

E-wychowanie dzieci w duchu przedsiębiorczości

Vademecum dla pedagogów

edycja 2011 / 2012

Grodziskie
Towarzystwo
Edukacyjne



Spis Treści

E-wychowanie – współczesny standard	3
Jak bezpiecznie szukać informacji w Internecie? Jak weryfikować źródła informacji?	6
Cyfrowe narodziny czyli dziecko online	12
Dlaczego raz opublikowane treści ciężko usunąć z Internetu?.....	14
Nauczycielu – czy wiesz co dzieci same robią w sieci?	16
Nasza szkolna umowa korzystania z Internetu i komputera	19
Czy uczeń wie, że zanim zostanie pracodawcą lub pracownikiem w niedalekiej przyszłości – sprawdzą go w serwisie społecznościowym	21
Ochrona danych osobowych uczniów w Internecie	22
Rady dla kadry pedagogicznej:.....	24
Poznaj ciemniejsze strony Internetu – warto wiedzieć, że tak jak w realnym świecie – w cyberprzestrzeni też możemy spotkać się z różnym zachowaniami.....	24
Prawo jest po stronie użytkowników Internetu przestrzegających zasad	29
Bądź świadomy! Czyli jak przestrzegać praw autorskich w Internecie	32
Cyberprzemoc – charakterystyka zjawiska	34
Skuteczna Polityka bezpieczeństwa internetowego w szkole – porady dla kadry pedagogicznej	36
POLITYKA BEZPIECZEŃSTWA INTERNETOWEGO.....	40
Co to jest PEGI	41
Gdzie szukać pomocy – Poradnik teleadresowy	44
Słowniczek internetowy dla kadry pedagogicznej	45

E-wychowanie – współczesny standard

Katarzyna Tokarska, Akademia Liderów Innowacji i Przedsiębiorczości

Internet, globalna sieć informacyjna, była w swoich początkach stworzona na potrzeby amerykańskiego departamentu obrony. Następnie została dopuszczona do użytku przez największe uniwersytety i ośrodki badawcze na świecie, po czym, w latach 90-tych, stała się ogólnodostępnym medium, takim jak radio czy telewizja. Możliwości Internetu są ogromne i powszechnie znane i coraz częściej używane. Pozwala on na błyskawiczną wymianę informacji oraz ich publikację w dowolnym formacie. Łączy w sobie zalety gazety, przekazu radiowego i telewizyjnego.

Do niewątpliwych zalet Internetu należy to, że umożliwia on upowszechnianie treści informacyjnych oraz edukacyjnych. Jest to medium, gdzie można znaleźć informacje i komentarze na każdy temat: dotyczące polityki, gospodarki i rozrywki. Internet to niezastąpiony pomocnik w pozyskiwaniu informacji za pomocą wyszukiwarek, takich jak Google albo portali typu Wikipedia. Coraz częściej jednak funkcja stricte informacyjno-rozrywkowa internetu zostaje wyparta na rzecz funkcji zawodowej i zarobkowej. Coraz częściej zaczynamy pracować przy pomocy tego medium, zarabiamy, załatwiamy formalności urzędowe, bankowe, czy dokonujemy zakupy. Tutaj szukamy pracy i ją znajdujemy. Tutaj realizujemy własne projekty i realizujemy pomysły biznesowe. Nie tylko odbieramy komunikaty wirtualnej rzeczywistości – ale tworzymy ją, a nawet łączymy z realiem.

Jesteśmy świadkami dużych zmian technologicznych. Zmiany te przekładają się na rzeczywistość wychowania, w tym na rzeczywistość szkolną, ale nie nastąpi to z dnia na dzień. Nowe media to nieograniczone możliwości zdobywania wiedzy, nawiązywania i utrzymywania kontaktów, pobudzania kreatywności i przede wszystkim realizowania przedsiębiorczych wyzwań i zarabiania pieniędzy.

„Najważniejsze jest, abyśmy wszyscy chcieli stale się uczyć, czerpać z nowych możliwości i rozwiązań techniki” – powiedziała Katarzyna Hall, minister edukacji narodowej dzisiaj podczas panelu dyskusyjnego „Nowe media: re-formatowanie edukacji”, który miał miejsce w październiku 2011 roku.

Niniejsze Vademecum zostało przygotowane na potrzeby projektu „E-wychowanie dzieci w duchu przedsiębiorczości” i jest próbą usystematyzowania informacji na temat jak bezpiecznie i efektywnie korzystać z nowych technologii i narzędzi coraz powszechniejszych także na terenie szkoły.

1. 500 milionów lat temu - pierwszy prosty mózg
2. 6 000 lat temu - pierwsze pismo
3. 1876 rok - pierwszy telefon
4. 1926 rok - pierwsza telewizja
5. 1988 - światłowód - umożliwiający przesyłanie ponad 3000 komunikatów jednocześnie
6. 2 lata – tyle potrzebował Facebook, aby mieć 50 milionów użytkowników.

Świat to ogromna i dynamiczna giełda informacji. Dostęp do niej to najbardziej pożądana i najlepiej opłacana rzecz.

Wikipedia istnieje od 2001 roku – dzisiaj zawiera 13 milionów artykułów w ponad 200 językach. Liczba informacji podwaja się co roku a milion książek jest publikowanych rocznie na całym świecie. Połowa wiedzy, której nauczył się student politechniki na pierwszym roku – będzie nieaktualna na trzecim.

Świat to ogromna giełda informacji, dostęp do niej to najbardziej pożądana i opłacalna rzecz.

Sukces następnych pokoleń zależy od ich umiejętności poszukiwania informacji, filtrowania jej i używania.

Zatem rolą współczesnego nauczyciela staje się inspirowanie podopiecznych zarówno do poszukiwania samych informacji jak i poszukiwania coraz to nowszych samych źródeł informacji. To jest klucz do rozwoju – dzisiejszy uczeń to nie tylko bierny odbiorca przekazywanej wiedzy czy treści, to przede wszystkim coraz bardziej świadomy jej poszukiwacz a może nawet kreator. To nowość odróżniająca XXI wiek od poprzednich epok i całkowicie zmieniająca dotychczasowe podejście do uczenia się i nauczania. Wszystko dzięki Internetowi....

Dzieci rozpoczynają swoją przygodę z Internetem w coraz młodszy wieku, dlatego też to po stronie dorosłych – rodziców i nauczycieli leżą starania, aby surfując w sieci czuły się pewnie i z łatwością trafiali na bezpieczne, edukacyjne i dostosowane do ich wieku treści. Promujmy to, co Internet ma najlepszego do zaoferowania „cyfrowemu pokoleniu”.

Jak Internet już teraz bezpłatnie i powszechnie wspiera edukację?

Najpopularniejszym i jednocześnie najbardziej innowacyjnym systemem internetowych narzędzi są narzędzia z rodziny Google.

Google bezpłatnie, powszechnie i do tego w wielu językach udostępnia mnóstwo aplikacji, których używanie staje się koniecznością w dotrzymywaniu kroku wyzwaniom współczesnego świata.

Rodzina Google to m.in.:

1. Google mail - szybka poczta email z wyszukiwarką i ochroną przed spamem,
2. Google alerty – bezpłatne aktualizacje na e-mail na interesujące tematy,
3. Google Chrome – przeglądarka stworzona z myślą o szybkości, prostocie i bezpieczeństwie poszukiwania informacji
4. Google Earth – informacje geograficzne o całym świecie w zasięgu ręki, doskonałe narzędzie do nauki geografii,
5. Google mapy - wskazówki dojazdu, mierzenie odległości, mapy poglądowe
6. Google News – wyszukuje i przegląda wiadomości wśród stale aktualizowanych 300 źródeł
7. Google Video – pozwala przeszukiwać zasoby sieciowe i publikować własne pliki.
8. Google.com – wyszukiwarka pozwalająca w ułamkach sekundy przeszukać miliardy stron internetowych
9. Google Blogger – darmowe blogowanie
10. Google dokumenty – stwarza możliwość opracowania online dokumentów i całych projektów, tworzenia ich, dzielenie się nimi i otwierania w dowolnym miejscu na świecie,
11. Google kalendarz – pozwala na zorganizowanie kalendarza a także zsynchronizowanie się z przyjaciółmi, powiadamiania o nowych wydarzeniach
12. Google Picasa – znajdowanie, edycja zdjęć a także publikacja własnych, tworzenia albumów wirtualnych – np. własnych zielników, ogrodów czy katalogów zwierząt świata
13. Google Sketch up – tworzenie modeli 3D w szybki i łatwy sposób,
14. Google tłumacz – błyskawicznie tłumaczy tekst, strony internetowe oraz pliki na ponad 50 języków.
15. Google współrzędne – pozwala zobaczyć, gdzie są Twoi znajomi
16. Youtube – pozwala na oglądanie, wysyłanie i dzielenie się swoimi filmami wideo.
17. Google Scholar - upraszcza wyszukiwanie tekstów naukowych. W jednym miejscu można wyszukiwać materiały z wielu dziedzin i źródeł: artykuły recenzowane, prace naukowe, książki, streszczenia i artykuły pochodzące z wydawnictw naukowych, towarzystw naukowych, repozytoriów materiałów zgłoszonych do publikacji, uniwersytetów i innych organizacji akademickich. Wyszukiwarka Google Scholar ułatwia znalezienie najbardziej odpowiednich naukowych materiałów źródłowych.

Rodzina Google stale się rozwija i dynamicznie poszerza wachlarz możliwości. Wymienione wyżej narzędzia są całkowicie bezpłatne. Wykorzystywanie ich do procesu dydaktycznego może znacznie wzbogacić elementy nauczania – ale przede wszystkim przygotowuje uczniów do przyszłego życia zawodowego. W powyższym zestawie nie zostały wymienione komercyjne, płatne aplikacje Google, które dedykowane są przedsiębiorcom do rozwijania ich biznesów.

Wszystkie narzędzia Google są powszechnie używane na całym świecie – brak umiejętności ich obsługi pozbawia dostępu nie tylko do nowych informacji, nowych form kontaktu, ale przede wszystkim odcina od dostępu do świata jako takiego, a nawet oddala.

Świat przed Google i po Google to zupełnie inna rzeczywistość.

Jak bezpiecznie szukać informacji w Internecie? Jak weryfikować źródła informacji?

Robert Kuryłowicz – Aurelius Interactive

Internet jest nieograniczonym źródłem informacji – jak dotąd wyszukiwarka Google zaindeksowała ponad 26 000 000 000 (26 miliardów) adresów WWW – to tak, jakby każdy człowiek na świecie miał na własność 4 strony WWW. W jaki sposób w takim gęstoku filtrować przydatne informacje, których wiarygodności możemy być pewni?

Po pierwsze wyszukiwarka

Wyszukiwarka informacji w sieci jest podstawowym narzędziem do szukania informacji w Internecie. Niewątpliwie najpopularniejszą (zarówno w Polsce, jak i na świecie) jest Google (www.google.pl). Pozostałe wyszukiwarki mają marginalny udział w rynku – jest to ok. 10% ilości wyszukiwań (inne wyszukiwarki to m.in. Bing, Yahoo, Netsprint), dlatego w artykule najwięcej miejsca poświęcimy wyszukiwarce Google.

Jak działa wyszukiwarka internetowa? W najprostszych słowach możemy określić, że próbuje ona najbardziej wartościowe strony WWW pod względem wpisanego, poszukiwanego słowa umieścić na początku wyników wyszukiwania. Czym zatem charakteryzuje się wartościowa strona WWW w oczach algorytmów wyszukiwarek:

- Prezentuje jasny i czytelny opis poszukiwanego słowa
- Zawiera unikalną treść, nie skopiowaną z innej witryny
- Jest stale polecana przez internautów na całym świecie
- Jest bezpieczna dla komputerów i całej sieci internetowej
- Jest zaprojektowana zgodnie ze standardami tworzenia stron WWW

Na temat wartości stron WWW dla wyszukiwarek powstały już setki publikacji i podręczników, dlatego nie będziemy zgłębiać tego tematu.

Najważniejsze w korzystaniu z wyszukiwarki internetowej są 2 rzeczy, mające kluczowy wpływ na szybkość i bezpieczeństwo poszukiwania informacji w sieci:

1. Zasada ograniczonego zaufania
2. Przemyślane konstruowanie tzw. zapytań do wyszukiwarki (słów kluczowych)

Zasada ograniczonego zaufania dotyczy wyświetlanych wyników wyszukiwania. Wprawdzie istnieje bardzo wysokie prawdopodobieństwo, że na liście wyników znajdziemy tylko bezpieczne serwisy, zawierające poszukiwane przez nas informacje (do tego wszakże dążą twórcy wyszukiwarek), ale niestety może się zdarzyć, iż lista wyników zawierać będzie również niebezpieczne strony WWW, które mogą wyrządzić szkody na komputerze, wyłudzić prywatne dane lub usunąć wszystko z naszego komputera.

Wyszukiwarki i firmy zajmujące się bezpieczeństwem w sieci nieustannie dążą do podniesienia jego poziomu, stosując różne wskazówki i informacje dla użytkownika. Google w wynikach wyszukiwania podpowiada użytkownikowi, że dana strona została zidentyfikowana jako potencjalnie niebezpieczna już w wynikach wyszukiwania:

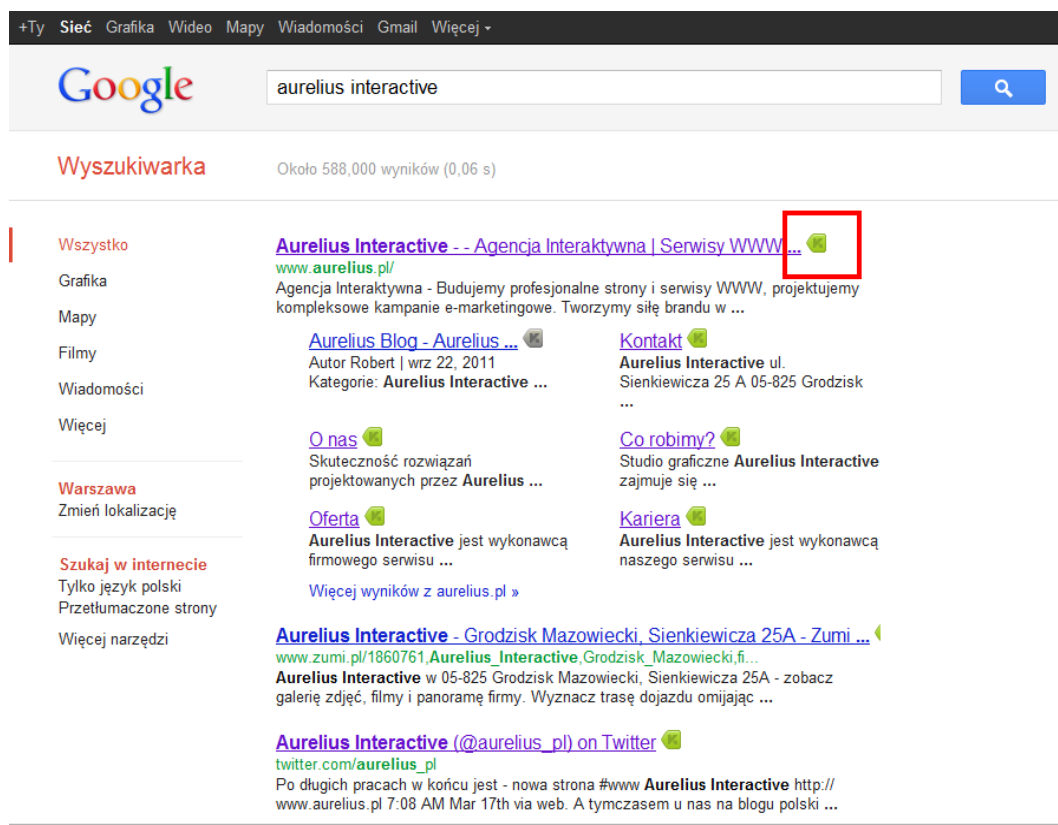
Przykładowa strona internetowa

Ta witryna może wyrządzić szkody na komputerze

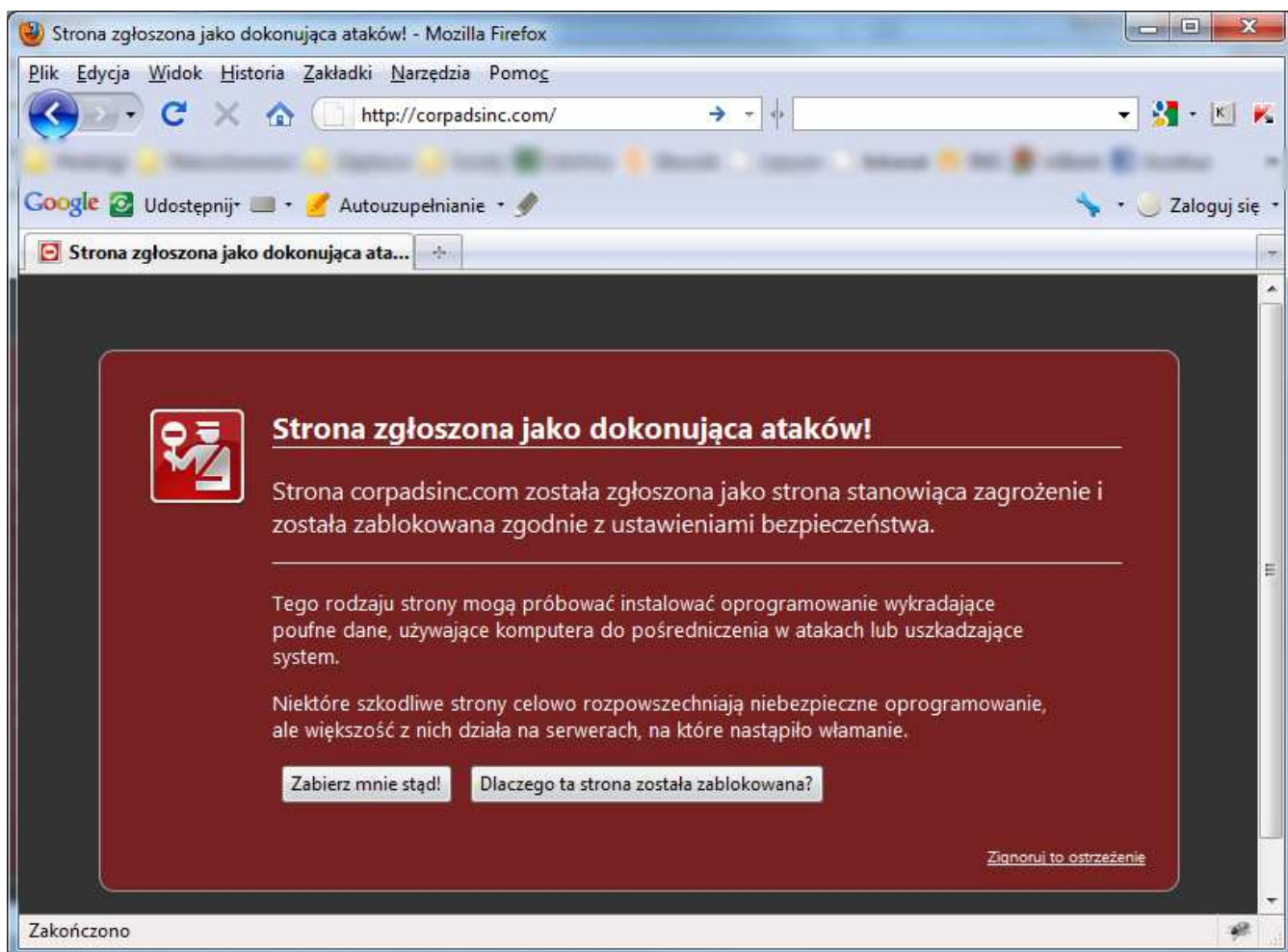
To jest przykładowa strona internetowa. Można ją wyświetlić, wpisując adres przykladowastrona.com lub przykladowestrony.com.

