

Poradnik

Bezpieczne i odpowiedzialne korzystanie z zasobów dostępnych w sieci

**Praca wspólna uczniów biorących udział w projekcie
"Cyberbezpieczniacy w escape roomie"**

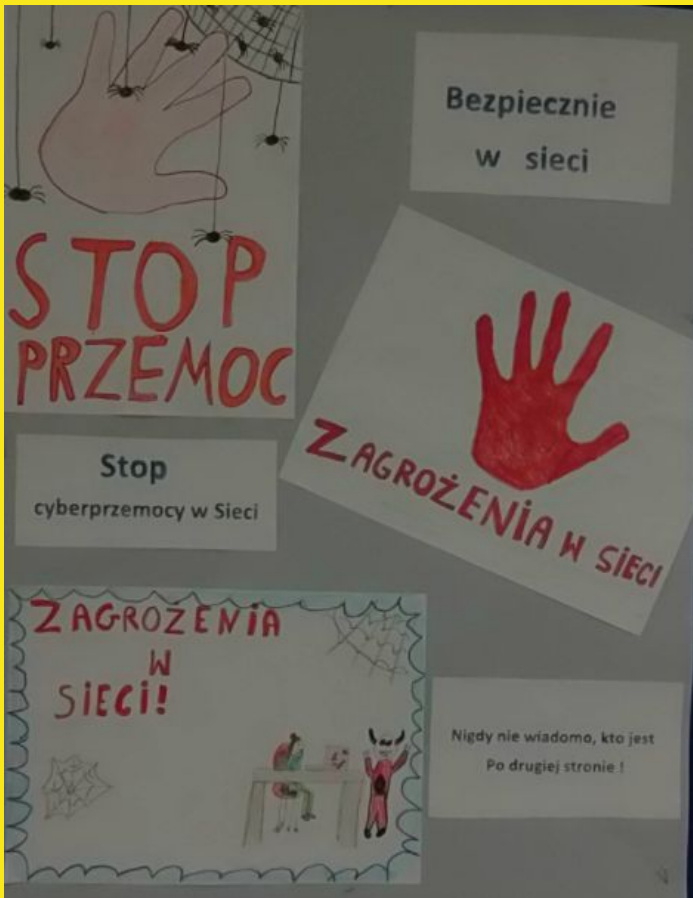
Internet to skarbnica wiedzy,
ale pamiętaj:

Nie wszystkie informacje,
które w nim znajdziesz muszą
być prawdziwe!

**Staraj się zawsze sprawdzić
wiarygodność informacji
w kilku
źródłach**

***Sprawdź
w wielu
źródłach***





- **Hasła, których używasz powinny być trudne do odgadnięcia**
- **Limituj czas, który spędzasz przy komputerze**
- **Przestrzegaj zasad netykiety**
- **Szanuj prawa autorskie udostępnianych w sieci plików**
- **Nigdy nie podawaj prawdziwych danych - używaj nicków**
- **Zgłaszaj włamania i przejęcia kont internetowych**
- **Unikaj klikania nieznanymi linków i załączników**

Znajomi z Internetu

*“Nie każdy jest tym,
za kogo się podaje”*

*Nigdy nie można mieć pewności
w stosunku do osób poznanych
w Internecie, kim tak naprawdę są.*



Pamiętaj!

Nie podawaj swoich danych osobowych.

Nie wysyłaj swojego zdjęcia.

*Nie umawiaj się na spotkania z osobą, którą
znasz tylko z sieci.*



Przykład dobrego hasła:

CH@ma\$is7x

Jak zapamiętać takie hasło?

Po prostu. **Ułóż z nim zdanie.**



***Zabezpiecz swój komputer hasłem i programem antywirusowym.**

***Pamiętaj by zmieniać hasło co najmniej raz na 3 miesiące.**

***Nie udostępniaj nikomu swojego hasła.**

*** Twoje hasło powinno być kombinacją dużych i małych liter, cyfr i znaków specjalnych.**

Zainstaluj oprogramowania filtrujące treści!

Aby unikać zagrożeń internecie i korzystać z niego w bezpieczny sposób, należy stosować oprogramowania ochrony rodzicielskiej, który ogranicza dostęp na strony które mogą nieść dla dziecka zagrożenie.

