



## DRODZY UCZNIOWIE,

Spędzając czas przed monitorem komputera lub smartfon'a należy zadbać o nasze bezpieczeństwo i bezpieczeństwo danych przechowywanych i przekazywanych za pośrednictwem mediów elektronicznych i sieci Internet. Na wstępie jednak należy zapoznać się z typowymi zagrożeniami spotykanymi w sieci.

- Wyłudzenia danych logowania i przejęcie konta, czasem kradzież tożsamości.
- Kontakty z osobami mającymi niewłaściwe intencje w stosunku do nas lub naszej własności.
- Dostęp do niewłaściwych treści.
- Utrata danych spowodowana zawirusowaniem komputera.
- Uzależnienie od treści internetowych lub gier komputerowych.
- Narażenie się na falę hejtu
- Nakłanianie do niewłaściwych zachowań w formie „wyzwań internetowych”

## ZASADY, KTÓRYCH WARTO PRZESTRZEGAĆ

- Nie podawać nikomu (nawet przyjacielowi) danych dostępowych do kont i aplikacji
- Nie podawać w sieci danych osobowych nawet znanym nam osobom tj. adres, nazwisko, data urodzenia, numer telefonu. Znane są przypadki podszywania się pod inne osoby w celu wyłudzenia danych.

- Wszędzie gdzie jest to możliwe korzystać z możliwości podwójnej autoryzacji poprzez kod wysłany za pomocą wiadomości sms lub kod wygenerowany w zewnętrznej, zintegrowanej z kontem aplikacji.
- Nie rozmawiać na kanałach przeznaczonych do rozmów z osobami nieznanymi i pod żadnym pozorem nie udostępniać im swoich danych czy zdjęć.
- Nie odwiedzać stron z niedozwoloną treścią, ponieważ właśnie na tych stronach często znajdują się wirusy i robaki internetowe, które mogą doprowadzić do zniszczenia danych, wykradzenie danych logowania czy zaszyfrowania dysku.
- Wyznaczenie sobie zasad i czasu korzystania z komputera i smartphona w celu uniknięcia uzależnienia, które już jest leczone w specjalnych ośrodkach dla dzieci i młodzieży uzależnionej od gier i multimediiów.
- Korzystanie tylko z komputera wyposażonego w oprogramowanie antywirusowe.
- Niekorzystanie z sieci wi-fi publicznych, ogólnodostępnych.
- Instalowanie oprogramowania wyłącznie z legalnego i znanego źródła.
- Bardzo oszczędne i rozważne udzielanie się w mediach społecznościowych w celu nienarażania się na hejt i niepoddawanie się presji hejtowania innych w sieci.
- Niepoddawania się presji i odmawianie udziału w „wyzwaniach” internetowych nawet tych, które z pozoru nie są groźne.
- W sytuacjach trudnych zawsze należy prosić o pomoc lub radę rodzica, nauczyciela, ewentualnie skorzystać z telefonu zaufania 116 111 lub telefonu dotyczącego bezpieczeństwa w sieci 800 100 100.