BEZPIECZNI W SIECI Z OSEHERO

To nasz uczniowski biuletyn o tym, jak być bezpiecznym, mądrym i świadomym użytkownikiem internetu. Każdy temat opracowaliśmy samodzielnie - bo bezpieczeństwo zaczyna Sie od wiedzy.

osehero

ZESPÓŁ SZKÓŁ PONADPODSTAWOWYCH 2 im. Stanisława Staszica

Dlaczego bezpieczeństwo w sieci to nasza sprawa?

Internet to część naszego życia.
Uczymy się, rozmawiamy, bawimy i kupujemy online. Spędzamy w sieci nawet ponad 5 godzin dziennie, więc warto wiedzieć jak robić to bezpieczne

W internecie czyhają zagrożenia: fałszywe wiadomości, oszustwa, hejt czy kradzież danych. Dlatego każdy z nas powinien myśleć, zanim kliknie i dbać o swoją prywatność.

„Internet to nasze życie – więc musimy wiedzieć, jak się w nim chronić.

Nasz biuletyn „Bezpieczni w sieci z OSEhero" powstał, by pokazać, że bezpieczeństwo zaczyna się od wiedzy i odpowiedzialności.

📲 Zeskanuj QR kod i posłuchaj naszych podcastów o bezpieczeństwie online!

💻 Młodzież w Polsce spędza w internecie średnio 4–6 godzin dziennie, a w weekendy nawet więcej.

⚠️ Co piąty Polak (18%) przyznał, że padł ofiarą oszustwa w sieci.

📱 Ponad 50% młodych osób otrzymało podejrzane SMS-y lub wiadomości z próbą wyłudzenia danych.

🛒 31% użytkowników internetu spotkało się z oszustwem przy zakupach ounline

🗝️ Twoje hasło to klucz do świata - nie zgub go!

Mini poradnik: Jak tworzyć silne hasła

1. 🔒 Używaj min. 12 znaków (litery, cyfry, symbole).
2. 🔄 Łącz małe i duże litery.
3. 🚫 Unikaj oczywistych haseł („123456”, „hasło”).
4. 💭 Nie używaj tego samego hasła do wszystkiego.
5. 🧠 Korzystaj z menedżera haseł – łatwiej zapamiętasz.

5 zasad bezpiecznego hasła

- „Długość ma znaczenie”
- „Mieszaj znaki”
- „Nie ujawniaj nikomu”
- „Zmieniaj regularnie”
- „Używaj managera haseł“

Quiz: „Zgadnij, które hasło jest bezpieczne“

A) kotek123

B) P@ssW0rd!

C) Q!7xLk#29pR

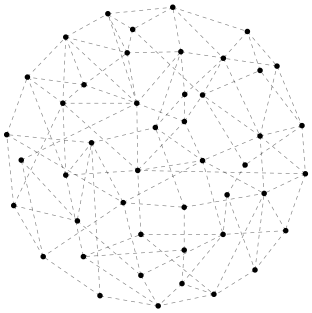
✳✳✳✳ 💡 *Które hasło jest najbezpieczniejsze?*

Chroń swoje dane - zaczynając od hasła!!

Phishing - jak nie złapać się na haczyk?

Przykłady fałszywych SMS-ów i maili (z opisem błędów):

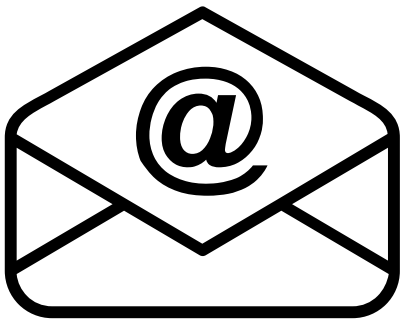
-Fałszywy SMS z linkiem do rzekomej przesyłki – zwróć uwagę na błędy językowe, dziwny adres strony lub nietypowy numer nadawcy.
Mail podszywający się pod bank – często zawiera prośbę o „natychmiastowe zalogowanie się", groźby zablokowania konta lub link do podejrzanej strony.
-Wiadomości z „nagrodami" lub „fakturami" – wyglądają profesjonalnie, ale adres nadawcy różni się od prawdziwego (np. „@bnk.pl" zamiast „@bank.pl").
-Wskazówka: zawsze sprawdzaj adres e-mail, link i ton wiadomości. Prawdziwe instytucje nigdy nie proszą o dane logowania przez SMS lub e-mail.

