze starych przeglądarek internetowych. Są one narażone na różnego rodzaju błędy i mogą być celem ataku.

Polityka prywatności na portalach społecznościowych

Dziś już powszechnie wiadomo, a przynajmniej tak powinno być, że informacja opublikowana w internecie pozostaje tam na zawsze. Ma to więc wpływ na wizerunek każdego użytkownika zarówno teraz, jak i w przyszłości. Wszystkie udostępniane w portalach społecznościowych materiały: wpisy, zdjęcia, filmy itp., są oglądane przez wielu ludzi, np. przyszłych pracodawców lub cyberprzestępców, i mogą zostać użyte przeciwko osobom je publikującym.

Co prawda istnieje możliwość ograniczenia takiego ryzyka przez wybranie odpowiednich ustawień prywatności na portalu, jednak to nie wystarczy. Korzystanie z niemal każdego portalu społecznościowego pociąga za sobą techniczną możliwość szerokiego udostępniania informacji. Nigdy nie ma pewności, że np. osoby z grona znajomych nie wykorzystają danych bez zgody użytkownika. Poza tym, mimo najbardziej restrykcyjnych ustawień prywatności, do wszystkich danych umieszczanych na portalu zawsze mają dostęp firma zarządzająca portalem i jej pracownicy. Trzeba też pamiętać, że przy zakładaniu konta na portalu każdy akceptuje jego regulamin i godzi się na wszystko, co jest w nim napisane. Przykładowo Facebook żąda udzielenia bezpłatnej licencji na korzystanie ze zdjęć użytkowników.

Co można zrobić, żeby móc korzystać z serwisów społecznościowych i zbytnio nie ucierpieć? Poniżej przedstawiamy zasady, o których warto pamiętać, zakładając konto na każdym portalu.

1. Zacznij od wybrania ustawień prywatności i bezpieczeństwa, wybierz złożone/unikatowe hasła dla konta.
2. Bądź ostrożny podczas instalacji aplikacji innych firm. Nie instaluj aplikacji ze źródeł, którym nie ufasz.
3. Przyjmuj zaproszenia wyłącznie od ludzi, których znasz.
4. Zapoznaj się uważnie z polityką prywatności i warunkami korzystania z usługi. Ogranicz ilość informacji osobistych, do których usługa może mieć dostęp.
5. Pisz i publikuj odpowiedzialnie. Zawsze pamiętaj, że wszystkie informacje, zdjęcia, filmy staną się publiczne (Prujszczyk, Śliwowski, 2010: 23).

Nie każdy użytkownik portali, zwłaszcza początkujący, wie, jakie informacje są gromadzone przez firmy zarządzające serwisami, jakie mogą być konsekwencje użytkowania kont oraz jak zadbać o swoje bezpieczeństwo. W tabeli zestawione zostały najważniejsze informacje na ten temat dotyczące Facebooka (Tab. 1).

Tab. 1. Jakie dane zbiera Facebook i jak sobie z tym radzić? (na podst. Niedyskretny profil, b.r.)

Jakie informacje zbiera?	Jakie są konsekwencje?	Jak możesz się chronić?
Dane podawane przy tworzeniu konta i aktualizacji profilu.	Dane profilowe ułatwiają wyszukanie cię, ale też profilowanie przez portal i firmy reklamowe.	Zadbaj o ustawienia prywatności i nie udostępniaj treści, które chcesz chronić.
Udostępniane zdjęcia, filmy, statusy (nawet nieopublikowane).	Nawet treści udostępnione tylko znajomym mogą być przekazane dalej, np. Facebook użyje twojego zdjęcia do polecania produktów.	Zadbaj o ustawienia prywatności i nie udostępniaj treści, które chcesz chronić.
Profile, statusy i zdjęcia, które „lubisz”.	Na podstawie lajków można określić twoją orientację seksualną lub wyznanie, choć ich nie ujawniasz.	Informacje o tym, co „polubiasz”, są zbierane i przetwarzane. Zamiast śledzenia na Facebooku, korzystaj z kanałów RSS.
Informacje o znajomych i dane z książki adresowej.	Facebook zbiera informacje nawet o osobach, które nie mają konta, tworzy im profile-cienie.	Nie udostępniaj listy kontaktów, nie publikuj informacji o innych bez ich zgody.
Informacje zbierane przez aplikacje mobilne.	Korzystanie ze smartfona pozwala portalom zbierać dodatkowe informacje i cię lokalizować.	Nie korzystaj z portali społecznościowych przez aplikacje, tylko za pomocą przeglądarek.
To, jakie strony odwiedzasz, i co na nich robisz.	Historia odwiedzanych stron mówi bardzo dużo, nawet to, czego nie chcesz ujawnić.	Blokuj śledzenie na stronach z przyciskami społecznościowymi (np. Disconnect). Nie loguj się przez konta społecznościowe do innych usług.
Dane, jak często, jak długo i za pomocą jakich urządzeń korzystasz z portalu.	Informacje techniczne pozwalają odróżnić cię od innych i analizować twoje działania.	Nie masz na to wpływu, chyba że zrezygnujesz z portali społecznościowych.

Prawa i obowiązki w internecie

(za: Ins@fe. Elementarz dla rodziców)

Prawa w internecie

- Mam prawo czuć się bezpiecznie w sieci.
- Mam prawo do współtworzenia internetu.
- Mam prawo do wyrażania w sieci własnych poglądów i opinii.
- Mam prawo do ochrony własnego wizerunku w internecie.
- Moje dane podlegają ochronie danych osobowych.
- Mam prawo do korzystania z rzetelnych źródeł informacji.
- Mogę pobierać programy z otwartą licencją, słuchać udostępnionej muzyki, oglądać legalne filmy.
- Mam prawo do poszerzania swojej wiedzy poprzez korzystanie z gier edukacyjnych, portali tematycznych i kursów online.
- Mam prawo do rozrywki w sieci.
- Mam prawo do komunikowania się z innymi internautami.

Obowiązki w internecie

- Szanuję innych użytkowników internetu i traktuję ich tak, jak chcę, żeby oni traktowali mnie.
- Przestrzegam praw autorskich.
- Nie używam internetu, aby szkodzić innym.
- Korzystam z internetu z rozwagą i ostrożnością.
- Mam obowiązek stosowania zasady ograniczonego zaufania wobec ludzi poznanych w sieci oraz informacji w niej znalezionych.
- Nie używam internetu, aby kraść.
- Nie używam internetu do oszukiwania, nie wprowadzam innych w błąd, dbam, żeby w internecie było jak najwięcej prawdziwych informacji.
- Mam obowiązek zachowania kultury w swoich wypowiedziach w sieci.
- Mam obowiązek brać odpowiedzialność za swoje działania w internecie.
- Mam obowiązek informować dorosłych o tym, co mnie zaniepokoi w internecie.

Wskazówki metodyczne

Strategie uczenia o bezpieczeństwie w użytkowaniu TIK

Kodeks TIK
(oprac. na podstawie Zasady…, 2013)

Jedną ze strategii uczenia o bezpiecznym korzystaniu z TIK jest stworzenie reguł, które obowiązują w szkole zarówno uczniów, jak i nauczycieli. Jest to Kodeks TIK. Bardzo ważne jest, by te zasady były wypracowane wspólnie z uczniami i odpowiadały zarówno na potrzeby uczniów, jak i nauczycieli. Kodeks powinien być użyteczny i powszechnie stosowany w praktyce szkolnej.

Kodeks TIK w szkole porządkuje sposób korzystania z technologii informacyjno-komunikacyjnych w nauczaniu i uczeniu się. Jego zadaniem jest wyjaśnienie, w jaki sposób komputer, internet, telefon komórkowy itp. mogą pomóc mądrej edukacji.

