

Niebezpieczeństwa w sieci

I jak się przed nimi chronić

```
... object to mirror_mod.mirror_object
operation == "MIRROR_X":
    mirror_mod.use_x = True
    mirror_mod.use_y = False
    mirror_mod.use_z = False
operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True
```

```
... selection at the end -add
... _ob.select= 1
... _ob.select=1
... context.scene.objects.active
... ("Selected" + str(modifier.name))
... mirror_ob.select = 0
... bpy.context.selected_objects
... data.objects[one.name].select
... print("please select exactly one mirror")
... OPERATOR CLASSES ----
```

```
... types.Operator):
... X mirror to the selected
... object.mirror_mirror_x"
... mirror X"
```

```
... context):
... context.active_object is not None
```

Jak chronić się przed wirusami?

Porady jak uniknąć zainfekowania komputera wirusem:

- Nie otwieraj nieznanych maili i linków
- Często wykonuj aktualizacje
- Sprawdzaj czy żadne nieznane Ci aplikacje lub programy nie działają w tle
- Nie wchodź na niezabezpieczone strony
- Nie otwieraj ani nie ściągaaj nieznanych plików z Internetu
- Jeżeli musisz coś pobrać, korzystaj tylko z zaufanych, zabezpieczonych stron

Najczęstsze objawy obecności wirusa na komputerze:

- Znaczne spowolnienie pracy komputera
- Nieuzasadnione wysokie wykorzystanie procesora
- Pojawiające się nieuzasadnione komunikaty i wyskakujące nagle okna
- Brak możliwości uruchomienia niektórych aplikacji
- Zniknięcie programu antywirusowego

Najlepsze bezpłatne programy antywirusowe:

- Avast
- McAfee
- Bitdefender
- TotalAV
- PC Protect
- Norton
- AVG
- Malwarebytes
- ScanGuard

Jak uniemożliwić wirusowi dostanie się do komputera?

- Stosowanie Firewall – zaporą ogniową (zapora ta blokuje wejście wszystkim wirusom i hackerom)
- Nie zwlekanie z aktualizacjami (większość wirusów omija zabezpieczenia przez brak najnowszych wersji systemu)

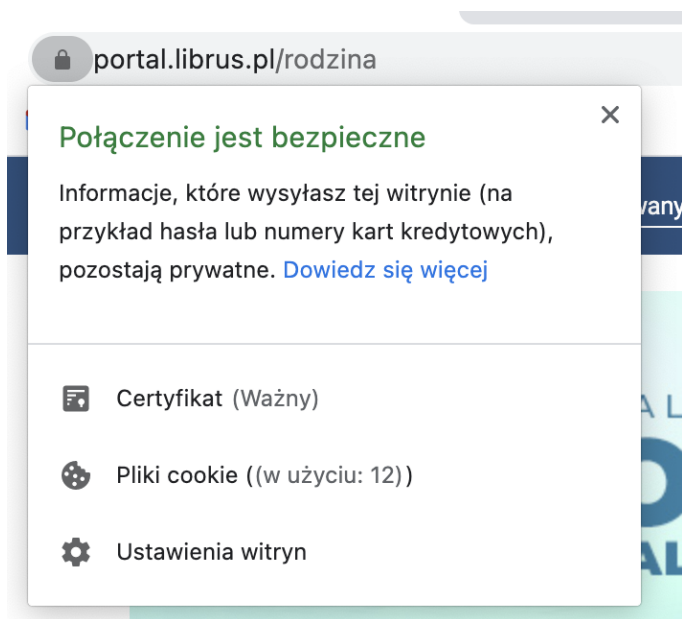
Nie wchodźcie w nieznane linki

Poprzez link można zrobić więcej niż tylko zainstalować komuś wirusa, ale również może zdobyć wasze dane i dostęp do waszych kont

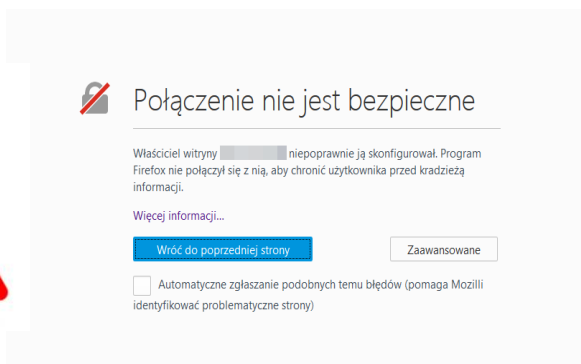


Jak unikać niebezpiecznych stron

1. Gdy otworzysz stronę, której nie jesteś pewien, najedź na kłódkę w lewym górnym rogu, i sprawdź czy połączenie jest bezpieczne.



2. Nie ignoruj powiadomień, które wysyła ci przeglądarka.



3. Nie akceptuj nieznanych ci treści.

Wraz z [zaufanymi partnerami IAB](#) i [innymi zaufanymi partnerami](#) przechowujemy i/lub odczytujemy informacje zawarte na Twoim urządzeniu, takie jak pliki cookie, przetwarzamy dane osobowe, takie jak unikalne identyfikatory, informacje przesyłane przez urządzenia końcowe niezbędne do personalizacji reklam i treści, udostępnienie funkcji mediów społecznościowych pomiaru ruchu jak również dla rozwoju i poprawy naszych produktów. Za Twoją zgodą my, jak i partnerzy możemy wykorzystywać precyzyjne dane geolokalizacyjne i identyfikację poprzez skanowanie urządzeń. Przechodząc do serwisu zgadzasz się na wskazane działania.