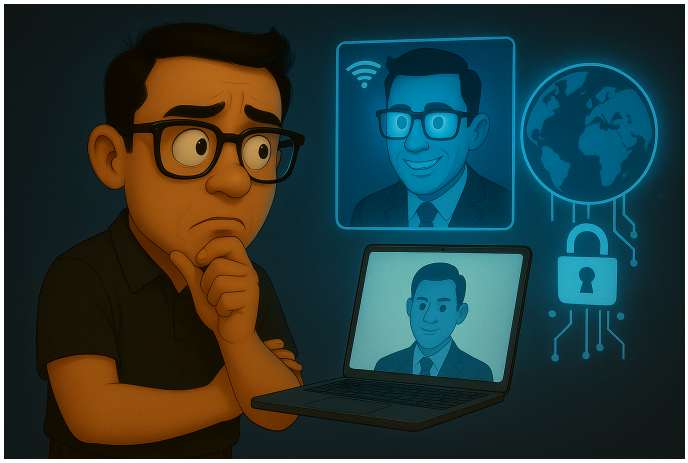


Poradnik: co robić, gdy klikniesz zły link:
Nie wpisuj żadnych danych! Natychmiast zamknij stronę. Zmień hasło do kont, które mogły być zagrożone (np. e-mail, bankowość).
Przeskanuj urządzenie programem antywirusowym.
Zgłoś incydent – np. w banku, w CERT Polska lub administratorowi IT (jeśli to komputer służbowy). Uważnie obserwuj swoje konta – czy nie pojawiają się nieautoryzowane logowania lub transakcje.

Ramka: „Czerwone flagi – czyli jak rozpoznać oszustwo"
Wiadomość budzi presję czasu („natychmiast", „ostatnia szansa").
Nadawca prosi o dane logowania, numer karty lub hasło.
Link prowadzi do dziwnej strony (np. z literówką w adresie).
Treść zawiera błędy językowe lub nietypowe formatowanie.
Oferta wydaje się „zbyt dobra, by była prawdziwa".

➡️ Zasada: jeśli masz choć cień wątpliwości – nie klikaj! Lepiej sprawdzić dwa razy niż dać się złapać na haczyk.





Co internet o tobie wie?

Ile zdradzasz o sobie w Internecie?

Jak często publikujesz swoje zdjęcia w mediach społecznościowych?

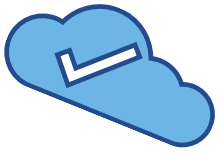
A. Prawie codziennie
B. czasami, np. z ważnych wydarzeń
C. Bardzo rzadko lub wcale

Czy masz publiczny profil dostępny dla wszystkich?

A. Tak, każdy może mnie znaleźć i zobaczyć moje posty
B. Częściowo – część treści jest publiczna, reszta prywatna
C. Nie, tylko znajomi widzą moje posty

Czy udostępniasz informacje o swoim miejscu pobytu (np. lokalizację, zdjęcia z wakacji na bieżąco)?

A. Tak, często
B. Czasami, ale raczej po fakcie
C. Nigdy – nie chcę zdradzać, gdzie jestem



Każde kliknięcie w internecie zostawia cyfrowy ślad – informacje o tym, co robisz online.
Aby chronić prywatność, warto sprawdzać ustawienia profili i udostępniać jak najmniej danych.
Pamiętaj: to, co trafia do sieci, zostaje tam na długo.

