Jak zapewnić uczniom bezpieczeństwo w internecie?

Poradnik dla nauczycieli

cyfrowobezpieczni.pl
BEZPIECZNA SZKOŁA CYFROWA

Poradnik dla nauczycieli

"Jak zapewnić uczniom bezpieczeństwo w Internecie"

został opracowany w ramach projektu Cyfrowobezpieczni.pl

Publikacja została opracowana przez Zespół Ekspertów Naukowej Akademickiej Sieci Komputerowej instytutu badawczego NASK

Skład zespołu: Monika Gajewska-Pol, Julia Gursztyn, Anna Maj, Martyna Różycka, Anna Rywczyńska, Krzysztof Silicki

Konsultacja merytoryczna: prof. APS dr hab. Maciej Tanaś

Więcej informacji na temat projektu:
CYFROWOBEZPIECZNI.pl - Bezpieczna Szkoła Cyfrowa,
na stronie www.cyfrowobezpieczni.pl

Projekt jest finansowany przez Ministerstwo Edukacji Narodowej w ramach zadania „Poprawa kompetencji pracowników szkoły, uczniów i ich rodziców w zakresie bezpiecznego korzystania z cyberprzestrzeni oraz reagowania na zagrożenia”

MINISTERSTWO EDUKACJI NARODOWEJ

Spis treści

Zarys problematyki: Internet - szanse i zagrożenia

Internet to nowoczesne medium, które odgrywa ogromną rolę w życiu młodego człowieka i może być przez niego z pożytkiem wykorzystywane. **Codzienne aktywności młodych internautów toczą się równolegle online i offline.** Rozwijanie zainteresowań, rozmowy z rówieśnikami czy odrabianie lekcji to czynności, które z dużą chęcią i swobodą realizowane są w sieci. Pozytywne aspekty technologii informacyjno-komunikacyjnych (TIK) doceniają także dyrektorzy, wyposażając swoje placówki w urządzenia cyfrowe (laptopy i tablety z dostępem do internetu, rzutniki, tablice interaktywne). W niniejszym poradniku przedstawiamy, **dlaczego warto wykorzystywać nowoczesne narzędzia informatyczne w procesie nauczania**, a także pokazujemy, w jaki sposób uczniowie mogą skutecznie i bezpiecznie wyszukiwać w sieci potrzebne informacje. Prezentujemy również definicje pozytywnych treści online oraz kryteria dla stron internetowych, których znajomość pozwoli Państwu polecać dzieciom i ich rodzicom odpowiednie serwisy edukacyjne, a w przypadku młodzieży - ułatwiać tworzenie własnych, bezpiecznych treści w sieci.

Jednak nie można zapominać, że globalna sieć oprócz pozytywnych treści kryje też wiele niebezpieczeństw. **Ważne jest, by nauczyciele kształtowali świadomość uczniów o zagrożeniach internetowych**, a w przypadku zaistnienia niebezpieczeństwa potrafili wskazać im właściwe rozwiązanie. W publikacji tej szczegółowo omawiamy różne formy cyberprzemocy, przedstawiamy ryzykowne zachowania online podejmowane przez nastolatków, a także radzimy, jak postępować w sytuacji uzależnienia od internetu. Ze względu na wagę tych problemów rekomendujemy szkołom przygotowanie oficjalnych procedur w przypadku cyberprzemocy, nadmiernego korzystania z internetu oraz reagowania w sytuacji naruszenia bezpieczeństwa infrastruktury szkolnej sieci, które powinny przybrać formę zarządzenia dyrektora lub uchwały rady pedagogicznej. W przypadku procedur dotyczących cyberprzemocy oraz nadmiernego korzystania z internetu zalecamy przeprowadzenie konsultacji z radą rodziców. Wypracowane procedury powinny być dobrze znane całemu środowisku szkolnemu. W poradniku omawiamy również symptomy nadużywania internetu oraz wskazujemy punkty kontaktowe udzielające wsparcia i informacji w zakresie trudności będących konsekwencjami ryzykownych zachowań w sieci.

Prezentujemy również jak ważne jest, by uczeń krytycznie podchodził do treści zamieszczonych w internecie, a także miał świadomość konsekwencji wynikających z nielegalnego kopiowania znajdujących się tam materiałów. Na łamach poradnika znajdą Państwo także nasze rekomendacje dotyczące zabezpieczenia infrastruktury TIK szkoły.

Nowoczesna szkoła – pozytywne wykorzystanie technologii informacyjno-komunikacyjnych w edukacji

Technologie informacyjno-komunikacyjne w edukacji

W dzisiejszych czasach nikt już nie ma wątpliwości, że **nowoczesne media, które na dobre zagościły w życiu prywatnym oraz zawodowym, muszą także stanowić integralną część współczesnego szkolnictwa**. Edukacja **medialna** powinna obejmować efektywne, kreatywne i bezpiecznie korzystanie z zasobów internetu, a sama sieć stać się narzędziem będącym podporą dla nauczania wszelkiego rodzaju przedmiotów szkolnych.

Wprowadzenie internetu do codziennego życia szkoły zwiększy atrakcyjność i unowocześni zajęcia edukacyjne, ułatwi komunikację pomiędzy kadrą nauczycielską a uczniami i rodzicami, pomoże w prowadzeniu projektów, otworzy szerzej na współpracę międzynarodową oraz zapewni dostęp do nieograniczonych zasobów globalnej sieci. Wykorzystywanie nowych technologii, czyli nowoczesnych narzędzi informatycznych w szkolnictwie takich jak: internetowe platformy edukacyjne, tablice multimedialne, e-podręczniki, narzędzia deweloperskie służące budowaniu stron lub tworzeniu aplikacji itp., może mieć **duży wpływ na rozwijanie u uczniów zdolności twórczych**. Podkreślając też możliwość kreowania zasobów sieciowych, pokazujemy uczniom, że niekoniecznie trzeba być tylko biernym odbiorcą.

Sieć może być również idealnym narzędziem do komunikacji szkolnej między rówieśnikami, nauczycielami i rodzicami. Dzięki telefonom komórkowym i internetowi komunikacja między domem rodzinnym dziecka i szkołą oraz innymi osobami i instytucjami odpowiedzialnymi za edukację z pewnością stała się wygodniejsza i szybsza.

Jak mówi rozporządzenie Ministra Edukacji Narodowej z dnia 23 grudnia 2008 r. w sprawie podstawy programowej, do jednych z najważniejszych umiejętności zdobywanych przez ucznia w trakcie kształcenia ogólnego należy

umiejętność posługiwania się nowoczesnymi technologiami informacyjno-komunikacyjnymi, w tym także dla wyszukiwania i korzystania z informacji. Nauczyciele powinni stwarzać uczniom warunki do nabywania umiejętności wyszukiwania, porządkowania i wykorzystywania informacji z różnych źródeł, z zastosowaniem technologii informacyjno-komunikacyjnych, na zajęciach z różnych przedmiotów. Dostęp do technologii w szkole przy odpowiednim przygotowaniu nauczyciela sprawi, że uczeń będzie również lepiej przygotowany do funkcjonowania na rynku pracy. Z badań Unii Europejskiej wynika, że 60 proc. dzieci, które obecnie rozpoczynają naukę, będzie pracować w zawodach jeszcze nieistniejących.

Dlaczego warto korzystać z TIK w szkole:

- Wspierają nauczanie kompetencji cyfrowych
- Usprawniają wymianę informacji (np.: dzięki narzędziu Moodle)
- Umożliwiają organizację zdalnych lekcji oraz wydarzeń edukacyjnych, takich jak np.: Webinaria – czyli tematyczne seminaria online
- Dają szybki i nieograniczony dostęp do zasobów sieci oraz multimedialnych narzędzi, które nie tylko przybliżą treści, ale również wpierają nauczanie przedmiotów ścisłych oraz nauk przyrodniczych poprzez możliwość zdalnego przeprowadzania eksperymentów edukacyjnych
- Wspierają proces uczenia się (przy porównaniu wyników testów przeprowadzonych w szkołach gimnazjalnych w 2004 r. przez Zakład Dydaktyki Chemii Uniwersytetu Adama Mickiewicza w Poznaniu uczniowie ze szkół, które wykorzystywały w procesie edukacji nowoczesne technologie informacyjno-komunikacyjne osiągnęli dużo lepsze wyniki od tych uczonych tylko tradycyjnymi metodami)
- Korzystanie z TIK jest coraz łatwiejsze dzięki coraz liczniejszym, łatwo dostępnym narzędziom i poradom m.in. na stronach:
  www.ore.edu.pl
  www.ceo.org.pl
  www.fabrykaprzyszlosci.pl
  www.edutikacja.oeiizk.waw.pl
  www.superbelfrzy.edu.pl
  www.edukator.pl
  www.etwinning.pl

Promocja pozytywnych treści - istotny element edukacji medialnej

Wykorzystanie nowych technologii podczas lekcji jest niezwykle ważne, jednak nie należy zapominać, by w ramach zajęć z edukacji medialnej promować pozytywną różnorodność internetu, pokazywać jego potencjał oraz podkreślać, że **każdy użytkownik może mieć wpływ na jakość i wartość zasobów sieci**. W Internecie znajduje się wiele nieprawdziwych informacji, treści szkodliwych, często wręcz nielegalnych, dlatego też **niezwykle ważne jest nauczenie młodych ludzi jak krytycznie podchodzić do internetowych źródeł**, jak skutecznie wyszukiwać potrzebną wiedzę. Ułatwieniem mogą być tzw. "*whitelists*" - czyli wykazy bezpiecznych i sprawdzonych stron, które spełniają ustalone kryteria, są regularnie kontrolowane przez ekspertów oraz adekwatne dla danej grupy wiekowej. Właściwe dopasowanie treści bądź aplikacji do wieku i umiejętności dziecka może być wyzwaniem dla pedagogów, pomocą mogą być właśnie profesjonalne serwisy, które zbierają oraz właściwie klasyfikują strony, aplikacje czy też gry (np.: **best.fdn.pl**)

Pozytywne treści - co to takiego?

