



Politechnika Łódzka



Sposoby radzenia sobie z zagrożeniami w sieci

dr inż. Rafał Grzybowski



Sieć = Internet

- ☐ Globalna sieć komputerowa, bez której spora liczba ludzi nie wyobraża sobie obecnie życia.
- ☐ Nie tylko usprawnia, ale wręcz umożliwia realizację rzeczy, które przed jego odkryciem były niemożliwe do wykonania.
- ☐ Oprócz wielkich korzyści, Internet niesie ze sobą jednak również zagrożenia.
- ☐ Skuteczną walką z nimi jest świadomość mogących się pojawić niekorzystnych zachowań i postaw.





- Internet jest miejscem rozrywki, zdobywania wiedzy, nawiązywania kontaktów, a więc narzędziem przekazywania różnych informacji. Niestety, często daje złudne poczucie, że kontrolujemy, kto ma dostęp do naszych danych.
- **Zbyt często też ulegamy złudzeniu prawdziwości informacji.**





Komunikacja za pomocą Internetu

- ☐ szybkie i nieskomplikowane nawiązywanie relacji
- ☐ możemy porozmawiać o problemach z kimś kogo w ogóle nie znamy
- ☐ poznawanie ludzi o podobnych zainteresowaniach
- ☐ **W Internecie wiele osób czuje się anonimowo, wyraża opinie, których nie odważyłoby się powiedzieć w świecie realnym.**

Pojawiają się agresja i wulgarność





Wszystko z umiarem

- ❑ Nie ma nic złego w wykorzystaniu Internetu do komunikowania się, przesyłania informacji, czy też rozmów towarzyskich.
- ❑ Coraz częściej odnotowujemy jednak przypadki zatraćania umiaru w tej kwestii.
- ❑ **Młodzi ludzie nierzadko wolą godzinami przesiadywać na portalach społecznościowych niż spotkać się z przyjaciółmi "twarzą w twarz,,!**
- ❑ Paradoksem portali społecznościowych jest sytuacja, w której dwie osoby są znajomymi na portalu, a w świecie realnym zachowują się jakby się nie znały.
- ❑ Spora część dzieci i dorastającej młodzieży rezygnuje z aktywności fizycznej, na rzecz wielogodzinnego siedzenia przed komputerem.





Zespół uzależnienia od Internetu (ZUI) „siecioholizm”

Skutki:

- zachwianie komunikacji
- depresja w przypadku braku styczności z siecią, wewnętrzna potrzeba użytkowania Internetu
- zaburzone funkcjonowanie, rozregulowanie rytmu snu.
- zachwianie więzi emocjonalnych w normalnym świecie,
- wyobcowanie,
- gubienie się w tym co wirtualne, a tym co realne.

**Uzależnienie od Internetu może okazać się
bardzo groźne i najczęściej wymaga
specjalistycznego i długiego leczenia**





Niebezpieczeństwa czyhające w sieci na dzieci

- ☐ nieodpowiednie dla nich treści takie jak pornografia, przemoc, rasizm czy promocja zachowań mogących szkodzić ich zdrowiu i życiu.
- ☐ dzieci nie potrafią krytycznie podchodzić do atrakcyjnie prezentowanych treści i obcowanie z takimi materiałami może zakłócić budowanie ich prawidłowego systemu wartości.

Niezwykle istotna jest więc próba przewidzenia możliwych do pojawienia się zagrożeń i szczerą, bezpośrednią rozmowę na ten temat z dziećmi.

Edukowanie ich w tym zakresie jest wręcz konieczne!



Niebezpieczeństwa czyhające w sieci na dzieci

Niebezpieczne mogą być także sytuacje, w których dzieci poznają w sieci przypadkowe osoby, nie zawsze posiadające dobre intencje. Na czatach, forach, portalach społecznościowych, czy grupach dyskusyjnych ujawniają się pedofile, poszukujący swoich ofiar nierzadko podszywają się pod osoby, którymi nie są.

Niezwykle istotna jest więc próba przewidzenia możliwych do pojawienia się zagrożeń i szczerą, bezpośrednią rozmową na ten temat z dziećmi.

Ania>Hej! Jestem Ania.
Mam 12 lat.
Szukam przyjaciół.
<Wojtek>Cześć Aniu, tu
Wojtek też mam 12 lat.
Chętnie Cię poznam.



Nigdy nie wiadomo,  **dziecko**
w sieci
kto jest po drugiej stronie



Politechnika Łódzka



Bo szczera rozmowa
jest cenniejsza od drogich prezentów

www.demotywatory.pl



Niebezpieczeństwa związane z przestępstwami internetowymi

- ☐ kradzieże tożsamości,
- ☐ włamania na konta bankowe,
- ☐ rozprzestrzenianie złośliwego oprogramowania



Najczęściej kradzione dane:

- Imię i Nazwisko
- Data urodzenia
- Numer i seria dowodu osobistego
- Adres domowy
- Dane o stanie zdrowia
- Numer telefonu
- Informacje o stanie finansów
- E-mail
- Nazwa użytkownika i hasło
- Dane ubezpieczeniowe



Niebezpieczeństwa związane z przestępstwami internetowymi

Złośliwym oprogramowaniem można się zainfekować przez odwiedzenie zarażonej strony internetowej lub przez kliknięcie na załącznik do maila od nieznanego nadawcy.

Przed zagrożeniami tego rodzaju teoretycznie chronią programy antywirusowe.

Teoretycznie, gdyż najłabszym ogniwem w najlepszym nawet systemie zabezpieczeń zawsze okazuje się człowiek!

Przykładem jest tu np. *phishing*.





7 zasad młodego internauty

1. Jeśli nie musisz podawać swoich danych – nie rób tego. Im mniej informacji o Tobie jest w sieci tym trudniej się pod Ciebie podszyć.
2. Staraj się unikać przekazywania poufnych informacji (np. haseł) pocztą elektroniczną, SMS-ami, czatem.
3. Przy logowaniu i przesyłaniu danych sprawdź, czy adres w przeglądarce zaczyna się od „https” i widnieje obok niego symbol kłódki.
4. Unikaj korzystania z niezabezpieczonego Wi-Fi. Jeśli go używasz, unikaj logowania się prawdziwymi danymi i nie wykonuj wrażliwych operacji (np. finansowych).
5. Jeśli korzystasz z komputera dostępnego dla innych osób, używaj w przeglądarkach trybu prywatnego (czasem zwanego „incognito”). Po zakończeniu Twojej sesji przeglądarka automatycznie kasuje całą jej historię oraz ciasteczka.
6. Zabezpieczaj swoje konta w Internecie hasłami, które trudno złamać (co najmniej 8 znaków, małe i wielkie litery, znaki specjalne, bez popularnych słów).
7. Chroń swoje hasła – nie udostępniaj ich innym, nie zapisuj w widocznym miejscu, nie zapamiętuj w komputerze (ani cudzym, ani własnym).



Politechnika Łódzka



Dziękuję za uwagę