

PIGUŁKA WIEDZY

Jak rozpoznawać dezinformację i bezpiecznie korzystać z Internetu



Dofinansowane przez
Unię Europejską

sieć
splot
wartości

Pro
Cultura
WŁĄCZAMY CYFROWO

Program finansowany jest przez Unię Europejską. Wyrażone opinie i poglądy są wyłącznie poglądami autora (autorów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Komisji Europejskiej.
Ani Unia Europejska, ani organ przyznający finansowanie nie mogą ponosić za nie odpowiedzialności.

Autorzy: **Daria Sowińska-Milewska i Łukasz Szczepańczyk**

Opracowanie graficzne: **Dominika Niemyska**

Publikacja powstała w 2026 roku w ramach projektu:

„Sprawdzam! Kompetencje medialne i informacyjne osób w późnej dorosłości”

jako materiał pomocniczy do wykładów online.

Niniejsza publikacja jest dostępna na warunkach licencji Creative Commons – Uznanie autorstwa – Użycie niekomercyjne 4.0 – Na tych samych warunkach.

Oznacza to, że będzie można dowolnie wykorzystać te utwory, w tym je kopiować, dystrybuować, wyświetlać i używać, pod warunkiem podania autora utworu. Więcej informacji o licencji znajduje się na stronie:

<https://creativecommons.org/licenses/by/4.0/deed.pl>

Publikacja dostępna jest bezpłatnie na stronie **pro-cultura.pl**

W redakcji materiału wspierała nas AI.

Zapraszamy do kontaktu:



Zeskanuj i sprawdź
nasze działania

Fundacja Pro Cultura

 <https://pro-cultura.pl>

 fundacja@pro-cultura.pl



Zeskanuj i odwiedź
Stację Pro Senior

Stacja Pro Senior

 <https://stacjaproseior.pl>

 redakcja@stacjaproseior.pl

Strefa wiedzy dla osób 55+... i nie tylko



Zeskanuj i sprawdź
praktyczne wskazówki

 <https://wlamczamycyfrowo.pl>

Poradniki, praktyczne wskazówki i ciekawostki, które pomogą Ci swobodnie korzystać z telefonu, Internetu i nowych technologii.

SPIS TREŚCI

W tej pigułce:

Wprowadzenie	4
Słowniczek	5
Dezinformacja - o co chodzi?	8
Techniki i narzędzia dezinformacji	9
Dlaczego ulegamy dezinformacji?	11
Jak rozpoznać dezinformację	13
Oszustwa wokół nas	14
Dekalog Cyberbezpieczeństwa	16
Co zrobić, jeśli już się stało?	18
Gdzie sprawdzać i gdzie szukać pomocy?	19

WPROWADZENIE

Internet ułatwia codzienne życie: pozwala kontaktować się z bliskimi, korzystać z bankowości, robić zakupy, załatwiać sprawy urzędowe i zdobywać informacje. Jednocześnie coraz trudniej ocenić, **czy to, co widzimy, słyszymy i czytamy, jest prawdziwe.**

Fałszywa informacja może dziś wyglądać bardzo bardzo przekonująco. Może przypominać wiadomość z banku, SMS od kuriera, artykuł znanego portalu albo post opublikowany przez znajomą osobę. Sztuczna inteligencja sprawia, że łatwiej tworzyć realistyczne zdjęcia, filmy, wiadomości, a nawet nagrania głosu. Z tego powodu dezinformacja, cyberoszustwa i AI coraz częściej łączą się ze sobą.

Oszustwo często nie zaczyna się od skomplikowanej technologii, ale od **wiarygodnej historii i silnych emocji**. Strach, pośpiech, ciekawość czy obietnica zysku mogą skłonić do kliknięcia w link, podania danych, wykonania przelewu albo zainstalowania aplikacji.

Nie trzeba jednak być specjalistą od komputerów, aby zwiększyć swoje bezpieczeństwo. Najważniejszy jest prosty nawyk:



To główna zasada tej pigułki wiedzy. W kolejnych częściach pokazane zostanie, jak rozpoznawać dezinformację, fake newsy, deepfake'i i najczęstsze cyberoszustwa oraz jak bezpiecznie korzystać z Internetu i narzędzi sztucznej inteligencji.