Na podstawie kilkuletnich badań nad stronami internetowymi adekwatnymi dla dzieci i młodzieży (badania prowadzone przez 20 instytucji z 15 państw Unii Europejskiej w ramach projektu POSCON) określone zostały **definicje pozytywnych treści online**, które mogą być wskazówką zarówno dla producentów treści online, jak i dla nauczycieli, którzy na poniższych wytycznych mogą bazować, polecając odpowiednie serwisy dzieciom i ich rodzicom lub chcących angażować młodzież w samodzielne kreowanie treści internetowych.

Szczegółowe kryteria dotyczące serwisów online, którymi nauczyciel może się, kierować wybierając treści internetowe do celów edukacyjnych oraz polecając serwisy interaktywne dzieciom i ich opiekunom:

- Odbiorcy treści muszą być jasno określeni i treści właściwie adresowane (język i zawartość dopasowane do rozwoju intelektualnego i emocjonalnego danej grupy wiekowej)
- Zawartość strony/serwisu, czy też proponowane na stronie usługi muszą być atrakcyjne, użyteczne, rzetelne i niezawodne (np.: znamy autora treści, dane kontaktowe twórców strony, bądź administratora są łatwo dostępne, treści są prawdziwe, sprawdzone merytorycznie, zawartość strony nie narusza cudzych praw autorskich)

- Zawartość strony/serwisu, czy też proponowane na stronie usługi muszą być bezpieczne (nie zawierać treści szkodliwych bądź nielegalnych, posiadać łatwy adres – dziecko nie pomyli się i nie trafi na inną stronę)
- Prywatność dziecka musi być właściwie zapewniona i chroniona (trzeba zwrócić uwagę, jakie dane dziecko musi podać przy rejestrowaniu się i jak te dane są chronione, czy serwis np.: nie zawiera usługi geolokalizacji umożliwiającej szybkie określenie miejsca przebywania dziecka, dla kogo dostępne są dane publikowane przez dziecko np. w portalach społecznościowych. Dobrą procedurą jest również konieczność wyrażenia zezwolenia przez rodziców/opiekunów prawnych na zalogowanie się dziecka do serwisu)
- Portale społecznościowe muszą posiadać odpowiednie instrukcje dla użytkownika, np.: ułatwiać chroniące użytkownika ustawienie prywatności, być stale moderowane, dawać łatwą możliwość zgłoszenia naruszenia oraz zawierać informacje, jak uchronić się przed cyberprzemocą, bądź gdzie zgłaszać jej przypadki, zaś w przypadku dzieci wymagać podczas rejestracji akceptacji rodzica/opiekuna w momencie logowania się
- W przypadku stron komercyjnych wymagane jest, by nie mieszać treści z reklamami. Mieć limity zakupowe dla dzieci, metody płatności wymagające akceptacji rodzica, a reklamy niezakłócające korzystania ze strony i właściwie opisane. Na stronach dla dzieci nie powinny pojawiać się reklamy używek.

pozytywne treści

- budują pozytywne relacje z rodziną i przyjaciółmi
- rozwijają kreatywność
- bawią
- pozwalają odkryć nowe możliwości i umiejętności
- wzmacniają umiejętności społeczne
- stymulują wyobraźnię
- uczą i rozwijają
- zwiększają udział w życiu społecznym
- pozwalają uczniom tworzyć i rozpowszechniać własne treści online
- rozwijają pozytywny wizerunek samego siebie
- ułatwiają pozyskiwanie i utrzymanie umiejętności życiowych

Cyberprzemoc – profilaktyka i skuteczne reagowanie

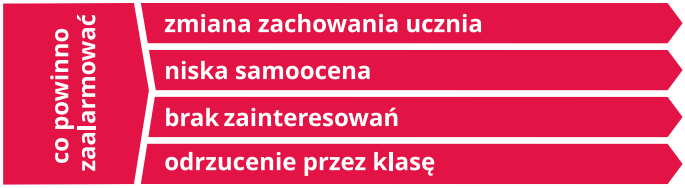
Zjawisko cyberprzemocy związane jest z istniejącą od zawsze przemocą, w tym przypadku najczęściej rówieśniczą. Nowe technologie dostarczyły kolejnych kanałów zastosowania przewagi fizycznej czy psychicznej. W języku polskim funkcjonuje wiele określeń dotyczących tego zjawiska: cyberdręczenie (*cyberstalking*), agresja elektroniczna, nękanie internetowe, prześladowanie w sieci (*cyberharassment*), mobbing elektroniczny (*cyberbullying*). Od tradycyjnie pojmowanej przemocy, czy to fizycznej czy też psychicznej, cyberprzemoc różni się możliwą skalą skrzywdzenia oraz długością trwania opresji, jakiej podlega dziecko. I w ten właśnie sposób definiuje się cyberprzemoc – jako długotrwałe zjawisko mogące przybrać formę nękania, straszenia, wyzywania czy też poniżania kogoś przy użyciu nowych technologii.

Internet to przestrzeń, w której dla młodych ludzi obecność jest obowiązkowa. Relacje społeczne młodzieży toczą się równolegle w świecie realnym i wirtualnym – dla nich to jedna rzeczywistość. Odrzucenie z grona osób należących do danej grupy, wykluczenie, niezauważanie bądź celowe ignorowanie również może być formą cyberprzemocy. Specyfika sieci powoduje, że dziecko może doświadczać cyberprzemocy stale i - z uwagi na wszechobecny dostęp do internetu - bez względu na miejsce, w jakim się znajduje.

? Co powinno zaniepokoić nauczyciela?

Przypadki cyberprzemocy często nie są ujawniane. Tylko ok. 9 proc. ofiar zgłasza problem nauczycielom, a 29 proc. rodzicom (J. Pyżalski, 2011). Co ważne, większość ofiar zna swoich prześladowców (66 proc.). **Nauczyciela czy wychowawcę powinna zaalarmować zmiana**

zachowania ucznia, niska samoocena, brak zainteresowań, odrzucenie przez klasę lub grupę. Należy mieć także świadomość, że każdy przypadek przemocy fizycznej lub psychicznej w szkole może mieć swoje odzwierciedlenie i kontynuację w sieci (np. nagranie telefonem komórkowym aktu przemocy lub upokarzającego zdjęcia, a następnie opublikowanie go w sieci).



Jak przeciwdziałać? Szkolne procedury

Jednym z podstawowych sposobów przeciwdziałania cyberprzemocy oraz pomocy w sprawnym reagowaniu na pojawienie się takiego zdarzenia w szkole jest **opracowanie przez placówkę własnej procedury postępowania w przypadku cyberprzemocy**. Procedura powinna uwzględniać przede wszystkim objęcie pomocą psychologiczno-pedagogiczną ofiary cyberprzemocy, poinformowanie rodziców ucznia o zaistniałym zdarzeniu i podjętych przez szkołę działaniach. Takie same procedury należy podjąć wobec sprawcy, którego dalsze zachowanie powinno być monitorowane. **Radzimy zawrzeć z uczniem-sprawcą kontrakt, którego nieprzestrzeganie skutkować powinno regulaminowymi konsekwencjami**. Szkoła ma obowiązek powiadomić policję i/lub sąd rodzinny, jeśli działania sprawcy/sprawców są jedną z kategorii przestępstw ściganych z urzędu. Należy pamiętać o zabezpieczeniu dowodów: maili, sms-ów, mms-ów, zdjęć, filmów lub komentarzy na portalach społecznościowych.

Cyberprzemoc wiąże się z tym, że zawsze po jednej stronie mamy sprawcę lub sprawców, po drugiej – ofiarę, ale bardzo często są jeszcze świadkowie. Świadkowie mogą z czasem przyłączyć się do sprawcy, ofiary lub pozostać obojętni. Według badań 19,6 proc. gimnazjalistów było sprawcami cyberbullingu, 6,6 proc. – ofiarami tego zjawiska, a 5,9 proc. ma doświadczenia w obydwu rolach (J. Pyżalski, 2012). **Szkoła, wypracowując model postępowania w przypadku ujawnienia cyberprzemocy, powinna objąć działaniami wszystkie trzy role: sprawcy, ofiary oraz świadka**, ponieważ tylko wówczas możliwe będzie skuteczne zakończenie sytuacji przemocowej oraz zapobieżenie wystąpieniu

cyberprzemocy w przyszłości. W internecie znaleźć można bardzo wiele materiałów edukacyjnych, filmów, scenariuszy lekcyjnych poświęconych temu problemowi (**kursor.edukator.pl, saferinternet.pl, dzieckowsieci.fdn.pl**).

