Internet - dużo możliwości, dużo zagrożeń [1]

Bezpieczeństwo dzieci w internecie

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** - 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.
2. Naucz swoje dziecko podstawowych zasad bezpieczeństwa Í krytycznego podejścia do treści zamieszczanych w Internecie.
3. 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 jesl 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.

SMS-y o podwyższonej płatności dostępne są w kilku wariantach cenowych. Pierwsze dwie cyfry numeru, pod który należy wysłać SMS. określają jego koszt:
70xx - koszt 50 gr + 22 proc. VAT
71xx - koszt 1 zł + 22 proc. VAT
72xx - koszt 2 zł + 22 proc. VAT
73xx - koszt 3 zł + 22 proc. VAT
74xx - koszt 4 zł + 22 proc. VAT
75xx - koszt 5 zł + 22 proc. VAT
76xx - koszt 6 zł + 22 proc. VAT
77xx - koszt 7 zł + 22 proc. VAT
78xx - koszt 8 zł + 22 proc. VAT
79xx - koszt 9 zł + 22 proc. VAT

Source URL:
http://www.jarzebinka.noweskalmierzyce.pl/pl/strona/internet-du%C5%BCo-mo%C5%BCliwo%C5%9Bci-du%C5%BCo-zagro%C5%BCe%C5%84

Links:
[1] http://www.jarzebinka.noweskalmierzyce.pl/pl/strona/internet-du%C5%BCo-mo%C5%BCliwo%C5%9Bci-du%C5%BCo-zagro%C5%BCe%C5%84