SŁOWNICZEK

Algorytm

zestaw reguł, według których serwis internetowy lub aplikacja wykonuje określone zadanie. W mediach społecznościowych algorytmy decydują m.in. o tym, jakie posty, filmy i reklamy zobaczymy. Często podpowiadają treści podobne do tych, które wcześniej oglądaliśmy.

Bańka informacyjna

sytuacja, w której docierają do nas głównie informacje i opinie zgodne z tym, co już myślimy. Może powstawać zarówno przez nasze własne wybory, jak i działanie algorytmów.

Bot

program, który automatycznie wykonuje określone działania w internecie. Boty mogą być użyteczne, ale mogą też służyć np. do masowego publikowania komentarzy lub rozpowszechniania określonych treści.

Clickbait

[czyt. klikbajt]

tytuł, zdjęcie lub komunikat przygotowany przede wszystkim po to, żeby wzbudzić ciekawość albo silne emocje i zachęcić do kliknięcia. Często przesadza, coś ukrywa albo obiecuje więcej, niż rzeczywiście znajduje się w materiale.

Cyberbezpieczeństwo

działania i nawyki pomagające chronić urządzenia, konta, pieniądze i dane podczas korzystania z Internetu.

Cyberoszustwo / scam

[czyt. skam]

próba nakłonienia kogoś do działania korzystnego dla oszusta, np. przekazania pieniędzy, podania danych, hasła lub kodu albo zainstalowania programu.

Deepfake [czyt. <i>Dipfejk</i>]	realistycznie wyglądający obraz, film lub nagranie głosu stworzone albo zmienione za pomocą sztucznej inteligencji tak, aby przedstawiało coś, co w rzeczywistości nie miało miejsca.
Dezinformacja	celowe tworzenie lub rozpowszechnianie fałszywych, zmanipulowanych albo wprowadzających w błąd informacji po to, aby wpłynąć na odbiorców i ich zachowanie.
Fake news [czyt. <i>fejk njus</i>]	fałszywa lub zmanipulowana wiadomość przedstawiana w taki sposób, aby odbiorca uznał ją za prawdziwą. Fake news może zawierać również prawdziwe elementy umieszczone w fałszywym kontekście.
Sztuczna inteligencja (AI) [czyt. <i>Ej aj</i>]	technologia potrafiąca na podstawie poleceń tworzyć nowe treści, np. teksty, obrazy, głosy i filmy. Może pomagać w codziennym życiu, ale może również zostać wykorzystana do przygotowania bardziej przekonujących oszustw.
Malinformacja	prawdziwa informacja wykorzystana w sposób, który ma komuś zaszkodzić, np. poprzez ujawnienie prywatnych danych lub przedstawienie faktów bez ważnego kontekstu.
Misinformacja	fałszywa lub błędna informacja przekazywana dalej bez zamiaru oszukania innych. Przykładem może być udostępnienie nieprawdziwej wiadomości, ponieważ sami uznaliśmy ją za prawdziwą. Brak zamiaru wprowadzenia w błąd odróżnia ją od celowej dezinformacji.

Phishing	oszustwo polegające na podszywaniu się pod zaufaną osobę lub instytucję, aby wyłudzić dane, hasła, kody albo pieniądze. Może wykorzystywać np. fałszywą stronę banku.
Smishing	phishing prowadzony za pomocą wiadomości SMS lub komunikatora. Przykładem może być wiadomość o konieczności dopłaty do przesyłki z linkiem prowadzącym do fałszywej strony.
Socjotechnika	wykorzystywanie wiedzy o ludzkich emocjach i zachowaniach, aby skłonić kogoś do określonego działania. Oszust może wykorzystywać m.in. strach, pośpiech, zaufanie, ciekawość czy obietnicę zysku.
Troll internetowy	osoba lub konto, które celowo publikuje prowokacyjne albo konfliktowe treści. Celem może być wywołanie emocji, kłótni lub zakłócenie dyskusji.
Uwierzytelnianie dwuskładnikowe (2FA)	dodatkowa ochrona konta. Oprócz hasła podczas logowania potrzebne jest drugie potwierdzenie, np. kod z aplikacji lub zatwierdzenie logowania na telefonie.
Vishing	odmiana phishingu prowadzona przez telefon. Oszust może np. podawać się za pracownika banku, policjanta, urzędnika lub członka rodziny.
Weryfikacja informacji (fact-checking)	sprawdzanie, czy informacja jest prawdziwa. Może polegać m.in. na sprawdzeniu autora, daty i źródła, dotarciu do źródła pierwotnego oraz porównaniu informacji z innymi wiarygodnymi źródłami.