Problem przemocy przy użyciu nowych technologii może dotknąć każdego, także pracownika szkoły: dyrektora, nauczyciela czy wychowawcę. Warto, żeby szkoła miała wypracowany schemat postępowania również i w takim przypadku. Fałszywe profile, modyfikacje fotografii i informacji tekstowych lub dźwiękowych, zamieszczanych na portalach społecznościowych lub uporczywe nękanie smsami spotkać mogą każdego.

Wiemy w jakiej skali zjawisko to występuje wśród młodzieży gimnazjalnej, natomiast naiwnością ze strony dorosłych byłoby myślenie, że przypadki tego typu nie zdarzają się również wśród młodszych dzieci. **Dlatego szkoła powinna przeprowadzać lekcje na temat cyberprzemocy na każdym etapie nauki**, żeby każdy z uczniów wiedział, co powinien zrobić w przypadku, kiedy dotknie go cyberprzemoc lub kiedy będzie jej świadkiem. Jasne i proste procedury, ujęte w dokumentacji szkolnej, pomogą zapobiegać temu zjawisku i zminimalizować jego niepożądane skutki.

Na koniec warto wspomnieć o nowym zjawisku – „wychowywaniu" przez publiczne poniżanie w sieci (*public shaming*), rodem ze średniowiecznego pręgierza. Takie ośmieszenie, poniżenie w formie zamieszczonego w internecie zdjęcia lub filmu, na którym dziecko publicznie kaja się, przeprasza lub trzyma kartkę z opisaną swoją przewiną stało się nową formą cyberprzemocy, stosowaną przez rodziców lub inne dorosłe osoby bliskie.

Najważniejsza zasada, jaką powinni kierować się dorośli, publikując w sieci informacje o dziecku (zdjęcia, wpisy) to uszanowanie jego godności i podmiotowości.

§ Prawo a cyberprzemoc

Mówi się, że prawo nie nadąża za życiem. Dzieje się tak zwłaszcza w przypadku internetu. Nie znaczy to jednak, że w sieci prawo nie funkcjonuje. **Nikt w sieci nie może czuć się anonimowo.**

W przypadku cyberprzemocy najczęściej dochodzi do naruszenia:

1. Artykułów Kodeksu karnego:
   - 190 – groźba karalna
   - 190a – uporczywe nękanie (*stalking*), podszywanie się
   - 191 – zmuszenie do określonego działania
   - 191a – naruszenie intymności seksualnej, utrwalenie wizerunku nagiej osoby bez jej zgody
   - 212 – zniesławienie
   - 216 – zniewaga
   - 267 – bezprawne uzyskanie informacji
   - 268 – utrudnianie zapoznania się z informacją
   - 268a – niszczenie danych informatycznych
   - 269 – uszkodzenie danych informatycznych
   - 287 – oszustwo komputerowe
2. Artykułu 107 Kodeksu wykroczeń – dokuczanie lub złośliwe wprowadzanie w błąd.

? Gdzie szukać pomocy w przypadku cyberprzemocy?

W Polsce istnieje punkt, w którym świadczona jest **bezpłatna i anonimowa pomoc dla nauczycieli, psychologów i pedagogów** poszukujących informacji lub wsparcia m.in. w przypadku cyberprzemocy. Zespół pomocowy prowadzony jest przez Fundację Dzieci Niczyje i oferuje pomoc pod numerem telefonu zaufania: **800 100 100** lub poprzez stronę **www.800100100.pl**.

Natomiast punkty **dla dzieci i młodzieży, tzw. telefony zaufania** prowadzone są przez psychologów Fundacji Dzieci Niczyje (tel. **116 111**) oraz Rzecznika Praw Dziecka (tel. **800 121212**).

Rekomendujemy, żeby informacja o telefonach zaufania była umieszczona na tablicy informacyjnej w centralnym punkcie szkoły.

Ryzykowne zachowania online

Niebezpieczne kontakty

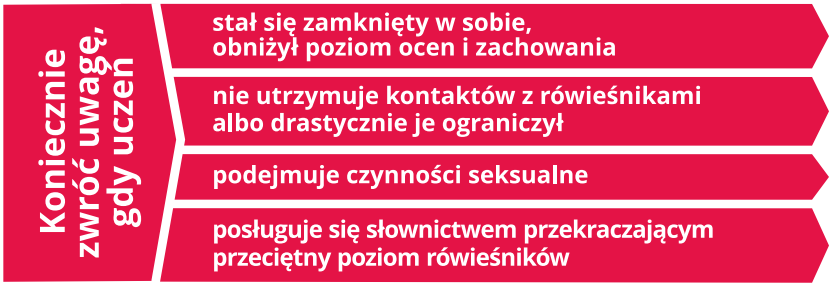
Komunikacja z innymi użytkownikami jest podstawową funkcją internetu. Chęć dzielenia się informacjami, przeżyciami i poglądami skłania nas do korzystania z portali społecznościowych, czytania serwisów informacyjnych czy uczestnictwa w grupach dyskusyjnych. Niestety wszędzie tam, gdzie jest możliwość bezpośredniej komunikacji pomiędzy osobą nieznajomą a młodym użytkownikiem, istnieje podwyższone ryzyko nawiązania niebezpiecznego kontaktu. Należy podkreślić, że **każda usługa internetowa, która pozwala na komunikację pomiędzy osobą nieznajomą a dzieckiem, wiąże się z podniesieniem poziomu zagrożenia**. Dlatego należy zwracać uwagę na wszystkie usługi, z których korzysta dziecko, nawet na gry dostępne na konsolach czy też urządzeniach mobilnych. Zasady bezpieczeństwa powinny obowiązywać zarówno w domu jak i w szkole.

Rolą nauczycieli i pedagogów jest uświadomienie młodym użytkownikom sieci, bez względu na to gdzie z niej korzystają, konieczności stosowania w praktyce zasad bezpiecznego korzystania z internetu.

Uwodzenie w sieci – najgroźniejsze zjawisko online

Jednym z rodzajów niebezpiecznych relacji online, o których najczęściej mówi się w mediach, jest kontakt z osobami o skłonnościach pedofilskich. Pedofil podejmuje komunikację w celu uwiedzenia dziecka, dążąc do pozyskania erotycznych lub pornograficznych materiałów z udziałem osoby niepełnoletniej, a także do spotkania się w świecie realnym, co może prowadzić do gwałtu.

Uwodzenie dziecka przez dorosłego może mieć kilka etapów, chociaż należy pamiętać, że każdy przypadek jest szczególny i powinien być rozpatrywany indywidualnie.



Proces uwodzenia jest długotrwały i może trwać kilka tygodni lub miesięcy. Celem jest zaprzyjaźnienie się z dzieckiem i odizolowanie go od jego otoczenia. Na początku pedofil wybiera swoją ofiarę szukając osoby, która będzie podatna na manipulację, samotna, bez wsparcia najbliższych. W wielu przypadkach wcale nie kłamie na temat swojego wieku, stawiając się w roli dorosłego przyjaciela, przewodnika, mentora. Następnie buduje zależność pomiędzy dzieckiem a sobą, odizolowuje je od otoczenia, dbając przy tym, aby znajomość była trzymana w tajemnicy. Zdarza się, że szantażuje swoją ofiarę, straszy ją oraz wpaja jej poczucie winy, jeśli ta nie odpowiada w wystarczająco krótkim czasie na wysyłane wiadomości.

Na tym etapie pedofil często doładowuje dziecku telefon lub nawet funduje mu aparat telefoniczny. Celem takiego działania jest chęć utrzymania ciągłego kontaktu z ofiarą oraz wzbudzenie u niej potrzeby odwzajemnienia się za otrzymany prezent. Kolejnym etapem jest narażenie dziecka na kontakt z materiałami pornograficznymi. W rozmowach pojawia się tematyka seksualna oraz prośby o przesłanie zdjęć czy filmów erotycznych zrobionych przez dziecko.

Osoba o pedofilskich skłonnościach może również eksponować materiały prezentujące seksualne wykorzystanie małoletnich (treści pornograficzne z udziałem dziecka), chcąc w ten sposób udowodnić, że inni też tak robią i jest to „normalne". Jeśli dziecko przesłało jakikolwiek materiał, na którym jest rozebrane, występuje w prowokującej pozie i nie chce tej znajomości kontynuować, wówczas **pedofil może zastosować szantaż w celu pozyskania dalszych materiałów** oraz podjąć próbę zrzucenia odpowiedzialności na ofiarę.

