

BEZPIECZEŃSTWO W SIECI



Szkoła Podstawowa nr 29 Leonardo w Gdańsku

- Współcześnie Internet jest głównym medium umożliwiającym kontakty międzyludzkie **i to przede wszystkim kompetencje społeczne (nabywane z wiekiem i doświadczeniem życiowym), a nie kompetencje techniczne są kluczowe dla zachowania bezpieczeństwa w sieci**. Dlatego też dorośli nie powinni w żadnym wypadku wycofywać się i pozostawiać dzieci i młodzież w Internecie samym sobie, ale muszą mądrze towarzyszyć im w poznawaniu wirtualnego świata.



ZASADY KORZYSTANIA Z INTERNETU

BEZPIECZEŃSTWO W SIECI

ZABEZPIECZ SWÓJ
KOMPUTER

NIE PODAWAJ
SWOICH
DANYCH

NIE WCHODŹ NA STRONY
DLA CIEBIE
NIE PRZEZNACZONE

NIE UMAWIAJ SIĘ
Z OSOBAMI POZNANYMI
PRZEZ INTERNET

NIE UFAJ OSOBOM
POZNANYM W SIECI

NIE PODAWAJ NIKOMU
SWOJEGO HASŁA

POINFORMUJ RODZICÓW,
JEŚLI COŚ JEST NIE TAK

NIE KLIKAJ
W NIEZNANE
ODNOŚNIKI



ZAGROŻENIA W INTERNECIE

Zagrożenia w Internecie

Cyberprzemoc

Uzależnienie

Niebezpieczne treści (przemoc)

Łamanie prawa (hazard)

Kradzież danych osobowych

Włamania komputerowe

Zagrożenia techniczne (wirusy)

Wyłudzenie poufnych informacji

NIEBEZPIECZNE TREŚCI

- W pierwszej kolejności w tej kategorii wymieniane są materiały, które mimo prawnych zakazów ciągle są w bardzo łatwy sposób dostępne także dla niepełnoletnich użytkowników. Niebezpieczne treści obejmują także przemoc i rasizm oraz przekazy promujące zachowania autodestrukcyjne.



NIEBEZPIECZNE KONTAKTY

- Internet umożliwia nawiązywanie nowych znajomości i łatwe znajdowanie ludzi o podobnych zainteresowaniach czy poglądach. Jest to jedna z jego ważnych funkcji, ale także tutaj może dochodzić do nadużyć.
- Zjawisko tzw. *groomingu* czyli uwodzenia dzieci i młodzieży w Internecie w celu późniejszego ich wykorzystania zalicza się do najczęstszych zjawisk zaobserwowanych w środowisku wirtualnym



CYBERPRZEMOC

- **Cyberprzemoc** jest przemocą poprzez użycie mediów i elektroniki. Objawia się głównie za pomocą Internetu przy użyciu np. telefonów komórkowych, kamer wideo, aparatów fotograficznych, a szczególnie komputerów. Tak nie wiele potrzeba, a jak bardzo można zaszkodzić. Choć wygląda na przemoc nie groźną, często ma bardzo poważne skutki.



RODZAJE CYBERPRZEMOCY

Najpopularniejsze z nich to:

- publikowanie poniżających filmów lub zdjęć;
- publikowanie ośmieszających, wulgarnych, komentarzy i postów;
- włamania na konta serwisów społecznościowych;
- flood, czyli wiadomościami w komunikatorze, telefonami, SMSami;
- podszywanie się pod inne osoby;
- wykluczanie z internetowych społeczności



HEJT

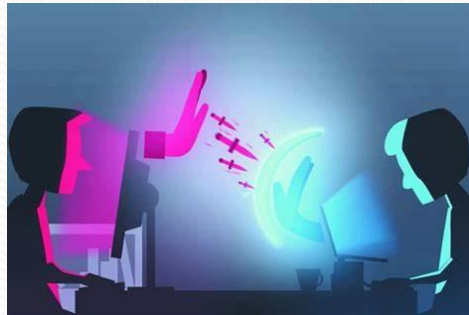
- Pozornie delikatniejszą formą cyberprzemocy jest hejt. Może polegać na umieszczeniu nienawistnego komentarza, obrazka, filmu czy udostępnieniu takiej treści.



HEJT 

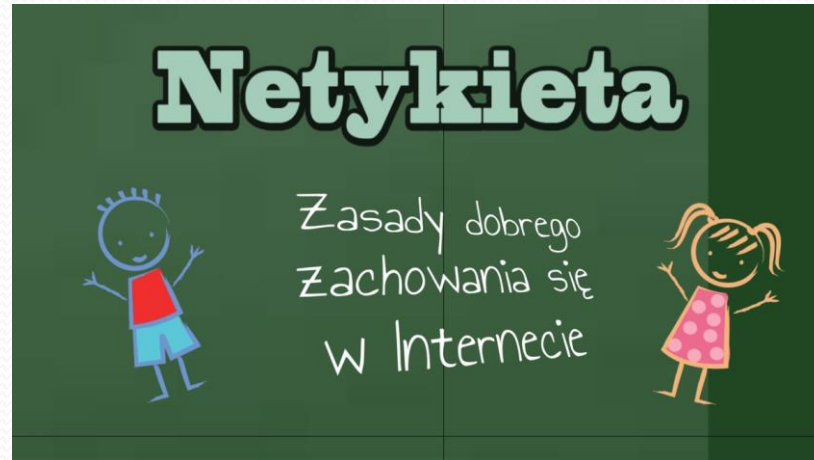
TROLL

- Unikanie rozmowy z „trollem”. Troll to użytkownik Internetu, który rozpoczyna dyskusje z innymi internautami, po to aby ich zdenerwować lub obrazić. Umieszcza w sieci kontrowersyjne, szokujące lub nieprzyjemne treści. Zasada postępowania jest prosta „**nie karmić trolla**”, czyli nie wchodzić z nim w żadną rozmowę.



NETYKIETA

- Netykieta to zasady dobrego zachowania w Internecie. Netykieta została stworzona przez internautów, aby ułatwić wszystkim bezpieczniejsze korzystanie z sieci.



10 ZASAD

1. Korzystaj z oprogramowania antywirusowego.
2. Otwieraj wiadomości tylko od znanych osób.
3. Ostrożnie pobieraj pliki z sieci.
4. Unikaj klikania w nieznane linki i załączniki w wiadomościach e-mail.
5. Nie podawaj w sieci danych osobowych, haseł, nie wysyłaj swoich zdjęć.
6. Chronź swoje konta na serwisach społecznościowych.
7. Stosuj trudne do odgadnięcia hasła, które są kombinacją liter i cyfr.
8. Czytaj regulaminy,
9. Sprawdzaj, czy strona, do której się logujesz, ma zabezpieczenia.
- 10. Pamiętaj, że osoba po drugiej stronie nie musi być tym, za kogo się podaje.**



PAMIĘTAJ!

Bezpieczeństwo w Internecie



Nie ufaj
osobom poznanym
w Sieci!

Zabezpiecz
swój
komputer!



Mów jeśli coś
Cię zaniepokoi!



Nie podawaj
swoich
danych!