Kodeks można opracować na dwa sposoby:

1. Nauczyciele w poszczególnych klasach wraz z uczniami przygotowują projekty całego kodeksu. Później propozycje są przedstawiane innym w ogólnodostępnej formie tak, aby można było je poznać i uzgodnić wspólną wersję.

2. Nauczyciele dzielą się zagadnieniami i razem z uczniami tworzą części kodeksu, które potem są omawiane, weryfikowane i łączone w całość. To zadanie można też podzielić w klasie: zespoły uczniów pracują nad całym kodeksem albo dzielą się między sobą poszczególnymi obszarami.

Praca nad kodeksem może odbywać się na godzinie wychowawczej, na lekcji informatyki lub w ramach zajęć dodatkowych albo podczas realizacji projektu uczniowskiego.

Oto propozycje zagadnień, które warto uwzględnić w kodeksie TIK. Opierają się one na doświadczeniach programu Szkoła z klasą 2.0 (Pacewicz i in., b.r.).

1. Ucz i ucz się z TIK, czyli jak sensownie wykorzystać TIK w szkole i w domu dla uczenia się?

2. Z informacji korzystaj samodzielnie i krytycznie, czyli do czego i w jaki sposób wykorzystywać zasoby internetu?

3. Nie kradnij i nie daj się okraść, czyli jak zgodnie z prawem korzystać z materiałów dostępnych w sieci?

4. Komunikujmy się, czyli jak używać TIK do komunikacji w szkole i z rodzicami?

5. Komputery pod ręką, czyli jak zapewnić dostępność komputerów i sieci w szkole, zamiast zamykać je w pracowni komputerowej?

6. Bądź bezpieczny w sieci, czyli jak postępować, aby chronić swoje dane i siebie w internecie?

7. Naucz tego innych, czyli w jaki sposób uczniowie przy wsparciu nauczycieli mogą szkolić w zakresie TIK innych, np. swoje koleżanki i kolegów, rodziców, dziadków lub sąsiadów?

Po rozważeniu powyższych zagadnień z wniosków można stworzyć Kodeks TIK i sprawić, że TIK w szkole i w domu będą użyteczne, dobrze wykorzystane i bezpieczne. Szkolny kodeks nie może być przeładowany, wystarczy kilka punktów, np.

1. Uczniowie w naszej szkole zawsze zaznaczają, skąd pochodzi materiał, który pobrali z internetu i kto jest jego autorem.

2. Telefony komórkowe uczniów i nauczyciela mogą być wykorzystane tylko wówczas, gdy pomogą w uczeniu się.

3. Nauczyciele w naszej szkole proponują uczniom korzystanie z internetowych narzędzi i zasobów – programów, stron, filmów itp. – ułatwiających uczenie się. Chętnie korzystają z pomysłów uczniów, jak stosować na lekcjach nowe technologie.

4. W naszej szkole dążymy do tego, by ze sprzętu komputerowego korzystali nauczyciele wszystkich przedmiotów.

5. Uczniowie naszej szkoły organizują i prowadzą zajęcia z TIK dla dorosłych. Uczą korzystania z internetu chętnych rodziców, dziadków, sąsiadów.

6. Uczniowie korzystają ze szkolnych komputerów w czasie przerw, podczas „okienek” i po lekcjach zgodnie z regulaminem. (Uwaga! Powinien on określać m.in., kto odpowiada za jego przestrzeganie i za sprzęt).

Warsztaty

Podczas warsztatów uczniowie mogą bezpośrednio doświadczać różnych sytuacji. Nie są skrępowani sztywnymi ramami zajęć szkolnych. Wcielają się w różne role. Mogą niejako na własnej skórze doświadczyć, jak czują się ofiary cyberprzemocy, jak łatwo ukraść komuś lub im samym hasło lub wizerunek, a przede wszystkim uświadomić sobie, że w internecie nic nie ginie, zostaje tam na zawsze. Jest to skuteczna forma propagowania bezpiecznego posługiwania się narzędziami TIK.

Do przeprowadzenia warsztatów warto zaprosić instytucje lub osoby z zewnątrz: stowarzyszenia, fundacje, psychologów lub edukatorów, którzy zajmują się tematem

bezpieczeństwa w sieci. Informacje na temat oferty szkoleń i warsztatów można szukać na stronach:

- wojewódzkich bądź gminnych ośrodków szkolenia nauczycieli,
- lokalnych poradni psychologiczno-pedagogicznych,
- bibliotek publicznych,
- organizacji pozarządowych (bazy.ngo.pl),
- poradni psychologicznych zajmujących się współpracą z jednostkami edukacyjnymi.

Kampanie społeczne i… internet

We współczesnym świecie do młodych ludzi bardziej przemawia obraz niż tekst lub wykład. Dlatego warto zainteresować uczniów kampaniami społecznymi propagującymi bezpieczne korzystanie z internetu i innych narzędzi TIK. Można ich zachęcić do tego, żeby sami zorganizowali taką kampanię, np. na terenie szkoły lub we współpracy z innymi szkołami. Można np. wykonać plakaty, nakręcić teledysk lub film i umieścić je na stronie internetowej szkoły. Oto kilka przykładów kampanii, które mogą być inspiracją:

Przytul hejtera
Kampania społeczna przeciwko przemocy werbalnej w internecie. Jej celem jest uświadomienie młodzieży szkodliwości internetowego hejtu i mowy nienawiści, a także zaprezentowanie metod reagowania na te zjawiska.

Myślę, więc nie ślę
Kampania pod hasłem „Myślę, więc nie ślę" ma na celu edukowanie na temat niebezpieczeństw związanych z sekstingiem oraz podniesienie świadomości społecznej wokół tego zjawiska.

Każdy ruch w internecie zostawia ślad
Nikt w sieci nie jest anonimowy. Każdy ruch w internecie zostawia ślad. Jedynie kwestią zaangażowanych środków jest zidentyfikowanie osoby, która popełniła w sieci przestępstwo.

Nigdy nie wiadomo kto jest po drugiej stronie
Akcja poświęcona została problemowi uwodzenia dzieci w internecie i rozpoczęła w Polsce dyskusję na temat tego problemu.
(źródło: Fundacja Dzieci Niczyje/Fundacja Dajemy Dzieciom Siłę)

Dzień Bezpiecznego Internetu **(DBI)**
DBI obchodzony jest w lutym w wielu krajach na świecie. Inicjatywa ta ma na celu przede wszystkim inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych, zaznajomienie rodziców, nauczycieli i wychowawców z problematyką bezpieczeństwa online oraz promocję pozytywnego wykorzystywania internetu (źródło: SaferInternet.pl).

Oprócz kampanii społecznościowych ważnym źródłem informacji o bezpieczeństwie w internecie jest sam internet. To naturalne środowisko uczniów, więc należy wskazać im tylko kierunek, by sami zdobyli potrzebną wiedzę. Można polecić im serwisy internetowe, strony na Facebooku albo zachęcić do obejrzenia filmów na YouTubie. Poniżej przedstawiamy kilka propozycji:

serwisy

Klikaj bezpiecznie
Niebezpiecznik
SaferInternet
Dyżurnet

YouTube

Bezpieczeństwo w sieci
Bezpieczeństwo w sieci / Portale społecznościowe – zasady, wskazówki, porady
Baw się w Sieci – bezpiecznie
W sieci
Dodaj znajomego
Nie hejtuj
Odwaga ratuje życie – Nie hejtuj, a nie będziesz hejtowany!

strona na Facebooku Stop naciągaczom

Scenariusze lekcji

Przykład 1
(oprac. na podstawie scenariusza Izabeli Meyzy, ABC…, b.r.)