Taka manipulacja jest niebezpieczna również z innego powodu. Jeśli uwiedzenie wychodzi na jaw, ofiara może odczuć, że straciła jedynego przyjaciela. Dlatego **niezwykle ważne jest, aby od początku budować w dziecku poczucie, że nie jest odpowiedzialne za to, co się stało**. Nawet jeśli ofiara sama wykonywała zdjęcia bądź filmy o tematyce seksualnej.

Proces uwodzenia może też trwać krócej i nie polegać na zbudowaniu silnej relacji z ofiarą. Do zespołu Dyżurnet.pl, zajmującego się przyjmowaniem zgłoszeń przypadków występowania w internecie treści zabronionych prawem, wpływają informacje o profilach nastolatków (również tych młodszych jedenasto-, dwunastoletnich) korzystających z serwisów o tematyce erotycznej i pornograficznej. Treści, które kierują dorośli użytkownicy internetu do dziecka noszą znamiona pedofilii. Są to zachęty do podjęcia zachowań seksualnych lub komentarze jawnie seksualne. Dziecko, które przypadkiem lub z ciekawości odwiedzi taki serwis, jest narażone na kontakt z treściami pornograficznymi.

⚠ Niebezpieczne i szkodliwe treści

Aby nie narażać osoby niepełnoletniej na kontakt z treściami pornograficznymi, **należy przede wszystkim uświadamiać dziecko, że w internecie są strony przeznaczone tylko dla dorosłych**. Należy również przestrzegać dziecko, żeby za każdym razem, kiedy natknie się na coś niepokojącego, zgłaszało to osobie dorosłej. Jednak dla pewności powinniśmy wyposażyć każde urządzenie, z którego korzysta dziecko, w aktywowany filtr kontroli rodzicielskiej. Trzeba pamiętać, że ochrona technologiczna nie jest doskonała, ale jest wysoce skuteczna w blokowaniu materiałów pornograficznych. Radzimy, by wychowawca poruszył ten temat podczas spotkań z rodzicami, a administratorzy zarządzający infrastrukturą szkolną ustawili odpowiednie zabezpieczenia na sprzęcie w szkolnej pracowni komputerowej.

Niestety, filtry kontroli rodzicielskiej nie zawsze dobrze radzą sobie z innymi kategoriami treści przeznaczonymi wyłącznie dla dorosłych użytkowników.

Do treści szkodliwych, z którymi najmłodsi nie powinni mieć styczności, zalicza się:

- treści związane z prezentowaniem przemocy (m.in. cyberprzemoc, wulgaryzmy, bójki i „ustawki", okrucieństwo wobec zwierząt)
- treści nawołujące do przemocy (m.in. treści rasistowskie i ksenofobiczne)
- treści prezentujące niebezpieczne zachowania (m.in. wyścigi samochodowe, zwiedzanie niebezpiecznych miejsc, jak budowy i ruiny, uprawianie sportów ekstremalnych bez asekuracji i zabezpieczeń)
- treści promujące zachowania autodestrukcyjne (m.in. treści nawołujące do samookaleczeń, samobójstw, restrykcyjnej diety, zażywania substancji psychoaktywnych)
- treści prezentujące niewłaściwy obraz rzeczywistości (m.in. treści dyskryminujące, spiskowe, pornograficzne)
- treści makabryczne (m.in. treści przedstawiające ofiary wojny lub wypadków, przypadki medyczne, bestialstwo wobec zwierząt).

Wymienione powyżej treści nie powinny znajdować się w szerokim, publicznym dostępie. Niestety przepisy prawne (nie tylko polskie) nie zawsze regulują kwestie związane z publikowaniem tego typu materiałów. Często założenie ostrzeżenia, które może pomóc w filtrowaniu treści, zależy od dobrej woli właściciela serwisu oraz od zasad moderacji. Niektóre strony internetowe nie akceptują treści szkodliwych (w części lub w całości), ale ich publikowanie zależy od szybkości i jakości moderacji. Niejednokrotnie treści szkodliwe są publikowane w komentarzach.

Kontakt z niebezpiecznymi treściami może prowadzić do wykrzywienia obrazu rzeczywistości oraz wzbudzić u młodego człowieka poczucie zagrożenia i lęku, a także spowodować różnego rodzaju zaburzenia jego rozwoju.

Pamiętaj!

Gdy natkniesz się na treści nielegalne (materiały pornograficzne z udziałem osoby małoletniej, zawierające twardą pornografię, treści pornograficzne bez zabezpieczenia, treści nawołujące do rasizmu i ksenofobii) **zgłoś incydent na policję lub do dedykowanego zespołu dyżurnet.pl**

Krytyczne podejście do informacji w sieci

Odbiorowi każdej informacji w internecie powinno towarzyszyć ograniczone zaufanie i krytyczne podejście do danego źródła wiedzy. Ze względu na specyfikę współczesnych mediów, którym zależy na krótkim czasie publikowania informacji, nawet największe serwisy medialne nie są w stanie uchronić się od przedstawiania nieprawdziwej i niesprawdzonej wiadomości.

Nauczyciele powinni wytłumaczyć uczniom, że czytając, a przede wszystkim cytując informację, powinni zwrócić baczną uwagę na to, kto ją publikował. Analizując zalety i wady danego produktu przed jego zakupem, należy sprawdzić kto jest twórcą opinii. Z pewnością bardziej wiarygodnym źródłem będzie niezależny raport wykonany przez ośrodek konsumenta (niezależnego badacza), niż informacje przedstawiane na stronie internetowej producenta. Należy podkreślić, że firmy promujące produkty lub usługi w kampaniach marketingowych wykorzystują fora internetowe do kształtowania opinii użytkowników. Pracownicy firmy lub osoby specjalnie w tym celu wynajęte prowadzą anonimowy tzw. „marketing szeptany" podszywając się pod zwykłych użytkowników. Dlatego bardzo trudno mieć pewność, że dana opinia jest obiektywna.

Omawiając z młodymi użytkownikami internetu kwestię podejścia do informacji publikowanych w sieci, radzimy przyjrzeć się, jak prowadzona jest najpopularniejsza encyklopedia internetowa – Wikipedia. Należy zwrócić uwagę uczniów na historię hasła, które ulegało zmianie, było edytowane przez wiele, często anonimowych osób, bądź nie jest weryfikowane przez ekspertów. Zgodnie z filozofią Wikipedii, encyklopedia tworzona jest wspólnym wysiłkiem internetowej społeczności, dlatego często rozwija się nierównomiernie i pewne dziedziny lub hasła są znacznie bardziej rozbudowane niż pozostałe.

Pamiętaj!

Zwracaj uwagę, szczególnie nastolatkom, że informacje publikowane w internecie **mogą być nieprawdziwe lub przekłamane.**

Przekaż uczniom zasady weryfikacji informacji: czy na stronie jest podany autor, instytucja, data publikacji, kontakt do autorów oraz czy strona jest powiązana z podobnymi tematycznie serwisami.

Praca twórcza czy odtwórcza? Problematyka plagiatu

Pokolenie kopiuj - wklej

Ochrona praw autorskich jest w ostatnich latach jednym z największych wyzwań, zwłaszcza w kontekście internetu, a **łamanie tych praw należy do najczęstszych naruszeń występujących w sferze publicznej**. Problem jest bardzo złożony, dlatego że dotyka praktycznie wszystkich środowisk niezależnie od wieku czy wykształcenia. Z wydanej w 2014 roku *Analizy wpływu zjawiska piractwa treści wideo na gospodarkę w Polsce* sporządzonego przez firmę PwC wynika, że około **7,5 mln Polaków korzysta regularnie z serwisów oferujących nielegalny dostęp do treści wideo** – co stanowi prawie 30 proc. wszystkich internautów i aż 94 proc. osób poszukujących treści wideo w internecie. Przyczyną korzystania z nielegalnie udostępnionych materiałów jest najczęściej bogatsza oferta i oczywiście tańszy bądź bezpłatny dostęp.

Według badania portalu Zadane.pl 55 proc. uczniów wszystkich poziomów edukacji korzysta z gotowych prac domowych.

§ Co podlega prawu autorskiemu?

Przedmiotem praw autorskich jest *każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości przeznaczenia i sposobu wyrażenia* (art. 1 ustawy o prawie autorskim i prawach pokrewnych). Twórcy przysługuje autorskie prawo majątkowe, które jednak po pewnym czasie może wygasnąć lub być przeniesione na inny podmiot, oraz autorskie prawo osobiste, które jest bezterminowe i niezbywalne, czyli trwale

związane z autorem. Przykładem twórczości objętej ochroną jest utwór muzyczny lub literacki, prace plastyczne, fotografie lub wzory przemysłowe.