www.przykladowastrona.com/ – Kopia – Podobne

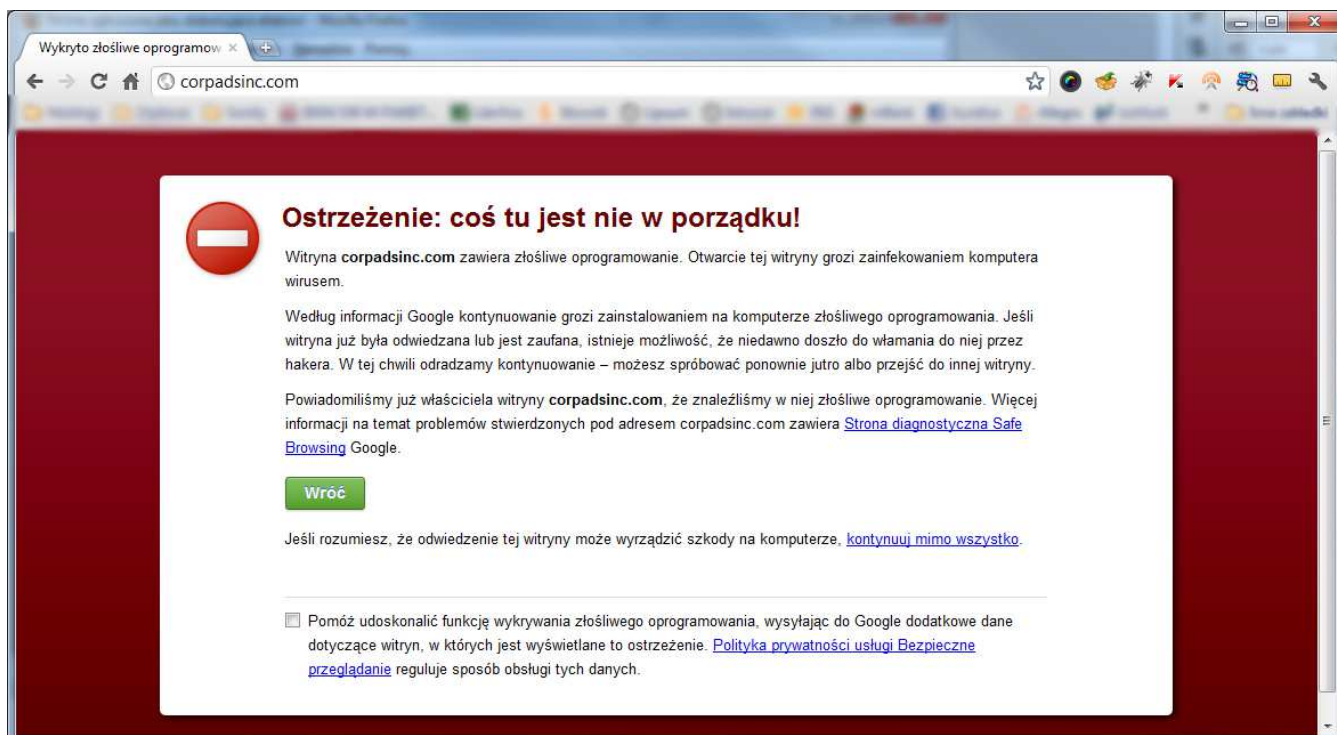
Podobnie, już w wynikach wyszukiwania, informuje o zagrożeniach program Kaspersky Internet Security. Przy każdej pozycji na liście wyników wyszukiwania Google znajduje się ikonka programu Kaspersky informująca o tym, czy dany adres WWW należy do grupy bezpiecznych serwisów. Zielona oznacza, że dana strona została zweryfikowana i jest bezpieczna. Czerwona oznacza potencjalne, wysokie zagrożenie, natomiast szara oznacza, że dany adres WWW nie został jeszcze przebadany przez firmę Kaspersky Lab:



Następnie, poszczególne przeglądarki internetowe ostrzegają użytkownika, że dana strona WWW może być potencjalnie niebezpieczna. Praktycznie wszystkie mają wbudowane bardziej lub mniej zaawansowane narzędzia bezpieczeństwa. Internet Explorer bazuje na ustawieniach systemowych systemu Windows (wcześniej zostało to omówione). Mozilla Firefox z kolei ma własny, indywidualny ekran z ostrzeżeniem przed witryną, która może zawierać potencjalnie niebezpieczne oprogramowanie:



Podobnie przeglądarka Chrome ma własny komunikat ostrzegający o niebezpiecznej stronie WWW:





WAŻNE – powyższe komunikaty i zabezpieczenia przeglądarek nie chronią przed pornografią i inną niepożądaną treścią.

Jeśli podczas przeglądania internetu zobaczymy taki komunikat, oznacza to, że dana strona WWW została zidentyfikowana jako serwis zawierający szkodliwe oprogramowanie (mogące uszkodzić komputer lub wyłudzić prywatne dane).

Do ochrony przed niepożądaną treścią wykorzystaj oprogramowanie do kontroli rodzicielskiej, ponieważ zadaniem powyższych zabezpieczeń jest ostrzeganie o niebezpiecznych stronach WWW, nie zaś o niepożądaney treści.

Nie wszystko złoto co się świeci – wyszukiwarkami można manipulować

W obecnych czasach różne firmy i organizacje korzystają z tzw. Pozycjonowania w wyszukiwarkach. W najprostszych słowach oznacza to zestaw różnych działań w Internecie, aby wyszukiwarki wyświetlały naszą stronę WWW na wysokich pozycjach w wynikach wyszukiwania, na konkretne słowa kluczowe. Warto o tym pamiętać, gdy poszukujemy w Internecie informacji o konkretnym produkcie lub usłudze – przykładowo po wpisaniu do wyszukiwania w Google frazy „historia samochodu” na pierwszej stronie wyników mamy zarówno wartościowe serwisy merytoryczne (np. Wikipedia), jak również typowo komercyjne serwisy firmowe, wypozycjonowanie w wynikach wyszukiwania.

Pozycjonowania nie należy traktować w kategoriach negatywnych, ponieważ Google – co do zasady – nie wyświetli bezwartościowej strony na początku wyników wyszukiwania – dany serwis musi zawierać wartościową treść, zaprezentowaną w przyjazny sposób, więc nawet jeśli w poszukiwaniu konkretnych informacji trafimy na stronę komercyjną, może się okazać, że znalezione tam informacje w 100% zaspokajają naszą ciekawość. Reasumując – zasada ograniczonego zaufania w internecie (w tym również do wyników wyszukiwania Google) jest podstawą w poruszaniu się w sieci – co do zasady możemy ufać wynikom wyszukiwania, odczytując pierwsze pozycje jako serwisy najlepiej odpowiadające naszym poszukiwaniom, ale nigdy nie odbierajmy tego jako prawdę oczywistą. Na bieżąco sprawdzajmy jakość wyszukiwań i docelową stronę, ewentualnie próbujmy inaczej formułować zapytania do wyszukiwarki.

Umiejętność formułowania trafnych zapytań to podstawa

Aby efektywnie szukać informacji w Internecie za pomocą wyszukiwarek, musimy odpowiednio formułować nasze zapytania (czyli słowa kluczowe). Jeśli bowiem będą one zbyt rozległe, źle sformułowane czy zbyt ogólne, będziemy marnować czas w przeglądaniu rozmaitych wyników zamiast od razu otrzymać poszukiwaną informację. Kolejną rzeczą jest zasada, aby nie marnować swojego czasu na przeglądanie kilkunastu stron z wynikami wyszukiwania. Jeśli dojdziemy do 3-4 strony wynikowej i nie odnajdziemy poszukiwanej informacji – spróbujmy inaczej sformułować nasze zapytanie.

Przykłady prawidłowego formułowania zapytań do wyszukiwarek:

1. „Mechanik Grodzisk Mazowiecki”, „adwokat warszawa”, „hydraulik olsztyn”

Jest to najpopularniejsza forma zapytania do wyszukiwarek – poszukujemy konkretnych usług w konkretnych lokalizacjach. Unikajmy rozwlekłych opisów, ograniczmy się do nazwy poszukiwanej usługi i lokalizacji – dzięki temu oprócz stron firmowych poszczególnych działalności zobaczymy również listy wynikowe rozmaitych baz danych oraz spisów firm, co da nam jeszcze szerszą ofertę do wyboru. Bądźmy jednak przygotowani na wysoką ilość reklam i wypozycjonowanych serwisów firmowych w wynikach wyszukiwania.

2. „Żeberka w piwie przepisy”, „przepis na żeberka w piwie”
W tym wypadku poszukujemy konkretnej rzeczy, ale zależy nam na szerokim spojrzeniu na dany temat. Dlatego nie ograniczamy wyników zbędnymi parametrami.
3. „Bank WBK opinie”, „opinie o banku WBK”
Typowy przykład frazy, gdy chcemy odnaleźć opinie innych osób na temat danej firmy, marki czy produktu. Tu również dodatek *opinie* ma kluczowe znaczenie, ponieważ determinuje on wyszukiwarkę do przedstawienia nam wyników z serwisów umożliwiających zamieszczanie opinii użytkowników o produktach.
4. „Jak zainstalować napęd do bramy Somfy Dexxo”, „Instalacja napędu do bramy Somfy Dexxo”
W ten sposób formułujemy zapytanie, jeżeli poszukujemy konkretnych wskazówek. Istnieje duże prawdopodobieństwo, że w wynikach wyszukiwania znajdą się fora dyskusyjne, na których użytkownicy wzajemnie pomagają sobie w różnych problemach lub też znajdziemy podręczniki producenta.
5. Bezpлатne porady prawne
Takie słowo kluczowe może stanowić wyjście do dalszych poszukiwań. Z pewnością w wynikach wyszukiwania znajdą się reklamy i wypozycjonowanie serwisu (frazę bardzo ogólną), ale jest duże prawdopodobieństwo, że znajdziemy serwis oferujący bezpłatne porady prawne lub przynajmniej informację, jak takiego serwisu szukać.

Odróżnij reklamy od naturalnych, tzw. „organicznych” wyników wyszukiwania.

Google jako wyszukiwarka oferuje przedsiębiorcom reklamę w wynikach wyszukiwania. Musimy zdawać sobie z tego sprawę, aby pomijać pozycje, które nas nie interesują.

Regułą jest, że reklamy są wyświetlane na początku wyników wyszukiwania (na lekko różowym tle) oraz po prawej stronie ekranu:

The screenshot shows a Google search for "adwokat poznań". The interface includes the Google logo, search bar, and navigation links. The results are divided into two main sections: "REKLAMY - LINKI SPONSOROWANE" (Sponsored Links) and "Wyszukiwarka" (Search Results).

REKLAMY - LINKI SPONSOROWANE: This section is highlighted with a red box and contains several sponsored results for lawyers in Poznań. Examples include "Adwokat Poznań | grzybkowski-guzek.pl", "Masiota - adwokat Poznań", "Adwokat Poznań Oferta", "Adwokat Chudak Zenon", and "Dobry adwokat Poznań". Each result includes a brief description and contact information.

Wyszukiwarka: This section contains organic search results. It is highlighted with a green box and includes results such as "Grzybkowski Guzek Jackowski - adwokaci Poznań", "Kancelaria Adwokacka Poznań - GTK-Adwokaci.pl", "Kancelaria Adwokacka Grzegorzcyk i Adwokat", "Kancelaria Adwokacka Poznań - Adwoka...", and "Kancelaria Adwokacka Arkadiusz Jaskuła". These results are interspersed with sponsored links and include details like addresses and phone numbers.

On the left side of the search results, there is a sidebar with filters and a section labeled "Wszystko" (Everything) with various categories like "Grafika", "Mapy", "Filmy", etc. Below this, there is a section labeled "Warszawa" with a sub-section "Zmień lokalizację" (Change location). At the bottom left, there is a section labeled "Szukaj w internecie" (Search in the internet) with options like "Tylko język polski" (Only Polish language) and "Przetłumaczone strony" (Translated pages).

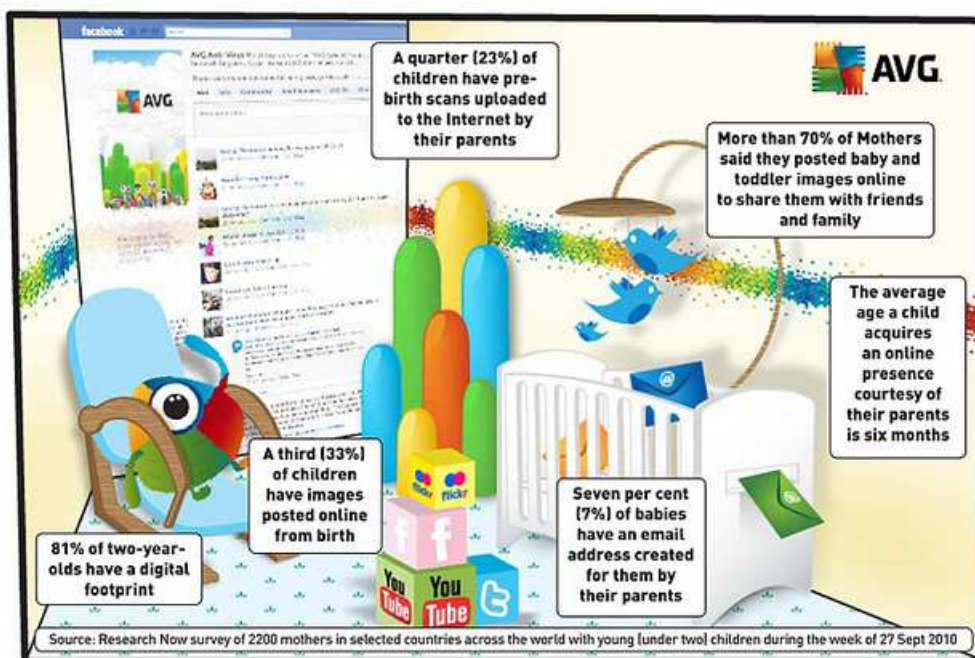
7 podstawowych zasad weryfikacji treści w Internecie (źródło: artelis.pl)

1. Ustal, kto jest autorem strony i jakie ma kwalifikacje, aby wypowiadać się na określony temat. Autorami stron są nierzadko pasjonaci, którzy nie mają wystarczającego wykształcenia ani wiedzy, by rzetelnie przedstawić jakieś zagadnienie. Bardziej wiarygodny będzie więc dla nas profesor uniwersytetu niż student czy uczeń szkoły średniej.
2. Ważne jest, czy autor strony oprócz tytułu naukowego podaje jakieś swoje osiągnięcia w danej dziedzinie (publikacje, nagrody), a także czy pracuje w jakiejś znaczącej instytucji (na uniwersytecie, w towarzystwie naukowym).
3. Strona jest bardziej wiarygodna wtedy, gdy można na niej znaleźć odnośniki do innych stron o podobnej tematyce (niestety, wtedy również trzeba się zastanowić nad ich wartością). Dobrze świadczy o autorze strony, jeśli podaje źródła, z których korzystał.
4. Ważny jest sam wygląd strony. Jeśli ktoś poświęcił wiele czasu na jej przygotowanie, zaopatrzył ją w zdjęcia, rysunki i animacje, to prawdopodobnie zadbał też o rzetelność przekazywanych informacji.
5. Warto sprawdzić, kiedy powstała strona i czy jest stale aktualizowana. Strona istniejąca od dawna i często aktualizowana jest bardziej wiarygodna niż strona, którą ktoś sporządził rok temu, po czym o niej zapomniał.
6. Warto sprawdzić, jak często jest odwiedzana dana strona. Jeśli znajdziemy na niej księgę gości, możemy zdobyć informacje na ten temat, a także poznać opinie innych dotyczące tej strony.
7. Możemy powiedzieć wiele o wiarygodności strony, jeśli uda nam się ustalić cel jej zbudowania. Instytucje tworzą strony, aby informować o swojej działalności. Osoby prywatne chcą natomiast przedstawić swoje dokonania, dać upust swojej pasji. Często możemy jednak trafić na strony, których celem jest przekonanie nas do pewnych poglądów lub do podjęcia pewnych działań. Są to zwykle strony firm, które chcą nam sprzedać swój produkt, lub organizacji, które starają się zyskać poparcie dla swoich idei. W takich wypadkach trzeba być szczególnie ostrożnym.

W Internecie są różne informacje – także o nas samych. Niestety nie zawsze umieszczone z naszą zgodą.

Publikowanie fotografii z USG, dzielenie się doświadczeniami ciążowymi na Twitterze, tworzenie albumów fotograficznych z porodu, a nawet zakładanie kont e-mail niemowlakom - dzisiejsi rodzice coraz częściej budują cyfrowy ślad swoich dzieci już od ich momentu narodzin, a nawet wcześniej - podaje AVG Technologies.

Z badania przeprowadzonego przez AVG Technologies, firmę specjalizującą się w dziedzinie bezpieczeństwa internetowego, wynika, że aż 81 procent dzieci poniżej drugiego roku życia posiada obecnie swój cyfrowy profil lub ślad w Internecie, a ich zdjęcia znajdują się w sieci. W Stanach Zjednoczonych 92 procent dzieci pojawia się w Internecie przed ukończeniem drugiego roku życia, w porównaniu do 73 procent dzieci z przebadanych krajów europejskich. Sondaż przeprowadzono wśród matek pochodzących z Ameryki Północnej, Europy, Australii/Nowej Zelandii oraz Japonii.



Cyfrowe narodziny w wieku 6 miesięcy

Według badań AVG średnia wieku, w którym dzieci obchodzą swoje cyfrowe narodziny, wynosi sześć miesięcy. Jednak zdjęcia i informacje o jednej trzeciej z nich (33%) pojawiają się w internecie już w ciągu pierwszych kilku tygodni po porodzie. W Wielkiej Brytanii 37 procent noworodków rozpoczyna swoje życie online tuż po narodzinach, podczas gdy w Australii i Nowej Zelandii jest to 41 procent.

Niemal jedna czwarta (23%) dzieci rozpoczyna cyfrowe życie w momencie, kiedy ich rodzice publikują w internecie zdjęcia z prenatalnych badań USG. Odsetek ten jest wyższy w Stanach Zjednoczonych (34 procent) oraz w Kanadzie (37 procent). Zdecydowanie mniej rodziców dzieli się zdjęciami USG swoich dzieci we Francji (13%), Włoszech (14%) i Niemczech (15%). Podobnie sytuacja prezentuje się w Japonii, gdzie odsetek ten wynosi tylko 14 procent.

Siedem procent niemowlaków i małych dzieci ma adres e-mail utworzony przez rodziców, a pięć procent ma profile w serwisach społecznościowych.

Na pytanie o motywację do publikowania zdjęć niemowląt w internecie, ponad 70 procent ankietowanych matek odpowiedziało, że chce podzielić się nimi z rodziną i przyjaciółmi. Zaskakiwać może jednak fakt, iż ponad jedna piąta (22%) matek ze Stanów Zjednoczonych stwierdziła, że chcą dodać więcej treści do swoich profili społecznościowych, a 18 procent z nich przyznało, że po prostu naśladują innych.