Przykładowe programy do ochrony rodzicielskiej:

1. *Beniamin*
2. *Opiekun dziecka w internecie*
3. *Kurupira Web Filter*

Ponadto warto stosować programy do blokady wyskakujących reklam np. Adblock

FOMO

(ANG. FEAR OF MISSING OUT)

FOMO to zjawisko, które może dotknąć każdego, niezależnie od wieku.

Przez FOMO określamy lęk przed odłączeniem od internetu, obawa przed wypadnięciem z obiegu, potrzeba ciągłego trzymania ręki na pulsie bieżących wydarzeń.



CZAS NA JOMO

W założeniu JOMO mamy czerpać radość z tego, że widzimy mniej. Zakłada ograniczenie niepotrzebnych informacji, social mediów. JOMO pozwala na spowolnienie swojego życia i czerpania radości realnych, nie wirtualnych.

Szkoła Podstawowa z Ol im. Wojciecha Kętrzyńskiego nr 2 w Szczytnie

Uważaj co udostępniasz!

Nie zamieszczaj

- obraźliwych komentarzy
#komentuj. **Nie obrażaj**
- przykrych postów
- zdjęć, na których są inne osoby, a nie masz zgody na publikację

W INTERNECIE
NIE JESTEŚ
ANONIMOWY

Szanuj innych w sieci

Pamiętaj, by traktować innych z szacunkiem. Swoje zdanie wyrażaj, nie obrażając nikogo. Nie reaguj agresją na agresję.



Mów jeśli coś jest nie tak!

Jeśli coś zaniepokoi Cię w Internecie,
koniecznie powiedz o tym
osobie dorosłej np. rodzicowi
lub nauczycielowi!

Możesz też zadzwonić pod bezpłatny
numer zaufania dla dzieci i młodzieży

116 111



**Szkoła Podstawowa nr 16 z Oddziałami integracyjnymi
im. Orłów Lwowskich w Przemyślu**

Korzystaj z umiarem z Internetu!



Domowe zasady ekranowe:
Home



Prawo autorskie obowiązuje również w internecie.


Jeśli korzystasz ze źródła internetowego, to podaj autora i link do strony z której korzystasz.

W ten sposób szanujemy pracę innych osób.

**Warto
zapamiętać!**

**Szkoła Podstawowa nr 5 im. Romualda Traugutta w Poznaniu-
Goreta Siadak**

Czytaj uważnie regulaminy stron



UWAŻNIE CZYTAJ REGULAMINY STRON

- Należy uważnie czytać regulaminy, ponieważ gdzieś może się pojawić mała wzmianka, że np. korzystając z usług danej strony zobowiązujemy się do cotygodniowych przelewów na konto administratora strony

Czytanie regulaminów powinno być ważnym punktem rejestrowania się na każdą stronę.

UWAGA - WIRUSY!

Przeglądanie internetu nie zawsze jest w pełni bezpieczne. Oprócz informacji znajduje się w nim bowiem wiele zagrożeń.

Jednym z nich są **wirusy** komputerowe mogące wyrządzić znaczne szkody nieświadomym internautom.



Ochronę przed nimi zapewniają programy **antywirusowe**. Zapewniają one ochronę przed wieloma rodzajami szkodliwego oprogramowania. Pamiętaj o aktualizacji antywirusa!

SEKSTING- wysyłanie intymnych zdjęć
Pamiętaj, że zdjęcia pozostają w Internecie
na zawsze!

Uzależnienie od Internetu i komputera
Pamiętaj, że życie realne jest ciekawsze niż
wirtualne!

PHISHING- podawanie się za inną osobą w celu
wyłudzenia danych osobowych

Nie udostępniaj swoich danych!