§ Prawo a cyfrowa rzeczywistość

Prawo autorskie, które obowiązuje w Polsce określa ustawa z 1994 roku. Co prawda podlegała ona nowelizacjom, jednak w dalszym ciągu nie do końca precyzyjnie odnosi się do kwestii łamania prawa online, zwłaszcza w odniesieniu do tzw. dozwolonego użytku prywatnego, co często utrudnia ściganie zachowań nielegalnych. Przykładowo, zapoznanie się z utworem za pośrednictwem nielegalnego serwisu jest zgodne z prawem. Jedynym warunkiem jest wykorzystanie go do użytku własnego. Dodatkowo mylące jest, że za materiały nielegalnie udostępnione płaci się, wykorzystując bankowość elektroniczną bądź za pośrednictwem sieci komórkowych, co może sugerować legalność całej operacji. **Często całkowicie nie ma się świadomości, że płaci piratom.**

Prawo polskie a prawa autorskie

Art. 115. (Ustawy o prawie autorskim i prawach pokrewnych)

1. Kto przywłaszcza sobie autorstwo albo wprowadza w błąd, co do autorstwa całości lub części cudzego utworu albo artystycznego wykonania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

2. Tej samej karze podlega, kto rozpowszechnia bez podania nazwiska lub pseudonimu twórcy cudzy utwór w wersji oryginalnej albo w postaci opracowania, (...).

Art. 116.0 Ustawy o prawie autorskim i prawach pokrewnych

1. Kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli sprawca dopuszcza się czynu określonego w ust. 1 w celu osiągnięcia korzyści majątkowej, podlega karze pozbawienia wolności do lat 3.

3. Jeżeli sprawca uczynił sobie z popełniania przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępczą, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności od 6 miesięcy do lat 5.

4. Jeżeli sprawca czynu określonego w ust. 1 działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ Dozwolony użytek

Zgodnie z art. 23. 2. ustawy o prawie autorskim i prawach pokrewnych zakres własnego użytku osobistego obejmuje korzystanie z pojedynczych egzemplarzy utworów przez osoby pozostające w związku osobistym, na przykład pokrewieństwa, powinowactwa lub stosunku towarzyskiego. Zapis ten miał urealnić prawo do kopiowania na przykład pojedynczych, pożyczonych płyt. Jednak dzisiaj nie oddaje on rzeczywistości, **ponieważ często dzieci i młodzież, aktywne na portalach społecznościowych, mają po kilkuset znajomych, są członkami wielotysięcznych grup tematycznych, a to, w gronie „znajomych", umożliwia dystrybucję materiałów na ogromną, nieograniczoną wręcz skalę.**

Główną drogą zmierzającą do poprawy poszanowania praw autorskich przez młodych użytkowników sieci są **kompleksowe akcje uświadamiające.** Podczas zajęć w szkole poświęconych tematowi poszanowania cudzej twórczości należy zapoznawać uczniów z zapisania prawa autorskiego **uświadamiać konsekwencje** karne związane z tego rodzaju wykroczeniami oraz uwrażliwiać też na straty jakie ponoszą twórcy.

W kontekście szkół niezwykle istotne jest, aby rodzice zdali sobie sprawę z powagi sytuacji związanej z kopiowaniem, przepisywaniem oraz nielegalnym ściąganiem plików. **Dorośli powinni mieć świadomość, jak istotne jest, aby młodzi ludzie uczyli się indywidualnej pracy oraz, że pozorna oszczędność w budżecie domowym związana ze ściąganiem nielegalnych plików jest obarczona odpowiedzialnością karną**.

Online? Offline? Czyli o problemie nadużywania internetu przez dzieci i młodzież

Współczesnych nastolatków, którzy z wrodzoną łatwością wykorzystują dynamiczny rozwój i potencjał internetu, zwykło określać się mianem **cyfrowych tubylców**. Dla tej grupy internet jest bowiem nieodłącznym elementem życia społecznego, codziennej aktywności i rozrywki. **Dziś raczej żaden nastolatek nie potrafiłby obejść się bez technologi cyfrowych.** Jak pokazują badania, zdecydowana większość gimnazjalistów (86,2 proc.) loguje się do sieci codziennie, w tym 43,2 proc. pozostaje online bez przerwy - głównie za sprawą urządzeń mobilnych (Pedagogium WSNS, 2014). Do połączenia się z siecią **nastolatki najczęściej wykorzystują smartfony** (54,3 proc.) oraz **laptopy** (52,5 proc.). Co więcej, coraz młodsze dzieci korzystają z multimediów - **ponad 40 proc. rocznych i dwuletnich dzieci w Polsce korzysta z tabletów lub smartfonów**, a wśród nich niemal co trzecie korzysta z urządzeń mobilnych codziennie lub prawie codziennie (*FDN, 2015*).

Dla młodych ludzi sieć często staje się pozornie prostym narzędziem do kształtowania swojego wizerunku, miejscem złudnie bezpiecznym, gwarantem anonimowości czy panaceum na ich problemy. Nic więc dziwnego, że **dzieci i młodzież narażone są na utratę kontroli nad czasem korzystania z internetu, co może prowadzić do zaniedbywania nauki, zdrowia, a także do unikania kontaktu z rówieśnikami.** Odsetek polskich nastolatków dysfunkcyjnie korzystających z sieci, czyli nadużywających internetu lub zagrożonych nadużywaniem, wynosi 13,3 proc. (EU NET ADB, 2012). Jak pokazały badania EU Kids Online (2011) z powodu nadmiernego używania internetu 35 proc. dzieci zaniedbuje rodzinę, znajomych, naukę szkolną albo hobby, a 38 proc. przyłapało się na tym, że surfuje po internecie bez celu, nie znajdując dla siebie nic interesującego.

Problem nadużywania internetu stał się w ostatnich latach częstym przedmiotem dyskusji społecznej, naukowej czy medialnej. Jest to skomplikowane i niejednoznaczne zjawisko, bo przysparza trudności nie tylko w pełnym zrozumieniu jego przebiegu, rozpoznaniu przyczyn

i skutków, ale także w osiągnięciu zgodności co do stosowanej definicji i nazewnictwa. Najczęściej używa się terminu „siecioholizm", „netoholizm", „patologiczne używanie" internetu, „nadużywanie", czy też „uzależnienie" od internetu.

Najwięcej kontrowersji powoduje jednak ostatni termin, gdyż zgodnie z opinią niektórych badaczy należy odróżnić problem „uzależnienia" od internetu od uzależnień fizjologicznych (m.in. alkoholizm, narkomania). Inni badacze wskazują zaś, że tego rodzaju uzależnienie mieści się w szerszej grupie uzależnień od określonej czynności (inaczej: uzależnienie behawioralne), do której zaliczyć można także m.in. uzależnienie od pornografii czy hazardu. Bez względu jednak na stosowaną terminologię, problem ten niewątpliwie istnieje i wymaga szczególnych starań na rzecz skutecznej profilaktyki, podejmowanej w szkole i w rodzinie. **Bardzo istotne jest, aby nauczyciele i rodzice podnosili świadomość i wiedzę na ten temat, by próbowali zrozumieć przyczyny i skutki nadużywania internetu przez najmłodszych, żeby mogli odpowiednio wcześnie rozpoznać problem i skutecznie mu przeciwdziałać.**

Charakterystyka nadmiernego korzystania z internetu

Warto zwrócić uwagę na to, że **problem nadużywania internetu nie sprowadza się jedynie do ilości czasu**, jaki dana osoba spędza w sieci. Muszą pojawić się dodatkowe okoliczności, które można scharakteryzować (Shapira N. A. i in., 2003) następująco:

1. Czas i intensywność korzystania z internetu wymyka się spod kontroli, użytkownik spędza w sieci więcej czasu niż planował i odczuwa trudną do odparcia potrzebę korzystania z internetu
2. Spędzanie czasu w sieci prowadzi do zaniedbywania innych aspektów życia, przysparza problemów na różnych płaszczyznach lub powoduje cierpienie uzależnionego bądź osób z jego otoczenia.

Objawy, jakie przejawia osoba dysfunkcyjnie korzystająca z internetu

Wyróżnia się kilka zachowań, które mogą być objawem patologicznego korzystania z internetu. Dr n. med. Bohdan Woronowicz z Instytutu Psychiatrii i Neurologii oraz Centrum AKMED w Warszawie zaliczył do nich przede wszystkim:

- spędzanie przy komputerze **coraz większej ilości czasu kosztem innych zainteresowań**

- **zaniedbywanie obowiązków** rodzinnych i szkolnych z powodu aktywności w internecie
- pojawianie się **konfliktów rodzinnych** związanych z internetem
- **kłamstwa** dotyczące czasu spędzanego w internecie
- podejmowanie **nieudanych prób** jego ograniczenia
- reagowanie **rozdrażnieniem** lub nawet **agresją**, gdy korzystanie z komputera jest utrudnione lub niemożliwe.

