Zagrożenia w Internecie

Internet jest nieocenionym narzędziem komunikacji, edukacji i rozrywki. Umożliwia wszechstronną komunikację i ułatwia kontakty niwelując ograniczenia przestrzenne i zapewniając porozumiewanie się w czasie rzeczywistym. Ułatwia naukę i rozwijanie zainteresowań, daje możliwość dyskusji o hobby z osobami je dzielącymi. Niestety Internet to nie tylko same korzyści. Z korzystaniem z Internetu wiążą się także rozmaite zagrożenia. Do najważniejszych należą:

1. **Rozpowszechnianie nielegalnych treści:**
   a. pornograficznych,
   b. ofert sprzedaży pirackiego oprogramowania komputerowego oraz nagrań audio i video,
   c. ofert sprzedaży przedmiotów pochodzących z kradzieży lub przemytu,
   d. 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. Oprogramowanie to może wyrządzić wiele szkód np.:
   a. wykraść poufne dane, np. hasła, numery kont bankowych,
   b. uszkodzić dokumenty, programy lub system operacyjny,
   c. otworzyć komputer na włamania,
   d. spowolnić prędkość Internetu,
   e. utrudnić lub uprzykrzyć celowo pracę na komputerze,
   f. dodać złośliwy kod HTML do plików na serwerach FTP,
   g. zniszczyć drogie podzespoły naszego komputera,
   h. uczynić nasz komputer *komputerem zoombie* - to znaczy, że będziemy należeć do sieci wyrządzającej szkody innym komputerom bez naszej wiedzy

   Typy szkodliwego oprogramowania:
   a. wirus - zaraża inne pliki w celu rozpowszechnienia się bez zgody użytkownika.
   b. robak - rozmnażają się wyłącznie przez sieć, np. za pomocą poczty e-mail.
   c. koń trojański - maskuje się pod innymi plikami lub programami. Wykonuje w tle szkodliwe operacje, np. otwiera port, przez który może zostać dokonany atak.
   d. tylne drzwi (ang. backdoor) - umożliwiają intruzom administrowanie naszym systemem przez Internet - zazwyczaj podszywają się pod inne programy. Są to też luki w programach lub systemach operacyjnych stworzone celowo.

e. program szpiegujący (ang. spyware) - śledzi czynności wykonywane na komputerze, gromadzi cenne informacje i wysyła je autorowi bez wiedzy użytkownika. Do cennych danych należą np. dane osobowe, hasła, numery kont, adresy e-mail, archiwa.
f. exploit - umożliwia przejęcie kontroli nad komputerem lub serwisem internetowym, wykorzystując luki w programach, systemach operacyjnych, błędy w zabezpieczeniach.
g. rootkit - pomaga we włamaniach do systemów informatycznych. Zagnieżdża się nawet w BIOS-ie na płycie głównej. Ukrywa niebezpieczne pliki i procesy, które umożliwiają utrzymanie kontroli nad systemem. Wykrycie rootkitów jest trudne, lecz większość programów antywirusowych radzi sobie z tym.
h. keylogger - zapisuje wszystkie naciśnięcia klawiszy. W ten sposób nasze poufne dane, które wpisujemy, są przesyłane do niepowołanych osób.
i. dialer - wykonuje drogie połączenia przez inny numer dostępowy. Szkodzi tylko komputerom, które łączą się z Internetem przez modem telefoniczny lub cyfrowy ISDN. Najczęściej występuje na stronach erotycznych.

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. Niepokojące symptomy sygnalizujące uzależnienie od Internetu, na które powinni zwrócić uwagę rodzice dzieci korzystających z komputera i Internetu:
   a. dziecko wpada w ciągi komputerowe siedzi po kilka godzin bez przerwy, nie może się oderwać,
   b. jest rozdrażnione, gdy nie może skorzystać z komputera,
   c. zaniedbuje inne ulubione zajęcia na rzecz komputera,
   d. jest zaangażowane w świat wirtualny przynosi szkody w realnym, np. nie odrabia lekcji, zaniedbuje przyjaciół,
   e. ucieka przed rzeczywistymi problemami w świat wirtualny,
   f. używa komputera by poprawić sobie nastrój.