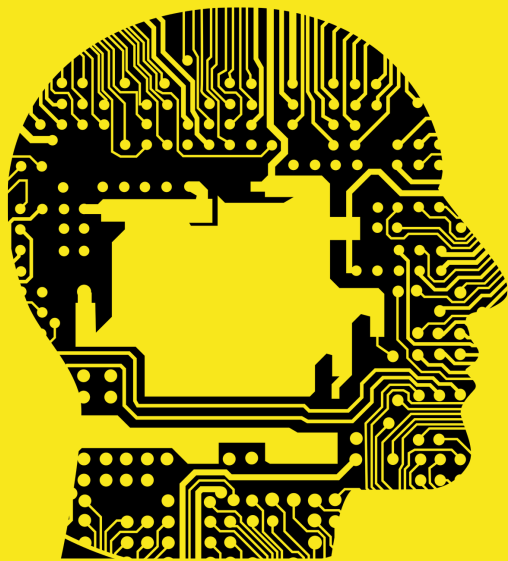


**Hejt- obrażanie innych
użytkowników w Internecie**
Kozak w Internecie, słaby w świecie!

Wirusy!
Zawsze instaluj program
antywirusowy!

Nie pobieraj plików z nielegalnych źródeł!
Korzystaj z otwartych zasobów internetowych
(licencja creative commons)

Jak bezpiecznie pobrać pliki?



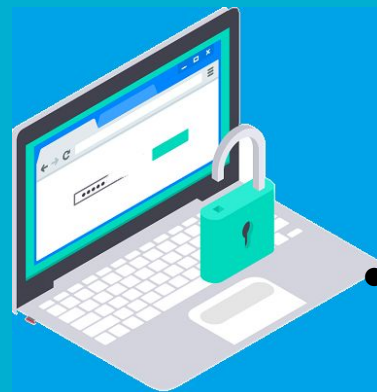
- Aktualizuj regularnie programy antywirusowe;
- Używaj bezpiecznego serwera proxy (VPN);
- Wybieraj zaufane źródła;
- Odwiedzaj oficjalną stronę autora lub producenta;
- Korzystaj z popularnych, sprawdzonych witryn (np. dobreprogramy.pl; instalki.pl)

Cracking

Cracking jest działalnością o charakterze przestępczym. Crackerzy angażują się w taką działalność, jak wykradanie numerów kart kredytowych, instalacja wirusów, niszczenie plików lub gromadzenie danych osobowych w celu ich sprzedaży.

Zabezpiecz się przed Crackingiem

- Nie otwieraj żadnych załączników, które zostały wysłane z podejrzanych adresów e-mail.
- Nigdy nie wysyłaj przez e-mail swoich danych logowania do bankowości ani szczegółów dotyczących kart kredytowych.
- Nie korzystaj z publicznych sieci Wi-Fi w przypadku czynności, które wymagają poufności.



1. WIZERUNEK PODLEGA OCHRONIE PRAWNEJ

**PAMIĘTAJ O OCHRONIE WIZERUNKU
OCHRONĘ PRAWNĄ WIZERUNKU PRZEWIDUJĄ
PRZEPISY PRAWA. CHRONIĄ ONE WIZERUNEK W
SYTUACJI, GDY DOSZŁO DO NIEPRAWIDŁOWOŚCI
POPRZEZ JEGO ROZPOWSZECHNIENIE BEZ ZGODY
OSOBY PORTRETOWANEJ.**

**KODEKS CYWILNY CHRONI WIZERUNEK, UZNAJĄC
GO ZA JEDNO Z DÓBR OSOBISTYCH CZŁOWIEKA.
ZAKAZUJE ON POD GROŹBĄ KARY, PODSZYWANIA
SIĘ POD INNĄ OSOBĘ ORAZ WYKORZYSTYWANIA
JEJ WIZERUNKU LUB INNYCH JEJ DANYCH
OSOBOWYCH W CELU WYRZĄDZENIA JEJ SZKODY
MAJĄTKOWEJ LUB OSOBISTEJ. JEST TO TZW.
KRADZIEŻ TOŻSAMOŚCI, OPISANA W ART.
190A PAR 2 KK.**



Rodzaje szkodliwych treści w sieci:

- ❖ pornografia,
- ❖ przemoc,
- ❖ wulgarność,
- ❖ rasizm i ksenofobia,
- ❖ sekty i inne formy psychomanipulacji,
- ❖ używki,
- ❖ broń i hazard.



Zespół Placówek Oświatowych nr 2 w Mławie