
Twoje Dane,
Twoja Sprawa.
NOTIFICATION
Akademia Młodych Detektywów:
Jak bezpiecznie poruszać się w cyfrowym świecie.
Cel misji:
Rozpoczęcie szkolenia!
TWOJE DANE
TWOJA SPRAWA
Moje natum
tost koże
zo temost!
Zamier jakopi


Jasna Strona: Możliwości
Jeden Internet. Dwie twarze. Dobry detektyw potrafi poruszać się po obu.
Ciemne Zaułki: Zagrożenia
Nauka, Pasje, Rozrywka, Znajomi
Oszuści, Kradzież danych, Kłamstwa, Utrata prywatności

ZASADA NR 1: REGUŁA SZCZOTECZKI DO ZĘBÓW

=

NIE POŻYCZAJ!

1. Sprzęt z dostępem do sieci jest osobisty.
2. Używasz go tylko Ty.
3. Nigdy nie loguj się na swoje konta przez cudze urządzenia!

Konstrukcja Cyfrowej Kłódki. Jak zbudować hasło nie do złamania?

Małe i duże LITERY

Nieoczywiste CYFRY

Tajne SYMBOLE (@, #, !, *)

RÓŻNE KONTA = RÓŻNE HASŁA.

Jeśli złodziej otworzy jedną szufladę z grą, nie dostanie się do Twojej poczty i banku!

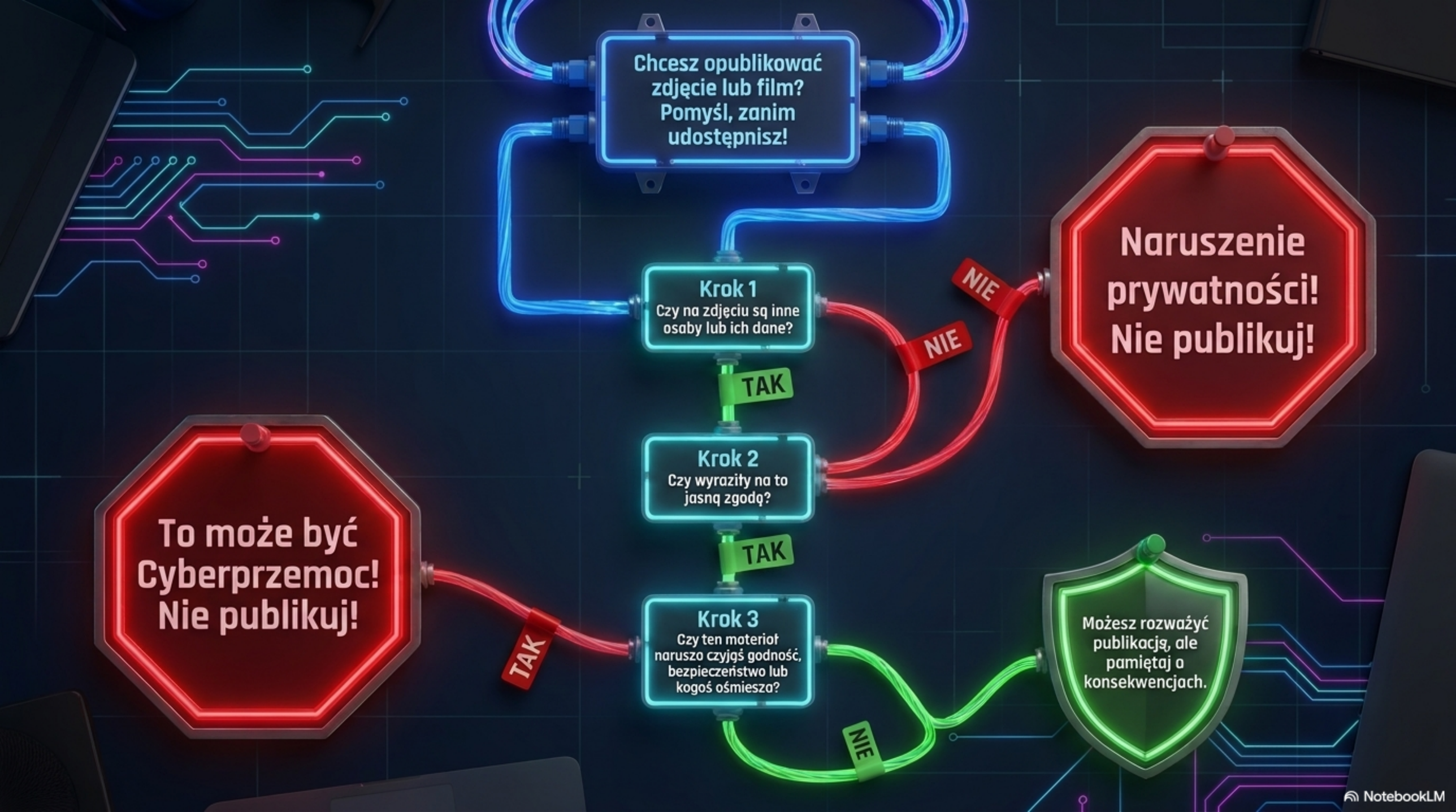
ZASADA NR 2: Twój Cyfrowy Ślad to Beton, nie Piasek.