W swoim badaniu firma AVG zapytała matki także o to, czy niepokoją się ilością informacji o swoich dzieciach, które w przyszłych latach będą dostępne w internecie (w skali od jednego do pięciu, gdzie pięć oznaczało wysoki poziom niepokoju). Z perspektywy globalnej, matki okazywały umiarkowanie zaniepokojone (przeciętnie 3,5), przy czym największe obawy wyrażały Hiszpanki (3,9), a najmniejsze — Kanadyjki (3,1).

To szokujące, kiedy pomyślimy, że 30-latek ma cyfrowy ślad ciągnący się wstecz przez najwyżej 10-15 lat, podczas gdy ogromna większość współczesnych dzieci będzie obecna w Internecie przed ukończeniem drugiego roku życia. Co więcej ilość tych informacji te będzie rosła przez całe ich życie — mówi J.R. Smith dyrektor generalny AVG Technologies. Badania pokazują, że coraz częściej cyfrowe narodziny dziecka zbiegają się z rzeczywistą datą porodu, a nawet ją poprzedzają. Zdjęcia USG jednej czwartej dzieci pojawiają się online, jeszcze zanim fizycznie przyjdą one na świat - dodaje.

To zrozumiałe, że dumni rodzice chcą dzielić się zdjęciami swoich dzieci z rodziną i przyjaciółmi. Specjaliści z AVG zalecają jednak, aby zawsze pamiętać o dwóch rzeczach.

Po pierwsze, publikując zdjęcia i informacje o swoich pociechach, tworzy się cyfrową historię ludzkiej istoty, która będzie jej towarzyszyć przez całe życie. Warto zadać sobie zatem proste pytanie: „w jaki sposób chcemy rozpocząć cyfrową przygodę naszego dziecka i co pomyśli ono w przyszłości o opublikowanych przez nas informacjach?”

Po drugie, zawsze należy zwracać uwagę na ustawienia prywatności w sieciach społecznościowych i innych profilach. W przeciwnym razie zdjęcia i specyficzne informacje o dziecku mogą być dostępne nie tylko dla rodziny i przyjaciół, ale dla całego świata online.

źródło: avg.pl

Dlaczego raz opublikowane treści ciężko usunąć z Internetu?

Robert Kuryłowicz – Aurelius Interactive

Sieć Internetowa stanowi pajęczynę różnego rodzaju powiązań – Internet to nic innego jak setki milionów komputerów połączonych ze sobą strumieniem transmisji danych. Aby zrozumieć ideę działania Internetu, musimy zdać sobie sprawę, że serwery i serwisy internetowe nie są bytem statycznym, który reaguje wyłącznie na nasze wywołanie (wpisanie jego adresu WWW). Są to organizmy dynamiczne, wciąż żywe, które stale komunikują się ze sobą, wymieniając różne dane i informacje. Jest to podstawowe założenie i dobrodziejstwo Internetu, ale również – w obecnych czasach – jego ogromna wada, ponieważ raz opublikowanych w sieci informacji nie da się już w prosty sposób usunąć. Co więcej – nawet, jeśli uznamy, że nam się to udało, zawsze w przyszłości mogą zostać ponownie opublikowane, celowo lub przez pomyłkę, w miejscu, w którym nawet nie zdajemy sobie sprawy.

Wiele serwisów WWW, jedna baza danych <=> Jeden serwis WWW, wiele baz danych

Każda bez wyjątku strona WWW, umożliwiająca jakąkolwiek interakcję lub zapisywanie informacji, posiada swoją bazę danych, którą administrują ludzie – administratorzy serwisu. Weźmy za przykład forum dyskusyjne o kulinariach – pozornie nieszkodliwe miejsce wymiany opinii i doświadczeń w kuchni. Jeśli jednak administrator postanowi uruchomić nowy serwis internetowy (np. o podróżach), z pewnością wykorzysta już istniejącą bazę danych ze swojego forum kulinarnego, czyli dane wszystkich użytkowników (aby na starcie projektu pochwalić się dużą ilością użytkowników oraz przesłać wszystkim informację o tym). Możemy o tym nawet nie wiedzieć (wszakże zaakceptowaliśmy regulamin forum kulinarnego – którego zapewne nie przeczytaliśmy do końca – w którym była informacja o przetwarzaniu danych osobowych w ramach grupy kapitałowej administratora serwisu). Po jakimś czasie chcemy usunąć swoje dane z tego forum, co czynimy z sukcesem – nie wiedząc, że nadal są publicznie dostępne w nowym forum internetowym o podróżach, jak również w zabezpieczonych kopiach zapasowych forum kulinarnego (w razie awarii serwerów forum zostanie przywrócone z kopii, w której znajdują się nasze dane – niekoniecznie celowo).

Setki serwisów w ramach jednej grupy

Często jest tak, że publikując pozornie nieszkodliwą informację (np. ogłoszenie o sprzedaży samochodu z numerem kontaktowym) w rzeczywistości rozpoczynamy jej nowe, długie życie. Obecnie właściciele i administratorzy serwisów internetowych, aby zwiększyć zasięg i efektywność, łączą siły współpracując ze sobą lub tworzą dziesiątki, lub nawet setki serwisów pobocznych, analogicznych tematycznie do strony głównej. Publikują w niej te same lub przeredagowane treści, powielając jednocześnie opublikowaną przez nas informację. Późniejsze usunięcie jej jest bardzo problematyczne, by nie rzec – niemożliwe. Często również inne serwisy WWW regularnie parsują (zczytują i zapisują) zawartość danego serwisu WWW, aby wyświetlić ją u siebie. Nie jesteśmy w stanie odnaleźć wszystkich stron, które w ten sposób zaczerpnęły opublikowaną przez nas informację.

Google znajdzie (prawie) wszystko

Roboty wyszukiwarek internetowych nieustannie przemierzają całą sieć Internetu, w poszukiwaniu nowych stron WWW i nowych informacji w serwisach, które wcześniej zostały już odwiedzone – proces ten nosi

nazwę indeksowania. Indeksacja robotów wyszukiwarek (np. Google) powoduje, że informacje przez nas opublikowane – jeżeli zostały niefortunnie udostępnione lub wskutek awarii systemów zabezpieczeń różnych stron WWW – są publicznie dostępne całemu światu, właśnie za pomocą wyszukiwarki, która daną informację zaindeksowała i udostępnia publicznie w wynikach wyszukiwania. Przykład? Wpiszmy w Google frazę „Jan Nowak telefon” – niechaj te wyniki wyszukiwania dadzą nam do myślenia.

Kopia zapasowa Internetu

Czy zdarzyło się Wam korzystać kiedykolwiek z serwisów WWW typu archiwum? Zapewne tak, choć sami nie zdawaliście sobie nawet z tego sprawy. W Internecie bowiem są tysiące serwisów WWW, które regularnie przemierzają cały Internet i indeksują (podobnie jak roboty wyszukiwarek) różną zawartość, tworząc kopie danej strony WWW na konkretną chwilę. Kopię taką można później w dowolnym momencie odtworzyć – nie zdajemy sobie zatem sprawy, że wystawiając samochód na sprzedaż w Internecie dziś, możemy udostępnić swoje dane kontaktowe komukolwiek na świecie za 10 lat (jest to ekstremalny przypadek, ale możliwy).

Serwisy typu archive ponadto gromadzą również zdjęcia, pliki audio, video, PDF, dokumenty Word oraz setki innych. Wciąż powstają nowe, coraz bardziej targetowane – gromadzące kopie stron publicznych i rządowych, serwisów muzycznych, aukcyjnych czy banków zdjęć.

Internet to ludzie – jacy są, wie każdy z nas

Musimy pamiętać, że cały Internet to przede wszystkim ludzie, dopiero potem komputery i serwery. Najgorszym błędem, jaki możemy popełnić, jest przeświadczenie, że Internet jest swego rodzaju tablicą – coś raz napisane można zawsze zetrzeć. Otóż nie można.

Za pomocą rozmaitych serwisów do publikacji treści (przede wszystkim serwisów społecznościowych, ale również innych tworców wyobraźni) możemy w dosłownie kilka sekund rozpropagować daną informację dosłownie na cały świat. Doskonałym przykładem jest polski serwis Wykop.pl – jego idea polega na tym, aby różnego rodzaju wartościowe lub atrakcyjne treści publikować jak najwyżej. Im więcej osób uzna daną informację za atrakcyjną i „wykopie ją” – tym wyżej w serwisie ona się znajdzie. O potęgę tego serwisu świadczy fakt, że news znajdujący się na stronie głównej wykop.pl generuje dla podmiotowej strony kilkaset tysięcy (!!!) odsłon na godzinę. Wystarczy zatem niefortunnie opublikować coś w Internecie, a społeczność uzna to za warte zainteresowania – dowiedzą się o tym tysiące osób na całym świecie. Obojętne nie pozostaną również inne serwisy, które z pewnością pobiorą tak często cytowaną informację do siebie, publikując bez naszej wiedzy czy zgody. Internet to żywy i bardzo dynamiczny organizm, nad którym po prostu nie da się już zapanować, dlatego musimy bacznie uważać, co wrzucamy do tego „cyberkotła”.

Korzystając z Internetu cały czas miejmy na uwadze jego fundamentalną zasadę:

RAZ OPUBLIKOWANEJ TREŚCI NIE DA SIĘ Z INTERNETU USUNĄĆ.

www.aurelius.pl

Nauczycielu – czy wiesz co dzieci same robią w sieci?

Ale dzieci także samodzielnie korzystają z internetu i to w coraz młodszym wieku. Do tego celu używają często najnowszej technologii – tabletów, smartfonów itp.

Jak pokazują najnowsze analizy Polskiego Badania Internetowego i Kid Protect – profil polskiego internauty dynamicznie się zmienia właśnie jeśli chodzi o wiek internauty.

Już 12% polskich internautów to osoby poniżej 16 roku życia.

9% internautów nie skończyło jeszcze 13 lat. Wśród najmłodszych użytkowników internetu większość stanowią chłopcy (w grupie 7-12 lat).

Dzieci oraz młodzież korzystają z Internetu niewiele mniej intensywnie od dorosłych. Połowa Internautów w wieku 7-12 zagląda do Internetu codziennie lub prawie codziennie, kolejnych 27% zagląda do Internetu kilka razy w tygodniu. W grupie nastolatków do internetu codziennie lub prawie codziennie zagląda 48%, a kilka razy w tygodniu informacji w sieci szuka kolejne 46% gimnazjalistów.

Sieć dla dzieci to przede wszystkim rozrywka oraz serwisy społecznościowe. Na przynajmniej jedną ze stron z kategorii „Kultura i rozrywka” oraz „Społeczności” wszedł każdy młody internauta. Pośród witryn najczęściej odwiedzanych przez najmłodszych (7-12) znajdują się witryny z grami, natomiast gimnazjaliści (13-15) chętnie zaglądają na strony związane z edukacją oraz portale horyzontalne.

W przeciągu ostatniego półroczia wzrósł odsetek młodych osób zaglądających na witryny erotyczne. Wśród osób w wieku 7-12 z 25% w październiku 2010 do 48% w maju 2011. Także gimnazjaliści zaglądają na witryny erotyczne częściej niż kilka miesięcy wcześniej – w maju 52% internautów w tej grupie wiekowej (w październiku 2010 – 42%).

10 najpopularniejszych kategorii tematycznych - wśród dzieci 7-12 lat

Lp.	Kategoria	Real Users	Zasięg
1.	Kultura i rozrywka	1 710 168	100%
2.	Społeczności	1 710 168	100%
3.	Firmowe	1 604 053	93,80%
4.	Wyszukiwarki i katalogi	1 550 128	90,64%
5.	E-commerce	1 484 928	86,83%
6.	Nowe technologie	1 455 156	85,09%
7.	Edukacja	1 414 791	82,73%
8.	Informacje i publicystyka	1 348 275	78,84%
9.	Styl życia	1 298 682	75,94%
10.	Hosting	835 943	48,88%

Źródło: Megapanel PBI/Gemi us, V 2011, n=13 515

100% dzieci w wieku 7-12 lat odwiedza witryny z kategorii rozrywka i społeczności.

Popularność wybranych kategorii tematycznych wśród dzieci:

Lp.	Kategoria	Real Users	Zasięg
1.	Erotyka	815 676	47,70%
2.	Randki	231 283	13,52%
3.	Zakłady bukmacherskie, kasyna	215 947	12,63%

Na strony o tematyce erotycznej zagląda prawie 48 % dzieci korzystających z internetu. Witryny poświęcone randkom i zakładom bukmacherskim cieszą się mniejszym zainteresowaniem.

TOP 10 - najpopularniejsze witryny wśród dzieci w wieku 7-12 lat

Lp.	Nazwa	Real Users	Zasięg	opis witryny
1.	google.pl	1 461 098	85,44%	Wyszukiwarka
2.	onet.pl	1 158 892	67,76%	Portal
3.	youtube.pl	1 121 778	65,59%	Wideo
4.	google.com	1 120 664	65,53%	Wyszukiwarka
5.	nk.pl	1 017 316	59,49%	Społeczność
6.	wikipedia.org	922 987	53,97%	Edukacja
7.	wp.pl	890 828	52,09%	Portal
8.	allegro.pl	850 344	49,72%	Aukcje
9.	facebook.com	789 332	46,16%	Społeczność
10.	interia.pl	718 330	42,00%	Portal

Źródło: Megapanel PBI/Gemi us, V 2011, n=127

Tak jak dorośli dzieci korzystają w internecie przede wszystkim z rozrywki.

Trzeba pamiętać o tym, że witryny społecznościowe przeznaczone są dla użytkowników powyżej 13 roku życia. W badaniu nie uwzględniono najnowszych witryn umożliwiających dostęp do bezpłatnej telewizji na życzenie – np. tvnplayer.pl, który ruszył dopiero jesienią 2011 roku czy Hbogo.pl, który umożliwia obejrzenie trailerów bezpłatnie.

Internet to zbiór, z którego można czerpać bez ograniczeń.

Tak jak w realnym świecie – tak i w wirtualnym – aby czuć się komfortowo, trzeba zwracać uwagę na kilka zasad bezpieczeństwa.

Nie pozwalamy uczniom na niektóre zachowania zagrażające ich bezpieczeństwu? Chcemy, aby nasi uczniowie przestrzegali porządku i ogólnie przyjętych norm społecznych. Podobne granice możemy wytyczyć, jeśli chodzi o korzystanie z komputera.

Zacznijmy od zaplanowania, gdzie w Waszej szkole będzie stał komputer.

Powinien być on w takim miejscu, aby uczeń korzystając z niego nie był całkowicie wyizolowany. Uczeń będzie odczuwał obecności pedagoga i jeśli będzie potrzebował pomocy, czy wyjaśnienia, istnieje większe prawdopodobieństwo, że o nie poprosi.

Zawrzyjmy z uczniami umowę dotyczącą czasu i sposobu korzystania z komputera.

Taka umowa powinna zawierać nie tylko obowiązki ucznia, ale również kadry pedagogicznej. Nie powinien być to jedynie zbiór zakazów. Można skorzystać z gotowych wzorów takiej umowy dostępnych w internecie pod adresami, np.:

www.dzieckowsieci/images/stories/pliki/umowa1.pdf

www.dzieckowsieci/images/stories/pliki/umowa2.pdf

Poniżej zamieściliśmy również naszą propozycję.

Oczywiście w zależności od potrzeb i wieku uczniów umowę można modyfikować. Ważne jest jednak, aby od razu, na początku, zostały ustalone i przestrzegane pewne zasady korzystania z komputera, czy pracowni komputerowej. Później ich wprowadzenie będzie o wiele trudniejsze ze względu na konieczność przełamywania określonych przyzwyczajeń.

Przedyskutujmy z uczniami znaczenie postanowień zawieranej umowy.

Nasza szkolna umowa korzystania z Internetu i komputera

Jako uczniowie Społecznej Szkoły Podstawowej nr 23 w Grodzisku Mazowieckim jesteśmy świadomi, że korzystanie z komputera oraz Internetu daje dużo przyjemności, rozrywki, pomaga w poznawaniu świata i kontaktach z innymi ludźmi oraz służy do pracy i zarabiania pieniędzy. Internet jest dobry i pożyteczny, ale są osoby, które używają go, aby krzywdzić innych. Dlatego też, będziemy mieć ograniczone zaufanie do osób poznanych w Internecie tak samo, jak do osób nowopoznanych w świecie rzeczywistym.

Oto zasady, które ustaliliśmy wspólnie z nauczycielem informatyki dotyczące korzystania z komputerów w szkolnej pracowni informatycznej.

1. Będziemy starali się sprawdzić każdą informację znaną w Internecie również w innych miejscach (np. na innych stronach internetowych, w bibliotece, zapytamy nauczycieli, rodziców)
2. Będziemy informowali nauczycieli o każdym przypadku, kiedy ktoś poznany w Internecie będzie próbował dręczyć, obrażać, wyzywać, zmuszać do czegoś mnie lub inne osoby.
3. Będziemy informowali nauczycieli i rodziców o każdym przypadku, kiedy ktoś poznany w Internecie będzie chciał się ze mną spotkać.
4. Będziemy informowali nauczycieli o każdym przypadku, kiedy zauważymy, że z używanym komputerem dzieje się coś dziwnego.
5. W sposób miły i grzeczny będziemy odnosili się do innych użytkowników Internetu. Nie będziemy odpowiadać na zaczepki słowne, ani używać wulgarnego języka
6. Będziemy prosić nauczycieli, rodziców o zgodę i pomoc podczas instalacji nowych programów oraz pomagać nauczycielom i rodzicom w obsłudze nowych programów, gier, jeśli będą chcieli je poznać
7. Będziemy chronili swoje dane (nazwisko, adres, nr. telefonu) i pod żadnym pozorem nie udostępnimy ich nikomu poznanemu przez Internet
8. Nie będziemy przeglądać stron zawierających treści przeznaczone dla dorosłych
9. Nie będziemy zaniedbywać swoich obowiązków w szkole i w domu z powodu korzystania z komputera
10. Będziemy dbali o szkolne komputery. Nie będziemy jeść ani pić podczas korzystania z komputera.

W przypadku złamania powyższych zasad zobowiązuje się do:

.....

.....

.....

.....

.....

.....

Podpis Ucznia:

My – Nauczyciele, wychowawcy jesteśmy świadomi, iż komputer i Internet mogą stanowić źródło rozrywki oraz mogą pomagać w poszerzaniu wiedzy naszego ucznia oraz ułatwiać kontakt z rówieśnikami oraz przygotowywać go do przyszłej pracy zawodowej. Naszym zadaniem jest pomóc naszemu uczniowi, aby korzystanie z niego było pożyteczne i bezpieczne.

Będziemy:

1. Starać się udzielać wszelkiej pomocy we właściwym i bezpiecznym korzystaniu z komputera
2. Starać się poznać nowe programy i gry używane przez uczniów,
3. Wyjaśniać kwestie związane z bezpieczeństwem komputera,
4. Udzielać pomocy w sytuacji, kiedy uczeń poczuje się dręczony, nękany przez innych użytkowników Internetu
5. Zgłaszać administratorom stron internetowych oraz odpowiednim organom przypadki znalezienia treści niezgodnych z prawem
6. Szanować prywatność każdego ucznia
7. Administrować „szkolnym systemem komputerowym”, instalować odpowiednie programy, które chronią przed wirusami.

W przypadku złamania powyższych zasad zobowiązujemy się do:

.....