DEZINFORMACJA – O CO CHODZI?

Dezinformacja to coś więcej niż po prostu fałszywa wiadomość. Może opierać się także na prawdziwych informacjach, ale przedstawionych w taki sposób, aby odbiorca wyciągnął z nich błędny wniosek.

W przeciwieństwie do zwykłej pomyłki lub błędnej informacji, dezinformacja zakłada świadome działanie mające wpłynąć na sposób myślenia lub zachowanie innych osób.

Dezinformacja szkodzi, ponieważ może prowadzić do błędnych decyzji, wzbudzać lęk, pogłębiać podziały, osłabiać zaufanie i utrudniać wspólne działanie społeczeństwa.

Nie każda nieprawdziwa informacja jest dezinformacją. Ktoś może się pomylić, źle coś zrozumieć albo przekazać dalej wiadomość, w którą sam wcześniej uwierzył. Warto odróżniać zwykły błąd od celowego kłamstwa.

Wiek dezinformacji?

Fałszywe informacje nie są niczym nowym. Istniały na długo przed Internetem. Dziś jednak zmieniła się **skala, szybkość i łatwość ich rozpowszechniania**. Każda osoba może w kilka sekund opublikować tekst, zdjęcie lub film i przekazać go dalej. Jednocześnie jesteśmy otoczeni ogromną liczbą informacji, których nie sposób dokładnie sprawdzać na bieżąco. Coraz ważniejsze stają się uważność i sceptycyzm, czyli umiejętność zatrzymania się przy informacji, zanim uznamy ją za prawdziwą. Warto sprawdzać jej źródło, kontekst i wiarygodność, zamiast przyjmować ją bez zastanowienia.

Każdą podejrzaną informację warto sprawdzić

TECHNIKI I NARZĘDZIA DEZINFORMACJI

1

TWORZENIE FAŁSZYWYCH TREŚCI

Wytwarzanie informacji lub materiałów, które **nie odpowiadają rzeczywistości**.

- zmanipulowane cytaty i fałszywe wywiady – przypisywanie osobom wypowiedzi, których nie udzieliły;
- fabrykowanie ekspertów i autorytetów;
- tworzenie fikcyjnych organizacji i instytucji;
- tworzenie fałszywych materiałów audio, obrazów i wideo, deepfake'i, czyli materiały wygenerowane lub zmanipulowane za pomocą AI, które mają wyglądać jak prawdziwe.

2

MANIPULOWANIE PRAWDZIWYMI INFORMACJAMI

Wykorzystanie prawdziwej informacji w taki sposób, aby **prowadziła odbiorcę do fałszywego lub mylącego wniosku**.

- wyrwanie wypowiedzi lub wydarzenia z kontekstu;
- manipulowanie kontekstem;
- selektywne przedstawianie informacji;
- pomijanie istotnych faktów;
- przedstawianie prawdziwych informacji w sposób wprowadzający w błąd;
- wyolbrzymianie faktów i tworzenie sztucznej sensacji.

3

MANIPULOWANIE WIARYGODNOŚCIĄ PRZEKAZU

Tworzenie **poзору wiarygodności** fałszywej lub zmanipulowanej informacji.

- podszywanie się pod wiarygodne źródła;
- wykorzystywanie nazw, logotypów i wyglądu znanych mediów lub instytucji;
- tworzenie pozornie wiarygodnych stron internetowych;
- publikowanie tej samej treści w wielu powiązanych źródłach;
- tworzenie pozoru szerokiego poparcia dla określonego przekazu;
- wykorzystywanie fikcyjnych lub nieweryfikowalnych źródeł.

4

WYKORZYSTYWANIE EMOCJI I PODZIAŁÓW

Wykorzystywanie istniejących **emocji, konfliktów, lęków i podziałów społecznych** w celu zwiększenia oddziaływania przekazu.

