

"Jak zadbać o bezpieczeństwo w sieci"

Z powodu zawieszenia zajęć dydaktyczno-wychowawczych w naszych szkołach, wskutek obecnej sytuacji epidemiologicznej w naszym kraju, kontakt pomiędzy uczniem a nauczycielem odbywa się w sposób zdalny z wykorzystaniem dziennika elektronicznego oraz edukacyjnych platform internetowych jak np. epodreczniki.pl. Istnienie internetu dostarcza nam całą plejadę możliwości poznawania świata, komunikowania się z innymi, zdobywania wiedzy oraz rozrywki. Niesie jednak też ze sobą potencjalne zagrożenia.

Pierwszy typ zagrożeń opiera się na technicznym działaniu samego internetu oraz systemu komputerowego jakiego używamy. Mówię tutaj o wirusach komputerowych i trojanach, których działania mogą pozbawić nas danych przechowywanych na komputerze, haseł, a co za tym idzie dostępów do naszych miejsc w sieci, poczty elektronicznej, a nawet środków finansowych zgromadzonych na naszym koncie bankowym, obsługiwanych często właśnie zdalnie poprzez komputer i internet. Drugi typ zagrożeń z kolei jest bardziej ludzki. Użytkownicy internetu mogą paść ofiarą oszustwa, cyberprzemocy, szerszenia nienawiści, mogą natknąć się też na pornografię.

Jako zwykli użytkownicy sieci możemy zabezpieczyć się, chociaż częściowo, przed tymi zagrożeniami. Postaram się w kilku punktach wymienić o czym należy pamiętać by ustrzec się przed nimi.

Przeciwdziałaj zagrożeniom działań systemu komputerowego

- Używaj legalnego oprogramowania i systemu operacyjnego. Wiele dostępnych obrazów systemu operacyjnego, ze złamanymi zabezpieczeniami posiada tzw. „backdoory”, luki wykorzystywane przez złośliwe oprogramowanie.
- Aktualizuj swój system operacyjny, sterowniki i oprogramowanie. Aktualizacje naprawiają błędy systemu oraz eliminują różne luki.
- Zainstaluj program antywirusowy i aktualizuj jego bazy wirusów.
- Ściągaj programy zawsze ze strony jego twórców/producenta.
- Nie otwieraj załączników pocztowych i linków do miejsc w sieci od nieznanymi nadawców. Jest to najczęstsza przyczyna infekcji trojanem lub szkodliwym skryptem.
- Czytaj ze zrozumieniem treści okien instalacyjnych i tego co akceptujesz.
- Nie podawaj osobom trzecim haseł do swoich kont lub programów. Nigdy żaden administrator danego systemu nie poprosi cię o podanie hasła np. do dziennika elektronicznego! Każda taka prośba to próba wymuszenia hasła.
- Nie używaj takiego samego hasła na wielu portalach. Wystarczy, by jeden portal został „shakowany”, spowoduje to najczęściej utratę innych kont, gdzie takie samo hasło było użyte.

Przeciwdziałaj zagrożeniom w sieci internet

- Bądź anonimowy! Nie podawaj swoich danych osobowych, ani numeru telefonu na nieznanym czacie, forum lub w rozmowie z nieznanym. Nie każdy w sieci jest tym za kogo się podaje.
- Nie umawiaj się sam na spotkanie z kimś poznanym w sieci.
- Nie upubliczniaj nieznanym swoich zdjęć, nie udzielaj zbyt wielu informacji na swój temat.
- Wszelkie próby zastraszania, czy cyberprzemocy zgłaszaj rodzicowi lub wychowawcy. Nie odpowiadaj na zaczepki.
- Jako rodzic/opiekun monitoruj jakie strony internetowe ogląda twoje dziecko. Istnieją programy blokujące treści z przemocą lub pornografią oraz systemowe narzędzia kontroli rodzicielskiej, jednak rozmowa z dzieckiem, wzajemne zaufanie i jasne zasady korzystania z sieci też są dobrym rozwiązaniem.
- Ustal ile czasu dziecko może spędzać przed ekranem komputera. Utrata kontroli nad czasem spędzonym w sieci czy w grze komputerowej przeistacza się szybko w uzależnienie.
- Monitoruj w co gra twoje dziecko! Symbole kategorii wiekowych PEGI powinny jasno odpowiedzieć na twoje pytanie, czy dana gra jest dla twojego dziecka.

Poniżej wstawiam odnośniki do bardziej obszernych poradników, gdzie znajdziecie Państwo nie tylko dokładniejsze opisy zagrożeń ale i porady jak uzyskać w razie problemów pomoc.

<https://akademia.nask.pl> - Poradnik dla rodziców - Jak zapewnić dzieciom bezpieczeństwo w internecie.

<https://bezpiecznaszkola.men.gov.pl> - Promujemy bezpieczeństwo w sieci

<https://www.gov.pl> – Dzień Bezpiecznego Internetu 2020

<https://cyfrowobezpieczni.pl> – Procedury bezpieczeństwa cyfrowego w szkołach