   Osoby, u których stwierdzono uzależnienie od Internetu lub zagrożenie tym uzależnieniem, najczęściej spędzają czas na następujących formach rozrywki:
   a. Internet Relay Chat (IRC) – usługa służąca do porozumiewania się z innymi osobami korzystającymi, z Internetu. Jest to forma pisanej rozmowy.
   b. Gry online – specyfika gier online (sieciowych) polega na tym, iż naszym przeciwnikiem nie jest komputer, lecz żywy człowiek. Według niektórych badaczy tego zjawiska, poprzez tego typu gry narasta w graczach poziom agresji, który następnie jest rozładowywany w świecie realnym, na zwykłych ludziach.
   c. World Wide Web (WWW)
   d. Grupy dyskusyjne (newsgroups) i listy adresowe

   Uzależnienie od Internetu pociąga za sobą wiele konsekwencji zarówno psychologicznych jak i fizjologicznych. Typowe skutki uzależnienia to:
   a. zaniedbywanie nauki, życia rodzinnego, zawodowego,
   b. zapominanie o posiłkach,

c. zaburzenia w sferze uczuć i emocji,
d. utrwalenie postaw egocentrycznych,
e. zaburzenia w sferze własnej tożsamości,
f. zmiana języka (zubożenie, techniczny slang, używanie skrótów),
g. niekontrolowanie czasu spędzanego w Sieci,
h. brak troski o własne zdrowie i higienę osobistą.

6. **Spam** - niechciane lub niepotrzebne wiadomości elektroniczne. Najbardziej rozpowszechniony jest spam za pośrednictwem poczty elektronicznej. Istotą spamu jest rozsyłanie dużej ilości informacji o jednakowej treści do nieznanych sobie osób. Aby określić wiadomość mianem spamu, musi ona spełnić trzy następujące warunki jednocześnie:
   a. Treść wiadomości jest niezależna od tożsamości odbiorcy.
   b. Odbiorca nie wyraził uprzedniej, zamierzonej zgody na otrzymanie tej wiadomości.
   c. Treść wiadomości daje podstawę do przypuszczeń, iż nadawca wskutek jej wysłania może odnieść zyski nieproporcjonalne w stosunku do korzyści odbiorcy.
7. **Wyłudzenia i oszustwa na aukcjach internetowych**
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).

Przestrzeganie jednak kilku zasad bezpiecznego korzystania z Internetu może ograniczyć ryzyko zetknięcia się z niewłaściwymi treściami przez dziecko.

Oto kilka zasad bezpiecznego korzystania z Internetu przez dzieci:

- Ustal ramy czasowe, w których dziecko może korzystać z Sieci.
- Uczul dziecko, by nie podawało w Internecie imienia i nazwiska, adresu zamieszkania, numeru telefonu itp. Powinno też chronić swój adres email i nie podawać go bez powodu w formularzach na stronach WWW oraz obcym osobom. W szczególności dziecko nie powinno wpisywać nigdzie poufnych danych, jeśli korzysta z Internetu w kafejce internetowej i innych miejscach publicznego dostępu do Sieci.
- żelazną zasadą powinno być nie otwieranie korespondencji pochodzącej z nieznanego źródła oraz wstrzemięźliwe nawiązywanie nowych kontaktów.
- zachowanie ostrożności przy pobieraniu programów z Internetu bądź korzystaniu z przenośnej pamięci czy CD-ROM-ów.