.....

.....

.....

.....

.....

Wychowawca klasy:

Dyrekcja:

Rodzice:

Czy uczeń wie, że zanim zostanie pracodawcą lub pracownikiem w niedalekiej przyszłości – sprawdzą go w serwisie społecznościowym

O ponad połowę w porównaniu do zeszłego roku wzrósł w Stanach Zjednoczonych odsetek pracodawców sprawdzających kandydatów do pracy w najpopularniejszych serwisach społecznościowych - wynika z badania przeprowadzonego przez firmę CareerBuilder. Dalszych 11% deklaruje chęć robienia tego w najbliższej przyszłości.

Z ubiegłorocznej analizy firmy CareerBuilder dotyczącej źródeł pozyskiwania przez amerykańskich pracodawców informacji o kandydatach ubiegających się o zatrudnienie wynikało, że 22% z nich sięga do serwisów społecznościowych.

Wyniki tegorocznej fali badania mówią, że w Stanach Zjednoczonych już blisko połowa (45%) pracodawców sprawdza swych przyszłych pracowników w popularnych portalach społecznościowych. I co więcej, ponad jedna trzecia z nich (35%) odrzuca zgłaszane aplikacje pod wpływem informacji uzyskanych z tych serwisów.

Wśród najczęściej wymienianych powodów nierozpatrywania kandydatury osoby, która zweryfikowana została za pośrednictwem serwisu społecznościowego znalazły się: prowokacyjne i nieodpowiednie zdjęcia oraz informacje (53% wskazań), informacje świadczące o nadmiernym korzystaniu z życia (picie alkoholu, branie narkotyków) - 44%, niestosowne wyrażanie się o byłym pracodawcy, współpracownikach oraz klientach (35%), a także ubogie umiejętności komunikacyjne (29%). Pracodawcy zwrócili też uwagę na niekulturalne komentarze zamieszczane w sieci, nieprawdziwe informacje dotyczące kwalifikacji, a także udostępnianie przez kandydata poufnych danych o byłym miejscu zatrudnienia.

Z badania CareerBuilder wynika także, że serwisy społecznościowe bywają przydatne w sensie pozytywnym w procesach rekrutacyjnych. Blisko jedna piąta pracodawców (19%) przyznała, że informacje uzyskane z sieci o kandydacie przyczyniły się do zatrudnienia go w firmie. Szczególnie w tym względzie zwracano uwagę na: sprawienie dobrego wrażenia i dostarczenie informacji o kwalifikacjach, kreatywności oraz dobrych umiejętnościach komunikacyjnych, a także uzyskanie referencji.

Pracodawcy, którzy wzięli udział w badaniu najczęściej sięgali do profili swych kandydatów w serwisach: Facebook (29%), LinkedIn (26%) oraz MySpace (21%). Jeden na dziesięciu sprawdził blogi, a 7% śledziło poczynania swych kandydatów na Twitterze. Branżami, które wyraźnie upodobały sobie wstępną, społecznościową weryfikację chętnych do pracy okazały się być: nowe technologie (63%) oraz usługi dla biznesu (53%). W badaniu wzięło udział ponad 2660 respondentów odpowiedzialnych za procesy rekrutacyjne w firmach oraz specjalistów z działów HR.

A jak jest u nas? Z badań przeprowadzonych przez serwisy Pracuj.pl i Profeo.pl wynika, że coraz bardziej popularne wśród internautów aktywnych zawodowo jest tzw. "personal branding" czyli świadome kształtowanie i rozwijanie swojego wizerunku w sieci. Okazuje się, że co trzeci internauta przynajmniej raz w miesiącu wpisuje swoje dane do wyszukiwarki sprawdzając w ten sposób co "mówi" o nim internet. Jeśli zaś chodzi o budowanie swojej marki za pośrednictwem społeczności - to największa uwaga internautów skupia się jednak na serwisach dla profesjonalistów i ludzi aktywnych zawodowo, a nie zwykłych "społecznościówkach". Wg innego badania przeprowadzonego przez Interaktywny Instytut Badań Rynkowych (IIBR) oraz serwis Profeo.pl. dla ponad 70% pracujących użytkowników biznesowych portali najważniejszym powodem korzystania z takich serwisów jest chęć zmiany miejsca zatrudnienia.

Źródło: <http://www.careerbuilder.com> Bożena Jaskowska

Ochrona danych osobowych uczniów w Internecie

Politycy i celebryci już wiedzą, jak niebezpieczny dla ich reputacji może być Internet. Mają jednak to szczęście, że social media nie istniały za ich licealnych czasów. "Młodzieńczego buntu" uniknąć trudno, ale lepiej żeby przyszły pracodawca czy małżonek nie poznał szczegółowej dokumentacji z jego przebiegu - przestrzega wyszukiwarka osób 123people.

Wyświetlana niedawno na ekranach naszych kin „Sala samobójców” Jana Komasy bez znieczulenia uświadamia nam, jak dużym niebezpieczeństwem może okazać się sieć. Błyskawiczny dostęp, ogromny zasięg i nieograniczona pojemność Internetu w połączeniu z kuszącą i coraz bardziej popularną tendencją do dzielenia się w sieci swoim prywatnym życiem może przynieść nieodwracalne konsekwencje dla życia osobistego i zawodowego. Szczególnie narażone są osoby młode, dla których chęć zaimponowania rówieśnikom jest ważniejsza niż konsekwencje zamieszczania w sieci wątpliwych moralnie treści na własny temat i na temat innych. Wszystko dzieje się pod prawdziwym imieniem i nazwiskiem, dostępne jest dla setek znajomych. Dla wielu dzisiejszych nastolatków zaowocuje to koniecznością zmiany tożsamości, bo jak twierdzi Eric Schmidt z Google, za jakiś czas nie będą w stanie identyfikować się z treściami, które dziś umieszczają na swój temat.

Czas testowania granic, kształtowania się tożsamości i wielu nieprzemyślanych decyzji do tej pory pozostawał w pamięci ograniczonego kręgu osób – mówi Ilona Grzywińska, Country Expert dla wyszukiwarki osób 123people. - W dobie Facebooka i iPhona informacje, zdjęcia czy filmy krążące w sieci są namacalnym dowodem naszego postępowania, niestety również tego nieodpowiedzialnego i kompromitującego w oczach rodziny, przyjaciół czy potencjalnego pracodawcy. Musimy mieć absolutną świadomość, że wszystko, co pojawia się w sieci na nasz temat, może zostać wykorzystane przeciwko nam w najmniej oczekiwanym momencie. Świadomość tego musimy zaszczerpić również dzieciom – dodaje Grzywińska.

Jak uchronić dziecko przed niekontrolowanymi treściami krążącymi na jego temat w sieci? Zabranianie dziecku korzystania z Internetu raczej nie wchodzi w grę, sieć i social media stały się integralną częścią naszego życia i pracy i właściwie nie jesteśmy już bez nich w stanie funkcjonować. Jedynym wyjściem wydaje się zdrowy rozsądek i ostrożność w surfowaniu, szczególnie w przypadku osób młodych, które są najbardziej skłonne do ryzykownych zachowań w sieci. Pomoże w tym kilka prostych zasad.

- Punktem wyjścia jest systematyczne monitorowanie informacji, które pojawiają się w sieci na nasz temat i na temat naszych dzieci. Wyszukiwarki uniwersalne, takie jak Google.com czy Yahoo.com oraz wyszukiwarki ludzi, jak www.123people.pl to pierwsze miejsce, którym użytkownicy poszukują informacji na temat danej osoby.
- Uświadom swoje dziecko, jakie treści mogą zaszkodzić jego reputacji. Pokaż, jakie informacje można udostępniać w sieci, a jakimi pod żadnym pozorem nie wolno się dzielić. Powiedz dziecku, jakie wpływ mogą mieć niepożądane treści na jego przyszłe życie zawodowe i osobiste.
- Sprawdź, jakie informacje możesz znaleźć w sieci na temat swojego dziecka i jego najbliższych znajomych. Wytłumacz dziecku, jak działają wyszukiwarki i jak wykorzystywać je do monitorowania informacji na własny temat.
- Sprawdź, co wyszukiwarki mówią o Tobie. Usuń u administratorów wszystkie informacje, które mogą zaszkodzić Twojej reputacji i mogą być nieodpowiednie w oczach Twojego dziecka.

- Pokaż dziecku, w jaki sposób można samodzielnie usunąć niepożądane treści i w jaki sposób skontaktować się z administratorem strony, jeśli usunięcie informacji wymaga jego interwencji.
- Kolejny krok to weryfikacja wszystkich informacji, które pojawiają się na Naszej Klasie, Facebooku i innych portalach społecznościowych.
- Usuń wszystkie zdjęcia, które przedstawiają Ciebie albo Twoje dziecko w sytuacjach dwuznacznych. Wskaż dziecku, jakich zdjęć nie powinno zamieszczać w sieci i dlaczego.
- Usuń tagi ze swoim nazwiskiem z niepożądanych fotografii znajomych. Pokaż dziecku, jak ono może to zrobić. Uświadom je, że nawet jeśli nie ma swojego nauczyciela wśród znajomych na Facebooku czy Naszej Klasie, ten może dotrzeć do zdjęć czy komentarzy dziecka.
- Sprawdź w wyszukiwarkach osób, takich jak www.123people.pl, czy na pewno przejrzałeś wszystkie portale społecznościowe, być może zdjęcia Twoje lub Twojego dziecka znajdują się w miejscu, o którym nie pamiętasz. Może się również zdarzyć, że fotografie Twoje lub Twojego dziecka wykorzystano bez Waszej wiedzy i zgody.
- Przejrzyj dokładnie listę znajomych dziecka. Jeśli znajdują się w niej profile fikcyjne, jak restauracje czy postacie z bajek – usuń je. Wy tłumacz dziecku, że pod fikcyjnym profilem może kryć się osoba, która może wykorzystać informacje o nim do swoich celów.
- Wchodząc w ustawienia prywatności ogranicz dostęp do profilu dziecka wszystkim tym, których nie zna dobrze. Pokaż, jak dziecko może to zrobić samodzielnie i wytłumacz, jakie osoby powinny wzbudzać jego nieufność.
- Wykasuj z profilu dziecka wszystkie nieodpowiednie komentarze i linki, również te umieszczone przez inne osoby. Naucz dziecko rozpoznawać, jakie komentarze mogą zaszkodzić jego reputacji.
- Kontroluj profil swojego dziecka i uświadom je, w jaki sposób bez jego woli lub wiedzy mogą zostać wykorzystane wszystkie informacje, które znajdują się na portalu społecznościowym.

Pamiętajmy, że wszystko co trafia do sieci, buduje naszą tożsamość internetową. A ta może mieć na przyszłość ucznia o wiele większy wpływ, niż się dzisiaj wydaje.

www.123people.pl

Rady dla kadry pedagogicznej:

- Niech komputery w pracowni komputerowej mają monitory ustawione w sposób pozwalający na zerknięcie na wyświetlane treści,
- Ustal z uczniami zasady korzystania z internetu w szkole i egzekwuj je.
- Nie karz dziecka za błędy, o których Ci mówi.
- Rozmawiaj z dzieckiem.
- Nie bój się przyznać do niewiedzy.
- Baw się siecią, poznawaj ją, nie bój się jej.
- Surfuj po sieci ze swoim uczniem.
- Pokazuj dziecku wartościowe miejsca.
- Wychowuj do sieci.
- Wspomagaj się programami filtrującymi
- Porozumiewaj się z rodzicami
- W przypadku przestępstwa niczego nie kasuj z komputera.
- Zawiadamiaj policję o przestępstwie, a administratorów sieci i stron internetowych o niewłaściwych zachowaniach
- Ucz uczniów zasad bezpieczeństwa, nie strasz jednak zagrożeniami.

Poznaj ciemniejsze strony Internetu – warto wiedzieć, że tak jak w realnym świecie – w cyberprzestrzeni też możemy spotkać się z różnym zachowaniami

Cyberprzestępczość	Cyberprzemoc
1. Dzieci nie są tylko ofiarami, ale i sprawcami przestępstw 2. Rodzaje cyberprzestępstw: ➤ Hacking, cracking (włamania) ➤ Oszustwa, wyłudzenia ➤ Wywiad przestępczy	➤ Przemoc między dziećmi istniała zawsze ➤ Konflikty z klasy przenoszą się do sieci ➤ Dzieci mają problemy adekwatne do swojego wieku ➤ Często sprawcami są dziewczynki ➤ Dokuczanie, obrażanie ➤ Groźby karalne ➤ Kompromitujące filmy i zdjęcia publikowane w sieci lub rozsyłane telefonami komórkowymi

Wirusy i zagrożenia techniczne

Wirusy to programy komputerowe, które infekują komputer i wykonują w nim nieuprawnione operacje. Mogą to być głupie żarty w postaci pojawiającego się komunikatu, ale wirus może też uszkodzić sprzęt, czy zniszczyć dane. Istnieje wiele wirusów i ciągle powstają nowe. Specjaliści z Panda Software, producenta programów antywirusowych, twierdzą, iż obecnie większość wirusów rozprzestrzenia się właśnie drogą internetową.

Włamanie komputerowe

W internecie na ogół spotkamy ludzi miłych i uczynnych. Niestety są w nim również przestępcy. Poważną grupę stanowią tzw. crackerzy, czyli ludzie włamujący się do cudzych komputerów, wyrządzając szkodę innym użytkownikom sieci. Mogą oni wykraść lub zniszczyć dane, włamać się do poczty użytkownika, konta bankowe (jeśli korzystasz z bankowości internetowej), dokonywać zakupów na czyjeś konto. Nawet jeśli nie wyrządzą szkód bezpośrednio Tobie, mogą wykorzystać Twój komputer do swoich celów

Obrót danymi osobowymi

Dzieci to bardzo atrakcyjna grupa klientów. Wydają dużo pieniędzy na zabawki i słodycze itp., często mają wpływ na decyzje dorosłych. Specjaliści od marketingu chętnie więc kierują w internecie reklamy do dzieci. Nieuczciwi marketerzy wyłudniają i handlują tymi danymi, kusząc dzieci konkursami, upominkami, nagrodami, itp. Aby założyć darmowe konto poczty elektronicznej trzeba często wypełnić szczegółową ankietę, zawierającą pytanie o dochód w rodzinie, zainteresowania, a nawet nawyki konsumenckie.

Internet jako narzędzie wywiadu dla przestępcy

Dzieci z natury są ufne. Chętnie opowiadają o sobie, swoim domu, rodzinie. W niedawnym telewizyjnym eksperymencie zbadano zachowania w chat roomie. Dziennikarz rozmawiał z 13-letnią dziewczynką, podając się za 14-letniego chłopca. W ciągu 15 minut dziewczynka opowiedziała dziennikarzowi dokładnie jak ma na imię, ile ma lat, kim z zawodu są jej rodzice, że marzy o psie, lubi oglądać filmy na DVD, a z internetu korzysta w domu. Wysłała dodatkowo swoje zdjęcie, podała adres poczty elektronicznej i numer telefonu. Gdyby na miejscu dziennikarz był włamywacz, mógłby łatwo ustalić adres, domyśliłby się, w jakich godzinach mieszkanie jest puste. Wiedziałby też, że w domu jest komputer, DVD, pewnie też dobry telewizor, a także że nie musi obawiać się psa. Informacje te pozwoliłyby zaplanować włamanie.

Oszustwa i wyłudzenia

Internet to coraz większe miejsce dokonywania transakcji handlowych. Dzieci również buszują po serwisach aukcyjnych (np. allegro – choć rejestracja dozwolona jest od 13 roku życia za zgodą rodziców) i robić tam zakupy. Najczęstsze oszustwo polega na tym, że kupujemy okazynie jakąś rzecz za bardzo atrakcyjną cenę. Zamawiamy za przesyłkę, płacimy, a w środku zamiast zamówienia – cegła. Ograniczone zaufanie – to najlepsza forma postępowania w takich sytuacjach.

Uzależnienie

Internet wciąga – nawet dorosłych. Wchodzisz na jedną stronę a poprzez linki idziesz do innych treści, tam znajdujesz następne i tak w nieskończoność. Zaczynasz przygodę z komunikatorem, chat roomem itp. – odkrywasz, jak łatwo poznać nowych ludzi, których w innych okolicznościach nie można by było spotkać i miło porozmawiać i czegoś ciekawego dowiedzieć. Zajmuje to Ci coraz więcej czasu. W pewnym momencie pocztę mailową „musisz” już odbierać codziennie, a Twój profil na Facebooku nie mieści już nowych „znajomych”. Uzależniasz się. Na świecie powstają już kluby Anonimowych Netoholików. Uzależnienie od Internetu leczy się tak samo jak narkomanię czy alkoholizm. Dzieci są szczególnie podatne na uzależnienia.

Fazy rozwoju uzależnienia od internetu:

I. Faza wstępna

- przebywanie w sieci sprawia przyjemność,
- wzrost ochoty na coraz częstsze przebywanie w sieci,

II. Faza ostrzegawcza

- Szukanie okazji do jak najczęstszego przebywania w sieci,
- Rozładowanie napięcia poprzez sieć,
- Próby korzystania z sieci w ukryciu

III. Faza krytyczna

- spadek innymi zainteresowaniami nie związanymi z siecią,
- Zaniedbywanie wyglądu zewnętrznego,

IV. Faza chroniczna – jedyny świat to świat wirtualny.

Gry

Komputer u młodzieży rozwija wyobraźnię, spostrzegawczość, koordynację wzrokowo-ruchową, logiczne myślenie, rozwój intelektualny. Jednak wielogodzinne spędzanie czasu przed komputerem na grach zainstalowanych na dysku lub grach sieciowych negatywnie wpływa na rozwój dziecka.

Gry mogą powodować oderwanie się od rzeczywistości, przejście do świata marzeń, gdzie są proste zasady, reguły. Gry brutalne, zawierające dużo walki, krwi, przemocy powodują zmiany w zachowaniach człowieka. Wzmaga to intensywna grafika, efekty dźwiękowe. Wywołują u młodzieży niepokój, podniecenie, frustrację, dostrzegają złe strony świata, przybierają imiona i nazwiska fikcyjnych bohaterów. Zafascynowane grą zapominają nawet o fizjologicznych potrzebach - nie jedzą, nie piją. Agresywne treści przenoszą do świata rzeczywistego.

Podział gier

- Symulatory –np. sterowanie samolotami na wojnie lub zawodach
- Strategiczne – klasyczne strategie wojenne - 9 Kompania; strategie czasu rzeczywistego z rozbudową – Red Alert
- Zręcznościowe – np. strzelanka, bijatyki, flipery
- Gry przygodowe – rozbudowana fabuła, skomplikowane wątki detektywistyczne -Ace Ventura
- Edukacyjne – wspomagają naukę przez zabawę
- Sportowe – np. piłka nożna FIFA09
- Logiczne – wymagają intensywnego myślenia
- RPG – odmiana gier przygodowych (Wiedźmin)

Gra TIBIA

- budujemy swoją postać, osiągamy różne poziomy (100 –po roku grania), zdobywamy sprawności, bogactwa. Jedną postacią gra wiele osób – „nadmiar sprawności” sprzedawany jest na allegro.

GRA GTA IV

- Seria *Grand Theft Auto* zyskała opinię gier brutalnych, niepoprawnych wychowawczo, dających zły przykład, budzących agresję ale należącą do najbardziej grywalnych. Sama nazwa wskazuje na typ rozrywki, z jakim będziemy mieli do czynienia (złodziej samochodów). Głównym atutem gry jest nieograniczona swoboda postępowania głównego bohatera (kradzieże, pobicia, morderstwa).

