Fake news - jak rozpoznawać dezinformację

Dezinformacja stanowi poważne zagrożenie w cyfrowym świecie. Fake newsy to celowo rozpowszechniane fałszywe informacje, które wyglądają jak prawdziwe wiadomości, a ich celem jest manipulowanie emocjami, wprowadzanie w błąd lub wywoływanie chaosu.

W tej prezentacji poznasz metody rozpoznawania fałszywych informacji, zrozumiesz dlaczego są one niebezpieczne oraz nauczysz się, jak skutecznie chronić siebie i swoją organizację przed dezinformacją.

Czym są fake newsy?

Celowa dezinformacja

To celowo rozpowszechniane fałszywe informacje, które wyglądają jak prawdziwe wiadomości.

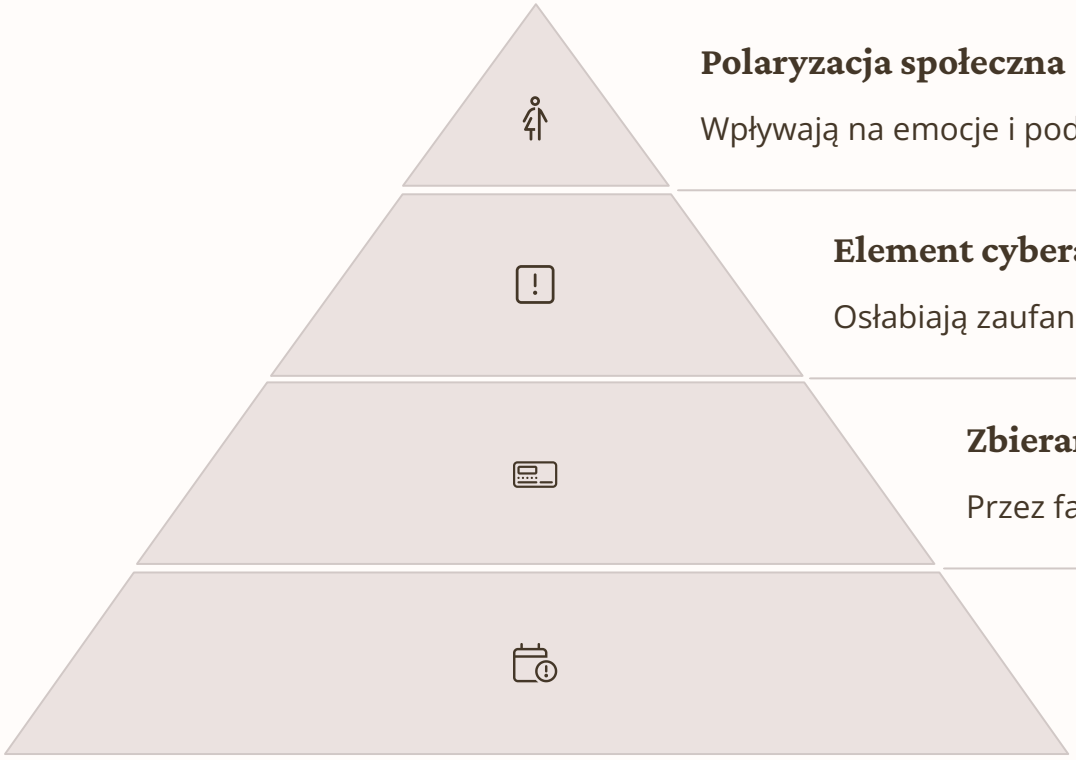
Manipulacja emocjami

Ich celem jest manipulowanie emocjami, wprowadzanie w błąd lub wywoływanie chaosu.

Szeroki zakres tematyczny

Mogą dotyczyć tematów politycznych, społecznych, zdrowotnych, technologicznych lub cyberbezpieczeństwa.

Dlaczego fake newsy są groźne?



