Bezpieczne korzystanie z Internetu

Szanowni Państwo,

Internet to nowoczesne medium, które odgrywa ogromną rolę w życiu młodego człowieka. Teraz kiedy uczeń wykorzystuje Internet do nauki zdalnej jest bardzo ważne, aby rodzice zwrócili szczególną uwagę czy jego dziecko bezpiecznie z niego korzysta.

Mówiąc o bezpieczeństwie, najważniejszy jest prosty przekaz, dlatego zebraliśmy najważniejsze wskazówki dotyczące bezpiecznego korzystania z Internetu.

1. zawsze korzystaj z aktualnego systemu operacyjnego, aktualnej przeglądarki internetowej i aktualnego programu antywirusowego,
2. twórz bezpieczne hasła logowania do poczty e-mail i kont w rozmaitych usługach – nie zawieraj w nich oczywistych słów oraz informacji takich jak imię czy data urodzenia i staraj się wymyślać długie hasła,
3. nie korzystaj z tego samego hasła na różnych stronach,
4. nie loguj się do ważnych usług, korzystając z publicznych hotspotów Wi-Fi (bo one szczególnie są narażone na cyberwłamania),
5. podczas logowania dwa razy sprawdź adres WWW strony i upewnij się, że strona logowania ma certyfikat bezpieczeństwa (warto też – jeśli to możliwe – korzystać z weryfikacji dwuetapowej),
6. nie podawaj w Internecie żadnych danych i nie udostępniaj żadnych zdjęć, do których dostępu nie powinny uzyskać żadne „osoby trzecie”,
7. nie wchodź na strony z linków w podejrzanych wiadomościach e-mail i nie otwieraj dodanych do nich załączników,
8. uważaj na skrócone adresy URL, które często mogą stanowić pułapkę.

Zwróć dziecku uwagę, aby:

- 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
- 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!
- 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
- 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
- nie odpowiadało na spam - w ten sposób potwierdzamy tylko nadawcy nasz adres poczty elektronicznej. Spowoduje to zwiększenie ilości otrzymywanego spamu lub phishingu
- 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
- **miało świadomość, że nasze działanie w sieci nie jest anonimowe.** W większości przypadków można precyzyjnie ustalić adres IP każdego komputera.
- 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

Młodzi ludzie wykorzystują Internet do nauki i rozrywki, komunikują się z innymi, poszukują informacji potrzebnych im w życiu codziennym. Jest narzędziem do tworzenia własnego wizerunku, aby bywa również wykorzystywany do zachowań AGRESYWNYCH.

SZCZEGÓLNĄ FORMĄ AGRESJI ELEKTRONICZNEJ JEST **CYBERPRZEMOC – definiowana jako przemoc rówieśnicza z wykorzystaniem Internetu i urządzeń mobilnych.**

Jakie formy przemocy stosują najczęściej młodzi użytkownicy sieci?

- Złośliwie komentują wpisy i zdjęcia
- Przerabiają i publikują ośmieszające zdjęcia, filmy
- Podszywają się pod kogoś w sieci
- Upubliczniają sekrety ofiary
- Dystrybuują nieprawdziwe informacje lub krzywdzące opinie czy oceny

PAMIĘTAJMY!!!!

Cyberprzemoc ma specyficzne cechy, który sprawiają, że ofiara narażona jest na duży dyskomfort emocjonalny, doświadcza wiele ataków i przykrości, których konsekwencje mogą być bardzo poważne i utrzymywać się również po zakończeniu prześladowania.

Jak zapobiegać?

- ROZMAWIAJMY Z DZIECKIEM - zarówno o zasadach bezpiecznego korzystania z Internetu jak i kulturalnym zachowaniu w sieci.
- ROZMAWIAJMY o potencjalnych konsekwencjach podejmowanych przez dziecko działań i zachowań.

- ❖ Pokazujmy i przypominajmy o możliwościach ochrony np. możliwość zablokowania użytkownika, blokowanie połączeń sms.
- ❖ Zwróćmy uwagę, ile czasu dziecko spędza na komputerze bądź korzysta z telefonu komórkowego. NA JAKICH PORTALACH SPOŁECZNOŚNIOWYCH I FORACH SIĘ UDZIELA I JAKIEGO RODZAJU TREŚCI KOMENTUJE I UDOSTĘPNIA.
- ❖ Informujmy dziecko jak należy się zachować, jeżeli ma do czynienia z brakiem kultury lub naruszeniem jego godności osobistej.

Zachęcamy do skorzystania ze strony http://www.sieciaki.pl/

Jeśli będą Państwo potrzebowali wsparcia – pozostajemy do Państwa dyspozycji.

Anna Kurek, Wioleta Sierant – pedagog szkolny, Michał Płaszczak – psycholog szkolny