Temat: ABC bezpieczeństwa w internecie

Klasy IV–VI szkoły podstawowej

Czas zajęć: 45 minut

Cele operacyjne

Uczniowie:

- znają różnicę między komunikacją prywatną i publiczną w sieci i poza nią;
- potrafią wskazać zagrożenia związane z korzystaniem z internetu w telefonach komórkowych i innych urządzeniach;
- wiedzą, jakich zasad należy przestrzegać, żeby się przed tymi zagrożeniami chronić.

Metody nauczania i formy pracy

- rozmowa kierowana, burza mózgów,
- praca indywidualna, w grupach, w parach.

Potrzebne materiały

małe karteczki, długopisy, karta pracy „Bezpieczeństwo w sieci", tablica i kreda lub papier i marker

Przebieg

Nauczyciel wprowadza uczniów w tematykę zajęć (1 minuta).

Mówi, że dowiedzą się, co dzieje się z informacjami, które zamieszczają w internecie, poznają podstawowe zasady bezpieczeństwa w sieci i zastanowią się, jak można się chronić przed zagrożeniami, które niesie użytkowanie internetu.

Ćwiczenie 1 (10 minut)

Nauczyciel rozdaje uczniom małe karteczki i prosi, żeby przypomnieli sobie jakąś informację dotyczącą każdego z nich, którą ostatnio zamieścili w internecie, a następnie zapisali ją na karteczce. Jeśli umieścili zdjęcie, mogą krótko napisać, co dokładnie przedstawia. Następnie nauczyciel prosi, by uczniowie wyobrazili sobie, że ich karteczki są wywieszone np. na szkolnej tablicy ogłoszeń lub na głównym placu w mieście. Ważne, by stworzyć sugestywny obraz sytuacji, dlatego należy dać uczniom trochę czasu na uruchomienie wyobraźni. Po chwili nauczyciel wprowadza modyfikację: uczniowie mają pomyśleć, że kartki zostaną na tablicy ogłoszeń na zawsze, że ktoś będzie mógł je przeczytać nawet za pół wieku, np. ich dzieci, wnuki. Znów chwila na wyobrażenie sobie sytuacji.

Po zakończeniu doświadczenia nauczyciel prosi, żeby uczniowie schowali kartki do kieszeni lub odłożyli na bok. Zadaje pytania:

- Co czuliście, wyobrażając sobie, że karteczka z informacją o was wisi na szkolnej tablicy?
- Kto mógłby ją przeczytać? (Nakierowanie na to, że oprócz uczniów, nauczycieli i rodziców do szkoły mógłby wejść każdy i mieć dostęp do ich prywatnych informacji: refleksji, wiedzy o tym, co myślą i co akurat robią).
- Co mógłby z tą wiedzą o was zrobić?
- Co czuliście, wiedząc, że kartka zostanie na tablicy na zawsze?

Następnie nauczyciel wyjaśnia, że właśnie tak działają portale społecznościowe. To, co zamieszczamy na swoich profilach, może być widoczne dla innych: naszych znajomych i nieznajomych. Dodatkowo: to, co zamieszczamy w internecie, może zostać tam na zawsze. Nigdy nie wiemy, kto i jak może to wykorzystać.

Na koniec ćwiczenia prosi uczniów o ponowne wyciągnięcie kartek. Zadaje pytanie:

- Spójrzcie na te kartki raz jeszcze. Czy po tym ćwiczeniu zamieścilibyście takie zdjęcie lub taką informację o sobie?

Ćwiczenie 2 (10 minut)

Nauczyciel zapisuje na tablicy dwa hasła: KOMUNIKACJA PRYWATNA i KOMUNIKACJA PUBLICZNA. Wyjaśnia, że to, co piszemy na naszym profilu na portalu społecznościowym lub umieszczamy na tablicy szkolnej, można zaliczyć do komunikacji publicznej, a oprócz niej istnieje też komunikacja prywatna. Prosi uczniów o podanie przykładów obu rodzajów komunikacji i zapisuje je na tablicy pod hasłami. Podkreśla, że mogą podawać przykłady nie tylko z internetu.

Jeżeli nie padnie to od uczniów, należy koniecznie dopowiedzieć lub ich nakierować na to, że z komunikacją prywatną mamy do czynienia w wypadku korzystania z:

- listu,
- e-maila,
- prywatnych wiadomości na portalach społecznościowych,
- czatu i komunikatorów internetowych,
- telefonu (rozmowa, SMS).

Komunikacja publiczna obejmuje:

- korzystanie z forów internetowych,
- zamieszczanie informacji na blogach i portalach społecznościowych,
- dyskusję na forum klasy.

Trzeba też podkreślić, że w sieci i poza nią obowiązują podobne zasady, lecz istnieją też pewne różnice: w internecie nigdy nie wiemy, z kim rozmawiamy i kto czyta informacje o nas, bo zawsze ktoś się może podawać za kogoś innego. Poza tym informacje przekazywane w internecie są zapośredniczone (czyta je też administrator usługi). Zadaniem uczniów jest odpowiedź na pytanie:

- Z których sposobów komunikacji korzystacie najczęściej?

Po uzyskaniu odpowiedzi nauczyciel informuje, że za chwilę przyjrzymy się, jak dbać o bezpieczeństwo, komunikując się przez internet.

Ćwiczenie 3 (14 minut)

Klasa jest dzielona na cztery grupy i uczniowie otrzymują karty pracy „Bezpieczeństwo w sieci”. Pracują nad zagadnieniami, a następnie przedstawiają odpowiedzi na forum.

Ćwiczenie 4 (10 minut)

Nawiązując do poprzedniego ćwiczenia, nauczyciel proponuje wspólne stworzenie zasad bezpieczeństwa, których warto przestrzegać w sieci. Na tablicy zapisuje: „Kodeks bezpieczeństwa w internecie" i zadaje uczniom pytanie:

- Co możemy robić, żeby dbać o nasze bezpieczeństwo w sieci?

Zapisuje powstałe w czasie burzy mózgów propozycje uczniów. Jeśli będzie taka potrzeba, uzupełnia ich wypowiedzi.

Po stworzeniu „Kodeksu" uczniowie wybierają zasadę, która wydaje im się najważniejsza, i opowiadają sobie krótko w parach, dlaczego akurat ją wybrali.

Jako zadanie dodatkowe można uczniom zaproponować stworzenie ulotek i plakatów na temat bezpieczeństwa w sieci, które posłużą do zrobienia w szkole akcji społecznej dotyczącej tego tematu. Inną propozycją jest zrobienie ogólnoszkolnego konkursu na plakat związany z bezpieczeństwem w sieci.

Ewaluacja

Po zakończonych zajęciach należy upewnić się, że uczniowie:

- rozumieją, że zamieszczanie niektórych informacji o sobie w sieci może stanowić problem;
- potrafią podać przykłady komunikacji prywatnej i publicznej w sieci;
- znają sposoby dbania o bezpieczeństwo w sieci;
- wiedzą, że w sieci trzeba przestrzegać podobnych zasad bezpieczeństwa jak poza nią.

Przykład 2
(oprac. na podstawie scenariusza Weroniki Paszewskiej, Bezpieczna…, b.r.)