Promocja czy pułapka?

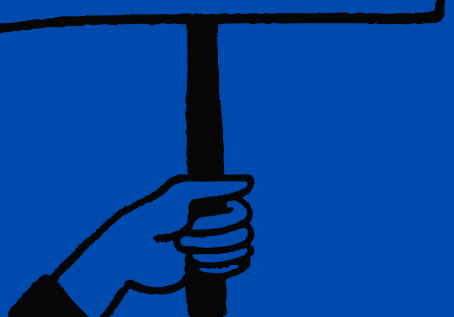
JAK SPRAWDZIĆ SKLEP INTERNETOWY?

1. *Poszukaj opinii – wpisz nazwę sklepu + „opinie” .*
2. *Sprawdź dane kontaktowe – legalne sklepy zawsze mają adres, NIP i możliwość zwrotu towaru.*
3. *Nie płać z góry nieznanym sprzedawcom – wybieraj płatność przy odbiorze lub przez zaufane systemy (np. PayU, Przelewy24).*

TOP STORY

Bartek dostał link do „płatności” za telefon i wpisał dane jak w banku.
Strona była fałszywa – stracił pieniądze.
➡️ Wniosek: Nigdy nie rób przelewu z linku – wejdź sam na stronę banku.

📊 Ciekawostka:
W 2024 roku aż 40% oszustw online dotyczyło fałszywych sklepów.



Nie hejtuj, reaguj!

🚫 STOP HEJTOWI I CYBERPRZEMOCY! 💻💬

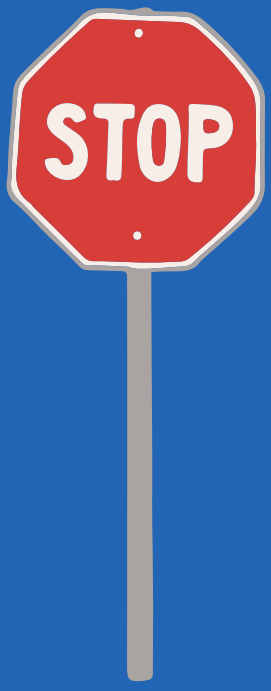
HEJT
To złośliwe, obraźliwe lub poniżające komentarze i zachowania wobec innych w internecie
Nie krytyka – to atak

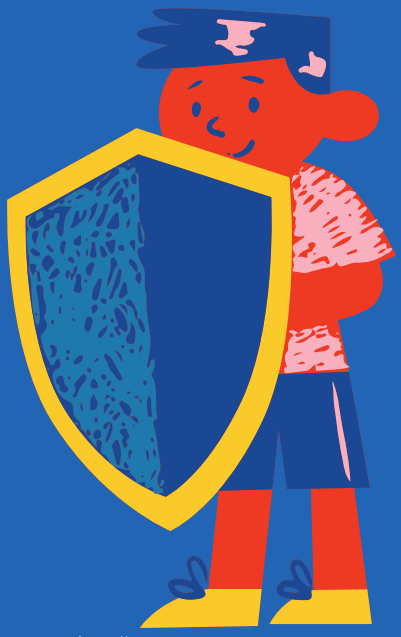
CYBERPRZEMOC
To krzywdzenie innych za pomocą technologii – np. wysyłanie obraźliwych wiadomości, publikowanie kompromitujących zdjęć czy rozprzestrzenianie plotek online

💡 PAMIĘTAJ
Słowa też potrafią ranić
Zanim klikniesz „wyślij" – pomyśl!

Gdzie szukać pomocy?

💬 Helpline.org.pl – wsparcie online w sprawach hejtu i cyberprzemocy.
📞 116 111 – telefon zaufania dla dzieci i młodzieży, 24/7.
👩 Porozmawiaj z kimś dorosłym, komu ufasz – nie jesteś sam!