GRA POSTAL

- W grze wcielamy się w tajemniczego „Kolesia”, który bez żadnych zahamowań likwiduje wszystkie żywe istoty, np. saksofonistów z orkiestry dętej, mieszkańców wiejskich terenów, objadających się pączkami stróżów prawa.

THE PUNISHER

- Komputerowa wersja popularnego komiksu. W tym przypadku historyjka nie jest ważna. Chodzi tu tylko o to, by zabijać w ciekawy sposób np. zgniatając głowę wiekiem trumny.

GRA SECOND LIFE

- Częściowo płatny, wirtualny świat. Postać, stworzona w *Second Life*, nie posiada jakichkolwiek statystyk czy profesji. Gracz sam wybiera płeć bohatera, ubiór, sytuację materialną. Nie ma tam chorób, biedy, starości, brzydoty. Drugie dno gry - nie ma tam również żadnych ograniczeń – (kupujemy sobie narządy płciowe – możemy ich użyć, zapłacić za wirtualny seks, prostytutkować się).

Problemy psychologiczne

Uzależnienie to tylko część. Internetowe przyjaźnie są najczęściej złudne. Ludzie nadal pozostają sobie obcy i anonimowi. Internet to narzędzie dla łatwego kontaktu z narkotykami. W 2007 roku znaleziono 238, a w 2008 roku 347 polskich stron i adresów o narkotykach. Na stronach tych znajduje się:

- wymiana informacji np. blogi (wspomnienia ponarkotykowe - „mój pierwszy raz”),
- wskazówki praktyczne np. jak brać lub jak uprawiać narkotyki,
- oferty handlowe bezpośrednie i pośrednie,
- upowszechnianie nowych środków – pseudonarkotyki (brak ich na liście narkotyków)
- top listy – ranking stron oferujących marihuanę
- muzik listy – muzyka, która wpływa na podświadomość młodzieży.

Kluby samobójców - w Internecie można znaleźć na forach lub blogach informacje jak skutecznie i bezboleśnie popełnić samobójstwo skupiające ludzi zagubionych w życiu, dość często szukających jak skutecznie pozbawić się życia. W 2007 roku 45 stron namawiających do samobójstwa.

Groźby karalne, nękanie

Wiele osób myśli, że w sieci są anonimowi (mylą się bardzo) – czują się przez to bardzo bezkarni i pozwalają sobie na zachowania, na które być może nie odważyliby się w codziennym życiu. Stają się wulgarni, grożą innym, próbują nękać. Tymczasem w takich sprawach dowody mają postać elektroniczną i mogą przybierać różnorakie formy np. mogą to być e-maile, sms-y, billingi telefoniczne, pliki tekstowe, graficzne, dźwiękowe

Szkodliwe treści

Choć tylko udostępnianie pornografii małoletnim jest karalne – to często dzieci mogą trafić w sieci na inne szkodliwe treści – na strony epatujące wulgarnością i przemocą, promujące hazard, używki, broń, propagujące rasizm, idee różnego rodzaju sekt, czy strony nawołujące do samobójstw.

Dostęp do pornografii

Zgodnie z polskim prawem udostępnianie pornografii osobom, które nie ukończyły 15 lat, jest przestępstwem. Jednak w internecie praktyczne jest do tego dostęp nieograniczony. Co gorsza wcale nie trzeba szukać pornografii, aby na nią trafić – wiele stron porno umieszcza w swoich pisach np. nazwisko Britney Spears.

Autorzy stron pornograficznych często rejestrują dla nich adresy łudząco podobne do adresów popularnych witryn, ale zawierających np. błąd ortograficzny lub inną domenę. Znanym przykładem jest witryna WhiteHouse.com. Zamiast informacji z siedziby amerykańskiego prezydenta znajduje się tam pornografia. Większość internautów wpisuje właśnie ten adres zamiast prawidłowego www.whitehouse.gov. Warto pamiętać, że zgodni z polskim prawem cała odpowiedzialność za skuteczne zabezpieczenie pornografii przed dostępem dzieci spoczywa na tym, kto takie materiały rozpowszechnia.

Pornografia dziecięca

Zgodnie z polskim prawem karalne jest utrwalanie, produkowanie, sprowadzanie i rozpowszechnianie pornografii dziecięcej, czyli pornografii z udziałem osoby, która nie ukończyła 15 roku życia. Karalne jest też jej posiadanie i przechowywanie. Znalezienie tego typu treści jest banalnie proste. W Polsce nie ma tronu z takimi materiałami, są one jednak dostępne w grupach dyskusyjnych, za pomocą poczty, na zakonspirowanych serwerach.

Pedofile

Trzeba sobie uświadomić sobie, że pedofilem może być każdy. Nie ma tu żadnych reguł. Jak i w poprzednich sytuacjach – pedofil w internecie zazwyczaj podaje się za kogoś innego, wykorzystując naiwność i ufność dziecka. Często podaje się za rówieśnika, a potem stopniowo osacza i uzależnia od siebie dziecko. Chętnie też odgrywa rolę „dobrych wujków” i „kumpli” – celując w dziecko, które zazwyczaj ma problemy w szkole, z rówieśnikami lub w domu. Pedofil będzie wówczas przekonywał dziecko, że jest jedyną osobą, która je rozumie i akceptuje. Pedofile chętnie korzystają z chat roomów, komunikatorów i poczty elektronicznej. Wykorzystują strony prowadzone przez dzieci oraz ich blogi. Uprawianie seksu z dzieckiem poniżej 15 lat jest w Polsce przestępstwem zagrożonym karą do 10 lat więzienia.

- Pedofil to osoba, której popęd seksualny jest ukierunkowany na dziecko.
- Nie każdy, kto molestuje, jest pedofilem.
- Nie każdy, kto jest pedofilem, molestuje.
- Najczęściej sprawcą osoba znana dziecku – nadużycie zaufania
- Rodzina rzadko jest wsparciem dla dziecka
- Nie ma reguły wieku, wykształcenia, miejsca zamieszkania, statusu majątkowego, wyglądu ani płci
- Ostrożnie można mówić o „zawodach ryzyka”
- Pedofile i psychomanipulatorzy w Sieci
- Wymieniają się materiałami, kontaktami i doświadczeniami.
- Dążą do spotkania lub cyberseksu.
- Potrafią manipulować.

Cyberseks

Nawet jeśli nie dochodzi do realnego spotkania i molestowania seksualnego, to bardzo często mamy do czynienia z cyberseksem, czyli rozmową na tematy seksualne, często polegającą na opowiadaniu fantazji erotycznych lub słownym przedstawianiu aktu seksualnego. Jeśli stroną takiego cyberseksu jest dziecko to wyrządza to szkody na jego psychice. Polskie parwo mówi, że karze do 10 lat więzienia podlega ten, kto „doprowadza małoletniego poniżej 15 lat do obcowania płciowego lub do poddania się czynności seksualnej albo do wykonania takiej czynności”

Prawo jest po stronie użytkowników Internetu przestrzegających zasad

Internet to tak samo bezpieczne miejsce jak inne – pod warunkiem, że znamy i przestrzegamy prawa.

Prawo nas chroni – warto wiedzieć jakie dokładnie mamy prawa i jakich zachowań wymagać od współkorzystających z nowoczesnych technologii.

Poniżej przedstawiamy najważniejsze przepisy prawne, na które możemy powoływać się i które możemy egzekwować w poszczególnych sytuacjach

Art. 190a Kodeks karny - stalking, uporczywe nękanie

§ 1.

Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności do lat 3.

§ 2.

Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej.

§ 3.

Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od roku do lat 10.

§ 4.

Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego

Art. 212, Art. 216 Kodeks karny – naruszenie czci (zniesławienie, znieważenie)

Sprawca:

- podlega grzywnie, karze ograniczenia albo pozbawienia wolności do roku, lat 2,
- Wypłacenie napiwku na rzecz pokrzywdzonego, Polskiego Czerwonego Krzyża albo na inny cel społeczny wskazany przez pokrzywdzonego.

Art. 267, Art. 268a Kodeks karny - włamania

Sprawca:

- podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2,3 lub 5.

Art. 190, Art. 191 Kodeks Karny - groźby

Działania:

- Groźenie komuś popełnieniem przestępstwa (np. pozbawieniem życia) przez Internet.
- Kierowanie do dziecka, za pomocą Internetu gróźb w celu zmuszenia go do określonego działania.

Formy:

- Przesyłanie gróźb drogą e-mailową lub za pomocą innych narzędzi dostępnych w Internecie, takich jak czat, komunikatory, forum.
- Grożenie innej osobie przy użyciu Internetu lub telefonu komórkowego stosując słowo, pismo, gest lub inne zachowanie oddziałujące na psychikę odbiorcy.

Sprawca:

- podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2,3 lub 5.

Art. 141 – Kodeks wykroczeń - wulgaryzmy

- Kto w miejscu publicznym umieszcza nieprzyzwoite ogłoszenie, napis lub rysunek albo używa słów nieprzyzwoitych, podlega karze ograniczenia wolności, grzywny do 1500 zł albo karze nagany.

Działania:

- Używanie w Internecie wulgarnych zwrotów (w miejscach dostępnych powszechnie, czyli nie wymagających np. znajomości hasła i logowania się).
- Umieszczenie w Internecie nieprzyzwoitego zdjęcia, rysunku, obrazu (w miejscach dostępnych powszechnie).

Formy:

- Nagminne używanie w Internecie, w miejscach komunikacji wielu osób (np. czat, forum) nieprzyzwoitych słów.
- Umieszczanie w Internecie, w miejscu powszechnie dostępnym zdjęć i obrazów o treści nieprzyzwoitej czy obsceniczej.

Art. 107 Kodeks wykroczeń - nękanie

- Kto w celu dokuczenia innej osobie złośliwie wprowadza ją w błąd lub w inny sposób złośliwie niepokoi, podlega karze ograniczenia wolności, grzywny do 1500 zł albo karze nagany.

Działania:

- Złośliwe niepokojenie jakiejś osoby w celu dokuczenia jej poprzez wykorzystanie Internetu.
- Wielokrotne powtarzanie jakiegoś działania w Internecie skierowanego na jakąś osobę wbrew jej woli.

Formy:

- Wielokrotne wysyłanie komuś w Internecie lub przy użyciu telefonu komórkowego niechcianych lub uprzykrzających informacji, obrazów, linków, itp., zwłaszcza, gdy dokonuje się tego korzystając z różnych form internetowej komunikacji naraz.
- Bardzo częste wysyłanie komuś e-maili i informacji za pomocą komunikatorów, czatów, pomimo wyraźnej niezgody odbiorcy.
- Wpisywanie bardzo dużej ilości niechcianych komentarzy pod zdjęciami czy wypowiedziami danej osoby w internecie.

Wykaz treści, których publikacja w Internecie jest prawnie zakazana:

- Treści, które naruszają rażąco zasady współżycia społecznego (sankcje określają różne ustawy, w tym kodeks karny, kodeks cywilny i kodeks pracy).
- Treści, za które określono sankcje w kodeksie karnym, a które:
 - namawiają do popełnienia lub doradzają w popełnieniu samobójstwa lub samookaleczenia (art. 151 Kodeksu karnego);
 - grożą innym osobom popełnieniem przestępstwa na jego szkodę lub szkodę osoby jego najbliższej (art. 190 Kodeksu karnego);
 - obrażają inne narodowości, rasy ludzkie, religie (art. 194-196 i art. 257 Kodeksu karnego oraz art. 23 Kodeksu cywilnego);
 - nawołują do popełnienia przestępstwa (art. 255 Kodeksu karnego);
 - propagują totalitarny ustrój państwa lub nawołuje do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość (art. 256 Kodeksu karnego).
- Treści, za które określono sankcje w kodeksie cywilnym, a które:
 - lżą osoby publiczne (art. 23 Kodeksu cywilnego);
 - zawierają pomówienia – informacje obarczające niepotwierdzonymi zarzutami inne osoby (art. 23 Kodeksu cywilnego);
 - obrażają inne narodowości, rasy ludzkie, religie (art. 23 Kodeksu cywilnego oraz art. 194-196 i art. 257 Kodeksu karnego).
- Treści, za które określono sankcje w ustawach szczególnych, a które:
 - promują alkohol (art. 2 (1) Ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi z dnia 26 października 1982 r.);
 - przyczyniają się do łamania praw autorskich lub naruszają prawa autorskie i licencje podmiotów trzecich. (Ustawa o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r.);
 - promują środki odurzające, narkotyki (art.1 Ustawy o przeciwdziałaniu narkomanii z dnia 24 kwietnia 1997 r.);
 - ujawniają bez czyjejs wyrażonej zgody dane osobowe, identyfikatory komunikatorów internetowych, fotografie, adres poczty elektronicznej, miejsce zamieszkania, pracy, przebywania, numery telefonów, tablic rejestracyjnych i inne poufne dane (Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych);
 - zawierają słowa powszechnie uznane za niecenzuralne (art. 3 Ustawy o języku polskim z dnia 7 października 1999 r.).

Bądź świadomy! Czyli jak przestrzegać praw autorskich w Internecie

Po pierwsze: jakie utwory są objęte ochroną prawną?

Zgodnie z ustawą ochroną o prawach autorskich i prawach pokrewnych ochroną objęty jest każdy utwór, czyli „przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia”. Może to być piosenka, artykuł prasowy, krótki wierszyk, czy program komputerowy.

Po drugie: korzystanie z plików audio-video nie jest przestępstwem, inaczej jest z udostępnianiem bez zgody

Utwór w Internecie to najczęściej plik. Nie ma znaczenia, czy go odsłuchujemy, oglądamy, czy czytamy, po prostu korzystamy. Bez znaczenia dla prawa jest także, czy korzystamy z plików po ściągnięciu ich i zachowaniu na swoim dysku, czy też wprost z Internetu. Do momentu, gdy z plików jedynie korzystamy, nawet gdy znalazły się one w sieci nielegalnie, nie popełniamy przestępstwa. Gdybyśmy jednak chcieli je udostępnić innym bez zgody, np. umieszczając w serwisie internetowym, albo z własnego dysku za pomocą programu typu peer to peer, możemy odpowiedzieć za rozpowszechnianie pliku bez zgody jego właściciela, twórcy.

Po trzecie: odpowiedzialność cywilna i karna za pobieranie plików

Opinie prawników na temat odpowiedzialności cywilnej za pobieranie plików z muzyką, czy filmami są różne.

Jedne odnoszą się do art. 23 ustawy o prawie autorskim i prawach pokrewnych, który mówi, że można bez zezwolenia twórcy nieodpłatnie wykorzystać już rozpowszechniony utwór w granicach użytku osobistego. Przykładem tego może być nagrywanie filmów emitowanych w telewizji.

Inna opinia odnosi się natomiast do art. 35 cytowanej wcześniej ustawy. Wynika z niego, że dozwolone korzystanie z plików nie może naruszać interesów ich twórców, np. uszczuplać ich zysk. Dodatkowo w myśl tego stanowiska, utwór rozpowszechniony oznacza, że udostępnianie go następuje po zgodzie jego twórcy. Dlatego, jeśli utwór trafił do Internetu bez zgody autora, to nie może być mowy o użytku osobistym. Zgodnie

z tą opinią taka sama odpowiedzialność, jak za ściąganie plików groziłaby za oglądanie w serwisach internetowych filmów umieszczonych bez wiedzy i zgody twórcy.

A co mówi prawo karne, jeżeli chodzi o pobieranie programów komputerowych?

Ściąganie nielegalnych programów z Internetu, ich kupowanie, pożyczanie lub po prostu posiadanie jest przestępstwem. Art. 278 § 2 kodeksu karnego mówi konkretnie o kradzieży programu komputerowego, a w art. 293 znajduje się zapis dotyczący paserstwa programu komputerowego. Prawo autorskie również zawiera przepisy sankcjonujące bezprawne zachowania dotyczące nielegalnych programów komputerowych, są to te same przepisy, które stosuje się także w odniesieniu do innych plików, np. muzycznych czy filmowych. Przepisy te umieszczone są w art. od 116 do 118 ustawy o prawie autorskim i prawach pokrewnych, które mówią o nielegalnym rozpowszechnianiu, zwielokrotnianiu programów komputerowych czy o ich paserstwie. Kary zawarte w ww. przepisach sięgają nawet do 5 lat pozbawienia wolności.

Po czwarte: naruszanie praw autorskich może słono kosztować

Jeśli sąd uznałby, że pobierając pliki, naruszyłeś prawa twórców, to Twój ulubiony piosenkarz mógłby domagać się od Ciebie zapłaty należnego wynagrodzenia. Wysokość takiej kary może wynieść trzykrotną wartość stosownego wynagrodzenia dla twórcy.

Po piąte: ci, którzy bezprawnie udostępniają pliki muszą liczyć się z odpowiedzialnością karną i cywilną

Jeśli tylko ściągasz i oglądasz filmy w swoim komputerze możesz być spokojny, jeśli jednak je udostępniasz, możesz spotkać się z policjantami. Praktyka wskazuje, że coraz częściej sprawami tymi zajmują się sądy i prokuratury.

Prawo jasno określa, że „kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór (...) podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch”. Jeśli podejrzany robił to, aby osiągnąć zysk, kara może wynosić nawet 3 lata. W przypadku, kiedy sprawca z okradania twórców z praw autorskich i udostępniania ich uczynił sobie stałe źródło dochodów, do więzienia może trafić nawet na 5 lat.

Po szóste: P2P

Peer to peer to sposób wymiany plików gwarantujący równorzędne prawa obu stronom. Każdy komputer podłączony do tej sieci może ściągać i udostępniać pliki. Internauci dzięki temu masowo wymieniają się plikami filmowymi, czy muzycznymi. W ten sposób każdy może udostępnić plik, który ma na twardym dysku, po to, aby osoba w innym miejscu na świecie mogła go sobie ściągnąć. Warto pamiętać, że wiele programów tego typu w sposób automatyczny udostępnia utwory i nie da się tego zablokować. Dlatego czasem nieświadomy tego użytkownik naraża się na odpowiedzialność karną. Są jednak programy, w których można kontrolować, co się udostępnia.

Cyberprzemoc – charakterystyka zjawiska

Poważne zagrożenia dla młodych internautów kojarzone są z problemem pedofilii lub innymi formami działań dorosłych przeciwko dzieciom. Kwestie te nie tracą niestety na aktualności, jednak w ostatnim czasie, wraz z coraz większą dostępnością nowych mediów dla dzieci i młodzieży, coraz szerszą gamą możliwości, jakie media te oferują, poważnym zagrożeniem dla najmłodszych stają się również ich rówieśnicy. Problem określany terminem cyberbulling lub coraz popularniejszym w Polsce terminem cyberprzemocy zauważony został zaledwie kilka lat temu, jednak bardzo szybko uznany został za istotną kwestię społeczną i przeciwdziałanie mu jest obecnie priorytetem większości programów edukacyjnych poświęconych bezpieczeństwu dzieci w sieciⁱ.

Zjawisko cyberprzemocy najkrócej definiuje się jako przemoc z użyciem technologii informacyjnych i komunikacyjnych. Technologie te to głównie Internet oraz telefony komórkowe. Część definicji ogranicza stosowanie terminu cyberbulling czyli cyberprzemoc wyłącznie do przemocy rówieśniczej, inne nie stawiają ograniczeń wiekowych, niewątpliwie jednak najczęściej terminów tych używa się właśnie w kontekście przemocy wśród najmłodszych. Podstawowe formy zjawiska to nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów z użyciem sieci oraz podszywanie się w sieci pod kogoś wbrew jego woli. Do działań określanych mianem cyberprzemocy wykorzystywane są głównie poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, serwisy społecznościowe, grupy dyskusyjne, serwisy SMS i MMSⁱⁱ.