Temat: Bezpieczna komunikacja w sieci

Szkoła ponadpodstawowa

Czas zajęć: 45 minut

Cele operacyjne

Uczniowie:

- rozumieją, że dane przesyłane w sieci przechodzą przez wiele pośrednich urządzeń, które mogą mieć dostęp do ich treści i pozostają poza kontrolą użytkownika;

- rozumieją niebezpieczeństwa związane z logowaniem się do niezabezpieczonych sieci;
- wiedzą, że zachowanie prywatności i anonimowości w sieci jest bardzo trudne;
- potrafią podać przykłady narzędzi zwiększających bezpieczeństwo komunikacji w sieci;
- potrafią wyjaśnić korzyści, jakie daje HTTPS i TOR.

Metody nauczania i formy pracy

- rozmowa kierowana,
- praca w grupach.

Potrzebne materiały

nożyczki, instrukcja dla grup „Działanie sieci” i materiał pomocniczy „Sieć”, komputery z dostępem do internetu

Przebieg

Wprowadzenie (5 minut)

Nauczyciel przedstawia w metaforyczny sposób internet jako pocztę. Komunikat przesyłany w sieci można porównać do pocztówki, ale nie listu. Informacje, które wysyłamy, są dość łatwo dostępne dla innych. Na zajęciach uczniowie zapoznają się z funkcjonowaniem sieci i tym, jak informacje przepływają w sieci. Dowiedzą się, jakie informacje są dostępne w momencie logowania się do niezabezpieczonych sieci, do sieci TOR oraz przy wykorzystaniu protokołu HTTPS. Podczas ćwiczenia w grupie zobrazują przepływ informacji według trzech scenariuszy. Nauczyciel prosi uczniów o zwrócenie uwagi, jakie korzyści użytkownikom daje logowanie się do sieci za pomocą HTTPS czy TOR.

Ćwiczenie 1 (30 minut)

Nauczyciel dzieli klasę na minimum 8-osobowe grupy. Każdej grupie rozdaje jedną instrukcję „Działanie sieci” i materiał pomocniczy „Sieć”. Prosi uczniów o zapoznanie się z instrukcjami i wykonanie zadań. Monitoruje pracę grup i w razie potrzeby udziela wskazówek.

Uczniowie odgrywają scenki ukazujące, w jaki sposób przepływają informacje w sieci. Są to: logowanie się w sieci niezabezpieczonej, logowanie się z użyciem HTTPS oraz komunikacja w sieci TOR. Każdy osoba w grupie ma przypisaną rolę:

- użytkownika,
- oszusta,
- dostawcy łącza internetowego użytkownika,
- administratora systemu,
- policji w kraju użytkownika,

- dostawcy łącza internetowego serwera strony internetowej,
- administratora strony,
- policji w kraju dostawcy strony.

Podsumowanie

Nauczyciel zadaje uczniom pytania:

- Jakie dane ujawniamy, logując się do niezabezpieczonych sieci?
- Jakie dane są o nas niedostępne, kiedy logujemy się do sieci z użyciem TOR i HTTPS?
- Jakie korzyści daje HTTPS i TOR?

Podsumowując wykonane ćwiczenie z rozmowie z uczniami, nauczyciel zwraca uwagę, że TOR jest narzędziem, które umożliwia działania internautów, np. w krajach, gdzie nie ma wolności słowa i gdzie aktywizm polityczny jest brutalnie tłumiony. Natomiast HTTPS jest narzędziem, które powinno być używane wszędzie, gdzie mamy do czynienia z logowaniem, na przykład w bankowości internetowej i sklepach internetowych.

Ewaluacja

Po zakończonych zajęciach należy upewnić się, że uczniowie:

- rozumieją mechanizm przepływu danych w sieci;
- rozumieją niebezpieczeństwa związane z logowaniem się do niezabezpieczonych sieci;
- wiedzą, że zachowanie prywatności i anonimowości w sieci jest bardzo trudne;
- potrafią podać przykłady narzędzi zwiększających bezpieczeństwo komunikacji w sieci;
- potrafią wyjaśnić korzyści, jakie daje HTTPS i Tor.

Przykład 3
(oprac. na podstawie scenariusza Weroniki Paszewskiej, Kto nas…, b.r.)

Temat: Kto nas śledzi w sieci?

Szkoła ponadpodstawowa

Czas zajęć: 45 minut

Cele operacyjne

Uczniowie:

- wiedzą, że ich aktywność w sieci jest śledzona przez różne podmioty;
- potrafią sprawdzić za pomocą wtyczki do przeglądarki Lightbeam, kto zbiera na ich temat informacje, gdy odwiedzają strony internetowe;

- potrafią wymienić wtyczki do przeglądarek internetowych zwiększające prywatność w sieci i opisać ich działanie.

Metody nauczania i formy pracy

- zajęcia praktyczne,
- praca w parach.

Potrzebne materiały

karty pracy dla grup „Świadomie w sieci”, komputery z dostępem do internetu, rzutnik

Przebieg

Wprowadzenie (5 minut)

Uczniowie zapoznają się z wtyczką do przeglądarek, która pozwala monitorować, kto nas śledzi w Internecie. Poznają działanie narzędzi ograniczających śledzenie i nauczą się, jak z nich korzystać.

Nauczyciel każdej parze mającej do dyspozycji komputer z dostępem do internetu rozdaje karty pracy „Świadomie w sieci” i informuje, że będą miały do wykonania kilka zadań. Zwraca też uwagę na:

- sprawne wykonywanie zadań (nietracenie czasu na inne czynności),
- zadawanie pytań w razie wątpliwości czy trudności.

Jeśli istnieje taka potrzeba, nauczyciel może omówić pojęcie wtyczki:

Rozszerzenie (inaczej: wtyczka) – dodatkowy moduł do programu komputerowego, który rozszerza jego możliwości. Stosowanie wtyczek jest coraz częstszym zabiegiem wśród programistów, a zwłaszcza tych tworzących otwarte oprogramowanie. Zaletą takiego rozwiązania jest to, że użytkownicy mogą wybierać pomiędzy funkcjami, które chcą mieć w programie, a których nie. Poza tym odciąża to autora od pisania całego kodu programu, a zrzuca część tego obowiązku na zewnętrznych programistów. Najpopularniejszymi programami oferującymi wtyczki są przeglądarki internetowe oraz programy pocztowe, np. Mozilla Firefox i Mozilla Thunderbird. W obu wypadkach dzięki wtyczkom można znacząco zwiększyć poziom bezpieczeństwa i prywatności komunikacji.

Ćwiczenia (40 minut)

Uczniowie zapoznają się z instrukcją do zadania 1. Oglądają film w języku angielskim z wystąpieniem Gary'ego Kovaca „Śledzenie śledzonych" i odpowiadają na pytania:

- Do czego zostały porównane ślady naszej aktywności w sieci?
- Do czego służy rozszerzenie Lightbeam (w filmie występuje pod starszą nazwą Collusion)?

Po kilku minutach nauczyciel prosi o zaprezentowanie odpowiedzi na forum klasy. Podsumowuje zadanie i zwraca uwagę, że rozszerzenie Lightbeam daje nam wiedzę, kto jest zainteresowany informacjami o nas w sieci.

Następnie uczniowie wykonują zadanie 2 z karty pracy. Na stronie www.addons.mozilla.org wyszukajcie dodatek o nazwie Lightbeam (to nowa wersja Collusion). Instalują go w przeglądarce. Otwierają różne strony internetowe i na bieżąco sprawdzają, jak zmienia się graf Lightbeam. Wymieniają kilka podmiotów, które śledziły ich aktywność, a nie były otwieranymi przez nich stronami internetowymi.

Nauczyciel w podsumowaniu zaznacza, że Lightbeam pokazuje nam, iż informacje o nas gromadzą nie tylko strony internetowe, które odwiedzamy, ale również podmioty powiązane z nimi. Zachęca uczniów do zainstalowania rozszerzenia w domu.