- Używajcie filtrów antyspamowych. Dostawca usług internetowych zazwyczaj oferuje usługę zablokowania spamu, którą należy aktywować w programie obsługującym Wasze konta e-mail.
- Spam prawie zawsze zawiera zaproszenia i załączniki. Pokażcie dzieciom, w jaki sposób można zablokować osobę wysyłająca spam, lub powiedzcie im, żeby zawsze kasowały podejrzane wiadomości bez ich otwierania.
- Dodajcie do Ulubionych (jedna z opcji w przeglądarce) adresy stron, na które Wasze dzieci wchodzą najczęściej. W ten sposób umożliwicie im przeglądanie ich ulubionych stron bez używania wyszukiwarki internetowej.
- Zapewnij bezpieczeństwo dziecku instalując program kontrolujące wyświetlanie stron i czas dostępu do Internetu.
- Umieśćcie komputer w dużym pokoju, tak abyście mogli kontrolować aktywność dzieci w sieci.
- Budujcie zaufanie, tak aby Wasze dzieci wiedziały, że mogą z Wami porozmawiać, jeśli popełnią jakiś błąd, oraz że zawsze wspólnie spróbujecie znaleźć rozwiązanie! Uczymy się na błędach!
- Wasze dzieci powinny wiedzieć, że nie należy rozpowszechniać wiadomości, które mogą sprawić przykrość innym;
- Pomóżcie swoim dzieciom zrozumieć, jakie wiadomości i zachowanie może sprawić drugiej osobie przykrość i jak można temu zapobiec;
- Upewnijcie się, że dzieci wiedzą, jak można zablokować otrzymywanie e-maili od osób, które nie znajdują się na ich liście kontaktów;
- Zapisujcie obraźliwe wiadomości – być może będą stanowiły ważny dowód;
- Poznajcie środowisko Waszego dziecka – jego przyjaciół, ich rodziców, nauczycieli oraz kolegów i koleżanki z klasy;
- Zachęcajcie swoje dziecko do tego, aby było z Wami szczere, nawet jeśli zachowa się bezmyślnie – każdy ma prawo do popełniania błędów, a razem jest łatwiej je naprawić! Upewnijcie się, że dziecko wie, że to nie z jego winy ktoś mu dokucza.
- Upewnijcie się, że korzystacie ze stron internetowych, z których legalnie można pobrać muzykę i filmy.
- Wyjaśnijcie dzieciom, jakie ryzyko niesie ze sobą pobieranie plików z sieci bez zachowania należytych środków ostrożności.
- Upewnijcie się, że Wasz komputer jest chroniony i że korzystacie z regularnie aktualizowanego oprogramowania antywirusowego.
- Nauczcie dzieci, że pliki internetowe, które chcą zapisać na twardym dysku, powinny być najpierw przeskanowane przez program antywirusowy.
- Określcie zasady dotyczące czasu, jaki dzieci mogą spędzać, grając w gry komputerowe.
- Obserwujcie, w co grają Wasze dzieci. Skoro pilnujecie ich podczas zabawy na podwórku, dlaczego nie robić tego, gdy grają w gry on-line?
- Porozmawiajcie o tematyce gry, w którą dziecko gra – sprawdźcie, czy ma ona walory poznawcze i edukacyjne.
- Ostrzeżcie dzieci, aby nie podawały swoich danych osobowych innym graczom.
- Ostrzeżcie dzieci, żeby nigdy nie spotykały się same z innymi graczami, a jeśli chcą pójść na takie spotkanie, któreś z Was powinno im towarzyszyć.
- Poproście dzieci, aby informowały Was o przypadkach przemocy w sieci, groźbach, wulgarnym języku używanym przez innych, lub innych nieodpowiednich treściach, które znajdą w Internecie.

- Nie pozwólcie, by Wasze dziecko grało w grę, która ma na nie zły wpływ. Możecie to zrobić, blokując dostęp do gry.
- Nie wyręczaj się komputerem w opiece nad dzieckiem. Rodzice często traktują telewizor jak opiekunkę dziecka. Nie jest to dobre, aczkolwiek treści w telewizji są w pewien sposób kontrolowane, natomiast w Internecie dziecko ma dostęp do wszelkich bulwersujących treści.
- Jeśli zauważysz szczególnie niebezpieczne strony lub inne jakieś niepokojące zdarzenia w Internecie, zgłoś to organizacjom zajmującym się ich zwalczaniem. Zwróć dziecku uwagę, że Internet nie jest anonimowy. Pamiętaj też, że dziecko może być nie tylko ofiarą ale również sprawcą cyberprzestępstwa (np. udostępniając innym piracką muzykę lub programy).

Sam w sobie Internet nie jest ani zły, ani dobry – jest po prostu narzędziem… Tylko odpowiednie korzystanie z niego może zapewnić brak szkodliwości dla naszego zdrowia i dla naszego komputera. Oczywiście nie mamy większego wpływu na to, co inni użytkownicy robią, na ich złe zamiary wobec nas, ale powinniśmy maksymalnie zabezpieczać się przed tego typu działaniami przez stosowanie programów antywirusowych. Brak zagrożeń w Internecie zależy tylko od jego użytkowników. To jak zostanie wykorzystany zależy przede wszystkim od nas.

Źródła:

- http://www.eioba.pl/a74373/bezpiecze_stwo_komputer_w_kilka_zasad
- http://www.cyberbaba.pl/content/view/664/169/
- http://siecioholizm.eu/mid.php?sel=w_pulapce_internetu
- http://pl.wikipedia.org/
- http://www.dzieckowsieci.pl/
- http://literka.pl/article/show/id/37837
- http://docs9.chomikuj.pl/114000044,0,0,zagrozenia-zwiazane-z-internetem.doc