W odróżnieniu od „tradycyjnej” przemocy (ang. bulling) zjawisko cyberprzemocy charakteryzuje wysoki poziom anonimowości sprawcy. Ponadto na znaczeniu traci klasycznie rozumiana „siła”, mierzona cechami fizycznymi czy społecznymi, a atutem sprawcy staje się umiejętność wykorzystywania możliwości, jakie dają media elektroniczne. Charakterystyczna dla problemu szybkość rozpowszechniania materiałów kierowanych przeciwko ofierze oraz ich powszechna dostępność w sieci sprawiają, że jest to zjawisko szczególnie niebezpieczne. Kompromitujące zdjęcia, filmy czy informacje potrafią zrobić w Internecie bardzo szybką „karierę”, a ich usunięcie jest często praktycznie niemożliwe. Dodatkową uciążliwością dla ofiar cyberprzemocy jest stałe narażenie na atak, niezależnie od miejsca czy pory dnia lub nocy. Kolejną ważną cechą problemu jest stosunkowo niski poziom kontroli społecznej tego typu zachowań. Sytuacja doznawania przez dziecko krzywdy za pośrednictwem mediów elektronicznych jest często trudna do zaobserwowania przez rodziców czy nauczycieli, szczególnie jeżeli mają ograniczoną wiedzę i doświadczenia związane z korzystaniem z mediów elektronicznychⁱⁱⁱ.

Pierwsze doniesienia medialne dotyczące zjawiska przemocy rówieśniczej w sieci pojawiły się na początku lat dwutysięcznych. Były to m.in. przypadek japońskiego ucznia nagrywanego w krępującej sytuacji w szatni szkolnej kamerą w telefonie komórkowym; sprawa zdjęcia amerykańskiej uczennicy, której fotografia przerobiona została na zdjęcie pornograficzne; czy głośna historia filmu, w którym chłopiec z Kanady nieporadnie odgrywa scenę z filmu „Gwiezdne Wojny”. W Polsce głośno o problemie przemocy rówieśniczej

z użyciem mediów elektronicznych zrobiło się wraz z historią gdańskiej gimnazjalistki, która popełniła samobójstwo w efekcie przemocy doznanej ze strony rówieśników. W historii ważną rolę odegrało nagranie kamera w telefonie komórkowym aktu krzywdzenia dziewczyny. Domniemywano, że groźba upublicznienia zarejestrowanego filmu przyczyniała się do tragicznego finału tej historii.

W Polsce problem przemocy rówieśniczej w sieci rozpoznany został na początku 2007 r. przez Fundację Dzieci Niczyje i firmę badawczą Gemius S.A. W toku badań Przemoc rówieśnicza a media elektroniczne^{iv} dzieci pytane były o doświadczenia następujących sytuacji:

- Przemoc werbalna w sieci (wulgarne wyzywanie, poniżanie, ośmieszania, straszenie, szantaż),
- Rejestrowanie filmów i zdjęć wbrew woli dziecka,
- Publikowanie w sieci filmów, zdjęć i informacji ośmieszających dziecko,
- Podszywanie się w sieci pod dziecko.

Respondenci pytani byli również o ich odczucia i reakcję w danej sytuacji oraz proszeni o próbę określania sprawcy zdarzenia.

Przemoc werbalna

Aż 52% internautów w wieku 12-17 lat przyznało, że za pośrednictwem Internetu lub telefonii komórkowej miało do czynienia z przemocą werbalną – niemal połowa badanych doświadczyła wulgarnych wyzywania (47%), co piąty poniżania, ośmieszania i upokarzania (21%), a co szósty straszenia i szantażowania (16%). Najbardziej negatywne reakcje towarzyszą przypadkom poniżania – zdenerwowanie (59%), strach (18%) lub wstyd (13%). Jedynie 30% dzieci deklaruje, że taka sytuacja nie robi na nich żadnego wrażenia. Jedynie nieznacznie niższy poziom negatywnych emocji towarzyszy sytuacjom straszenia i szantażu w sieci. Mimo to blisko połowa dzieci nie informuje nikogo o takich przypadkach. Jedynie co dziesiąte dziecko zawiadamia o takich przypadkach swoich rodziców lub nauczyciela.

Filmy i zdjęcia

Ponad połowa nastoletnich internautów (57%) przyznaje, że była przynajmniej raz obiektem zdjęć lub filmów wykonanych wbrew jej woli. Względnie rzadko (18%) sytuacja taka jest zdarzeniem jednorazowym – w 2/5 przypadków (39%) zdarzenie takie powtarzało się. Zdecydowanie najczęściej autorami takich zdjęć są rówieśnicy – znajomi ze szkoły (87%) lub spoza szkoły (30%). Zdecydowana większość (80%) „niechcianych obrazów” ma niegroźny z pozoru kontekst humorystyczny. Jednakże aż połowa badanych (49%) deklaruje w takich sytuacjach wyraźnie negatywne odczucia. Popularnymi motywami robienia zdjęć/filmów są złośliwość (21%) oraz popisywanie się przed innymi (17%). Celem co ósmego zdjęcia lub filmu jest ośmieszenie bohatera (12%).

O sytuacji niechcianych zdjęć i filmów dzieci zazwyczaj nikogo nie informują (54%). Jeżeli zdecydują się komuś opowiedzieć o takiej sytuacji, to są to najczęściej rówieśnicy (24%). Zdecydowanie rzadziej zawiadamiani są rodzice (6%).

Kompromitujące materiały

14% internautów w wieku 12-17 lat zgłasza przypadki publikowania w sieci kompromitujących ich materiałów: informacji (9%) oraz zdjęć lub filmów (5%). W znaczącej większości sytuacje takie ograniczają się do pojedynczego lub kilkukrotnego zdarzenia (po 39 wskazań). Sprawcami są najczęściej rówieśnicy (ze szkoły: 59%, spoza szkoły: 43%), znacznie rzadziej dorośli (10%) czy też znajomi z Internetu (13%). W 15% przypadków informacje, zdjęcia lub nagrania pochodziły od osób obcych lub nieujawniających swojej tożsamości. Pomimo stosunkowo nieznacznej skali problemu, zasługuje on na szczególną uwagę ze względu na wysoki stopień negatywnych emocji, które towarzyszą ofiarom – zdenerwowanie (66%), wstyd (33%) i strach (12%). Na tle innych form cyberprzemocy, przypadki publikacji kompromitujących materiałów są stosunkowo często zgłaszane osobom dorosłym (rodzice: 13%, pedagodzy: 12%). Jedynie 27% ofiar nikogo nie informuje o takich zdarzeniach.

Podszywanie się

Blisko jedna trzecia dzieci doświadczyła w sieci sytuacji, w której ktoś się pod nie podszywał. Przeważnie były to pojedyncze przypadki (19%), rzadziej z kilkukrotnymi (8%) lub wielokrotnymi (2%) powtórzeniami. Najczęściej podszywającą się osobą był rówieśnik (ze szkoły: 56%, spoza szkoły: 22%), zdecydowanie rzadziej dorosły (5%) lub znajomy z Internetu (6%). Za aż co piąty przypadek odpowiadały osoby nieznajome (20%). Podszywanie się jest zdecydowanie najbardziej irytującym działaniem spośród analizowanych. Aż 65% osób zareagowało w takich sytuacjach zdenerwowaniem, tylko co czwarty respondent deklarował, że nie wywarło to na nim żadnego wrażenia (24%). Przykrość sprawiło to 14% poszkodowanym, a strach wzbudziło u 5% osób.

Skuteczna Polityka bezpieczeństwa internetowego w szkole – porady dla kadry pedagogicznej

Cele polityki:

- Zapewnienie uczniom bezpieczeństwa on-line.
- Edukacja na rzecz bezpieczeństwa dzieci w Internecie, przekazanie wiedzy na temat:
- Specyfiki mediów elektronicznych
- Specyfiki zagrożeń związanych z korzystaniem z Internetu dzieci i młodzieży.
- Zasad bezpiecznego korzystania z Internetu
- Sposobów na zapewnienie dzieciom bezpieczeństwa on-line
- Sposobów przekazywania wiedzy dotyczącej bezpieczeństwa w Sieci
- Procedur reagowania w sytuacji zagrożenia oraz systemu reagowania na ujawnienie cyberprzemocy.

Sposoby osiągania celów:

- wprowadzenie działań profilaktycznych w szkole, uświadamiających uczniom nauczycielom, rodzicom, zasady korzystania i zagrożenia płynące z użytkowania różnych technologii komunikacyjnych.
- opracowanie konkretnych procedur reagowania w szkole na zjawisko cyberprzemocy.
- podejmowanie interwencji w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy.

1) PROCEDURA UJAWNIANIA CYBERPRZEMOCY

- a) **ustalenie okoliczności zdarzenia: rodzaj materiału, sposób jego rozpowszechniania, ustalenie sprawcy oraz świadków zdarzenia.**
- jeśli wiedzę o zajściu, posiada nauczyciel nie będący wychowawcą, należy przekazać informacje wychowawcy klasy, który jest zobowiązany poinformować o fakcie pedagoga szkolnego oraz dyrektora.
 - pedagog, wychowawca oraz dyrektor wspólnie dokonują analizy zdarzenia i planują dalsze postępowanie.

- do zadań szkoły należy także ustalenie okoliczności zdarzenia, sprawców, ofiar, oraz odnalezienie ewentualnych świadków.
- włączenie nauczyciela informatyki, szczególnie na etapie zabezpieczania dowodów i ustalania tożsamości sprawcy.

b) zabezpieczanie dowodów:

- wszelkie dowody cyberprzemocy należy odpowiednio zabezpieczyć i zarejestrować.

Zanotować datę i czas otrzymania materiału, treść wiadomości oraz jeśli to możliwe, dane nadawcy-adres użytkownika, adres e-mail, numer telefonu komórkowego, adres strony WWW, na której ukazały się szkodliwe treści itp.

- tak zabezpieczone dowody są materiałem, z którym powinny zapoznać się wszystkie zaangażowane osoby.

c) identyfikacja sprawcy

- świadomość, że znalezienie miejsca pochodzenia materiału nie zawsze jest równoznaczne z odnalezieniem osoby odpowiedzialnej za działania cyberprzemocy. Sprawcy zazwyczaj ukrywają swoją tożsamość: korzystają z internetowych bramek smsowych, podszywają się pod innych użytkowników sieci, wykorzystują telefony innych uczniów.
- w identyfikacji sprawcy pomagają rozmowy z innymi uczniami oraz świadkami zdarzenia bądź osobami trzecimi.
- **JĘŚLI USTALENIE SPRAWCY NIE JEST MOŻLIWE** należy skontaktować się z dostawcą usługi. Jest on ustawowo zobowiązany do usunięcia z Sieci kompromitujących, obraźliwych bądź krzywdzących materiałów oraz do zablokowania konta. Jednak dane sprawcy nie mogą być udostępnione osobom prywatnym, ani szkole. Aby je pozyskać konieczny jest kontakt z policją.
- w przypadku gdy numer telefonu sprawcy jest zastrzeżony, operator sieci komórkowej musi podjąć kroki umożliwiające ustalenie danych oraz udostępnienie ich policji. W tym celu należy przekazać informacje o dacie i godzinie rozmowy, bądź nagrania na pocztę głosowej.
- w przypadku, gdy zostało złamane prawo, a nie udało się ustalić tożsamości sprawcy, należy bezwzględnie skontaktować się z policją. Zgodnie z kodeksem polskiego prawa, które mówi o obowiązku zawiadamiania o przestępstwie (art.304§1 i 2 k.p.k - w przypadku cyberprzemocy przestępstwami ściganymi z urzędu są: włamania, groźby: karalna i bezprawna. Jeśli posiada się wiedzę o tych przestępstwach należy zawiadomić policję lub prokuraturę).

2) DZIAŁANIA WOBEC SPRAWCY CYBERPRZEMOCY:

a) jeśli sprawca cyberprzemocy jest nieznany (nie jest uczniem szkoły)

- należy podjąć wszelkie czynności w celu przerwania aktu cyberprzemocy. Zaczynając od zawiadomienia administratora serwisu(w celu usunięcia krzywdzących materiałów), kończąc na powiadomieniu policji lub prokuratury.

b) jeśli sprawca jest znany i jest on uczniem szkoły

- należy przeprowadzić rozmowę w celu ustalenia okoliczności oraz przyczyn zajścia oraz poszukania rozwiązania sytuacji konfliktowej.

- uczeń-sprawca powinien otrzymać jasny komunikat, że szkoła nie toleruje żadnych form przemocy.
- należy omówić skutki postępowania oraz konsekwencje, które zostaną wobec niego zastosowane.
- sprawca musi zostać zobligowany do zaprzestania jakichkolwiek form przemocy oraz dosunięcia Internetu krzywdzących materiałów.
- w rozmowie ze sprawcą należy zwrócić szczególną uwagę na omówienie sposobów zadośćuczynienia wobec ofiary.
- w przypadku gdy w zdarzeniu brała udział większa grupa uczniów, należy przeprowadzić rozmowę ze wszystkimi z osobna, zaczynając od lidera grupy.
- nie należy konfrontować sprawcy i ofiary cyberprzemocy.

d) powiadomienie rodziców sprawcy

- rodzice sprawcy powinni zostać poinformowani o zaistniałym zdarzeniu, jego przebiegu oraz powinni zapoznać się z materiałem dowodowym, oraz decyzją dotyczącą dalszego postępowania z dzieckiem, a także o środkach dyscyplinarnych podjętych wobec ich dziecka.
- w miarę możliwości szkoła powinna podjąć próbę współpracy z rodzicami i opracować wspólny plan działania, o którego zobowiązany jest uczeń.

e) objęcie sprawcy opieką psychologiczno-pedagogiczną

- praca ze sprawcą powinna opierać się na pomocy uczniowi w zrozumieniu wyrządzonej krzywdy oraz konsekwencji swojego zachowania. Ma ona za zadanie wpłynąć na zmianę postawy i postępowania ucznia, w tym zmienić cele oraz sposób użytkowania nowych technologii.
- w trudnych, uzasadnionych przypadkach można zaproponować rodzicom oraz uczniowi, poradę specjalisty z poza szkoły bądź udział w programie terapeutycznym.

f) zastosowanie środków dyscyplinarnych wobec ucznia-sprawcy

- trzeba pamiętać, że celem sankcji wobec sprawcy jest przede wszystkim zatrzymanie fali przemocy i zapewnienie poczucia bezpieczeństwa poszkodowanemu uczniowi.
- wzbudzenie refleksji na temat swojego zachowania, zrozumienie krzywdy, skrucha, zadośćuczynienie i powstrzymanie przed podobnym zachowaniem w przyszłości.
- pokazanie innym uczniom, że cyberprzemoc nie jest tolerowana i że szkoła efektywnie reaguje na jej przejawy.
- podejmując decyzję o rodzaju kary trzeba wziąć pod uwagę : rozmiar i rangę szkody, czas trwania prześladowania, determinacje oraz świadomość popełnianego czynu.

g) DZIAŁANIA WOBEC OFIARY CYBERRZEMOCY

- wsparcie psychiczne (ofiara cyberprzemocy musi otrzymać pomoc i wsparcie emocjonalne, musi także zostać zapewniona, iż szkoła podejmie odpowiednie kroki w celu rozwiązania problemu)
- porada (uczeń będący ofiarą cyberprzemocy powinien otrzymać poradę, jak ma się zachować, aby mógł czuć się bezpiecznie i co musi zrobić by nie doprowadzić do eskalacji prześladowania)
- monitoring - po zakończeniu interwencji warto monitorować sytuację ucznia, by dociec czy przypadkiem sytuacja po ukaraniu sprawców się nie zaogniła. W tym miejscu konieczna jest również współpraca z rodzicami, którzy powinni zostać przygotowani przez pedagoga szkolnego, jak zapewnić bezpieczeństwo i komfort psychiczny poszkodowanemu.

- W szczególnie agresywnych przypadkach cyberprzemocy, powinno się zaproponować rodzicom i dziecku pomoc specjalisty.
- w sytuacji gdy przypadek cyberprzemocy wymaga założenia sprawy sądowej, szkoła powinna powiadomić o takiej ewentualności rodziców ofiary oraz ucznia. Jednocześnie pomóc jej w przygotowaniu odpowiednich dokumentów sądowych uzasadniających i przedstawiających dowody winy oskarżonego.

3) OCHRONA ŚWIADKÓW CYBERPRZEMOCY

- ważne by w wyniku interwencji świadkowie nie zostali narażeni na działania odwetowe ze strony sprawcy.
- postępowanie interwencyjne wymaga od pedagogów wyjaśnianych sprawę, dyskrecji i poufnego postępowania.
- niedopuszczalne jest konfrontowanie świadka ze sprawcą ani upublicznianie jego udziału w sprawie. Jest to nieprofesjonalna metoda wyjaśniania sprawy, może ona sprawić, że świadek stanie się kolejną ofiarą, może również sprawić, iż następnym razem uczeń nie zgłosi informacji o zagrażającym zdarzeniu.

j) sporządzanie dokumentacji z zajścia:

- pedagog szkolny zobowiązany jest do sporządzenia notatki służbowej z rozmów ze sprawcą poszkodowanym i jego opiekunami, a także ze świadkami zdarzenia.
- Dokument powinien zawierać datę i miejsce rozmowy, dane personalne osób biorących w niej udział i opis ustalonego przebiegu wydarzeń.
- jeśli rozmowa przebiegała w obecności wychowawcy (będącego w tym przypadku świadkiem) powinien on również podpisać sporządzoną notatkę.
- jeżeli zostały odnalezione i zabezpieczone dowody cyberprzemocy (wydruki, opisy smsów itp.), należy je również włączyć do dokumentacji pedagogicznej.

k) powiadomienie sądu rodzinnego

- jeżeli zaistniałego przypadku cyberprzemocy nie można rozwiązać przy użyciu środków wychowawczych jakimi dysponuje szkoła, sprawę należy przekierować, zgłaszając ją do sądu rodzinnego z zawiadomieniem o postępowaniu w sprawach nieletnich.
- jeśli rodzice sprawcy cyberprzemocy odmawiają współpracy lub nie stawiają się w szkole, a uczeń nie zaniechał dotychczasowego postępowania, dyrektor szkoły powinien pisemnie powiadomić o zaistniałej sytuacji sąd rodzinny, zwłaszcza jeśli do szkoły napływają informacje o innych przejawach demoralizacji dziecka.
- w przypadkach szczególnie drastycznych aktów agresji z naruszeniem prawa, dyrektor szkoły zobowiązany jest zgłosić te fakty policji i do sądu rodzinnego.

