GŁOS WIELKOPOLSKI junior

e_PCHŁA

Szkoła Podstawowa nr 4
Grota Roweckiego 10
63-100, Śrem

Wydanie specjalne 01/15

WWW.JUNIORMEDIA.PL

ORGANIZATOR PROJEKTU GRUPA WYDAWNICZA polskapresse

PARTNER Fundacja Orange

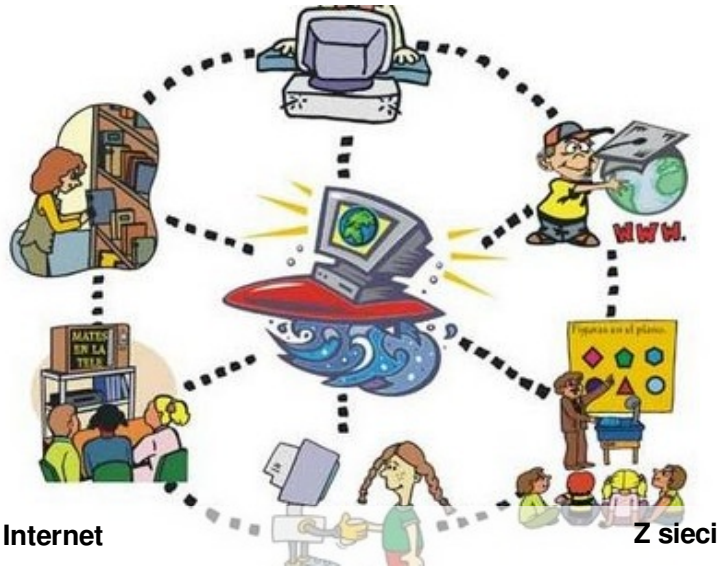
INTERNET - Narzędzie, które może być wykorzystywane w różny sposób - zarówno pozytywny i twórczy, jak i niebezpieczny i szkodliwy.

DBI 2015 **http://www.saferinternet.pl/**

Zbliża się Dzień Bezpiecznego Internetu 2015, który obchodzić będziemy 10 lutego. Wydarzenie to odbędzie się w Polsce po raz jedenasty.

Tak jak w zeszłym roku, wszystkie działania podejmowane w ramach DBI realizowane będą pod hasłem „Razem tworzymy lepszy Internet". Tak jak w zeszłym roku, wszystkie działania podejmowane w ramach DBI realizowane będą pod hasłem „Razem tworzymy lepszy Internet". Podczas obchodów DBI chcemy podkreślić to, że każdy internauta może przyczynić się do tego, że Internet będzie miejscem bezpiecznym i pozytywnym. Każdy z nas ponosi odpowiedzialność za to, co robi w Sieci i w jaki sposób z niej korzysta.

Dzień Bezpiecznego Internetu (DBI) obchodzony jest z inicjatywy Komisji Europejskiej od 2004 roku i ma na celu inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych. W Polsce Dzień Bezpiecznego Internetu od 2005 roku organizowany jest przez Fundację Dzieci Niczyje oraz Naukową i Akademicką Sieć Komputerową (NASK) – realizatorów unijnego programu Safer Internet. Głównym partnerem wydarzenia jest Fundacja Orange.
DBI ma na celu przede wszystkim inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych, zaznajomienie rodziców, nauczycieli i wychowawców z problematyką bezpieczeństwa dzieci w Internecie oraz nagłośnienie tematyki dotyczącej bezpieczeństwa online.
Podczas obchodów DBI organizatorzy zachęcają szkoły, organizacje pozarządowe, firmy i osoby prywatne do wspierania tego przedsięwzięcia przez organizację lokalnych inicjatyw na rzecz bezpieczeństwa młodych internautów (m.in. zajęć edukacyjnych, happeningów, gazetek szkolnych, kampanii informacyjnych, konkursów) oraz zgłaszania ich za pośrednictwem umieszczonego na stronie formularza.
Chcą również zwrócić szczególną uwagę na potencjał sieci, który dzieci mogą wykorzystać zarówno w edukacji, kontaktach z rówieśnikami jak również jako formę twórczej rozrywki.



Internet **Z sieci**

DBI **DBI**

Zagrożenia w Internecie:

`1. Rozpowszechnianie nielegalnych treści:

- pornograficznych,
- ofert sprzedaży pirackiego oprogramowania komputerowego oraz nagrań audio i video,
- ofert sprzedaży przedmiotów pochodzących z kradzieży lub przemytu,
- propagujących używanie narkotyków oraz wskazujące, gdzie można się w nie zaopatrzyć.