Wskazówka Detektywa:

W Internecie nic nie ginie. Raz umieszczony materiał może pozostać tam na zawsze.

Pamiętaj!

Nawet jeśli usuniesz post, ktoś inny mógł już zrobić zrzut ekranu (screenshot) i go zapisać. Zastanów się dwa razy, zanim klikniesz Opublikuj.


Chcesz opublikować zdjęcie lub film? Pomyśl, zanim udostępnisz!
Krok 1
Czy na zdjęciu są inne osoby lub ich dane?
NIE
Naruszenie prywatności! Nie publikuj!
TAK
Krok 2
Czy wyraziły na to jasną zgodę?
NIE
TAK
To może być Cyberprzemoc! Nie publikuj!
Krok 3
Czy ten materiał naruszo czyjgś godność, bezpieczeństwo lub kogoś ośmiesza?
TAK
NIE
Możesz rozważyć publikację, ale pamiętaj o konsekwencjach.

ILUZJA

CASE FILE

AKTA SPRAWY:
Fałszywa Rzeczywistość.

Dowody:
Filtry, retusz, boty, kupione lajki.

Nie wierz we wszystko, co widzisz. Influencerzy pokazują zafałszowany, idealny wycinek życia. Nie porównuj się!

Wskazówka: Zdjęcia można łatwo edytować. Nie ufaj wszystkiemu, co widzisz w mediach społecznościowych.

KARTOTEKA ZAGROŻEŃ: Nowe generacje cyber-przestępców.

POSZUKIWANY

Alias: Fałszywy Pomocnik

Modus Operandi:
Oprogramowanie typu CHEAT.

POSZUKIWANY

Alias: Złodziej Pamięci i Twarzy

Modus Operandi:
Sztuczna Inteligencja (AI) i technologia Deepfake.

POSZUKIWANY

Alias: Złodziej Energii

Modus Operandi:
Juice Jacking (Wyciskanie Danych z portów USB).

Akta Sprawy #1: Programy do Cheatowania

Kryptonim pułapki: Fałszywy Prezent.

Jak atakuje? (Raport detektywa):

- Kusi Cię możliwością oszukiwania w grze (darmowe monety, super moce).
- Ściągasz piracki program z nieznanego źródła.
- Zamiast pomóc – program w tle wykrada Twoje hasła, instaluje szkodliwy kod i niszczy komputer!

WERDYKT:

Nigdy nie używaj czitów z sieci. Oszukiwanie niszczy nie tylko zabawę innych, ale też Twój własny sprzęt.

Akta Sprawy #2: Sztuczna Inteligencja (AI) to Maszyna, a nie Człowiek!

Czarna Lista Detektywa:
Działanie AI: Uczy się na wszystkim, co jej wyślesz. Zapisuje to w pamięci. Nie posiada świadomości, uczuć, ani moralności!

Złota Zasada AI: Jeśli nie powiedziałbyś tego obcemu na środku ulicy – NIE WPISUJ tego do czatu sztucznej inteligencji!

Zdemaskuj Oszusta o Stu Twarzach: DEEPFAKE

Cel Oszusta: *Podrobienie twarzy i głosu Twoich znajomych za pomocą AI, by wyłudzić kody BLIK lub hasła.*

Skanuj Wady (Jak rozpoznać Deepfake?)

1. Brak naturalnych emocji i rzadkie mruganie oczami (pusta twarz).
2. Zniekształcony, mechaniczny, nietypowy glos lub zle zgranie ruchu warg ze slowami.
3. Dziwne, rozmyte tło, zniekształcone detale (szczególnie wokół włosów i krawędzi twarzy).
4. Podejrzany kontekst: wywieranie presji czasu.

Akta Sprawy #3: Juice Jacking
(Wyciskanie Danych z Portów USB)

Zagrożenie

Atak:
Zmodyfikowane, publiczne gniazdka wykradają dane!

Bezpieczeństwo

Obrona:
Własny powerbank!

Tarcza Ochronna Detektywa:

Unikaj darmowych, publicznych portów USB.
Korzystaj ze **WŁASNEGO** powerbanku!

Procedura Ratunkowa – Złota Zasada Detektywa!

Zalecenie Głównego Inspektora

Prawdziwy detektyw wie, kiedy WEZWAĆ WSPARCIE.
Jeśli padniesz ofiarą oszustwa, ktoś będzie Cię nękał,
albo zobaczysz coś, co Cię przestraszy –
ZGŁOŚ TO ZAUFANYM DOROSŁYM.
Dorośli są po to, aby stanąć po Twojej stronie
i pomóc Ci rozwiązać zagadkę.
Nie jesteś z tym sam!

Podsumowanie: Bądź Cyber-Detektywem!

Unikaj publicznych USB.
Używaj własnego powerbanka!

Uważaj na phishing.
Sprawdzaj linki i nadawcę!

Nie podawaj danych
osobowych!

Zgłaszaj zagrożenia
zaufanym dorosłym!