W kolejnym kroku uczniowie zapoznają się z instrukcją do zadania 3, które polega na odnalezieniu na stronie Mozilli jednej z następujących wtyczek: Disconnect, Adblock, BetterPrivacy, HTTPS Everywhere, i opisaniu jej funkcji. Po 10 minutach chętne zespoły prezentują w 3–4 zdaniach wybranej wtyczki. W razie potrzeby nauczyciel może też krótko przedstawić poszczególne wtyczki:

AdBlock – jedno z najpopularniejszych rozszerzeń do przeglądarek internetowych, automatycznie blokuje i usuwa reklamy ze stron internetowych. Zwiększa wygodę i bezpieczeństwo korzystania z sieci. Ogranicza przepływ informacji o historii przeglądania.

Better Privacy – wtyczka do przeglądarek internetowych, która zarządza flash cookies i umożliwia ich skuteczne usuwanie np. przy zamykaniu przeglądarki.

Disconnect – wtyczka do przeglądarek internetowych, która blokuje wybrane skrypty śledzące.

HTTPS Everywhere – wtyczka do przeglądarek internetowych, która automatycznie włącza protokół HTTPS tam, gdzie istnieje taka możliwość.

Dodatkowo nauczyciel może zaprezentować uczniom na rzutniku tabelę na stronie panopticlick.eff.org (po kliknięciu przycisku Test me). Pokazuje ona, jakie informacje są dostępne w trakcie korzystania z przeglądarki internetowej. Pogrubiona liczba na górze wskazuje, jak unikatowa – wśród innych testowanych – jest informacja wysyłana z używanej

właśnie przeglądarki. Nauczyciel zaznacza, jak duża liczba informacji jest udostępniana przy samym wejściu do sieci. Zachęca uczniów do powtórzenia ćwiczenia na własnych komputerach w domu.

Ewaluacja

Po zakończonych zajęciach należy upewnić się, że uczniowie:

- wiedzą, że ich aktywność w sieci jest śledzona przez różne podmioty;
- potrafią zainstalować w przeglądarce wtyczkę Lightbeam i sprawdzić jej działanie;
- potrafią wymienić, jakie wtyczki do przeglądarek internetowych zwiększają prywatność w sieci i opisać ich działanie.

Przykład 4

(oprac. na podstawie scenariusza Stop cyberprzemocy, 2012)

Temat: Stop cyberprzemocy

Klasy VII–VIII szkoły podstawowej

Czas zajęć: 90 minut

Cel ogólny

Zwrócenie uwagi uczniów na zjawisko cyberprzemocy oraz uwrażliwienie ich na specyfikę problemu, związaną przede wszystkim z możliwymi konsekwencjami tego typu działań, zarówno dla ich ofiar, jak i sprawców.

Cele operacyjne

Uczniowie:

- wiedzą, jakie formy może przyjmować cyberprzemoc,
- uświadamiają sobie, jakie emocje może rodzić cyberprzemoc u jej ofiar, jakie może nieść dla nich konsekwencje,
- znają możliwe konsekwencje przemocy w sieci dla sprawców tego typu działań,
- wypracowują i przyswajają reguły bezpiecznego i kulturalnego korzystania z sieci,
- znają zasady reagowania w sytuacjach cyberprzemocy (jak powinna zachować się ofiara cyberprzemocy i gdzie może szukać pomocy, jak powinni zachować się świadkowie cyberprzemocy),
- wiedzą, jak zachowywać się, by zmniejszyć ryzyko bycia ofiarą cyberprzemocy.

Metody nauczania i formy pracy

- prezentacja filmu, burza mózgów, analiza przypadków, dyskusja,
- praca w grupach.

Potrzebne materiały

film „Stop cyberprzemocy", komputery z dostępem do internetu, rzutnik

Przebieg

Część I

Wprowadzenie (5 minut)

Nauczyciel informuje uczniów, że zajęcia dotyczą bezpieczeństwa związanego z używaniem internetu i telefonów komórkowych.

Prowadzący pyta uczniów o to, do jakich celów używają internetu oraz telefonów komórkowych. Uczniowie spontanicznie odpowiadają. Nauczyciel przyporządkowuje odpowiedzi do trzech podstawowych zastosowań internetu: komunikacja, zdobywanie informacji, rozrywka.

Nauczyciel zwraca uwagę na fakt, że oprócz zalet korzystania z mediów elektronicznych, wiążą się z nimi również zagrożenia. Zapowiada, że przedmiotem zajęć będzie dyskusja na temat przemocy rówieśniczej w sieci.

Ofiary cyberprzemocy (40 minut)

Prezentacja filmu (5 minut)

Nauczyciel prosi uczniów o uważne obejrzenie filmu „Stop cyberprzemocy". Zwraca uwagę, że film powstał na podstawie prawdziwych historii, które zdarzają się w szkołach. Mówi, że w filmie uczniowie zobaczą wydarzenia oraz usłyszą wypowiedzi swoich rówieśników, do których będzie odnosić się dalsza część zajęć.

Analiza filmu (10 minut)

Po obejrzeniu filmu nauczyciel zaprasza uczniów do dyskusji, której celem jest wskazanie specyfiki cyberprzemocy i jej konsekwencji dla ofiary. Uczniowie ustalają, jakich form przemocy doświadczyła Dominika – bohaterka prezentowanego filmu – i zastanawiają się, jak mogą się czuć w takich sytuacjach ofiary cyberprzemocy.

Moderując dyskusję nauczyciel akcentuje kolejne etapy historii Dominiki:

- Dominika została sfilmowana wbrew swojej woli.
- Film został rozesłany przy użyciu telefonu komórkowego.
- Ktoś zamieścił film w internecie.
- Dominika dostawała wulgarne SMS-y.

Nauczyciel pyta uczniów, czy doświadczyli podobnej sytuacji, byli jej świadkami lub słyszeli o podobnych historiach. Ewentualne wypowiedzi wykorzystuje w rozmowie o sytuacji ofiar cyberprzemocy.

Oczekiwane wnioski z dyskusji/komentarz nauczyciela:

- Świadomość, że ktoś dysponuje ośmieszającym filmem lub zdjęciem bywa bardzo trudna do zniesienia i krzywdząca.
- Rozsyłanie i publikowanie kompromitujących materiałów w sieci powoduje u ofiar strach i wstyd.
- Wulgarne SMS-y, wiadomości e-mail itp. potrafią bardzo krzywdzić, zwłaszcza jeżeli są otrzymywane od osób z najbliższego otoczenia (szkoła, klasa).

Ofiary przemocy rówieśniczej często nie potrafią sobie same poradzić z taką sytuacją. Wbrew pozorom przemoc w sieci potrafi być bardziej dotkliwa niż przemoc w realnym świecie.

Analiza historii (10 minut)

Nauczyciel dzieli uczniów na cztery grupy. Każdej grupie przekazuje kartkę z opisaną historią przypadku cyberprzemocy. Każda historia jest inna. Uczniowie pracują w grupach. Zapoznają się z historią i opracowują odpowiedzi na pytania, które nauczyciel zapisuje na tablicy:

- Jak się czuł/a bohater/ka prezentowanej historii i co mogło się z nim/nią dalej dziać?

- Jak powinna się zachować ofiara prezentowanej historii?

Historia Kasi
Zbyszek nagrał kamerą w telefonie swoją koleżankę z klasy Kasię, kiedy całowała się z chłopakiem. Następnie rozesłał MMS-em film do swoich kolegów z klasy. Niektórzy z nich wysyłali go dalej. Jeszcze tego samego dnia ktoś opublikował film w internecie. Film cieszył się dużą popularnością. Na stronie z filmem zaczęły pojawiać się przykre dla dziewczyny komentarze.

