Informacje dla rodziców „Bezpieczny i przyjazny Internet”

Internet jest nieocenionym źródłem informacji, pozwala na swobodną wymianę opinii, utrzymywanie kontaktów z rodziną czy znajomymi. Umożliwia szybsze zdobywanie wiedzy i informacji o różnych wydarzeniach, kreatywne spędzanie czasu oraz rozrywkę w postaci np. gier. Poza zaletami ma jednak też i ciemne strony.

Błyskawiczny rozwój techniki powoduje, że dostępność usług telekomunikacyjnych stale się zwiększa. Nowe technologie dają nam bardzo dużo możliwości, niejednokrotnie jednak wykorzystywane są również do nieuczciwych lub sprzecznych z prawem praktyk. Dlatego tak ważne jest, by przed niebezpieczeństwami w sieci ustrzec najmłodszych użytkowników Internetu - to oni są najbardziej podatni na zagrożenia telekomunikacyjne.

Nowe negatywne zjawiska, które obserwujemy w związku z upowszechnieniem się dostępu do sieci, to:

1. **grooming** [czyt. gruming]- uwodzenie dzieci przez osoby dorosłe, najczęściej o skłonnościach pedofilskich;
2. **cyberprzemoc** lub cyberbullying - publikacja materiałów zawierających obraźliwe treści wobec jednej lub kilku osób, najczęściej nieświadomych umieszczenia takich informacji na swój temat w sieci, w celu ich szykanowania bądź poniżania;
3. **spam** - masowo przesyłane w sieciach telekomunikacyjnych (w Internecie oraz SMS-ami) informacje niezamówione, najczęściej o charakterze komercyjnym. Spam stanowi jeden z kanałów dystrybucji szkodliwego oprogramowania (np. wirusów lub robaków internetowych), jest wykorzystywany do zbierania i weryfikowania adresów poczty elektronicznej dla potrzeb budowania nielegalnych baz danych teleadresowych;
4. **phishing** - próby kradzieży danych wrażliwych. Dokonywany jest poprzez wysyłanie do użytkowników wiadomości łudząco podobnej do wiadomości od zaufanego podmiotu (np. banku), z treści której wynika konieczność przesłania danych takich jak np. numer konta, karty kredytowej, kodów pin etc. Następnie tego typu dane przekazane przez nieświadomego użytkownika posłużyć mogą do kradzieży tożsamości („identity theft") i pieniędzy.

Chrońmy dziecko przed tymi zagrożeniami!

Co zrobić, by uchronić dziecko przed niebezpieczeństwem w sieci?

1. Odkrywaj Internet i funkcje komputera razem z dzieckiem. Bądź jego pierwszym przewodnikiem po świecie Internetu i usług telekomunikacyjnych. Interesuj się tym, co dziecko robi „on-line”. Kontroluj jakie informacje i zdjęcia umieszcza Twoje dziecko na portalach społecznościowych.
2. **Możesz stworzyć bezpieczny profil dla dziecka na komputerze** - pozwala to na: ograniczenie uprawnień użytkownika, uruchamiania niedozwolonych aplikacji, ustalenie limitów czasowych korzystania z Internetu/komputera.
3. **Można zmodyfikować ustawienia przeglądarki**. Zależnie od systemu, jego wersji oraz typu przeglądarki, dostępne są różne opcje. Najważniejsze z nich, to m.in. możliwość zdefiniowania z jakich stron dziecko może korzystać (tzw. „White list”) oraz z jakich absolutnie nie („Black list”) podczas surfowania w Internecie. Przeglądarki posiadają taką funkcję, jak kontrola treści i ustawienia prywatności – dzięki temu możliwe jest dokładne zdefiniowanie tego, co dziecko może wyszukać w sieci.
4. Możliwe jest także **zainstalowanie specjalnej aplikacji nadzorującej działania dziecka na komputerze i w Internecie** takie jak: Cenzor, Motyl, Opiekun Dziecka, X-Guard.
5. **Naucz swoje dziecko podstawowych zasad bezpieczeństwa** i krytycznego podejścia do treści zamieszczanych w Internecie.
6. **Rozmawiaj z dzieckiem o cyberprzemocy.** Pamiętaj, że w dobie powszechnej dostępności do mobilnych urządzeń z funkcjami aparatu i kamery, zdjęcia i filmy mogą być wykorzystane przez dzieci do szykanowania rówieśników. Powiedz dziecku, że zamieszczanie takich filmów i zdjęć na stronach internetowych może wyrządzić komuś krzywdę Pamiętaj, że cyberprzemoc to również zamieszczanie przez dzieci na forach internetowych treści oczerniających rówieśników.