Możesz wyrazić zgodę na powyższe cele przetwarzania poprzez kliknięcie w przycisk "przejdź do serwisu", możesz również nie wyrażać zgody poprzez wybór ustawień zaawansowanych. W sytuacji braku zgody będziemy przetwarzać dane osobowe w innych celach na innych podstawach prawnych (informacje w tym zakresie dostępne są w naszej [polityce prywatności](#)). Poprzez kliknięcie w przycisk "ustawienia zaawansowane" możesz zarządzać swoimi preferencjami przed wyrażeniem zgody lub odmową udzielenia zgody. Cele przetwarzania Twoich danych bez konieczności uzyskania Twojej zgody w oparciu o uzasadniony interes Radio Muzyka Fakty Grupa RMF sp. z o.o. sp. k. oraz informacje o możliwości sprzeciwienia się takiemu przetwarzaniu znajdziesz w [polityce prywatności](#).

USTAWIENIA ZAAWANSOWANE

PRZEJDŹ DO SERWISU

Jak chronić nasze dane osobowe w Internecie ?

☐ NIE PODAWAJ SWOICH DANYCH!

-pamiętaj aby w sieci nie podawać swoich danych osobowych takich jak:
imię, nazwisko, adres, numer telefonu, numer szkoły i haseł do portali społecznościowych.

☐ NIE UFAJ OSOBOM POZNANYM W SIECI!

-nie zapomnij, że osoba poznana w Internecie niekoniecznie jest tym za kogo się podaje.

☐ MÓW JEŚLI COŚ JEST NIE TAK!

-bądź świadomy tego, że wokół ciebie są osoby które z chęcią ci pomogą. Jeżeli ktoś lub coś zaniepokoi cię w Internecie, koniecznie poinformuj o tym rodziców, wychowawcę lub inną zaufaną osobę dorosłą.

☐ WYLOGUJ SIĘ!

-nie zapomnij o tym aby, odchodząc od komputera wylogować się ze wszystkich portali na przykład: poczty, Messengera, Instagrama i innych. Jeśli o tym zapomnisz nieznajome osoby będą miały łatwy dostęp do twoich danych.

Emilia Jabłońska i Wiktoria Haręzga 8B

NIEZNAJOMI W INTERNECIE

- W większości przypadków są to osoby które mają złe zamiary wobec nas, wiele razy słyszano o starszych osobach podających się za naszych rówieśników albo o osobach chcących zhakować nam sprzęt, dlatego zawsze należy zachować ostrożność.

— + Skala automatyczna ▾

Kontakt z obcymi osobami w sieci



Na czym polega

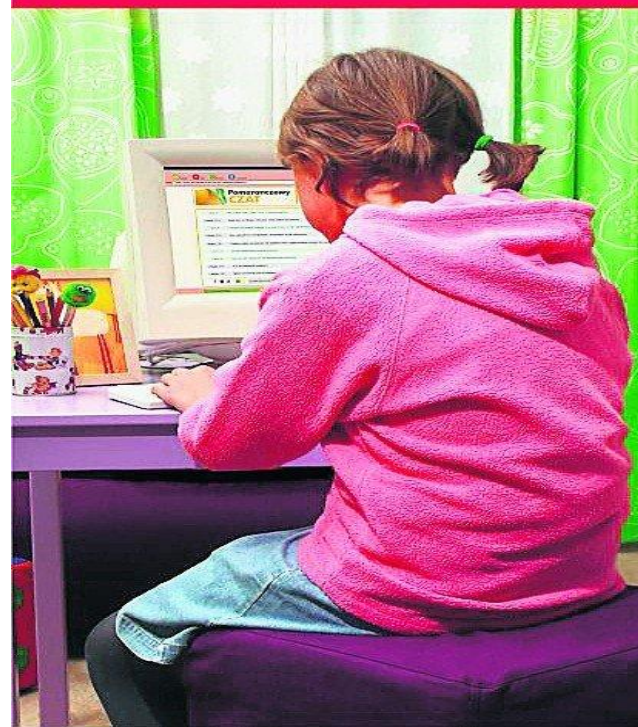
- 32 na 100 uczniów prowadziło rozmowy z obcą osobą
- 1 na 10 się z nią spotkał
- Obcy w sieci:
 - niektórzy mają złe intencje
 - inni mogą obrazić lub poniżyć dziecko



Co robić

- Powtarzać dzieciom, żeby nie rozpoczynały rozmów z nieznajomymi (SP 1-6)
- Pokazywać analogie do rozmów z obcymi na dworze
- Prosić o informowanie rodziców o każdej próbie nawiązania kontaktów przez nieznajomych
- Pozostawić możliwość spotkania w przypadku starszych dzieci
- Pozostawić możliwość spotkania:
 - w towarzystwie osoby dorosłej
 - w miejscu publicznym

<Ania>Hej! Jestem Ania.
Mam 12 lat.
Szukam przyjaciół.



<Wojtek>Cześć Aniu, tu
Wojtek też mam 12 lat.
Chętnie Cię poznam.





Jak być anonimowy w internecie? I co to VPN?

- VPN ->(wirtualna sieć prywatna) po jego zainstalowaniu IP twojego komputera będzie niewidoczne dla przypadkowych osób i będziesz bezpieczniejszy/a przeglądając przypadkowe strony internetowe. np: North VPN , SurfShark VPN.