- wzbudzanie strachu, złości, oburzenia lub poczucia zagrożenia;
- wzmacnianie istniejących konfliktów i kryzysów społecznych;
- tworzenie skrajnych przekazów;
- wykorzystywanie mitów i stereotypów;
- przedstawianie rzeczywistości w kategoriach „my–oni”;
- wzmacnianie podziałów między grupami społecznymi.

Twoje cyberbezpieczne notatki

DLACZEGO ULEGAMY DEZINFORMACJI?

Dezinformacja wykorzystuje naturalne mechanizmy działania naszego umysłu:

1	Emocje strach, złość i oburzenie przyciągają uwagę i utrudniają spokojną analizę.
2	Autorytet i wiarygodność nadawcy łatwiej wierzymy osobom, które postrzegamy jako ekspertów, autorytety lub osoby, które lubimy.
3	Efekt potwierdzenia chętniej przyjmujemy informacje zgodne z naszymi wcześniejszymi przekonaniami.
4	Oszczędzanie wysiłku poznawczego korzystamy ze skrótów myślowych i nie analizujemy szczegółowo każdej informacji.
5	Znajomość i powtarzanie informacji informacja wielokrotnie powtarzana może wydawać się prawdziwa tylko dlatego, że jest nam znajoma.
6	Zakotwiczenie pierwsza usłyszana informacja może stać się punktem odniesienia dla późniejszych ocen.
7	Efekt śpiocha możemy zapomnieć źródło i kontekst informacji, ale zachować samą informację, która z czasem zaczyna wydawać się prawdziwa.
8	Odporność przekonań na zmianę sprostowanie nie zawsze usuwa wpływ wcześniej poznanej fałszywej informacji, stąd ważne jest nie tylko prostowanie, ale także wyjaśnianie, co było fałszywe i jaka informacja jest prawdziwa.

Pomyśl!

- Który z tych mechanizmów najłatwiej może uruchomić się u mnie?
- Czy bardziej działają na mnie emocje?
- Czy ufam informacjom pochodzącym od osób, które lubię lub którym ufam?
- Czy łatwiej przyjmuję informacje zgodne z moimi przekonaniami?
- Czy zdarza mi się uznać coś za prawdziwe tylko dlatego, że słyszę o tym kolejny raz?
- Czy sprawdzam informacje, które wydają mi się oczywiste?
- Czy potrafię zmienić zdanie, kiedy pojawiają się wiarygodne dowody, że się mylę?

Każda i każdy z nas inaczej patrzy na świat.



To, co dla jednej osoby jest szóstką, dla drugiej może być dziewiątką.

Nie zawsze oznacza to, że jedna osoba kłamie, a druga mówi prawdę. Czasami patrzymy na tę samą sytuację z dwóch różnych perspektyw.

JAK ROZPOZNAĆ DEZINFORMACJĘ

Zatrzymaj się, jeśli:

- informacja wywołuje silne emocje;
- ktoś próbuje Cię przestraszyć albo oburzyć;
- pojawia się presja czasu: „pilne”, „natychmiast”, „udostępnij”;
- nie wiadomo, kto jest autorem;
- nie ma źródeł lub źródło jest niejasne;
- tytuł jest bardzo sensacyjny;
- informacja brzmi „zbyt dobrze, żeby była prawdziwa”;
- widzisz zdjęcie lub film, ale nie znasz ich pochodzenia;
- ktoś przedstawia się jako ekspert, ale nie wiadomo, kim jest;
- informacja potwierdza dokładnie to, w co już wierzysz.

Uwaga na clickbaity!

Clickbait to chwytliwy tytuł, nagłówek lub obraz, którego celem jest nakłonienie do kliknięcia linku do materiału lub artykułu. Słowo „clickbait” pochodzi od angielskich słów *click* (kliknięcie) i *bait* (przynęta). To właśnie „przynęta na kliknięcia” – sposób, w jaki portale zdobywają odsłony, a tym samym zarabiają na reklamach.

Clickbait często obiecuje sensację, szok albo „tajemnicę”, ale po kliknięciu okazuje się, że artykuł nie zawiera niczego nowego ani ważnego a czasem prawdziwego.