Wypowiedzi uczniów: jak reagować

- „Gdy widzę hejt – nie udaję, że nic się nie dzieje. Zgłaszam to!"
- „Wspieram osobę, którą ktoś obraża. Wystarczy jedno dobre słowo."
- „Robię zrzut ekranu i zgłaszam hejt dorosłym lub na platformie."
- „Nie odpisuję agresją na agresję. Lepiej zachować spokój."
- „Pamiętam, że każdy zasługuje na szacunek – także w sieci."

Wirusy trojany i inne potwory- złośliwe oprogramowania jak sie przed tym bronic?

Jak przebiega atak wirusów komputerowych?

1. **Zakażenie systemu**
2. Wirus trafia do komputera np. przez:
   - zainfekowany załącznik e-mail,
   - pobrany plik lub program z niepewnego źródła,
   - zainfekowany pendrive lub inne urządzenie,
   - fałszywe aktualizacje i reklamy (malvertising).
3.
4. **Aktywacja wirusa**
5. Użytkownik nieświadomie uruchamia zainfekowany plik (np. klikając w dokument, link lub instalator).
6. W tym momencie wirus zaczyna działać w tle.
7. **Rozprzestrzenianie się**
8. Wirus kopiuje się do innych plików, folderów lub komputerów w sieci lokalnej.
9. Może też pobierać dodatkowe złośliwe oprogramowanie.
10. **Działanie szkodliwe (atak właściwy)**
11. Wirus może:
    - usuwać lub szyfrować pliki,
    - spowalniać system,
    - szpiegować użytkownika,
    - otwierać dostęp zdalny dla hakera.
12.
13. **Ukrywanie śladów**
14. Niektóre wirusy potrafią się maskować (np. jako systemowe procesy), by trudniej je było wykryć przez antywirusa.

Jak się przed tym bronić?

✅ Zainstaluj program antywirusowy i regularnie go aktualizuj.
✅ Aktualizuj system operacyjny i wszystkie programy — szczególnie przeglądarkę i dodatki.
✅ Nie otwieraj podejrzanych załączników ani linków z e-maili lub komunikatorów.
✅ Pobieraj oprogramowanie tylko z oficjalnych stron i sklepów.
✅ Wykonuj regularne kopie zapasowe (backup) ważnych danych.
✅ Nie korzystaj z pirackiego oprogramowania — często zawiera wirusy.
✅ Zachowaj ostrożność przy podłączaniu obcych pendrive'ów.
✅ Używaj zapory sieciowej (firewalla) i silnych haseł.
✅ Włącz ochronę w czasie rzeczywistym w programie antywirusowym.

TWOJE ZDJĘCIA TWOJA ODPOWIEDZIALNOŚĆ

ZASADY PUBLIKOWANIA ZDJĘĆ

1. Podstawa prawna
2. Zasada zgody
3. Wyjątki od obowiązku uzyskania zgody
4. Obowiązek informacyjny (RODO)
5. Zasady bezpieczeństwa i publikacji
6. Prawa osób na zdjęciach
7. Procedura usuwania zdjęć
8. Zgody rodziców / opiekunów
9. Rekomendacje praktyczne

JAK USTAWIĆ PRYWATNOSC NA TIK TOKU I INSTAGRAMIE

1.Otwórz Instagram.

2.Przejdź do swojego profilu → kliknij ≡ (menu) → Ustawienia i prywatność.

3.W sekcji Prywatność konta włącz Konto prywatne.

✅ Tylko zaakceptowani obserwujący zobaczą Twoje posty i relacje.

1.OTWÓRZ APLIKACJĘ TIKTOK.

2.WEJDŹ W PROFIL → ≡ (TRZY KRESKI W PRAWYM GÓRNYM ROGU).

3.WYBIERZ USTAWIENIA I PRYWATNOŚĆ → PRYWATNOŚĆ.

4.WŁĄCZ OPCJĘ KONTO PRYWATNE.