? Czynniki ryzyka i przyczyny nadużywania internetu

Przyczyny dysfunkcyjnego korzystania z internetu przez dzieci i młodzież są skomplikowane i mogą być różne dla danej osoby. **Na pewno nie bez znaczenia jest tutaj** sytuacja życiowa oraz cechy osobowościowe dziecka. Wśród istotnych czynników należy wymienić następujące:

uzależniający potencjał internetu	Internet jest nieograniczony. Jest dostępny w każdym miejscu i każdej chwili. Pozostawanie stale online nie wiąże się ze zwiększonymi kosztami. Korzystanie z internetu to forma aktywności dostarczająca nieregularnych pozytywnych wzmocnień.
niekonstruktywna strategia radzenia sobie ze stresem	Dziecko ucieka w świat wirtualny przed trudnościami życiowymi, gdy brakuje mu akceptacji, ma problemy rodzinne lub niepowodzenia w szkole. Szereg ogólnych problemów psychologicznych - nieśmiałość, niska samoocena, lęki, depresja, neurotyzm.

? Co najczęściej uzależnia

- gry internetowe
- hazard online
- aktywność na portalach społecznościowych
- pornografia i cyberseks.

? Jak postępować w przypadku nadużywania internetu przez dziecko

Skuteczne przeciwdziałanie nadużywaniu internetu przez dzieci i młodzież powinno bazować na wiedzy na temat tego problemu, zrozumieniu jego przyczyn, a także odpowiednio wczesnym rozpoznaniu symptomów takiego zachowania. Przede wszystkim bardzo istotna jest obserwacja, rozmowa i próba zrozumienia wirtualnych nawyków i zainteresowań dzieci. Nie ulega wątpliwości, że to przede wszystkim zadanie rodziców. Jednak należy podkreślić, że także nauczyciele i pedagodzy mogą odegrać tu znaczącą rolę.

- Rekomendujemy, żeby szkoła opracowała **wewnętrzne procedury reagowania i postępowania** w przypadku pojawienia się problemu nadużywania internetu przez ucznia.
- W przypadku zaobserwowania u ucznia niepokojących zachowań (np. zdenerwowanie, kiedy nie może skorzystać z komputera, izolacja, zaniedbywanie nauki, higieny osobistej oraz zdrowia, unikanie aktywnego wypoczynku) radzimy, żeby **nauczyciel porozmawiał z dzieckiem**, spróbował ustalić przyczynę oraz zaoferował swoją pomoc.
- W przypadku, gdy uczeń nadmiernie korzysta z internetu, szkoła powinna **nawiązać współpracę z rodzicami lub opiekunami** dziecka w celu ustalenia zasad dalszego postępowania.
- Niezwykle istotne jest udzielenie przez nauczyciela lub szkolnego pedagoga **wsparcia dla rodziców**, którzy nie zawsze rozumieją trudności i problemy dziecka, co powoduje, że nie radzą sobie z trudną sytuacją.
- Rekomendujemy, żeby pedagog lub psycholog szkolny pomógł uczniowi i jego rodzicom **skontaktować się ze specjalistyczną placówką** w przypadku, gdy wskazane jest przeprowadzenie diagnozy problemów ucznia i objęcie dziecka dalszą terapią.
- Nie należy zapominać, że długotrwałe korzystanie z nowych mediów może mieć **negatywny wpływ na zdrowie psychofizyczne** powodując m.in.: poczucie zmęczenia, brak koncentracji, pogorszenie wzroku, wady postawy, bóle głowy, czy problemy psychologiczne (lęk, depresja, bezsenność, zawroty głowy).

Pamiętaj!

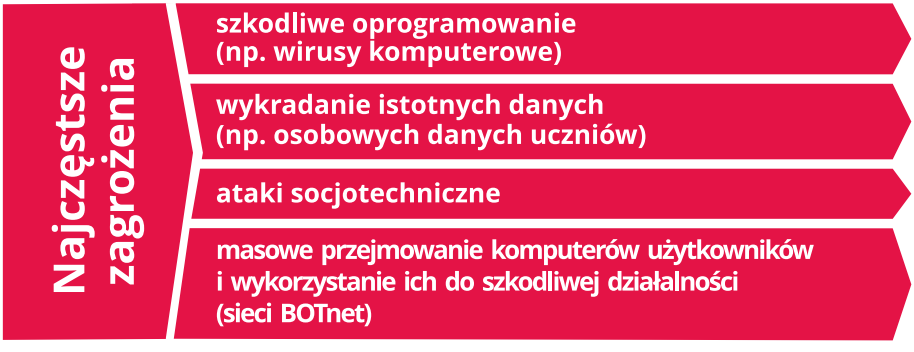
Nauczyciel lub rodzic może skorzystać z bezpłatnej i anonimowej pomocy telefonicznej i online dla dorosłych (tel. 800 100 100, www.800100100.pl), wówczas gdy potrzebuje wsparcia i informacji w zakresie pomocy dzieciom przeżywającym trudności będące konsekwencjami zachowań ryzykownych (m.in. nadużywanie internetu)

Szkoła w sieci - jak zabezpieczyć infrastrukturę informatyczną w placówce edukacyjnej?

Dostęp do Internetu w szkole to infrastruktura składająca się z konkretnego sprzętu i oprogramowania, które stanowią stale rozwijająca się bazę technologiczną dla coraz powszechniejszych usług elektronicznych. **Infrastruktura ta podlega jednak rozmaitym zagrożeniom,** którym należy poświęcić uwagę, aby zapewnić jej bezpieczne funkcjonowanie.

Zagrożenia

Wśród typowych czynników zagrażających bezpieczeństwu można wymienić między innymi niedoskonałości i luki w programach (systemy operacyjne, aplikacje), błędy konfiguracyjne sprzętu i oprogramowania, niedostateczne czy nieumiejętne administrowanie infrastrukturą. Niezwykle **istotna jest świadomość użytkowników na temat zagrożeń** oraz stosowanie przez nich dobrych praktyk bezpiecznego korzystania z internetu.



Placówki szkolne, coraz lepiej wyposażone w infrastrukturę sieciową i aplikacyjną, podlegają w tym samym stopniu co inne instytucje i przedsiębiorstwa typowym zagrożeniom w cyberprzestrzeni. Jednocześnie pełnią one ważną misję edukacyjną w stosunku do dzieci i młodzieży w zakresie bezpiecznego korzystania z internetu, zatem powinny być chronione.

Kadra placówki szkolnej powinna zatem zadbać, aby infrastruktura TIK spełniała standardy bezpieczeństwa, a korzystanie z niej odbywało się zgodnie z opracowanymi w placówce regulaminami.

Aspekty technologiczne

- Dostęp do internetu od wiarygodnego dostawcy (wpisanego do rejestru UKE)
- Bezpieczna infrastruktura na styku danej placówki z internetem, zawierająca typowe elementy: zapora (firewall), system antywirusowy oraz inne zabezpieczenia, takie jak IDS/IPS, filtrowanie dostępu do treści szkodliwych itp.
- System zarządzania dostępem użytkowników do usług i aplikacji. Błędem jest oferowanie anonimowego dostępu do internetu czy też dostępu do sieci i aplikacji wewnętrznych na terenie placówki
- Bezpieczna sieć bezprzewodowa (WiFi) zapewniająca odpowiednie mechanizmy uwierzytelniania i szyfrowania
- Bezpieczna i stale monitorowana witryna internetowa szkoły
- Dzienniki zdarzeń (logi) zbierane z kluczowych elementów infrastruktury potrzebne przy systematycznej administracji oraz w razie wystąpienia incydentu
- Wypracowane podejście do wykorzystywania na terenie placówki urządzeń prywatnych należących do kadry oraz uczniów – takich jak laptopy, tablety, smartfony korzystające z lokalnej sieci WiFi.

Elementy organizacyjne

- Odpowiednie zarządzanie (administrowanie) wszystkimi elementami infrastruktury
- Polityka określająca podstawowe zasady i standardy bezpieczeństwa przyjęte w instytucji
- Regulaminy korzystania z usług i aplikacji na terenie placówki oraz zdalnie (np. przez rodziców poprzez sieć internet)
- Procedury reagowania na pojawiające się zagrożenia i incydenty naruszające bezpieczeństwo
- Zasady i wymagania przy zakupie usług, sprzętu, aplikacji, systemów informatycznych gwarantujące odpowiedni poziom bezpieczeństwa już na etapie budowania infrastruktury IT.

Na wszystkich lekcjach, podczas których omawiane są zagadnienia technik komputerowych czy internetu, należy włączyć aspekt bezpiecznego korzystania z sieci z uwzględnieniem aktualnych trendów w zakresie cyberzagrożeń.

Warto promować wiedzę o cyberbezpieczeństwie na terenie placówki, między innymi, uczestnicząc w kampaniach i konkursach, takich jak projekt Cyfrowobezpieczni.pl (**www.cyfrowobezpieczni.pl**), ECSM (**bezpiecznymiesiac.pl**), czy Dzień Bezpiecznego Internetu, umieszczając informacje o cyberbezpieczeństwie na stronie internetowej placówki szkolnej.

Kadra nauczycielska, w szczególności osoby, które uczą przedmiotów związanych z technikami komputerowymi oraz możliwościami internetu, powinna systematycznie podnosić swoje kwalifikacje uczęszczając na kursy i szkolenia, zapraszając ekspertów i wykorzystując e-learning.

