„Szkolne Zasady Bezpieczeństwa w Internecie”

ZSOiZ im. Jana Pawła II w Gromniku

Ogólne zasady korzystania z Internetu w ZSOiZ:

1. Korzystanie ze szkolnego wi-fi jest bezpłatne.
2. Po wejściu do klasy, każdy uczeń odkłada ściszony lub wyłączony telefon do specjalnie przygotowanych kieszonek z numerkami, a po skończonej lekcji przed wyjściem z klasy każdy zabiera swój telefon.
3. Uczeń może korzystać z Internetu w czasie lekcji na wyraźną prośbę nauczyciela.

Bezpieczeństwo dot. osobistych danych:

1. Nie udostępniaj przypadkowo poznanym osobom w sieci swojego numeru telefonu, nazwiska, adresu itp. Nigdy nie wiesz kto i w jakim celu będzie próbował je wykorzystać.
2. Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich. Można je podawać tylko w takich serwisach, w przypadku których przeglądarka wyświetla ikonę kłódki.

Bezpieczeństwo dot. poczty elektronicznej:

1. Używaj oprogramowania zabezpieczającego przed spamem dla każdego posiadanego adresu e-mail.
2. Wystrzegaj się nieoczekiwanych lub podejrzanych wiadomości e-mail, bez względu na to, kto jest nadawcą. W przypadku takich wiadomości nie należy nigdy otwierać załączników ani klikać znajdujących się w nich łączy.

3. Uważaj na wiadomości z prośbą o podanie szczegółów konta (banki i inne instytucje finansowe bardzo rzadko proszą o podanie takich szczegółów drogą elektroniczną).
4. Nie przesyłaj pocztą elektroniczną informacji dotyczących danych finansowych.
5. Nigdy nie podawaj komuś swojego hasła i postaraj się, aby to które posiadasz, było mało przewidywalne. (data urodzenia, inicjały ulubionego wokalisty itp.)

Bezpieczeństwo dotyczące przeglądania stron internetowych i pobierania programów z Internetu:

1. Należy korzystać z usług oceniających reputację stron, aby mieć pewność, że odwiedzany serwis internetowy nie stwarza żadnych zagrożeń.
2. Uważaj na strony internetowe, które wymagają instalacji oprogramowania.
3. Pamiętaj aby skanować wszystkie programy pobierane z Internetu za pomocą aktualnego oprogramowania zabezpieczającego.
4. Zawsze czytaj umowy licencyjne i jeżeli razem z daną aplikacją mają być zainstalowane inne „programy", przerwij proces instalacji.
5. Używaj programów antywirusowych i antyspamowych i nie zapomnij włączyć opcji update'owania tych programów. Aktualizacja na bieżąco chroni Twój komputer przed najnowszymi wirusami, które pojawiają się codziennie.
6. Unikaj stron, które oferują niesamowite atrakcje (pieniądze, darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) - często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.