Polaryzacja społeczna

Wpływają na emocje i podziały

Element cyberataków

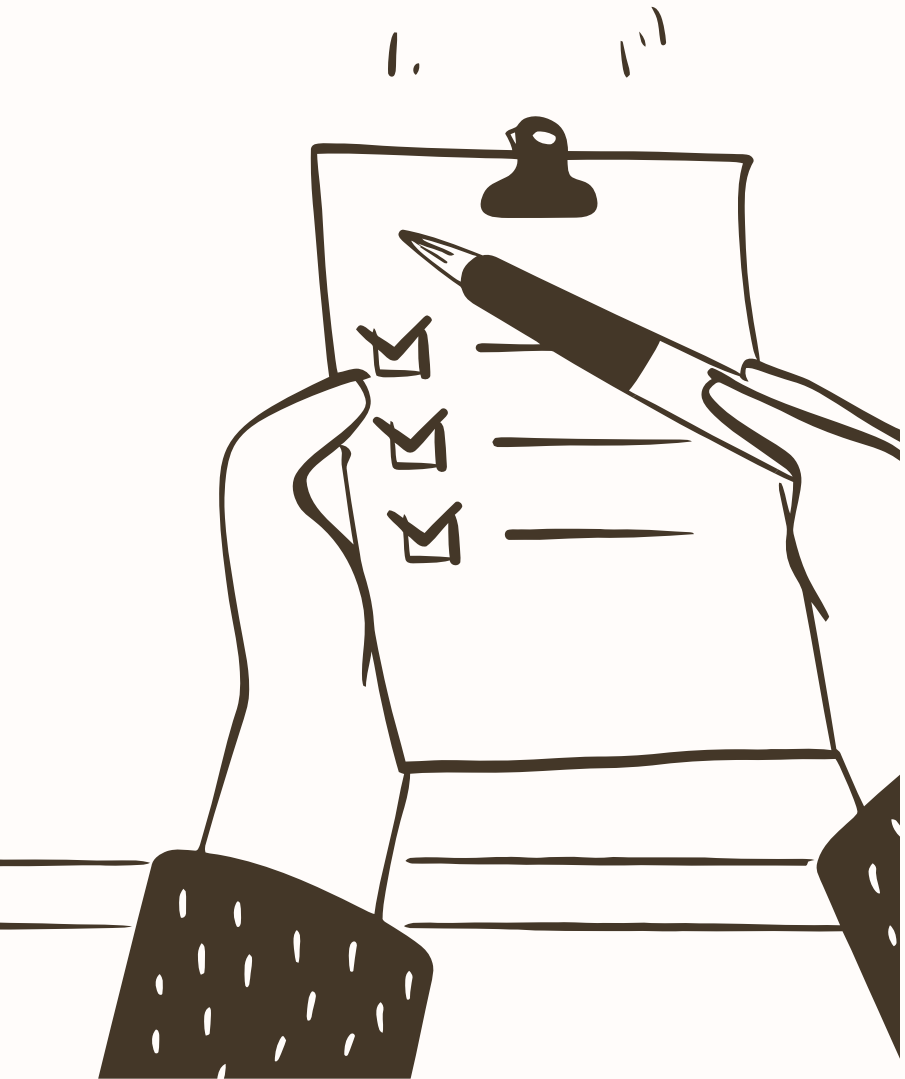
Osłabiają zaufanie do instytucji

Zbieranie danych osobowych

Przez fałszywe strony informacyjne

Błędne decyzje pracowników

Wpływ na działania służbowe



Jak rozpoznać fake newsa?

Sprawdź źródło

Czy strona jest znana i wiarygodna? Czy link pochodzi z zaufanej domeny (np. zamiast onet.pl jest oneet-news.com)?

Zwróć uwagę na język

Fake newsy często zawierają emocjonalny, krzykliwy język ("SZOK!", "Zobacz zanim usuną!"). Brak konkretnych danych lub źródeł.

Zweryfikuj treść w innych źródłach

Czy tę samą informację podały znane media? Wpisz tytuł w wyszukiwarkę – jeśli pojawia się tylko w jednym miejscu, to sygnał ostrzegawczy.

Oceń grafikę i daty

Zdjęcia mogą być wyjęte z kontekstu lub zmodyfikowane. Sprawdź, czy data publikacji zgadza się z treścią.

Przykłady dezinformacji związanej z bezpieczeństwem

Fałszywe zagrożenia

"Nowy wirus atakuje tylko użytkowników Windows 11 – pobierz łatkę tutaj!" (link do złośliwego pliku)

Phishing

"Twoje dane wyciekły – sprawdź na tej stronie" (link phishingowy)

Zmyślone zmiany zasad

"Nie trzeba już używać haseł – Google zmieniło zasady!" (zmyślona informacja z ryzykiem przejęcia konta)

Zachęty do rezygnacji z ochrony

"Antywirusy szpiegują użytkowników – wyłącz swój!" (zachęta do rezygnacji z ochrony)

Jak się chronić przed dezinformacją?

Weryfikuj przed udostępnieniem

Nie udostępniaj informacji bez sprawdzenia – nawet jeśli wydają się sensacyjne lub wzbudzają silne emocje.

Ostrożność w social mediach

Zachowaj ostrożność w social mediach, szczególnie w grupach dyskusyjnych i komentarzach.

Ucz się rozpoznawać manipulację

Zwracaj uwagę na pytania bez odpowiedzi, które mają "zasiać wątpliwość".

Korzystaj z narzędzi weryfikacji

Używaj platform jak Demagog.org.pl, FakeHunter czy Snopes do sprawdzania faktów.