Poziom zainteresowania edukacją przez uczniów w zakresie cyberbezpieczeństwa ściśle zależy od postawy i podejścia kadry w stosunku do Internetu i nowych technologii. Rekomendujemy, by nauczyciele zapoznali uczniów z zasadami bezpiecznego zachowania w sieci.

Zasady bezpiecznego zachowania w sieci:

NALEŻY

- regularnie zmieniać hasła do urządzeń, aplikacji i serwisów internetowych; hasła powinny być odpowiednio długie i zawierać małe, duże litery, cyfry oraz znaki specjalnie
- jeśli to możliwe używać haseł dwuskładnikowych (np. urządzenia generujące hasła jednorazowe czy sms w telefonie)
- korzystać z szyfrowanych połączeń z witrynami internetowymi (zamknięta kłódeczka w pasku adresowym przeglądarki), szczególnie przy podawaniu wrażliwych danych - można sprawdzić dane witryny po kliknięciu w kłódeczkę
- zwracać uwagę na zagrożenia nie tylko przy korzystaniu z poczty elektronicznej czy surfowaniu po stronach WWW - wirusy czy phishing zdarza się także na portalach społecznościowych czy internetowych grach komputerowych

- czytać regulaminy usług internetowych, z których korzystamy
- mieć włączone systemy antywirusowe czy filtrujące oraz zapory sieciowe, które pomogą nam dbać o bezpieczeństwo.

NIE NALEŻY

- otwierać załączników e-maili oraz klikać na adresy internetowe (*linki*) zawarte w e-mailach pochodzących z nieznanych źródeł - załączniki mogą zawierać szkodliwe programy a linki prowadzić do zarażonych stron internetowych
- podawać identyfikatorów lub haseł na nie zaufanych stronach internetowych
- dokonywać ważnych operacji w internecie poprzez publiczne, otwarte sieci WiFi
- ściągać na urządzenia mobilne aplikacji, które nie pochodzą z oficjalnych sklepów – np. Google, Apple, ponieważ mogą mieć ukryte funkcje narażające nasze bezpieczeństwo lub prywatność.

Jeśli zdarzy się incydent, ważna jest odpowiednia reakcja!

- Rekomendujemy, by placówka szkolna posiadała ustanowioną rozporządzeniem dyrektora lub uchwałą rady pedagogicznej **procedurę reagowania w sytuacji naruszenia bezpieczeństwa infrastruktury szkolnej sieci.** W ramach tej procedury powinien być ustanowiony pojedynczy punkt kontaktowy (osoba, zespół osób), do których można zgłosić zdarzenie. Rodzice powinni zachęcać dyrekcję szkoły do jej wprowadzenia
- Jeśli komputer przestaje sprawnie działać, na przykład jest wolny, zawiesza się, nie zawsze oznacza to awarię – należy sprawdzić czy nie jest zawirusowany, czy ma działający program antywirusowy lub jaka jest data ostatniej aktualizacji. Należy również przeskanować programem antywirusowym całą zawartość urządzenia
- Jeśli placówka szkolna padnie ofiarą oszustw w internecie, należy zgłosić przestępstwo na Policję. Wówczas urządzenie komputerowe (jego zawartość) jest dowodem w sprawie i powinno być zabezpieczone do ewentualnej analizy.

Profil administratora IT w placówce szkolnej

W badaniu European Schoolnet: *The School IT Administrator* można prześledzić profil typowego administratora infrastruktury TIK w naszym kraju na tle Europy. **95% respondentów (administratorów IT) dzieli funkcje nauczycielskie z zarządzaniem infrastrukturą komputerową w szkole.** 88% ma także jeszcze inne obowiązki, jak np. prowadzenie szkolnego laboratorium czy sali komputerowych. Wysoko, na tle średniej unijnej kształtują się kwalifikacje tych osób w dziedzinie informatyki (80% respondentów deklaruje takie kwalifikacje – średnia w badaniu UE to 60%). Jeśli chodzi o edukację oraz wsparcie, to szkolni administratorzy głównie korzystają z krótkich kursów dostępnych poza szkołą, pomocy kolegów czy akademii organizowanych przez producentów rozwiązań. W mniejszym stopniu są to formalne kursy organizowane przez placówki, pozwalające na zdobywanie usystematyzowanej wiedzy i certyfikację.

Wśród największych wyzwań czy zagrożeń polscy administratorzy w placówkach szkolnych wymieniają: bezpieczeństwo, zarządzanie urządzeniami przynoszonymi do szkoły (ang. Bring Your Own Device - BYOD), zarządzanie infrastrukturą TIK, a także wsparcie i rozwój personelu odpowiedzialnego za TIK.

Wyzwania i zagrożenia

Największe wyzwania i zagrożenia w zarządzaniu szkolną infrastrukturą wg administratorów (badania European Schoolnet).

Największe wyzwania i zagrożenia	▸ zapewnienie bezpieczeństwa ▸ zarządzanie prywatnymi urządzeniami przynoszonymi do szkoły ▸ zarządzanie infrastrukturą IT ▸ wsparcie i rozwój personelu odpowiedzialnego za IT
Największe problemy	▸ współdzielenie zadań nauczycielskich i technicznych ▸ zbyt rozbudowane środowisko techniczne w stosunku do możliwości jego sprawnego bezpiecznego utrzymania ▸ przestarzała infrastruktura

Aplikacja mobilna - oprogramowanie działające na urządzeniach przenośnych (m.in. smartfon, tablet), które powstaje dla różnych systemów operacyjnych (m.in. Android, Apple iOS, Windows Phone) i napisane jest w różnych językach programowania. Aplikacje mogą być wykorzystywane do różnych celów np. komunikacji, edukacji, rozrywki. Są one oferowane przez sklepy internetowe (m.in. Google Play, App Store), bezpłatnie lub za opłatą.

CERT - zespół ds. reagowania na przypadki naruszenia bezpieczeństwa teleinformatycznego (ang. Computer Emergency Response Team). Najstarszym w Polsce jest działający w NASK zespół CERT Polska (**www.cert.pl**).

Cyberprzemoc - przemoc z użyciem mediów elektronicznych. Do takich działań zalicza się m.in. nękanie, wyzywanie, straszenie, poniżanie kogoś w internecie lub przy użyciu telefonu, robienie komuś zdjęć lub filmów bez jego zgody, ich publikowanie i rozsyłanie lub podszywanie się pod kogoś w sieci. Cyberprzemoc może dotknąć wszystkich użytkowników internetu, bez względu na wiek czy poziom umiejętności posługiwania się komputerem. Sprawcy cyberprzemocy mają wrażenie, że są anonimowi, co pobudza i zachęca ich do działania.

Cyberprzestępczość - inaczej przestępczość komputerowa, czyli niezgodna z prawem działalność skierowana przeciwko systemom komputerowym lub wykonywana przy pomocy systemów komputerowych, sieci komputerowych czy internetu, jako narzędzi służących do dokonania przestępstwa.

Cyberstalking (dosł. cyberdręczenie) - zjawisko natrętnego i złośliwego dręczenia pojedynczej osoby, grupy osób lub całej organizacji przy użyciu technologii informacyjnej, w szczególności internetu. Prześladowca określany jest często jako stalker. Jest to zjawisko z grupy cyberprzemocy.

Edukacja medialna - kształtowanie umiejętności świadomego, krytycznego, odpowiedzialnego i selektywnego korzystania ze środków masowego przekazu, tworzenia i nadawania przekazów medialnych.

Erotyka dziecięca - treści, które przedstawiają dziecko w seksualnym kontekście, natomiast nie są nielegalne. Małoletni są upozowani

w erotycznych i wyzywających pozach, ubrani w erotyczną bieliznę. Wytwarzanie takich treści jest formą wykorzystania seksualnego małoletnich, a materiały są atrakcyjne dla osób o pedofilskich skłonnościach.

Filtr rodzicielski - program lub usługa, chroniąca przed dostępem dziecka do materiałów szkodliwych - treści pornograficznych i przemocy w internecie. Usługę oferują niektórzy dostawcy internetu. W popularnych wyszukiwarkach można również ustawić filtr rodzicielski. Rodzic może także nabyć taką usługę w postaci programu do zainstalowania na komputerze. Filtr rodzinny nie daje 100 proc. gwarancji bezpieczeństwa dziecka.

Hacking - uzyskanie nieuprawnionego dostępu do komputera, systemu komputerowego, danych czy informacji zawartych w systemach komputerowych.

Hejt internetowy - termin ten stosuje się przede wszystkim do takich wypowiedzi, które są agresywne i nie mają podłoża ideologicznego.

Hosting - udostępnianie przez dostawcę usług internetowych zasobów serwerowni. Usługa polega na oddaniu do dyspozycji m.in. określonej objętości dysku twardego, maksymalnej ilości danych do przesłania przez łącza internetowe serwerowni.

Hotspot - bezpłatny i otwarty punkt umożliwiający dostęp do internetu najczęściej za pomocą łączności bezprzewodowej WiFi.

HTTPS (ang. Hypertext Transfer Protocol Secure) - szyfrowana wersja protokołu HTTP. Zapobiega to przechwytywaniu i zmienianiu przesyłanych danych.