Zwróć dziecku uwagę, aby:

1. Nigdy nie podawało w Internecie swojego prawdziwego imienia i nazwiska, a posługiwało się nickiem, czyli pseudonimem. Nie powinno też podawać swojego adresu domowego i numeru telefonu, ponieważ nigdy nie może mieć pewności z kim rozmawia.
2. Nigdy nie wysyłało nieznajomym swoich zdjęć oraz zachowało szczególną ostrożność publikując swoje zdjęcia w sieci. Nigdy do końca nie wiemy, do kogo naprawdę trafią oraz w jaki sposób zostaną wykorzystane!
3. Jeżeli wiadomość, którą otrzymało pochodzi od nieznanego nadawcy, jest wulgarna lub niepokojąca {np. jest napisana w obcym języku, zawiera dziwne znaczki), nie powinno jej otwierać ani na nią odpowiadać, tylko pokazać ją rodzicom lub innej zaufanej osobie dorosłej.
4. Pamiętało, że nigdy nie ma pewności, z kim rozmawia w Internecie - ktoś, kto podaje się za rówieśnika, w rzeczywistości może być dużo starszy i mieć wobec dziecka złe zamiary.
5. Nie odpowiadało na spam - w ten sposób potwierdzamy tylko nadawcy nasz adres poczty elektronicznej. Spowoduje to zwiększenie ilości otrzymywanego spamu lub phishingu.
6. Nie brało udziału w „łańcuszkach internetowych" - informacje w nich zawarte nie są prawdziwe, ponadto jest to jeden ze sposobów uzyskiwania adresów poczty elektronicznej przez spamerów.
7. Miało świadomość, że nasze działanie w sieci nie jest anonimowe. W większości przypadków można precyzyjnie ustalić adres IP każdego komputera.
8. Zwracało szczególną uwagę na numery telefonów, z których przychodzą niejednoznaczne SMS-y, (np. „ktoś zostawił dla Ciebie wiadomość, aby ją odsłuchać wyślij SMS na numer...") oraz na numery, na które, zgodnie z treścią SMS-a, należy odpowiedzieć (np. 71XX, 72XX itd.), W większości przypadków odpowiadający wpada w pułapkę wysyłania kolejnych płatnych SMS-ów, co przekłada się na wysokość rachunku telefonicznego.
9. Było krytyczne wobec źródeł informacji w Internecie. Użytkownicy sieci powinni pamiętać, że nie wszystkie informacje w Internecie są prawdziwe.
10. Przestrzegało **netykiety**. Netykieta to nieformalny zbiór zasad zachowania w Internecie. Jak w codziennym życiu, tak i w Internecie należy przestrzegać nieformalnych zasad etycznych regulujących zachowanie wobec innych. Obejmuje to bycie grzecznym, używanie odpowiedniego języka, powstrzymywanie się od podnoszenia głosu (używania wielkich liter) lub atakowania innych osób. Dzieci, tak jak dorośli, nie powinny czytać cudzych wiadomości e-mail ani kopiować materiałów chronionych prawem autorskim.

Pamiętaj, że...

- ➡ znieważając, nękając innych w Internecie,
- ➡wysyłając w Sieci groźby np. "zabiję cię", "popamiętasz mnie"
- ➡używając wulgarnych słów na portalach internetowych,
- ➡podszywając się pod kogoś innego na czacie, portalu społecznościowym lub serwisie aukcyjnym,
- ➡zamieszczając w Sieci muzykę lub filmy, których nie jest autorem

... twoje dziecko popełnia wykroczenie lub nawet przestępstwo! W zależności od wieku, dziecko lub rodzic może ponieść konsekwencje prawne. Pamiętaj, że anonimowość w Sieci w praktyce nie istnieje, a granica między głupim żartem a przestępstwem jest bardzo cienka.

Polecane strony:

www.saferinternet.pl
www.dzieckowsieci.pl
www.dbi.pl
www.dyzurnet.pl – można zgłosić strony nielegalne i niebezpieczne dla dziecka!
www.helpline.org.pl
www.sieciaki.pl
www.saferinternet.org

Źródła:

http://rodzice.net/news/bezpieczenstwo-dzieci-w-internecie/
http://www.idg.pl/news/367924/bezpieczenstwo.dziecka.w.sieci.porady.dla.rodzicow.html