2. Nielegalne uzyskiwanie danych:

a. phishing – to wyłudzanie poufnych informacji osobistych (np. haseł lub szczegółów karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne,

b. pharming - bardziej niebezpieczna dla użytkownika oraz trudniejsza do wykrycia forma phishingu.Charakterystyczne dla pharmingu jest to, że nawet po wpisaniu prawidłowego adresu strony www, ofiara zostanie przekierowana na fałszywą (choć mogącą wyglądać tak samo) stronę www. Ma to na celu przejęcie wpisywanych przez użytkownika do zaufanych witryn haseł, numerów kart kredytowych i innych poufnych danych

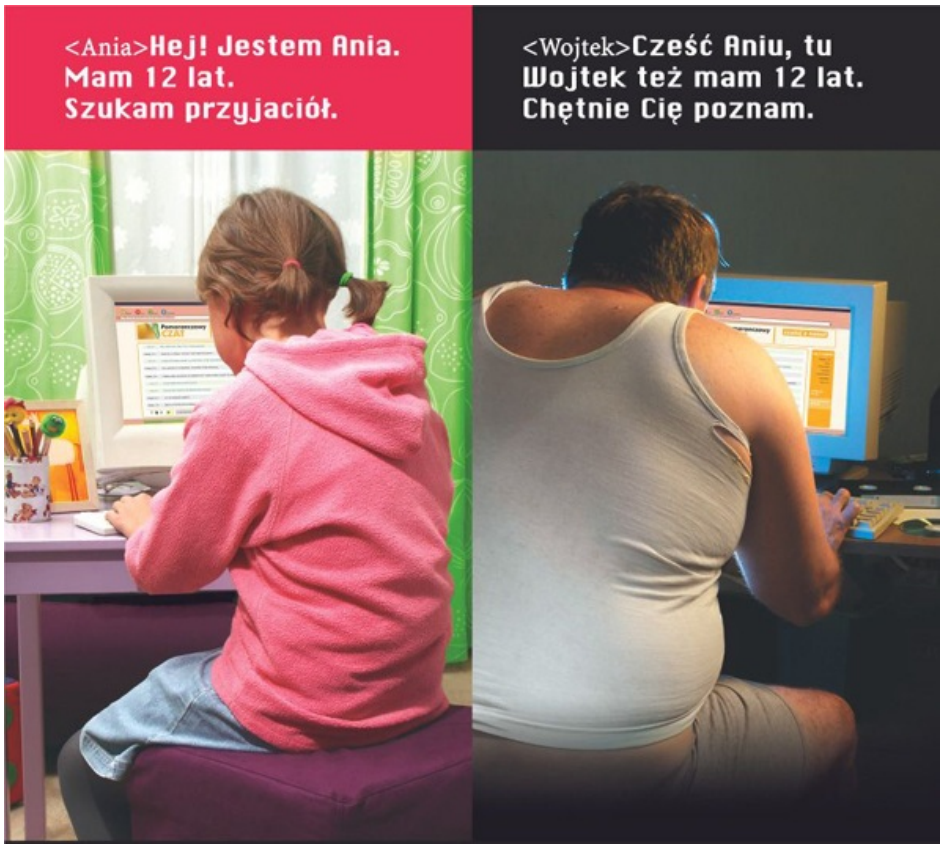
3. Włamania sieciowe i zainfekowanie komputera programem wirusowym – otwieranie każdej przychodzącej poczty wraz z załącznikami, korzystanie z sieci P2P, używanie nośników danych tj., pendrive, dyskietka itp. - grozi ściągnięciem szkodliwego oprogramowania na komputer.

4. Kontakt z nieznajomymi- wszelkiego rodzaju komunikatory, czaty umożliwiają na szybkie poznawanie wielu ludzi, niekoniecznie uczciwych. Przez Internet łatwiej można zakamuflować swoje „prawdziwe" intencje, bo sieć zapewnia dosyć dużą anonimowość. Te elementy sprawiają, że Internet stał się dobrym narzędziem dla przestępców, osób reprezentujących sekty religijne oraz różnego rodzaju dewiantów, którzy mają ułatwione zadanie w nawiązywaniu nowych kontaktów w poszukiwaniu swoich potencjalnych ofiar.

5. Infoholizm (siecioholizm) czyli Uzależnienie od Internetu - Niewielu ludzi zdaje sobie sprawę z tego, że komputer może uzależnić w taki sam sposób jak alkohol, praca czy narkotyki.

6. Spam - niechciane lub niepotrzebne wiadomości elektroniczne.

7. Wyłudzenia i oszustwa na aukcjach internetowych



Spotkania w sieci **Z sieci**

8. Cyberbulling (cyberprzemoc) prześladowanie, zastraszanie, nękanie, wyśmiewanie innych osób z wykorzystaniem Internetu i narzędzi typu elektronicznego takich jak: SMS, e-mail, witryny internetowe, fora dyskusyjne w Internecie i inne. Taka forma znęcania się nad swoimi ofiarami, zdaniem psychologów wynika z tego, że łatwiej poniżać, dyskredytować i szykanować, gdy istnieje szansa ukrycia się za internetowym pseudonimem i nie ma potrzeby konfrontacji z ofiarą oko w oko.