Kontrola rodzicielska - opcje, stosowane głównie w usługach telewizji kablowej i satelitarnej, telefonach komórkowych, użytkowaniu komputera, w tym w grach video i korzystaniu z internetu, a także w systemach operacyjnych, które mają pomóc rodzicom w ochronie dzieci przed dostępem do nieodpowiednich dla nich treści (m.in. agresja, brutalne sceny, zachowania seksualne).

Ksenofobia - niechęć, wrogość wobec innych grup etnicznych. Zazwyczaj dotyczy cudzoziemców lub mniejszości narodowych i oparta jest na ich stereotypowym postrzeganiu.

Materiały przedstawiające seksualne wykorzystywanie dziecka - termin określający materiały (tekst, film, zdjęcie, zapis audio), które powstały podczas seksualnego wykorzystania dziecka.

Moderator - osoba lub grupa osób o specjalnych uprawnieniach, której zadaniem jest zapewnienie porządku oraz przestrzegania przez użytkowników regulaminu strony www, forum internetowego, listy dyskusyjnej, serwisu społecznościowego.

Mowa nienawiści (ang. hate speech) - znieważenie, pomawianie lub rozbudzanie nienawiści wobec osoby, grupy osób lub innego wskazanego podmiotu.

Nadmierne korzystanie z internetu - zjawisko dotyczące spędzania w internecie znacznej ilości czasu, co może powodować niekorzystne konsekwencje w życiu społecznym, w nauce oraz w pracy.

Netykieta - zbiór zasad określający właściwe zachowania w internecie.

Prawa autorskie - ogół praw przysługujących autorowi utworu, pomysłu, dzieła, upoważniających autora do decydowania o użytkowaniu swojej własności intelektualnej i czerpaniu z niej korzyści finansowych.

Program antywirusowy - przeciwdziała programom szpiegującym lub wirusom poprzez skanowanie wszystkich pobieranych przez komputer plików i blokowanie tych, które mogą zagrażać użytkownikowi.

Prywatność - w kontekście internetowym mówimy o umiejętności dbania o ochronę swoich danych, właściwego kontrolowania umieszczanych przez siebie oraz publikowanych przez innych informacji na nasz temat.

Rasizm - pogląd głoszący tezę o nierówności ludzi, wynikający z ideologii przyjmującej wyższość jednych ras nad innymi.

Serwer - potocznie jest to komputer udostępniający zasoby innym komputerom podłączonym do sieci. Zasobami mogą być między innymi strony internetowe (serwer WWW), poczta e-mail (serwer pocztowy), bazy danych (serwer baz danych).

Serwis społecznościowy - serwis internetowy, który istnieje w oparciu o zgromadzoną wokół niego społeczność internautów. Tworzy tak zwane media społecznościowe (ang. social media).

Sexting - zjawisko dotyczące przesyłania za pomocą komputera lub urządzeń mobilnych z dostępem do internetu swoich zdjęć, wiadomości czy też samodzielnie wykonanych materiałów wideo o charakterze seksualnym.

Siecioholizm – patrz: nadmierne korzystanie z internetu

Spam - niechciane lub niepotrzebne wiadomości elektroniczne.

Treści nielegalne - treści internetowe, które łamią prawo krajowe lub namawiają do jego łamania. Najczęściej są to treści szerzące rasizm, faszyzm i ksenofobię oraz treści pornograficzne z udziałem osoby małoletniej, ale odnosić się mogą do każdej informacji, której upublicznienie może być nielegalne (np. dane osobowe).

Treści szkodliwe - wywołują negatywne emocje u odbiorcy lub promują niebezpieczne zachowania. Do szkodliwych treści zalicza się m.in.: treści obrazujące przemoc, obrażenia fizyczne bądź śmierć, np. zdjęcia/filmy prezentujące ofiary wypadków, okrucieństwo wobec zwierząt, treści nawołujące do samookaleczeń lub samobójstw, zachowań szkodliwych dla zdrowia czy zażywanie niebezpiecznych substancji; treści dyskryminacyjne, zawierające postawy wrogości a nawet nienawiści; treści pornograficzne.

Technologie informacyjno–komunikacyjne - zespół technologii przetwarzających, gromadzących i przesyłających informacje w formie elektronicznej.

Wirus – złośliwy program komputerowy posiadający zdolność powielania się.

Wyszukiwarka - narzędzie internetowe pozwalające na przeszukiwanie stron internetowych pod kątem danej informacji, którą chcemy znaleźć np.: google, bing.

Bibliografia

1. Analizy wpływu zjawiska piractwa treści wideo na gospodarkę w Polsce, raport PwC na zlecenie Stowarzyszenia Dystrybutorów Programów Telewizyjnych „Sygnał", 2014. https://www.pwc.pl/pl/publikacje/piractwo/analiza_wplywu_zjawiska_piractwa_tresci_wideo_na_gospodarke_w_polsce_raport_pwc.pdf
2. Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych.
3. Bezpieczeństwo dzieci online – kompendium dla rodziców i profesjonalistów, praca zbiorowa pod red. A. Wrzesień – Gandolfo, 2014.
4. Rozporządzenie Ministra Edukacji Narodowej z dnia 23 grudnia 2008 r. w sprawie podstawy programowej wychowania przedszkolnego oraz kształcenia ogólnego w poszczególnych typach szkół (Dz. U. z dnia 15 stycznia 2009 r.).
5. Bartoszewicz M., Skuteczność edukacyjna wizualizacji wybranych zagadnień chemicznych, 2006.
6. Gulińska H., Bartoszewicz M., Scenariusze lekcji przyrody prowadzonych z wykorzystaniem tablicy StarBoard, 2006
7. Final POSCON Report, 2014. http://www.positivecontent.eu/app/download/5794080994/POSCON_FINAL_Report.pdf
8. www.sieciaki.pl/best
9. Pyżalski J., Cyberbulling jako nowa forma agresji rówieśniczej wśród gimnazjalistów, 2011.
10. Pyżalski J., Agresja elektroniczna i cyberbulling jako nowe ryzykowne zachowania młodzieży, 2012.
11. Chocholska P., Osipczuk M., Uzależnienie od komputera i Internetu u dzieci i młodzieży, 2009.
12. Augustynek A., Uzależnienie komputerowe. Diagnoza, rozpowszechnienie, terapia, 2010.
13. EU NET ADB, Fundacja Dzieci Niczyje (2013). Badanie nadużywania Internetu przez młodzież w Polsce.
14. Greenfield D., The Addictive Properties of Internet Usage, w: Young K. S., Abreu N. de (ed.), Internet Addiction. A Handbook and Guide to Evaluation and Treatment, 2011.
15. Kirwil L., Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo-część 2. Częściowy raport z badań EU Kids online przeprowadzonych wśród dzieci 9-16 lat i ich rodziców, 2011.
16. Millward Brown Poland dla FDN, Korzystanie z urządzeń mobilnych przez małe dzieci w Polsce, 2015.
17. Nastolatki wobec Internetu,Pedagogium WSNS, badania zrealizowane na zlecenie Rzecznika Praw Dziecka i NASK, 2014.
18. Shapira N. A. i in., Problematic internet use: proposed classification and diagnostic criteria,"Depression and Anxiety" 17, 2003.
19. Tanaś M., Dydaktyczne granice użyteczności komputerów [w:] Technologia informacyjna w procesie dydaktycznym, praca zbiorowa pod red. M. Tanasia, 2005.

Internet to nowoczesne medium, które odgrywa ogromną rolę w życiu młodego człowieka i może być przez niego z pożytkiem wykorzystywane. Codzienne aktywności młodych internautów toczą się równolegle online i offline.

Pozytywne aspekty technologii informacyjno-komunikacyjnych (TIK) doceniają także dyrektorzy, wyposażając swoje placówki w urządzenia cyfrowe. W niniejszym poradniku przedstawiamy, dlaczego warto wykorzystywać nowoczesne narzędzia informatyczne w procesie nauczania, a także pokazujemy, w jaki sposób uczniowie mogą skutecznie i bezpiecznie wyszukiwać w sieci potrzebne informacje. Prezentujemy również definicje pozytywnych treści online oraz kryteria dla stron internetowych, których znajomość pozwoli Państwu polecać dzieciom i ich rodzicom odpowiednie serwisy edukacyjne.

Jednak nie można zapominać, że globalna sieć oprócz pozytywnych treści kryje też wiele niebezpieczeństw. Ważne jest, by nauczyciele kształtowali świadomość uczniów o zagrożeniach internetowych, a w przypadku zaistnienia niebezpieczeństwa potrafili wskazać im właściwe rozwiązanie.

B:) cyfrowo bezpieczni.pl

kontakt@cyfrowobezpieczni.pl

Projekt jest finansowany przez Ministerstwo Edukacji Narodowej w ramach zadania „Poprawa kompetencji pracowników szkoły, uczniów i ich rodziców w zakresie bezpiecznego korzystania z cyberprzestrzeni oraz reagowania na zagrożenia”

MINISTERSTWO EDUKACJI NARODOWEJ