Bezpieczeństwo w sieci

Niezwykle ważnym zadaniem nauczyciela jak i wszystkich rodziców jest dbanie o bezpieczeństwo związane z aktywnością w sieci. Surfowanie w Internecie może być świetną zabawą oraz inspirującą formą spędzania wolnego czasu jak również przyczyną niepowodzeń dziecka, problemów w nauce, problemów zdrowotnych, zaburzeń funkcji poznawczych. Zbyt długie i częste korzystanie z komputera może doprowadzić do uzależnień, ucieczki od świata realnego, dysfunkcji neurologicznych. Badania wykazały, iż wiele osób, które na co dzień pracują przy komputerze, cierpi na dolegliwości bólu kręgosłupa, głowy, łzawienie oczu, rozdrażnienie.

Internet jest narzędziem, który poza całym swoim dobrodziejstwem niesie ze sobą również niebezpieczeństwa. Jest sposobem komunikowania się, źródłem wiedzy, placem zabaw, jak również wielkim śmietnikiem.

Można w nim zetknąć się z pornografią, pedofilią, przemocą, wulgaryzmami, sektami, używkami, rasizmem, itp. Największym problemem jest jednak to, że informacje te są ogólnie dostępne, nie zabezpieczone żadnym hasłem a co za tym idzie dostępne dla naszych dzieci. Problemem jest również to, że dzieci wcale nie muszą ich szukać, by na nie trafić.

Rozwiązaniem, oczywiście nie stu procentowym jest odpowiednie zabezpieczanie komputera programami filtrującymi, które niestety są zawodne i czasami blokują to czego nie powinny blokować a przepuszczają to co powinny blokować. Jest to jakieś rozwiązanie, ale połowiczne.

Niebezpieczeństwem w sieci jest to, że nie możemy zweryfikować osoby, z którą się komunikujemy, podawane dane mogą być nieprawdziwe a osoba może podawać się zupełnie za kogoś innego. Pedofilem np. może być każdy, nie ma tutaj znaczenia wiek, wykształcenie czy zamieszkanie. Są to osoby, które szukają w Internecie ofiar, wykorzystując czaty, komunikatory, blogi, strony dla dzieci, portale społecznościowe. Często podają się za dzieci, wymieniają się kontaktami i informacjami, dążą do spotkania, często manipulują.

Kolejnym niebezpieczeństwem, na które narażone są nasze dzieci a co za tym idzie nasi uczniowie jest cyberprzemoc. Cyberprzemoc to agresja elektroniczna polegająca na stosowaniu przemocy poprzez prześladowanie, zastraszanie, nękanie, wyśmiewanie innych osób z wykorzystaniem Internetu. Często konflikty w klasie przenoszone są do Internetu. Zaczyna się obrażanie, dokuczanie, prezentowanie kompromitujących filmików, nagrywanych na telefonach komórkowych.

Zamiarem osoby stosującej cyberprzemoc (stalkera) jest ośmieszenie innej osoby, stosowanie krzywdzących wpisów i publikowanie zdjęć na portalach społecznościowych, witrynach internetowych, forach dyskusyjnych i komunikatorach.

Dzieje się tak, ponieważ osoba oczerniająca czuje się anonimowa i bezkarna, gdyż np. skorzystała z serwera umieszczonego w innym kraju. Dzieci nie znają prawa i jego konsekwencji. Stosują metody, które często mogą skończyć się tragicznie dla osoby, której ten atak dotyczy.

Główne przyczyny to oczywiście błędy wychowawcze, brak nadzoru, brak zainteresowania dzieckiem, brak wychowania w sieci, brak przekazywania pozytywnych wartości.

Oto kilka porad dla rodziców i nauczycieli wartych zastosowania:

- ustaw komputer w widocznym, wspólnym miejscu, do którego każdy z domowników będzie miał dostęp,
- nie karzemy dziecka za błędy, o których nam opowiada,
- rozmawiamy z dzieckiem,
- nie boimy się przyznania do niewiedzy,
- bawimy się siecią, poznajemy ją, przyda nam się to w kontaktach z dzieckiem,
- surfuj po sieci ze swoim dzieckiem,
- pokazuj dziecku wartościowe strony,
- stosuj programy filtrujące,
- ustal zasady korzystania z internetu i egzekwuj je,
- w przypadku stwierdzenia przestępstwa niczego nie usuwaj z komputera,
- o wszelkich przejawach przemocy zawiadamiaj policję i administratorów serwisów,
- ucz dziecka zasad bezpieczeństwa, zasad netykiety
- nie strasz dziecka zagrożeniami ale przestrzegaj przed nimi,
- wyjaśnij dziecku, że osoba po drugiej stronie nie musi być tym za kogo się podaje,
- uczul, aby nie podawać w sieci danych osobowych i nie wysyłać zdjęć,
- jeśli umówi się na spotkanie, wyślij z nim koleżankę lub kolegę,
- jeśli twoje dziecko coś zaniepokoi lub zawstydzi, umów się, aby cię o tym poinformowało,

- poinformuj dziecko, że nie jest anonimowe w sieci,
- przestrzegaj przed głupimi dowcipami czy żartami,
- naucz dziecko jak zrobić „**zrzut ekranu**”; naciskamy klawisz PrtSc (Print Screen) i wklejamy zawartość schowka do programu graficznego lub edytora tekstu poleceniem „wklej”
- chroń swoje dane programami antywirusowymi i typu anty-spyware,
- uczul, aby nie otwierać maili od nieznanych osób,
- naucz tworzenia bezpiecznych haseł na portalach społecznościowych, koncie pocztowym, aby nie doszło do włamania i podszycia się pod twoje dziecko; np. fragment wiersza, piosenki lub zdanie: „**Moja siostra ma na imię Kasia i ma 12 lat**”, wybieramy ze zdania pierwsze litery i mamy – **MsmniKim12l** – bezpieczne hasło gotowe,

Błaszczyk Krzysztof