Historia Agnieszki
Agnieszka po powrocie do domu ze szkoły usiadła przed komputerem. Chciała sprawdzić pocztę, ale nie mogła zalogować się do swojego konta. Jej hasło nie działało. Następnego dnia w szkole okazało się, że ktoś włamał się na konto Agnieszki i podszywając się pod nią, wysłał kilku kolegom z jej klasy wulgarne e-maile. Adresaci tych wiadomości obrazili się na Agnieszkę

i nie chcieli z nią rozmawiać. Od kilku z nich Agnieszka dostała bardzo nieprzyjemne SMS-y. Wiele osób z klasy miało do Agnieszki pretensje za jej zachowanie wobec kolegów.

Historia Tomka
Tomek bardzo często rozmawia na komunikatorze ze swoimi znajomymi ze szkoły i osobami, które zna tylko z internetu. Od jakiegoś czasu dostaje od osoby ukrywającej się pod różnymi nickami nieprzyjemne, ośmieszające go wiadomości. Pisał do tej osoby, żeby przestała wysyłać takie wiadomości, starał się ustalić, kto do niego pisze, jednak bezskutecznie.
W końcu Tomek sam zaczął odpowiadać w nieprzyjemny sposób anonimowemu nadawcy. Wiadomości przychodziło jednak coraz więcej, w pewnej chwili ktoś zaczął Tomkowi grozić śmiercią.

Historia Krzyśka
Krzysiek od kilku miesięcy ma w sieci bloga, w którym często zamieszcza zdjęcia. W ubiegłym tygodniu dodał parę fotek ze swoich urodzin. Kilka dni później dostał w e-mailu od nieznajomej osoby jedno ze zdjęć urodzinowych zmontowanych tak, że pokazywało Krzyśka w wulgarny i poniżający sposób. W e-mailu była też wiadomość, że to samo zdjęcie niedługo zawiśnie w ulubionym serwisie społecznościowym Krzyśka.

Postępowanie w przypadkach cyberprzemocy (15 minut)

Nauczyciel prosi wybrane osoby z każdej grupy o przeczytanie historii. Następnie cała grupa odpowiada na pytania:

- Jak się czuł/a bohater/ka prezentowanej historii i co mogło się z nim/nią dalej dziać?
- Jak powinna się zachować ofiara prezentowanej sytuacji?

W odpowiedzi na pierwsze pytanie warto zwrócić uwagę na negatywne emocje, których zazwyczaj doznają ofiary cyberprzemocy, takie jak: strach, poczucie osaczenia, odrzucenia i niesprawiedliwości. Warto również pokazać możliwe zachowania będące konsekwencjami tych emocji, np. unikanie szkoły, ograniczenie kontaktów ze znajomymi, ucieczka z domu, a w skrajnych wypadkach nawet próby samobójcze.

Przy odpowiedzi na drugie pytanie nauczyciel kieruje pracą klasy tak, aby w wypowiedziach uczniów pojawiły się najważniejsze zasady postępowania w przypadkach cyberprzemocy. Zasady zapisywane są na dużej kartce lub na tablicy. Ważne, aby pojawiły się wśród nich m.in.

- szukać pomocy u zaufanej osoby dorosłej (nauczyciela, rodziców),
- nie odpowiadać na zaczepki w sieci,
- blokować w komunikatorach i poczcie elektronicznej kontakt z niepożądanymi osobami,
- wymagać natychmiastowego usunięcia filmu lub zdjęcia zrobionego wbrew woli ofiary, prosić administratora serwisu o usunięcie kompromitujących materiałów z sieci,

- dokumentować dowody przemocy (zachowywanie SMS-ów, historii rozmów, zrobienie screenshota itp.).

Jeżeli uczniowie nie wymienią tego w swoich odpowiedziach, nauczyciel dopisuje do listy zasad punkt:

- szukać pomocy na stronie 116111.pl.

Nauczyciel informuje uczniów o różnych możliwościach skorzystania z pomocy na stronie 116111.pl: rozmowa z konsultantem na czacie lub wysłanie wiadomości za pośrednictwem strony (warto w tym miejscu zaprezentować tę stronę internetową). Uczniowie mogą też zadzwonić pod bezpłatny numer telefonu zaufania 116 111.

Omawiając historię Agnieszki i Krzyśka, należy zapytać klasę, czy można było jakoś uniknąć sytuacji, w której znaleźli się jej bohaterowie. Należy zwrócić przy tej okazji uwagę na konieczność dbania o to, by hasła, którymi posługują się internauci, były trudne do odgadnięcia i pilnie strzeżone (historia Agnieszki) oraz że nie należy publikować w sieci swoich zdjęć (historia Krzyśka). Przed ewentualną przerwą nauczyciel podsumowuje dotychczasowe ustalenia i zapowiada, że w drugiej części kontynuowana będzie tematyka przemocy w sieci.

Część II

Formy cyberprzemocy (10 minut)

W celu podsumowania pierwszej części zajęć oraz uporządkowania wiedzy o cyberprzemocy nauczyciel prosi uczniów o wskazanie, jakie działania z wykorzystaniem sieci i telefonów komórkowych mogą być krzywdzące dla innych. Prosi uczniów o przypomnienie sobie form cyberprzemocy z filmu i prezentowanych historii, następnie zapisuje na tablicy lub papierze ustalone z uczniami formy. Ważne, aby wśród odpowiedzi znalazł się możliwie wyczerpujący katalog sytuacji definiowanych jako cyberprzemoc.

Formy cyberprzemocy:

- rejestrowanie niechcianych filmów lub zdjęć telefonem komórkowym,
- publikowanie ośmieszających zdjęć i filmów w internecie,
- rozsyłanie ośmieszających materiałów przy użyciu telefonu (SMS, MMS),
- wysyłanie wulgarnych SMS-ów,
- wyzywane, straszenie, obrażanie w sieci i przez telefon komórkowy,
- grożenie komuś w sieci i przez telefon komórkowy,
- włamania na blog, profil lub konto pocztowe,
- podszywanie się w sieci pod inną osobę i działanie na jej niekorzyść.

Sprawcy cyberprzemocy (10 minut)

Nauczyciel zapowiada, że kolejna część zajęć będzie dotyczyć odpowiedzialności za przemoc w sieci.

Nauczyciel odtwarza fragment filmu z wypowiedzią sprawcy (Robert). Zwraca uwagę uczniów, że sprawcami cyberprzemocy nie są zazwyczaj niebezpieczni przestępcy, ale zwykli nastolatkowie. Odwołuje się do historii z filmu. Najpierw prosi uczniów o wskazanie sprawców przemocy wobec Dominiki. Wysłuchuje odpowiedzi. W podsumowaniu zwraca uwagę klasy na fakt, że sprawcą jest nie tylko osoba, która zarejestrowała film, ale również ci, który go sobie przesyłali, publikowali go w internecie i ci, którzy przesyłali dziewczynie wulgarnie wiadomości. Podkreśla, że wszystkie te osoby są odpowiedzialne za krzywdę Dominiki.

Nauczyciel zwraca uwagę na wypowiedź „To miał być żart… Nie wiedzieliśmy, że tak bardzo ją skrzywdzimy…". Następnie pyta uczniów, czy takie działania można uznać za żart. Prowadzący podkreśla, że nawet pozornie śmieszna lub błaha sytuacja może doprowadzić ofiarę przemocy rówieśniczej do cierpienia. Tłumaczy, że „niewinne" intencje nie są wytłumaczeniem i nie zwalniają z odpowiedzialności za przemoc.