Prześladowanie przez Internet jest szczególnie groźne dlatego, że kompromitujące czy poniżające materiały są dostępne w krótkim czasie dla wielu osób i pozostają w sieci na zawsze, jako kopie na wielu komputerach, nawet po ustaleniu i ukaraniu sprawcy.

Formy cyberprzemocy:

a. zdjęcia i filmy,
b. przemoc werbalna,
c. poniżanie, ośmieszanie,
d. upokarzanie, straszenie, grożenie, szantaż,
e. publikowanie kompromitujących materiałów,
f. podszywanie się za kogoś (kradzież tożsamości),
g. kontakt z nielegalnymi treściami w Internecie (pornografia dziecięca, teksty rasistowskie, ksenofobiczne, szowinistyczne).

Powiedz STOP cyberprzemocy **Z sieci**

10 zasad

bezpiecznego korzystania z Internetu:

1. Korzystaj z oprogramowania antywirusowego
2. Otwieraj wiadomości tylko od znajomych osób
3. Ostrożnie pobieraj pliki z sieci
4. Unikaj klikania w nieznane linki i załączniki w wiadomościach e-mail
5. Nie podawaj w sieci danych osobowych, ani haseł, nie wysyłaj swoich zdjęć
6. Chroń swoje konta na serwisach społecznościowych
7. Stosuj trudne do odgadnięcia hasła, które są kombinacjami liter i cyfr
8. Czytaj regulaminy
9. Sprawdzaj, czy strona, do której się logujesz, ma zabezpieczenie SSL
10. Pamiętaj, że osoba po drugiej stronie, nie musi być tym, za kogo się podaje!

Zasady www.kidprotect.com

POZNAJ BEZPIECZNY INTERNET

Sieciaki.pl

www. sieciaki.pl

Więcej informacji na stronie www.sieciaki.pl
lub www.dzieckowsieci.pl

Informacje - nie udzielaj
Nieznajomi – nie ufaj Ty – odpowiadaj za siebie
Etykieta – przestrzegaj
Rodzice – ufaj
Nieuczciwość – wystrzegaj się
Edukacja – ucz się i ucz rodziców
Tabela – planuj czas

Internet nie jest groźny, ale używając go należy zachować zdrowy rozsądek. Dlatego też każdy posiadacz komputera powinien zadbać o należyte jego zabezpieczenie przed zagrożeniami zarówno z Internetu, jak i zewnętrznych źródeł przenoszenia danych, jak np.: pendrive. CDROM. Komputer może zostać zainfekowany złośliwym programem przede wszystkim poprzez nierozważne działania użytkownika.

POJĘCIE PRYWATNOŚCI

Mówiąc o prywatności w Internecie, mamy na myśli ochronę poufności dotyczącej różnych osobistych danych. Między innymi danych osobowych tzn. : imię, nazwisko, adres zamieszkania, numer, telefonu, adres e-mail, wizerunek.Są to informacje, których nie podajemy wszystkim, e zazwyczaj chcemy utrzymać we względnej tajemnicy – a przynajmniej ograniczamy liczbę osób, które mogą mieć do nich dostęp.

DLACZEGO CHRONIMY PRYWATNOŚĆ?

Dlaczego ujawnianie tych informacji może być niebezpieczne?
Przede wszystkim dlatego, że:
Nigdy nie wiadomo, kto i w jaki sposób może je wykorzystać.
Łatwo wyobrazić sobie kombinację - podanie swojego adresu zamieszkania i geolokalizacji, wskazującej odległe miejsce, w którym aktualnie spędzamy wakacje. Idealne okoliczności dla włamywacza!

JAK CHRONIĆ SWOJĄ PRYWATNOŚĆ?

Co to znaczy: uważać na swoją prywatność? Na co powinniśmy zwracać uwagę podopiecznym?
To zagadnienie ma wiele płaszczyzn, zaczynając od najbardziej podstawowych:
Należy być czujnym przy logowaniu do serwisu.
Nie zaleca się korzystania z funkcji: „Zapamiętaj hasło” – szczególnie jeżeli korzystamy z innego niż własny komputera (u znajomych, w kafejce internetowej).
Należy pamiętać o wylogowaniu z serwisu! Często wśród młodzieży zdarzają się przypadki żartobliwego lub złośliwego „przechwycenia” konta w profilu, właśnie po znalezieniu cudzej niewylogowanej sesji.
Nie wolno udostępniać innym osobom swoich danych niezbędnych do logowania - młodzi ludzie często wymieniają się tymi danymi, okazując w ten sposób dowód zaufania czy przyjaźni, a jednocześnie nie zdając sobie sprawy z tego, że udostępniają naprawdę niezliczoną ilość informacji osobistych i mogą stracić nad nimi kontrolę, a nawet stać się ofiarą cyberprzemocy. Tak jak nie rozdaje się kolegom i koleżankom swoich dokumentów, tak nie powinno się udostępniać im wszystkich informacji o sobie.