OSZUSTWA WOKÓŁ NAS

Oszustwa również wykorzystują nasze emocje i mechanizmy działania umysłu.

Przykłady mechanizmów wykorzystywanych przez oszustów:

- Presja czasu: „To ostatnia sztuka”, „oferta wygasa za 15 minut”. To wymusza emocjonalną decyzję, zanim przeanalizujesz fakty.
- Reguła niedostępności: Sprawianie, że produkt wydaje się rzadszy, a przez to bardziej wartościowy.
- Love bombing: Zalewanie nadmierną uwagą, komplementami lub udawaną troską, aby szybko zbudować fałszywe zaufanie
- Społeczny dowód słuszności: Pokazywanie sfalszowanych opinii lub historii osób, które „już zarobiły”.
- Huśtawka emocjonalna: Wywoływanie strachu (np. „stracisz oszczędności”), a potem oferowanie „bezpiecznego” rozwiązania (inwestycji)
- Chciwość/radość: „Zarobię fortunę bez wysiłku”.
- Strach: „Muszę kupić teraz, bo potem będzie za późno”, strach o kogoś bliskiego
- Poczucie bycia wyjątkowym: „Tylko dla wybranych”, „dostałeś szansę, jakiej inni nie mają”.

Celem oszusta jest zazwyczaj doprowadzenie nas do **konkretnego działania, które przyniesie mu korzyść**.

Twoje cyberbezpieczne notatki

Przykłady oszustw:

Jak kontaktuje się oszust?	Przykład	Czego może chcieć?
SMS	dopłata do paczki	kliknięcie, dane, płatność
telefon	„pracownik banku”	dane, kod, przelew
komunikator	„wnuczek potrzebuje pieniędzy”	przelew
e-mail	fałszywa faktura	kliknięcie, załącznik
reklama	„pewna inwestycja”	wpłata pieniędzy
fałszywa pomoc techniczna	„masz wirusa”	zdalny dostęp
fałszywa strona	bank, sklep, urząd	login, hasło, dane
media społecznościowe	“adorator”	pieniędzy w formie pożyczki
bezpośrednio	kurier chcący zwrócić nam pieniądze za zakup	użycia karty w terminalu

Dekalog cyberbezpieczeństwa

1

Aktualizuj telefon i komputer

Regularnie instaluj aktualizacje systemu i aplikacji. Aktualizacje usuwają błędy i luki bezpieczeństwa. Warto też zabezpieczyć urządzenie blokadą ekranu, np. kodem PIN, hasłem, odciskiem palca lub rozpoznawaniem twarzy.

2

Używaj silnych i różnych haseł

Nie używaj jednego hasła do wielu kont. Szczególnie dobrze zabezpiecz pocztę, bankowość, konto Google lub Apple oraz media społecznościowe. Hasła powinny być długie i trudne do odgadnięcia.

3

Włącz 2FA lub MFA

Uwierzytelnianie dwuskładnikowe daje dodatkową ochronę konta. Oprócz hasła potrzebne jest wtedy jeszcze drugie potwierdzenie, np. kod lub akceptacja logowania w aplikacji.

4

Nigdy nie podawaj haseł i kodów

Nie przekazuj innym osobom haseł, kodów SMS, kodów BLIK ani kodów służących do zatwierdzania logowania. Jeśli ktoś o nie prosi, potraktuj to jako sygnał ostrzegawczy.

5

Nie klikaj automatycznie w linki i uważaj na załączniki

Link w SMS-ie, e-mailu lub komunikatorze może prowadzić do fałszywej strony. Podejrzany załącznik może zawierać szkodliwe oprogramowanie. Jeśli wiadomość dotyczy banku, urzędu lub innej instytucji, otwórz jej stronę samodzielnie albo skorzystaj z oficjalnej aplikacji.

6**Nie instaluj programów na polecenie nieznanej osoby**

Szczególnie ostrożnie podchodź do programów umożliwiających zdalny dostęp do telefonu lub komputera. Oszust może dzięki nim zobaczyć ekran, przejąć urządzenie lub uzyskać dostęp do kont.

7**Ograniczaj ilość danych o sobie w internecie**

Nie publikuj bez potrzeby informacji o miejscu zamieszkania, rodzinie, wyjazdach, codziennych zwyczajach czy dokumentach. Im więcej ktoś o nas wie, tym łatwiej może przygotować wiarygodną próbę oszustwa.