Nauczyciel odwołuje się ponownie do wypowiedzi sprawcy: „Teraz my mamy problem…". Pyta uczniów, jakie konsekwencje grożą sprawcom cyberprzemocy.

Prowadzący w podsumowaniu zwraca uwagę na potencjalne konsekwencje:

- wezwanie do szkoły rodziców,
- obniżenie oceny ze sprawowania,
- możliwość przeniesienie do innej szkoły,
- odpowiedzialność karna (w sytuacjach łamania prawa, np. groźby karalne, publikowanie nielegalnych treści, zniesławienie).

Nauczyciel zwraca uwagę na ostatni fragment wypowiedzi sprawcy: „Chciałbym to jakoś odkręcić". Pyta uczniów, czy można odwrócić sytuację przedstawioną w filmie. Przy tej okazji wyeksponowane powinny zostać te cechy cyberprzemocy, które często wpływają na nieodwracalność jej skutków, np.

- szybkie rozprzestrzenianie i duża popularność materiałów publikowanych w sieci,
- brak możliwości całkowitego usunięcia tego typu materiałów z internetu,
- długotrwałe doznawanie cierpienia przez ofiarę.

Nauczyciel zwraca uwagę uczniów na to, że mimo często nieodwracalnych skutków cyberprzemocy osoba, która uświadomi sobie, że wyrządziła komuś za pośrednictwem sieci krzywdę, nie powinna pozostawać bierna. Nawiązując do sytuacji z filmu, prowadzący zajęcia pyta klasę, co może/powinien zrobić Robert (sprawca) lub osoby, które znajdą się w podobnej sytuacji. Ważne, aby efektem dyskusji były m.in. następujące wnioski:

- sprawca powinien przeprosić swoją ofiarę i zapewnić ją o niepodejmowaniu takich działań w przyszłości,
- w kontakcie z administratorami serwisów internetowych powinien podjąć próbę usunięcia krzywdzących treści z sieci,
- powinien reagować w sytuacji kontynuowania krzywdzących działań przez inne osoby.

Rola świadków cyberprzemocy (5 minut)

Nauczyciel przypomina wypowiedź świadka z filmu (Michał) i pyta, jak należy się zachować w podobnej sytuacji. Wysłuchuje odpowiedzi uczniów. Prowokuje dyskusję dotyczącą tego, czy pomoc kolegom ze szkoły jest obowiązkiem.

Nauczyciel podkreśla, że nie można pozostawać obojętnym wobec krzywdy kolegów z klasy, szkoły czy podwórka. Akcentuje, że reakcja jest obowiązkiem, a zaniechanie działania stawia świadka po stronie sprawców!

Zasady odpowiedzialnego korzystania z internetu i telefonów komórkowych (20 minut)

Na zakończenie zajęć nauczyciel proponuje uczniom stworzenie kodeksu bezpiecznego i odpowiedzialnego korzystania z internetu i telefonów komórkowych. Dzieli uczniów na cztery grupy, z których każda powinna odpowiedzieć na jedno, wskazane pytanie:

- Co robić, żeby nie zostać ofiarą cyberprzemocy?
- Jak korzystać z internetu i telefonu, by nie krzywdzić innych?
- Co robić, będąc świadkiem cyberprzemocy?
- Co robić, będąc ofiarą cyberprzemocy?

Praca w grupach (10 minut)

Zadaniem uczniów jest wypracowanie zasad odnoszących się do przyporządkowanego grupie aspektu bezpieczeństwa.

Dyskusja na forum (10 minut)

Nauczyciel zaprasza grupy do zaprezentowania wypracowanych zasad bezpieczeństwa. Zasady zapisywane są na dużej kartce lub tablicy. Ważne, by wśród zasad znalazły się m.in. następujące zapisy:

Co robić, żeby nie zostać ofiarą cyberprzemocy?

- dbać o prywatność swoich danych osobowych,
- nadawać swoim profilom w sieci bezpieczny status (prywatny),
- chronić swoje hasła i loginy,

- nie zamieszczać w sieci swoich zdjęć i filmów,
- nie wymieniać się z kolegami telefonami komórkowymi.

Jak korzystać z internetu i telefonu, żeby nie krzywdzić innych?

- traktować innych z szacunkiem (nie wyzywać, nie obrażać, nie straszyć itp.),
- nie zamieszczać w internecie materiałów (filmów, zdjęć, tekstów), które mogą kogoś skrzywdzić,
- zawsze pytać o zgodę, jeżeli chcemy komuś zrobić zdjęcie lub nakręcić film z jego udziałem,
- nie rozsyłać za pomocą telefonu komórkowego zdjęć, filmów oraz tekstów, które mogą komuś sprawić przykrość.

Co robić, będąc świadkiem cyberprzemocy?

- nie przesyłać dalej krzywdzących materiałów, które otrzymujemy w sieci,
- zawsze pomagać kolegom i koleżankom, którzy padli ofiarą cyberprzemocy,
- informować o krzywdzie kolegi lub koleżanki kogoś dorosłego – nauczyciela, pedagoga szkolnego, rodziców,
- polecić ofierze cyberprzemocy kontakt z doradcami na stronie 116111.pl lub skontaktować się z nimi osobiście.

Co robić, będąc ofiarą cyberprzemocy?

- nie odpowiadać na zaczepki w sieci,
- domagać się skasowania filmów i zdjęć nagranych wbrew naszej woli,
- natychmiast szukać pomocy u kogoś dorosłego – nauczyciela, pedagoga szkolnego, rodziców,
- zachowywać dowody cyberprzemocy,
- interweniować u dostawców usług internetowych,
- szukać pomocy na stronie 116111.pl.

Stworzony w ten sposób kodeks bezpieczeństwa można powiesić w pracowni komputerowej lub zaprezentować na łamach gazetki szkolnej.

Ewaluacja

Po zakończonych zajęciach należy upewnić się, czy uczniowie:

- wiedzą, jakie formy może przyjmować cyberprzemoc,
- uświadamiają sobie, jakie emocje może rodzić cyberprzemoc u jej ofiar, jakie może nieść dla nich konsekwencje,
- znają możliwe konsekwencje przemocy w sieci dla sprawców tego typu działań,
- wypracowują i przyswajają reguły bezpiecznego i kulturalnego korzystania z sieci,

- znają zasady reagowania w sytuacjach cyberprzemocy,
- wiedzą, jak zachowywać się, by zmniejszyć ryzyko bycia ofiarą cyberprzemocy.

Warsztaty „Mowa nienawiści, czyli o granicach wolności słowa?"

(oprac. na podstawie scenariusza warsztatów Anny Dąbrowskiej, Od mowy…, 2015)

Temat: Mowa nienawiści, czyli o granicach wolności słowa?

Klasy VII–VIII szkoły podstawowej

Cele

praktyczne zapoznanie z procesem powstawania mowy nienawiści

Metody nauczania i formy pracy

- dyskusja, praca nad definicją,
- praca indywidualna, w grupach.

Materiały pomocnicze

- kartki A4 dla każdej osoby uczestniczącej, kartki A3 dla każdej osoby
- uczestniczącej, kartki A4 z przygotowanymi wcześniej sylwetkami osób, kredki, wycinki prasowe lub cytaty z internetu będące przykładami mowy nienawiści

Przebieg zajęć

1. Rozdaj osobom uczestniczącym czyste kartki A4. Poproś, aby na nich narysowały zwierzę/owada, który napawa ich odrazą, niechęcią.