✅ TYLKO OSOBY, KTÓRE ZAAKCEPTUJESZ, BĘDĄ MOGŁY CIĘ OBSERWOWAĆ I OGLĄDAĆ TWOJE FILMY.

Nie wierz we wszystko co widzisz

Jak działa dezinformacja?
Dezinformacja to celowe wprowadzanie ludzi w błąd, by wpłynąć na ich opinie, emocje lub decyzje. W sieci rozchodzi się błyskawicznie, bo wiele osób udostępnia informacje bez sprawdzenia ich źródła.

Najczęstsze techniki manipulacji:
Clickbaitowe nagłówki 📣
Fałszywe zdjęcia lub filmy 🎭
„Eksperci", którzy nie istnieją 🧍‍♂️
Mieszanie prawdy z fałszem ⚖️

1.„Jeśli coś jest popularne w internecie, to znaczy, że to prawda." → ❌ Fałsz! Popularność nie oznacza wiarygodności.
2.„Każdy może opublikować dowolną informację w sieci." → ✅ Prawda! Dlatego warto sprawdzać źródła.
3.„Niektóre fałszywe informacje wyglądają bardzo profesjonalnie." → ✅ Prawda! Manipulatorzy używają logotypów i układu przypominającego prawdziwe media

Kto i po co zbiera twoje dane?

Pliki cookies – to małe pliki, które strony internetowe zapisują w Twojej przeglądarce. Dzięki nim strony „pamiętają" Twoje logowanie, język, zawartość koszyka czy ostatnio oglądane produkty. Ale nie tylko! Cookies pomagają też firmom śledzić Twoje zachowania w sieci – co czytasz, co lubisz i w co klikasz. Na tej podstawie tworzone są profile użytkowników, które służą do wyświetlania spersonalizowanych reklam.

Jak przepływają nasze dane:
Ty → strona internetowa → serwery reklamowe → firmy analizujące dane → reklamodawcy.
Twoje dane krążą między wieloma firmami – to właśnie dlatego po obejrzeniu butów w jednym sklepie, widzisz reklamy tych samych butów na innej stronie.

Po co to wszystko?
Firmy chcą lepiej poznać użytkowników, by sprzedawać więcej i skuteczniej. Twoje dane to wartość rynkowa – im więcej o Tobie wiedzą, tym precyzyjniej mogą Ci coś „podsunąć".

Jak ograniczyć śledzenie i chronić swoją prywatność:

- Wejdź w ustawienia przeglądarki i ogranicz lub blokuj pliki cookies (zwłaszcza cookies stron trzecich).
- Korzystaj z trybu prywatnego (incognito), który nie zapisuje historii ani ciasteczek.
- Zainstaluj rozszerzenia blokujące reklamy i śledzenie – np. uBlock Origin, Privacy Badger, DuckDuckGo Privacy Essentials.
- Regularnie czyść historię przeglądania, cookies i pamięć podręczną.
- Nie loguj się do konta Google czy Facebooka na każdej stronie – w ten sposób łączą Twoje dane z różnych miejsc.

ZOSTAŃ CYFROWYM BOHATEREM

Cyfrowy bohater to ten, kto klika z głową, a nie z przyzwyczajenia.

Dzięki projektowi „Bezpieczni w sieci z OSEhero" wiemy, że kliknięcie może chronić lub szkodzić. Wybór należy do nas.

W biuletynie „Bezpieczni w sieci z OSEhero" znalazły się najważniejsze informacje o tym, jak chronić siebie i swoje dane w internecie. Poruszono tematy silnych haseł, phishingu, cyfrowego śladu, hejtu, fake newsów oraz bezpiecznych zakupów online. Uczniowie wyjaśnili też, czym są wirusy, jak dbać o prywatność i co zrobić, by unikać cyberzagrożeń. Całość pokazuje, że bezpieczeństwo w sieci zaczyna się od wiedzy i świadomych decyzji każdego użytkownika.