Hasła są jak szczoteczki do zębów - nie pokazujemy publicznie, nie oddajemy nikomu, czasem wymieniamy na nowe.

Korzystając z serwisów społecznościowych np. FACEBOOK-a, często nie zdajemy sobie sprawy, że dochodzi do publikowania informacji również o naszych znajomych. Oznaczanie swoich znajomych na zdjęciach (tzw. tagowanie) jest bardzo popularne, ale pamiętajmy, że w ten sposób możemy narazić ich na różne nieprzyjemności i w sposób nieuprawniony korzystamy z ich wizerunku. Dbajmy o bezpieczeństwo również swoich znajomych!

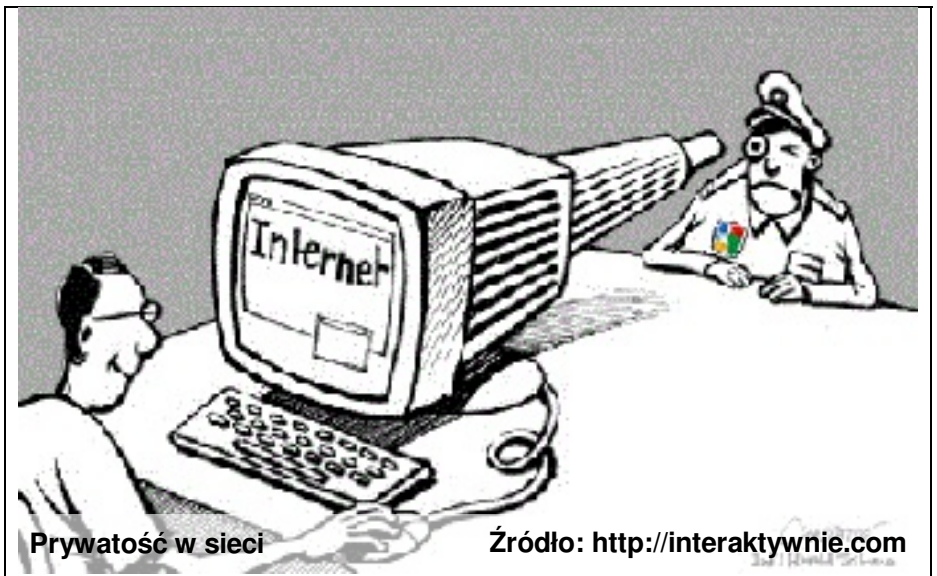
Duże portale społecznościowe umożliwiają zmiany w ustawieniach prywatności konta. Zazwyczaj istnioją trzy rodzaje ograniczeń do konta:

Za pomocą ustawień prywatności można też zablokować wyszukiwanie profilu przez wyszukiwarce wyszukiwarkę internetowej, w ten sposób nikt postronny nie dotrze do naszego konta.

Jeżeli konto będzie dostępne tylko dla znajomych, nadal nie zwalnia to jego posiadacza z odrobiny czujności. Do listy swoich znajomych należy dodawać wyłącznie osoby, które rzeczywiście znamy i którym ufamy.
może być ono dostępne tylko dla osób zaakceptowanych jako znajomych w serwisie może obejmować również grupę ich znajomych (czyli np. jeżeli mam 20 znajomych w serwisie, a każdy z nich ma 20 swoich, oznacza to, że udostępniamy prywatne informacje o sobie 400 osobom!)
a w najgorszym wypadku konto może być dostępne dla każdego użytkownika serwisu (tzw. konto publiczne). Tę opcję powinny wykorzystywać tylko firmy bądź konta-fankluby.

Nie warto powiększać listy wirtualnych przyjaciół wyłącznie w celu markowania pokazywania swojej popularności.
Przyjmując nową osobę do swoich znajomych, udostępniamy jej swoje prywatne informacje. Jeśli przestaniemy darzyć zaufaniem któregoś ze znajomych, po prostu usuńmy go ze swojego profilu.

Źródło: Poradnik bezpieczeństwa mobilnego - Fundacja Nowoczesna Polska



Prywatość w sieci **Źródło: http://interaktywnie.com**

Chroń prywatność **www.chip.pl**