2. Rozdaj osobom uczestniczącym czyste kartki A3. Poproś, aby swoje rysunki zwierząt/owadów położyły na środek kartki A3. Na powstałej w ten sposób ramce osoby uczestniczące mają napisać atrybuty, jakimi charakteryzują się narysowane przez nie zwierzęta/owady.

   Zadbaj, aby znalazły się tam cechy dotyczące wyglądu, zapachu, charakteru (co robi? jakie jest?).

3. Poproś, aby osoby uczestniczące zastanowiły się, co chciałyby zrobić z narysowanym przez siebie zwierzęciem/owadem, gdyby niespodziewanie znalazł się on u nich w domu – środki zaradcze. Następnie uczestnicy notują te pomysły na ramce (innym kolorem).

   Zadbaj, aby wśród odpowiedzi znalazły się: oznaczyć, wygonić, zamknąć, zabić.

4. Zbierz rysunki, nie zabierając ramek. Rozdaj materiał pomocniczy (karty z opisami ludzi), np.

    - „Anna, 16 lat, uczennica, ciemny kolor skóry”,
    - „Jan, 72 lata, lekarz, Żyd”,
    - „Maria, 42 lata, krawcowa, porusza się na wózku inwalidzkim”,
    - „Michał, 35 lat, nauczyciel akademicki, homoseksualista”

    Karty mogą się powtarzać.

    Zapytaj, co się stanie, kiedy zamiast zwierząt/owadów w ramkach znajdą się te (i inne) osoby?

    Bazując na ramkach osób uczestniczących (atrybuty – jaki jest?), wprowadź pojęcie mowy nienawiści, natomiast na podstawie zapisanych na ramkach zalecanych środkach zaradczych – pojęcie aktów nienawiści.

    Jeśli zajęcia prowadzone są w klasie, zamiast przygotowanych kart z osobami mogą znaleźć się imiona samych osób uczestniczących.

5. Wyjaśnij, kto najczęściej posługuje się mową nienawiści (politycy, media, przywódcy religijni, dziennikarze) i gdzie najczęściej można ją usłyszeć (media, kościół, ulica–graffiti, szkoła).

    Powiedz, że za chwilę uczestnicy spróbują odnaleźć jej przykłady w wycinkach prasowych/cytatach z internetu.

    Wytłumacz, dlaczego tak jest (warto, aby znalazły się tu między innymi aspekty związane z manipulacją, populizmem; mowa nienawiści chętnie korzysta ze stereotypów i uprzedzeń dotyczących różnych grup; można operować wymyślonym przykładem szkolnym: co się stanie, jeżeli w szkole pojawi się plotka, że któraś z osób jest...; czy taka informacja może zmienić zachowanie się wobec tej osoby innych osób? dlaczego?).

6. Podziel osoby uczestniczące na cztery grupy.

    Rozdaj przygotowane wcześniej wycinki prasowe/cytaty z internetu. Poproś, aby każda grupa odnalazła w nich mowę nienawiści.

7. Poproś grupy o krótkie omówienie wykonanej pracy.

8. Podsumuj pracę grup.

Sprawdź, czy potrafisz...

- wyjaśnić, jakie są przyczyny istnienia zagrożeń w użytkowaniu TIK.
- rozpoznać i opisać wybrane przykłady zagrożeń.
- podać sposoby zapobiegania ryzyku różnych zagrożeń.
- omówić sposoby zapoznawania uczniów z zasadami bezpieczeństwa narzędzi TIK.
- przygotować scenariusz warsztatów na temat bezpieczeństwa w internecie i przeciwstawiania się cyberprzemocy.
- zaplanować wraz uczniami kampanię społeczną dotyczącą bezpieczeństwa w sieci.

Bibliografia

ABC bezpieczeństwa w sieci, (b.r.), Cyfrowa Wyprawka [online, dostęp dn. 20.10.2017].

Bezpieczna komunikacja w sieci, (b.r.), Cyfrowa Wyprawka [online, dostęp dn. 20.10.2017].

Diagnoza społeczna 2013. Warunki i jakość życia Polaków. Raport, (2014), Czapiński J., Panek T. (red.), [online, dostęp dn. 21.10.2017, pdf. 47,4 MB]

Ins@fe. Elementarz dla rodziców, (b.r.), [online, dostęp dn. 20.10.2017].

Iwan E. i in., (2016), *Materiały do prowadzenia zajęć edukacyjno-profilaktycznych z zakresu bezpiecznego, świadomego i odpowiedzialnego korzystania z internetu*, Lublin: Fundacja Sempre a Frente [także online, dostęp dn. 20.10.2017, pdf. 6,2 MB].

Kto nas śledzi w sieci?, (b.r.), Cyfrowa Wyprawka [online, dostęp dn. 20.10.2017].

Iwan E. i in., (b.r)., *Materiały do prowadzenia zajęć edukacyjno-profilaktycznych z zakresu bezpiecznego, świadomego i odpowiedzialnego korzystania z internetu*, Lublin [online, dostęp dn. 21.10.2017, pdf. 6,4 MB]

Niedyskretny profil, (b.r.), Akademia Cyfrowa Wyprawka/Fundacja Panoptykon [online, dostęp dn. 20.10.2017].

Od mowy nienawiści, poprzez tolerancję, do porozumienia. Scenariusze lekcji, warsztatów, debat, (2015), Koba L., Drozdowicz B, Błasińska K. (red.), Gdańsk: Fundacja Instytut Równowagi Społeczno-Ekonomicznej [także online, dostęp dn. 20.10.2017, pdf. 393 kB].

Pacewicz A. i in., (b.r.), *Szkoła z klasą 2.0. Przewodnik po programie* [online, dostęp dn. 20.10.2017, pdf. 1,8 MB].

Portale społecznościowe – codzienne wyzwania, (b.r.), Cyfrowa Wyprawka [online, dostęp dn. 20.10.2017].

Postrzeganie zagadnień zwigzanych z ochrong danych i prywatności przez dzieci i młodzież. Raport z badań, (b.r.) [online, dostęp 21.10.2017, pdf. 646 kB].

Prujszczyk G., Śliwowski K., (2010), *Bezpieczeństwo informacyjne w serwisach Web 2.0* [online, dostęp 21.10.2017, pdf. 1,4 MB].

Prywatność w sieci – odzyskaj kontrolę!, (b.r.), Cyfrowa Wyprawka [online, dostęp dn. 20.10.2017]

Pyżalski J., Klichowski M., Przybyła M., (2014), *Szanse i zagrożenia w obszarze wykorzystania technologii informacyjno-komunikacyjnych (TIK), ze szczególnym uwzględnieniem aplikacji mobilnych (TIK-mobApp) przez dzieci w wieku 3-6 lat*, Poznań: Uniwersytet im. Adama Mickiewicza [online, dostęp dn. 20.10.2017, pdf. 1,7 MB].

Pyżalski J., (2012), Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży, Kraków: Wydawnictwo Impuls.

Stop cyberprzemocy, (2012), Fundacja Dzieci Niczyje [online, dostęp dn. 20.10.2017].

Wojtasik Ł., (2014), Seksting wśród dzieci i młodzieży, „Dziecko krzywdzone. Teoria, badania, praktyka" Vol. 13 Nr 2 [także online, dostęp dn. 21.10.2017, pdf. 396 KB].

Zasady korzystania z TIK: Kodeks TIK, (2013), [online, dostęp dn. 20.10.2017].

Spis tabel


Fundusze
Europejskie
Wiedza Edukacja Rozwój


ORE
Ośrodek
Rozwoju
Edukacji


Unia Europejska
Europejski Fundusz Społeczny