POLITYKA BEZPIECZEŃSTWA INTERNETOWEGO

Są to działania profilaktyczne mające na celu zapewnienie bezpieczeństwa dzieciom korzystającym z nowych technologii oraz zapobieganiu cyberprzemocy wśród uczniów:

- organizowanie szkoleń, wykładów i warsztatów oraz aktywizowanie uczniów do wymiany wiedzy. Podanie pomysłów na tworzenie filmów amatorskich, układanie scenariuszy w obrębie tematu bezpiecznego użytkowania Internetu, jego dobrodziejstw i zagrożeń.
- traktowanie „bezpieczeństwa dzieci w Internecie” również w kontekście propagowania otwartości na odmienność, tolerancji, kształtowania zachowań prospołecznych, wrażliwości na krzywdę i eliminowania obojętności oraz bierności.
- prowadzenie zajęć i warsztatów z zakresu komunikacji interpersonalnej, asertywności, umiejętności radzenia sobie ze stresem, zastępowania agresji.
- przeprowadzanie konkursów związanych z tematem bezpieczeństwa w cyberprzestrzeni.
- poinformowanie uczniów, że mogą się zwracać do nauczycieli z informacją o wszelkich przejawach przemocy również tej z użyciem nowych technologii.
- dopuszczanie anonimowych form zgłaszania informacji dotyczących aktów przemocy na terenie szkoły.
- konsekwentne reagowanie na zgłaszane problemy oraz zaistniałe incydenty.

a) pedagogizacja rodziców

- aktywne włączanie rodziców we wszystkie działania podejmowane przez szkołę
- poinformowanie rodziców o procedurach postępowania wobec dzieci zachowujących się agresywnie oraz stosujących przemoc z udziałem nowych technologii
- organizacja szkoleń, spotkań informacyjnych dotyczących tematu bezpieczeństwa internetowego.
- tworzenie możliwości wyrażania swojego zdania i własnych propozycji w tym zakresie.

b) działania skierowane do Rady Pedagogicznej

- zapoznanie Rady Pedagogicznej z założeniami programu polityki bezpieczeństwa internetowego przydział zadań, ustalenie odpowiedzialnych za ich wykonanie.
- przeszkolenie Rady Pedagogicznej
- zachęcanie do poruszania tematyki bezpieczeństwa dzieci w sieci, oraz włączania tej problematyki do programów zajęć
- zachęcanie do korzystania z propozycji edukacyjnej opracowanej zewnętrznie i udostępnionych w formie elektronicznej lub drukowanej
- niezwłoczna i zdecydowana interwencja na wszystkie przejawy przemocy w tym te z udziałem nowych technologii
- kontynuowanie tzw. drzwi otwartych mających na celu indywidualny kontakt nauczyciela z rodzicem
- zredagowanie ankiet diagnozujących wymienione w programie problemy.
- zwołanie Rady Pedagogicznej poświeconej polityce bezpieczeństwa internetowego.

Co to jest PEGI

Ogólnoeuropejski system klasyfikacji gier (Pan-European Game Information, PEGI) to system ratingu wiekowego stworzony w celu udzielenia rodzicom w Europie pomocy w podejmowaniu świadomych decyzji o zakupie gier komputerowych. Został on uruchomiony wiosną 2003 r. Ten jeden, nowy system zastąpił liczne krajowe systemy ratingu wiekowego i jest teraz stosowany w znacznej części Europy, a mianowicie w 30 krajach (Austria, Dania, Węgry, Łotwa, Norwegia, Słowenia, Belgia, Estonia, Islandia, Litwa, Polska, Hiszpania, Bułgaria, Finlandia, Irlandia, Luksemburg, Portugalia, Szwecja, Cypr, Francja, Izrael, Malta, Rumunia, Szwajcaria, Czechy, Grecja, Włochy, Holandia, Słowacja i Wielka Brytania).

System wspierają najwięksi producenci konsol, w tym Sony, Microsoft i Nintendo, a także wydawcy i twórcy gier interaktywnych w całej Europie. System ratingu wiekowego opracowała Europejska Federacja Oprogramowania Interaktywnego (Interactive Software Federation of Europe, ISFE).

Co oznaczają poszczególne znaki?

Znaki ratingu PEGI znajdują się z przodu i z tyłu opakowania. Wskazują one następujące kategorie wiekowe: 3, 7, 12, 16 i 18. Dostarczają wiarygodnych informacji o stosowności treści gry z punktu widzenia ochrony nieletnich. Rating wiekowy nie uwzględnia poziomu trudności ani umiejętności niezbędnych do danej gry.



PEGI 3

Treść gier oznaczonych w ten sposób uznaje się za odpowiednią dla wszystkich grup wiekowych. Dopuszczalna jest pewna ilość przemocy w komicznym kontekście (zwykle podobna do prezentowanej w kreskówkach w rodzaju Królika Bugsa czy Toma i Jerry'ego). Dziecko nie powinno utożsamiać postaci pojawiających się na ekranie z postaciami rzeczywistymi. Powinny one być w całości wytworem fantazji. Gra nie powinna zawierać dźwięków ani obrazów, które mogą przestraszyć dziecko. Nie powinny w niej występować wulgaryzmy.



PEGI 7

Gry, które w innym przypadku zostałyby zakwalifikowane do grupy 3, lecz zawierają dźwięki lub sceny potencjalnie przerażające najmłodszych odbiorców, mogą być uznane za odpowiednie dla tej grupy wiekowej.



PEGI 12

Gry wideo pokazujące przemoc o nieco bardziej realistycznym charakterze, skierowaną przeciw postaciom fantastycznym i/lub nierealistyczną przemoc wobec postaci o ludzkim lub rozpoznawalnych zwierząt, ponadto w tej kategorii wiekowej dopuszczalna jest nieco bardziej dosłowna nagość. Ewentualne wulgaryzmy muszą mieć łagodny charakter i nie mogą zawierać odwołań do seksu.



PEGI 16

Ten symbol jest nadawany, jeżeli przemoc lub aktywność seksualna wyglądają tak jak w rzeczywistości. Młodzież w tym wieku powinna również być odporna na brutalniejsze wulgaryzmy, sceny pokazujące używanie tytoniu lub narkotyków oraz sceny popełniania przestępstw.



PEGI 18

Za gry dla dorosłych uznaje się gry przedstawiające daleko posuniętą przemoc i/lub specyficzne rodzaje przemocy. Daleko posunięta przemoc jest najtrudniejsza do zdefiniowania, ponieważ w wielu przypadkach jest to pojęcie bardzo subiektywne, ale ogólnie można ją określić jako sceny przemocy powodujące u widza uczucie odrazy.

Opisy zamieszczone z tyłu opakowania podają najważniejsze przyczyny przeznaczenia gry dla danej grupy wiekowej. Jest osiem takich opisów: przemoc, wulgaryzmy, lęk, narkotyki, seks, dyskryminacja, hazard i gra w Internecie z innymi ludźmi.

**Wulgarny język**

W grze jest używany wulgarny język.

**Dyskryminacja**

Gra pokazuje przypadki dyskryminacji lub zawiera materiały, które mogą do niej zachęcać.

**Narkotyki**

W grze pojawiają się nawiązania do narkotyków lub jest pokazane zażywanie narkotyków.

**Strach**

Gra może przestraszyć młodsze dzieci.

**Hazard**

Gry, które zachęcają do uprawiania hazardu lub go uczą.

**Seks**

W grze pojawiają się nagość i/lub zachowania seksualne lub nawiązania do zachowań o charakterze seksualnym.

**Przemoc**

Gra zawiera elementy przemocy.

**Online**

gra może grać online

Wiele portali i serwisów internetowych zawiera gry o niewielkich rozmiarach. W celu obsłużenia tego szybko rozwijającego się segmentu stworzono oznaczenie „PEGI OK”. W grę internetową niewielkich rozmiarów dostępną w portalu i oznaczoną symbolem „PEGI OK” mogą grać osoby w każdym wieku, ponieważ nie zawiera ona potencjalnie nieodpowiednich treści.

Oznaczenie „PEGI OK”:

Operator witryny internetowej lub portalu oferującego gry ma prawo do korzystania z oznaczenia „PEGI OK” na podstawie złożonego PEGI oświadczenia, że gra nie zawiera materiałów wymagających formalnego ratingu.

Gry kwalifikujące się do oznaczenia „PEGI OK” NIE MOGĄ zawierać żadnego z poniższych elementów:

- przemoc
- czynności seksualne lub aluzje o charakterze seksualnym
- nagość
- wulgaryzmy
- hazard

- popularyzacja lub zażywanie narkotyków
- popularyzacja alkoholu lub tytoniu
- przerażające sceny

Gry zawierające którykolwiek z tych elementów wymagają ratingu przy użyciu standardowego systemu PEGI. Otrzymują one zwykły rating PEGI (3, 7, 12, 16 lub 18) złożony z oznaczenia ratingu wiekowego i deskryptora lub deskryptorów treści. Dotyczy to również przypadków, gdy możliwe jest pobranie przypadkowej gry na komputer konsumenta lub pobierana jest opłata za możliwość udziału w grze.

PEGI zapewnia doradztwo dotyczące stosowności gier dla poszczególnych grup wiekowych. Jednak każde dziecko jest inne. To rodzice powinni podjąć ostateczną decyzję co do tego, jakie obrazy i doświadczenia są odpowiednie dla ich dzieci. Poniżej podajemy kilka wskazówek.

- Zawsze sprawdzaj klasyfikację wiekową podaną na opakowaniu gry lub poszukaj jej, korzystając z wyszukiwarki udostępnionej w naszym portalu.
- Z góry ustal, w co, jak długo i kiedy dziecko może grać. W razie sprzeciwu dziecka wyjaśnij przyczyny swojej decyzji.
- Poszukaj streszczenia lub opisu treści gry, a najlepiej sam w nią najpierw zagraj.
- Graj ze swoimi dziećmi, nadzoruj je podczas gry i rozmawiaj o tym. Wyjaśnij im, dlaczego niektóre gry nie są dla nich odpowiednie.
- Zachęcaj dzieci do rozmowy o grach.
- Pamiętaj, że niektóre gry internetowe umożliwiają pobranie dodatkowego oprogramowania, które może zmienić treść gry i jej klasyfikację wiekową.

W gry internetowe zazwyczaj gra się w wirtualnych grupach, w których konieczne jest kontaktowanie się z nieznanymi osobami. Powiedz dzieciom, aby nie podawały swoich danych i mówiły Ci o niewłaściwych zachowaniach.

Źródło: www.pegi.info

Gdzie szukać pomocy – Poradnik teleadresowy

Numer 112 jest numerem alarmowym pod który możesz zadzwonić, gdy znajdziesz się w niebezpieczeństwie i będziesz potrzebować pomocy ze strony **Policji, straży pożarnej lub pogotowia**. Jest to numer uniwersalny co oznacza, że możesz pod niego zadzwonić zawsze gdy czujesz się zagrożony/a z jakiegokolwiek powodu.

116 000 - to numer telefonu, z którego mogą skorzystać m.in. młode osoby, które myślą o ucieczce z domu, ale także wszystkie osoby, które wiedzą coś o losach zaginionych. Linia obsługiwana jest przez całą dobę, a połączenie jest całkowicie bezpłatne.

Helpline; www.helpline.org.pl; 800 100 100. Helpline to miejsce, którego celem jest pomoc młodym Internautom w sytuacjach **zagrożenia w Internecie** oraz podczas korzystania z telefonów komórkowych. Znajdziesz tu porady na temat zapobiegania niebezpiecznym sytuacjom, a także informacje o sposobach postępowania w przypadku wystąpienia zagrożenia. Z numerem 800 100 100 można połączyć się **bezpłatnie** z każdego telefonu stacjonarnego oraz z telefonów komórkowych (poza siecią Play) i działa od **poniedziałku do piątku w godzinach 11:00-17:00**.

Dziecięcy Telefon Zaufania Rzecznika Praw Dziecka 800 12 12 12 jest telefonem skierowanym do wszystkich dzieci **potrzebujących pomocy**. Dzwoniąc pod ten numer połączysz się ze specjalistą, który postara Ci się pomóc. Z numerem 800 12 12 12 można połączyć się **bezpłatnie** z każdego stacjonarnego numeru oraz telefonów komórkowych Orange. Telefon działa w godzinach **8:15-20:00**.

Niebieska Linia 801 12 00 02. Tu możesz zadzwonić jeśli jesteś ofiarą **przemocy w rodzinie** lub znasz kogoś kto doświadcza takiej przemocy w domu. Połączenie z numerem Niebieskiej Linii jest **płatne za pierwszy impuls** według stawki operatora. Telefon czynny jest od **poniedziałku do soboty w godzinach 8:00-22:00** oraz w **niedziele i święta w godzinach 8:00-16:00**.

801 800 967 Infolinia dla Wychowawcy - pod tym numerem dyżurują specjaliści, którzy udzielają porad dotyczących problemów, z jakimi mają do czynienia nauczyciele i wychowawcy w szkole czy placówce oświatowej. Linia działa **w poniedziałki i czwartki w godz. 17:00-19:00**, całkowity koszt połączenia wynosi 35 gr.

Adres IP – liczba nadawana interfejsowi sieciowemu, grupie interfejsów (broadcast, multicast), bądź całej sieci komputerowej opartej na protokole IP, służąca identyfikacji elementów warstwy trzeciej modelu OSI – w obrębie sieci oraz poza nią (tzw. *adres publiczny*).

Adres IP nie jest "numerem rejestracyjnym" komputera – nie identyfikuje jednoznacznie fizycznego urządzenia – może się dowolnie często zmieniać (np. przy każdym wejściu do sieci Internet) jak również kilka urządzeń może dzielić jeden publiczny adres IP. Ustalenie prawdziwego adresu IP użytkownika, do którego następowała transmisja w danym czasie jest możliwe dla systemu/sieci odpornej na przypadki tzw. IP spoofingu (por. man in the middle, zapora sieciowa, ettercap) – na podstawie historycznych zapisów systemowych

Dzień Bezpiecznego Internetu, DBI – (ang. *Safer Internet Day*) obchodzony jest w całej Europie w pierwszej połowie lutego. Jest inicjatywą Komisji Europejskiej, mająca na celu zwrócenie uwagi na kwestię bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych^[1].

6 lutego 2007 roku w 40. krajach na świecie - i po raz trzeci w Polsce – obchodzony był Dzień Bezpiecznego Internetu. Został ustanowiony z inicjatywy Komisji Europejskiej w ramach programu "Safer Internet"^[2]. Chodzi głównie o to, by dzieci i młodzież nie były narażone na niebezpieczeństwa w trakcie korzystania z zasobów internetowych.

W Polsce Dzień Bezpiecznego Internetu organizowany jest przez Fundację Dzieci Niczyje oraz NASK, odpowiedzialne za realizację programu "Safer Internet" w Polsce.

Internet (skrótowiec od ang. *inter-network*, dosłownie "między-sieć") – ogólnosiwiatowa sieć komputerowa, określana również jako sieć sieci^[1]. W sensie logicznym, Internet to przestrzeń adresowazrealizowana przy wykorzystaniu protokołu komunikacyjnego IP, działająca w oparciu o specjalistyczny sprzęt sieciowy oraz istniejącą już infrastrukturę telekomunikacyjną. (źródło: <http://pl.wikipedia.org/wiki/Internet>)

World Wide Web [ˌwɜːldˌwaɪdˈweb] (po angielsku: "ogólnosiwiatowa sieć"), w skrócie **Web** lub częściej **WWW** – hipertekstowy, multimedialny, internetowy system informacyjny oparty na publicznie dostępnych, otwartych standardach IETF i W3C. WWW jest usługą internetową, która ze względu na zdobytą popularność, bywa błędnie utożsamiana z całym Internetem.

Wyszukiwarka internetowa (ang. *search engine*) to program lub strona internetowa, której zadaniem jest ułatwienie użytkownikom znalezienie informacji w sieci.

Określenie *wyszukiwarka* stosujemy do:

- Stron internetowych serwisów wyszukiwujących - czyli implementacji oprogramowania wyszukiwającego działającego z interfejsem WWW ogólnodostępnym dla internautów
- Oprogramowania przeznaczonego do indeksowania i wyszukiwania informacji w sieciach komputerowych: internecie, intranecie.

Gromadzą w sposób automatyczny informacje o dokumentach tekstowych oraz plikach zgromadzonych w sieci (obszarze wyznaczonym dla wyszukiwarki do indeksowania).

Wyszukiwarki stanowią wymarzony cel reklamodawców, ponieważ mają oni praktycznie pełną gwarancję, że osoba wyszukująca dane hasło jest nim zainteresowana. Tak więc większość wyszukiwarek oferuje reklamy zależne od treści zapytań (np. AdWords oferowany przez Google). Nie zawsze są one właściwie oddzielone od wyników poszukiwań, co stało się źródłem protestów grup ochrony praw konsumentów oraz kilku do dziś nierozstrzygniętych spraw sądowych.

Ze względu na szeroką krytykę procedury nieoddzielania reklam od wyników, większość wyszukiwarek z niego zrezygnowała i wyraźnie zaznacza teraz reklamy.

Serwis społecznościowy — serwis internetowy, który istnieje w oparciu o zgromadzoną wokół niego społeczność.

Kontrola rodzicielska to opcje, stosowane głównie w usługach telewizji kablowej i satelitarnej, telefonach komórkowych, użytkowaniu komputera, w tym w grach video i korzystaniu z Internetu, pomocne rodzicom w procesie wychowawczym dziecka. Stanowią pomoc w ochronie nieletnich przed brutalnością, zachowaniami seksualnymi, wulgarnością pojawiającą się w grach komputerowych, telewizji oraz Internecie.

Założone cele realizują poprzez:

- pomoc rodzicom w świadomym wyborze gier komputerowych, stosując oznaczenia na opakowaniach gier - system PEGI (przyjęty w Polsce),
- ochrona przed dostępem do treści szkodliwych i niebezpiecznych w Internecie (komputerach i telefonach) - filtry rodzinne,
- blokowanie dostępu do pornograficznych i erotycznych kanałów TV.

Filtr rodzinny, strażnik dostępu, kontroler treści, filtr treści – program lub usługa, chroniąca przed dostępem do materiałów pornograficznych i przemocy w Internecie. Usługę oferują niektórzy dostawcy Internetu, wliczając ją w abonament miesięczny. Istnieje również możliwość samodzielnego nabycia i zainstalowania programu. Filtr rodzinny nie gwarantuje bezpieczeństwa dzieci.

Netykieta (kontaminacja *net* (ang.) – "sieć" i *etiquette* (fr.) – "formy zachowania się") – zbiór zasad przyzwoitego zachowania w Internecie, swoista *etykieta* obowiązująca w sieci (ang. *net*).

Netykieta, podobnie jak zwykłe zasady przyzwoitego zachowania, nie jest dokładnie skodyfikowana, nikt też nie zajmuje się systematycznym karaniem osób łamiących te zasady, jednak uparte łamanie zasad netykiety może się wiązać z różnymi przykrymi konsekwencjami, jak np.: zgłoszenie nadużycia do działu abuse i odcięcie "niegrzecznego" osobnika od określonej usługi internetowej przez jej administratora.

Zasady netykiety wynikają wprost z ogólnych zasad przyzwoitości lub są odzwierciedleniem niemożliwych do ujęcia w standardy ograniczeń technicznych wynikających z natury danej usługi Internetu.