8**Weryfikuj osoby, z którymi rozmawiasz**

Nie zakładaj, że rozmówca jest tym, za kogo się podaje. Jeśli dzwoni „pracownik banku”, zakończ rozmowę i samodzielnie skontaktuj się z bankiem przez oficjalną infolinię lub aplikację. Jeśli ktoś podaje się za bliską osobę i prosi o pieniądze, skontaktuj się z nią pod innym, znanym numerem.

9**Ustal rodzinne hasło bezpieczeństwa**

Warto uzgodnić z bliskimi proste hasło lub pytanie, którego nie zna osoba postronna. Może ono pomóc potwierdzić tożsamość osoby dzwoniącej w nagłej sytuacji, zwłaszcza gdy prosi ona o pieniądze lub pomoc.

10**Rób kopie zapasowe ważnych danych**

Nie przechowuj wszystkich zdjęć, dokumentów i ważnych plików tylko w jednym miejscu. Kopia zapasowa w chmurze lub na dodatkowym nośniku może pomóc po awarii, kradzieży urządzenia albo cyberataku.

Do zapamiętania:

CO ZROBIĆ, JEŚLI JUŻ SIĘ STAŁO?

KLIKNIĘTY LINK	→	zamknij stronę, niczego nie pobieraj ani nie uruchamiaj.
PODANE LOGIN / HASŁO	→	zmień hasło, wyloguj aktywne sesje, sprawdź 2FA (lub MFA).
PODANY KOD / ZATWIERDZONE LOGOWANIE	→	zabezpiecz konto i skontaktuj się z usługodawcą.
PODANE DANE KARTY	→	natychmiast skontaktuj się z bankiem.
BLIK / PRZELEW	→	natychmiast skontaktuj się z bankiem, następnie zgłoś sprawę.
UDOSTĘPNIONY ZDALNY DOSTĘP	→	przerwij połączenie, odłącz Internet i skontaktuj się z zaufaną pomocą techniczną.
ZASZYFROWANY KOMPUTER	→	odłącz urządzenie od sieci, nie kasuj danych, skontaktuj się ze specjalistą.

GDZIE SPRAWDZAĆ I GDZIE SZUKAĆ POMOCY?

GDZIE SPRAWDZAĆ INFORMACJE?

- źródło pierwotne;
- oficjalna strona instytucji;
- inne wiarygodne źródła;
- wyszukiwarka;
- serwisy fact-checkingowe: <https://fakenews.pl/>; <https://demagog.org.pl/>
- wyszukiwanie obrazem – gdy sprawdzamy zdjęcie.

Materiały NASK <https://www.nask.pl/> wskazują właśnie na sprawdzanie wiarygodności źródła, ocenę przedstawionej sytuacji, porównanie z innym źródłem i oddzielanie faktów od opinii.

GDZIE SZUKAĆ POMOCY?

- CERT Polska – incydenty i cyberbezpieczeństwo: <https://incydent.cert.pl/>
- bank – gdy chodzi o pieniądze lub dane bankowe;
- Policja – w przypadku oszustwa/przestępstwa;
- zaufana osoba lub specjalistka/specjalista IT – gdy potrzebna jest pomoc techniczna.

Twoje cyberbezpieczne notatki

Ważne numery – warto zapisać!

8080

podejrzane SMS-y

prześlij podejrzany SMS do CERT Polska.

Numer służy do przyjmowania wiadomości, nie do rozmów.

+48 828 828 828

zastrzeżenie kart płatniczych

całodobowy numer do szybkiego zastrzeżenia zgubionej, skradzionej lub zagrożonej karty.

112

numer alarmowy

dzwoń, gdy potrzebna jest pilna pomoc służb i zagrożone jest życie, zdrowie lub mienie.

ZAPAMIĘTAJ

Nie wiesz, co zrobić? Nie klikaj, nie przelewaj pieniędzy i nie podawaj danych. Zatrzymaj się, skontaktuj się z zaufaną osobą lub właściwą instytucją i sprawdź sytuację innym kanałem.

Twoje cyberbezpieczne notatki