Zalecane etykiety:

Dla grup i list dyskusyjnych są to:

- zakaz pisania wulgaryzmów
- zakaz spamowania (m.in. wysyłania niechcianych linków do stron)
- zakaz wysyłania tzw. "łańcuszków szczęścia"
- nakaz zapoznania się z wykazem FAQ przed zadaniem pytania
- stosowanie się do reguł pisania obowiązujących w danej grupie (sposób kodowania polskich liter, zasad cytowania, możliwości wysyłania (lub nie) wiadomości formatowanych w HTML-u, możliwości dołączania (lub nie) plików binarnych, co zwykle jest szczegółowo opisane w FAQ danej grupy)
- zakaz nadmiernego cross-postowania czyli wysyłania e-maili lub postów do kilku grup naraz
- zakaz wysyłania listów (e-maili) do wielu osób naraz z jawnymi adresami poczty elektronicznej (stosujemy kopię ukrytą)
- zakaz pisania nie na temat (OT – OffTopic)

- zakaz pisania kilka razy z rzędu (szczególnie restrykcyjnie używany na forach posiadających funkcję edycji postu)
- zakaz odpowiadania nad cytowanym fragmentem (topposting)
- zakaz pisania wiadomości wielkimi literami
- Dla usług interaktywnych (IRC, komunikatory, czaty, fora dyskusyjne na stronach WWW):
- zakaz floodowania
- nakaz zapoznania się z FAQ danego kanału/forum/czatu i przestrzeganie zawartych tam zasad szczegółowych
- zakaz nagabywania osób, które sobie tego nie życzą
- zasady dotyczące znaków diakrytycznych – użytkownicy niektórych kanałów IRC nie życzą sobie używania polskich liter, natomiast na forach internetowych pisanie bez polskich znaków diakrytycznych bywa źle widziane; sprawy te regulowane są czasem przez lokalną netykietę lub FAQ, jak np. dla www.pl.irc^[1])
- zasady korzystania z różnych języków na kanałach wielonarodowościowych
- zakaz ciągłego pisania wielkimi literami
- zakaz pisania naprzemiennie wielkich i małych liter (tzw. nowomowa internetowa, poke-pismo)
- nakaz używania emotikon z rozważą (mają być dodatkiem do tekstu, a nie główną treścią)
- w dyskusjach, zwłaszcza w Usenecie i na forach internetowych zwracamy się po nicku lub imieniu jeśli rozmówca wyraża na to zgodę. Nigdy samym nazwiskiem. Nie należy się obrażać, jeśli ktoś zwraca się do nas "per ty", a nie w formie grzecznościowej, i nie należy się obawiać używania takiej bezpośredniej formy.

ADSL – Asymetric Digital Subscriber Line – Asymetryczne, szerokopasmowe łącze internetowe. Przesyłanie danych do użytkownika (z Internetu) jest szybsze od odwrotnego transferu. Technologia ta stworzona została z myślą o użytkownikach częściej odbierających dane (np. ze stron internetowych, programów p2p) niż wysyłających dane. Przykładem łącza ADSL może być np. neostrada.

Aplikacja – inaczej program komputerowy lub użyteczny element oprogramowania.

Aukcja internetowa - rodzaj aukcji przeprowadzanej za pośrednictwem Internetu. W ramach internetowego serwisu aukcyjnego internauci składają kolejne oferty kupna. Aukcję wygrywa ta osoba, która zaproponuje najwyższą cenę. Z punktu widzenia prawnego aukcje internetowe mają taką samą wagę jak te tradycyjne.

Admin – popularne w środowisku internetowym określenie administratora – osoby odpowiedzialnej za przestrzeganie zasad panujących w danym serwisie/portalu/stronie internetowej. Adminowi przysługuje prawo banowania użytkowników (od angl. ban – zakazywać), czyli uniemożliwienia ponownego wejścia na dany serwis/portał/stronę internetową bądź wypowiadania się w określonym temacie na forum internetowym. Pomocą administratorowi mogą służyć ustanowieni przez niego moderatorzy, którzy obserwują, co robią inni użytkownicy.

Atak DOS/DDOS – Denial Of Service/Distributed Denial Of Service – Przeciążenie systemu ofiary. W wersji DDOS polega na tym, iż na sygnał, z dużej ilości komputerów, w tym samym czasie, wysyłana jest prośba do systemu ofiary o skorzystanie z usług, jakie oferuje. Dla każdej takiej prośby atakowany komputer musi przydzielić pewne zasoby (pamięć, zasoby procesora, pasmo sieciowe), co przy bardzo dużej ilości żądań, z którymi ofiarą nie może sobie poradzić, prowadzi do przerwy w działaniu lub nawet zawieszenia systemu.

Awatar – obrazek umieszczany przez użytkowników forów internetowych, portali społecznościowych, itp. w swoim profilu, w pobliżu internetowego pseudonimu. Pojawia się wszędzie tam gdzie dany użytkownik się wypowiada. Jest ilustracją, dodatkową informacją na temat użytkownika, jest jego „wirtualną twarzą”. Awatarem może być zdjęcie internauty, logo lub jakakolwiek grafika.

Blog – rodzaj pamiętnika, bądź dziennika prowadzonego w Internecie, w formie strony internetowej. Na blogu oprócz tekstu mogą znajdować się również zdjęcia i klipy filmowe.

Botnet – sieć komputerów zainfekowanych przez wirusa (komputerów zombie), pozostająca pod kontrolą innych osób, może służyć do popełniania przestępstw.

Cyberstalking – anonimowe dręczenie innych osób za pomocą Internetu.

Cyberbullying – prześladowanie, poniżanie i nękanie za pomocą Internetu.

Czat – serwis internetowy służący do komunikacji pomiędzy wieloma użytkownikami Internetu. Na czacie prowadzi się rozmowę w czasie rzeczywistym, poprzez wpisywanie kolejno wiadomości tekstowych, które następnie wyświetlają się na monitorach rozmówców. Zwykle istnieją dwa rodzaje rozmowy – prywatna, której przebieg mogą śledzić tylko dwie osoby, oraz publiczna, dostępna dla wszystkich zalogowanych użytkowników (źródło Wikipedia – pl.wikipedia.org). Internauci przeważnie występują pod pseudonimami, które niekiedy mogą stanowić pewne źródło informacji niestety bardzo mało wiarygodne (np. pseudonim Jacek34 - prawdopodobnie oznacza, iż użytkownik ma na imię Jacek i ma 34 lata). W części czatów dostępne są również graficzne emotikony, stworzone dla ułatwienia ekspresji emocji

DSL – Digital Subscriber Line – inaczej szerokopasmowe łącze internetowe

E-mail – poczta elektroniczna – usługa polegająca na przesyłaniu wiadomości tekstowych (listów) z jednego komputera do drugiego za pomocą Internetu.

Emotikony – graficzne znakiobrazujące emocje (np. uśmiech, zdenerwowanie, szczęście, łzy itp.) wykorzystywane przez internautów podczas rozmów. Używanie emotikonów podczas internetowych rozmów stało się do tego stopnia popularne, że pewne sekwencje znaków powodujące wyświetlenie się emotikonu używane są przez młodzież również podczas pisania sms-ów oraz tradycyjnych listów. Przykłady takich sekwencji to: ;) – uśmiech z przymrużeniem oka, :) – normalny uśmiech, :(- smutek, ;(- płacz, :D – uśmiech „pełną gębą”, :P – wystawia język, :/ - krzywi się, :| - zmartwiony, :] – krzywy uśmiech, :O – zdziwiony, :> – spogląda z niedowierzaniem.

ESRB – jeden z systemów klasyfikacji gier

FAQ – Frequently Asked Questions – z angl. „najczęściej zadawane pytania”, najważniejsze informacje dotyczące korzystania z określonego programu/serwisu itp., rodzaj „instrukcji obsługi”.

Firewall – patrz. zaporą ogniową

Forum dyskusyjne – zorganizowane w ramach strony lub portalu internetowego miejsce wymiany poglądów przez użytkowników. Na niektórych forach możliwe jest dołączanie do tekstu emotikonów, zdjęć, a nawet filmów.

Grooming – zjawisko uwodzenia dzieci za pomocą Internetu w celu wykorzystania seksualnego, przez osoby, które mogą mieć skłonności pedofilskie.

Hacker – osoba szukająca i wykorzystująca luki w zabezpieczeniach systemu komputerowego.

IMHO – In My Humble Opinion – zwrot używany podczas rozmów internetowych oznacza: „moim zdaniem”.

IP – Internet Protocol Address – unikatowy numer przyporządkowany urządzeniom podłączonym do sieci Internetowej. Adres IP jest przyznawany każdemu użytkownikowi przez jego dostawcę Internetu (ISP)

ISP – Internet Service Provider – dostawca usługi internetowej np. Telekomunikacja Polska, Tele2, Netia.

Komunikator internetowy – oprogramowanie służące do kontaktu między użytkownikami Internetu

Login – od angielskich słów log in (zalogować), ciąg znaków identyfikujący użytkownika, podawany przez niego w procesie rejestracji konta np. na portalu społecznościowym, w serwisie mailowym, czy też w systemie operacyjnym. Bez znajomości loginu i hasła nie uzyskamy dostępu do konta użytkownika.

LOL – Lot Of Laugh – zwrot używany podczas rozmów przez społeczność internetową, oznacza: „dużo śmiechu”.

P2P – Peer-2-Peer – model komunikacji umożliwiający jednoczesny, wzajemny odbiór i przesył danych z dwóch lub większej ilości komputerów. Technologia P2P wykorzystywana jest przez różnego rodzaju programy służące do wymiany danych (obrazów, muzyki, filmów) między użytkownikami Internetu. Najpopularniejsze z nich to: eMule/eDonkey, Soulseek, Bitorrent, WinMX, Kazaa, eMesh, Bearshare i inne. Korzystanie z sieci P2P umożliwia pobieranie danych i to praktycznie za darmo ale niejako „w zamian” wymusza udostępnianie zgromadzonych na komputerze zasobów. P2P działa na zasadzie „bierzesz to dawaj”. Z punktu widzenia prawnego możemy mieć do czynienia z naruszaniem praw autorskich, jeśli użytkownik pobiera bądź udostępnia dane chronione prawem.

PEGI – Pan European Game Information – jeden z systemów klasyfikacji gier, najpopularniejszy w Europie.

Portal internetowy - rodzaj serwisu informacyjnego, dla którego nośnikiem jest Internet. Cechą charakterystyczną portalu jest zgromadzenie w jednym miejscu dostępu do różnorodnych usług, co ma zachęcać użytkownika do ustawienia adresu portalu jako strony startowej w przeglądarce www i traktowania go jako bramy do Internetu. Zazwyczaj portal zawiera informacje będące przedmiotem zainteresowania szerokiego grona odbiorców takie jak: aktualne wiadomości, prognoza pogody, katalog stron WWW, chat, forum dyskusyjne wyszukiwarka internetowa. W celu przyciągnięcia większej ilości użytkowników portale mogą oferować darmowe konta poczty elektronicznej, miejsce na strony WWW i dostęp do innych usług (np. multimedia, pobieranie plików, grupy dyskusyjne). Dla zarejestrowanych użytkowników mogą być dostępne dodatkowe usługi lub usługi o wyższej jakości niż dla użytkowników nierejestrowanych (źródło: Wikipedia – pl.wikipedia.org). Najpopularniejsze polskie portale internetowe to: Onet, Interia, Wirtualna Polska, o2.

Portale społecznościowe – portale internetowe nastawione na interakcję między użytkownikami Internetu. W przeciwieństwie do tradycyjnego portalu przepływ informacji odbywa się nie według modelu twórca portalu → użytkownik ale przede wszystkim użytkownik → użytkownik. Sam portal pełni rolę klamry spajającej społeczność, która powstała w jego ramach. Ważną cechą portalu społecznościowego jest to, że użytkownicy są jednocześnie jego współtwórcami. Kreują i decydują o tym, co się na nim dzieje. W przeciwieństwie do stron WWW i tradycyjnych portali, które są „odgórnie” stworzone przez właściciela i mogą być w zasadzie jedynie przeglądane, portale społecznościowe istnieją przede wszystkim dzięki aktywności swoich użytkowników. Najpopularniejsze portale społecznościowe to: grono.net, epuls.pl, znajomi.interia.pl, fotka.pl, myspace.com, youtube.com. Na temat bezpieczeństwa portali społecznościowych powstał w Biurze Rzecznika Praw Dziecka raport „Internetowe portale społecznościowe a bezpieczeństwo dzieci” dostępny pod adresem: www.brpd.gov.pl/uploadfiles/publikacje/Raport.doc.

Profil użytkownika – jest istotną częścią każdego portalu/serwisu społecznościowego, pokazuje kim jest użytkownik. Często zawiera, opis jego zainteresowań, poglądów, itp. Niekiedy w profilu użytkownika znajdziemy informacje na temat internetowych przyjaciół użytkownika, a nawet będziemy mogli odsłuchać jego ulubione piosenki, lub obejrzeć klip filmowy(umożliwiają to portale np.: www.youtube.com, www.myspace.com lub polski www.wrzuta.pl). Jeśli użytkownikiem jest dziecko, to ww. informacje mogą być wykorzystane przez osoby o skłonnościach pedofilskich, w procesie uwodzenia dziecka. Dlatego też, część portali społecznościowych umożliwia zamaskowanie części danych znajdujących się w profilu i udostępnienie ich wyłącznie osobom, które użytkownik oznaczy jako zaufane.

Screen – inaczej obraz ekranu komputera.

Spam – niechciane wiadomości rozsyłane najczęściej drogą e-mailową lub za pomocą komunikatorów internetowych. Mają przeważnie charakter komercyjny – reklamowy. Dużą grupę spamu stanowią również tzw. „łańcuszki szczęścia” oraz wiadomości pozornie niewinne, zawierające w załączniku złośliwe oprogramowanie.

Surfowanie – popularne określenie oznaczające przeglądanie stron internetowych, poszukiwanie informacji w Internecie itp.

System operacyjny – OS - program komputerowy bądź zbiór programów, który zarządza sprzętem oraz aplikacjami komputera (źródło Wikipedia - pl.wikipedia.org), jest bazą, podstawą do działania innych programów komputerowych. Najpopularniejszymi programami operacyjnymi są Windows, Linux, MacOS.

Wortal – portal wertykalny – portal internetowy specjalizujący się w określonej dziedzinie np. edukacja, medycyna, gry komputerowe. W odróżnieniu od portalu internetowego, który stara się połączyć informacje z różnych dziedzin i jest „wszystkim w jednym” wortal skupia się na konkretnym zagadnieniu.

Zapora ogniowa – oprogramowanie służące do ochrony systemu komputerowego przed zagrożeniem z zewnątrz np. z Internetu. Do jego podstawowych zadań należy filtrowanie połączeń wchodzących i wychodzących oraz odmawianie żądań dostępu pochodzących ze źródeł uznanych za niebezpieczne. Źródło: vademecum Komputer i internet.

Literatura:

- Andrzejewska A., Bednarek J, Szarżała D., *Cyberprzestrzeń – szanse, zagrożenia, uzależnienia*, Wydaw. Pedagogium, Warszawa 2007.
- Andrzejewska A., *Dziecko w cyberprzestrzeni*, Wydaw. Pedagogium, Warszawa 2007.
- Andrzejewska, *(Nie)bezpieczny komputer*, Wydaw. APS, Warszawa 2008.
- Bednarek J., *Multimedia w kształceniu*, Wydaw. PWN, Warszawa 2006.
- Gała A., Ulfik I. (red.), *Oddziaływanie „agresywnych” gier komputerowych na psychikę dzieci*, Wydaw. UMCS, Lublin 2000,
- Fundacja Kidprotect.pl „Aktywność dzieci w Internecie” – sierpień 2011
- Wojtasik L. „Jak reagować na przemoc. Poradnik dla szkół”

<http://www.bezpiecznyuczen.pl/>

<http://www.kidprotect.pl/>

<http://www.chrondziecko.pl/>

<http://www.fdn.pl/>

<http://www.sieciaki.pl/>

<http://www.dzieckowsieci.pl/>

<http://www.dyzurnet.pl/>

<http://www.dbi.pl/>

<http://www.policja.pl>

<http://www.brpd.pl>

<http://www.nk.pl/bezpieczeństwo>

Grodziskie Towarzystwo Edukacyjne dziękuje

Akademia Liderów

Innowacji i Przedsiębiorczości

Fundacja dr Bogusława Federa

KRS 0000318482

ul. Orzeszkowej 2 A

05-827 Grodzisk Mazowiecki

www.Wiedza3G.pl

biuro@Wiedza3G.pl

tel./fax 22 734 34 81

za sfinansowanie w ramach nieodpłatnej działalności pożytku publicznego

Projektu „E-wychowanie dzieci w duchu przedsiębiorczości”

Akademia Liderów Innowacji i Przedsiębiorczości Fundacja dr Bogusława Federa posiada status organizacji pożytku publicznego i działa na rzecz wdrażania i rozwijania idei przedsiębiorczości.

Głównym celem działania Fundacji jest wspieranie postaw innowacyjnych i przedsiębiorczych w istniejących organizacjach i przedsiębiorstwach a także pomoc w tworzeniu nowych przedsiębiorstw (start up) opartych na wiedzy i przetwarzaniu informacji. Fundacja Akademia Liderów Innowacji i Przedsiębiorczości została założona w 2008 roku przez dra Bogusława Federa. Fundacja jest niezależną organizacją pozarządową, zorientowaną na budowę innowacyjnego, przedsiębiorczego społeczeństwa ludzi świadomie podnoszących swoje kompetencje i umiejętności, zaangażowanych w rozwój własny oraz chcących korzystać z międzynarodowej wymiany myśli.

Fundacja upowszechnia Wiedzę 3 GENERACJI w ramach programów:

- Programy Innowacyjności i Przedsiębiorczości – obejmujące przedsięwzięcia i uczestnictwo w prowadzonych badaniach naukowych, badawczo-rozwojowych i wdrożeniowych, organizacji konferencji, seminariów, warsztatów i kurów,
- Programy Wsparcia – obejmujące pomoc menedżerom i przedsiębiorcom w prowadzeniu już istniejących organizacji a także pomoc absolwentom i studentom w projektowaniu, przygotowaniu, finansowaniu i otwieraniu przedsiębiorstw opartych na wiedzy, innowacyjności i przetwarzaniu informacji,
- Programy Wymiany Międzynarodowej – obejmujące wizyty menedżerów i przedsiębiorców oraz wymianę wykładowców, trenerów, studentów i absolwentów oraz przedsiębiorców, w tym organizację praktyk i warsztatów.

Przełącz swój 1% podatku na wsparcie i rozwój młodych przedsiębiorców i cele statutowe Akademii Liderów:

- Pobierz bezpłatny Program PIT-OPP 2011 do wypełniania rocznych zeznań podatkowych — www.Wiedza3G.pl
- Wpisz KRS 0000318482 w zeznaniu podatkowym za 2011 rok

Projekt „E-wychowanie dzieci w duchu przedsiębiorczości”

Partnerzy Akademii Liderów:



Wydział Prewencji
Komendy Wojewódzkiej Policji z
siedzibą w Radomiu



Stowarzyszenie Krzewienia
Edukacji Finansowej



Aurelius Interactive
www.aurelius.pl

Specjalne podziękowania za pomoc dla:

- Pani Naczelnik Doroty Pater – Naczelnik z Wydziału Prewencji Komendy Wojewódzkiej Policji z siedzibą w Radomiu
- Urzędu Patentowego w Warszawie – za udostępnienie publikacji merytorycznych dla dzieci
- Aurelius Interactive – za pomoc merytoryczną oraz przygotowanie składu niniejszej publikacji

ⁱ Ł. Wojtasik (red.) „Jak reagować na cyberprzemoc. Poradnik dla szkół”, Biblioteka programu dziecko w Sieci Fundacji Dzieci Niczyje, s. 6

ⁱⁱ Tamże, s. 6

ⁱⁱⁱ Tamże s. 6-7

^{iv} Badanie on-line Przemoc rówieśnicza a media elektroniczne, styczeń 2007 FDN, Gemius S.A., N=891 internautów w wieku 12-17 lat