

DOWIEDZ SIĘ WIĘCEJ

CERT Polska: cert.pl
Bezpieczne Dane: bezpiecnedane.gov.pl
Aplikacja Cyberalerty



WERYFIKACJA INFORMACJI

PAP: pap.pl/fact-checking
AFP: sprawdzam.afp.com
Stowarzyszenie Demagog: demagog.org.pl
Stowarzyszenie Pravda: pravda.org.pl
Fundacja Przeciwdziałamy Dezinformacji: fakenews.pl

ZGŁASZANIE OSZUSTW W SIECI

CERT Polska: incydent.cert.pl
Aplikacja mObywatel
Policja (Centralne Biuro Zwalczania Cyberprzestępczości):
tel. 47 72 136 99, kontakt.bzc@cbzc.policja.gov.pl



www.e-nergia.org

DEZINFORMACJA I OSZUSTWA W SIECI
NIE DAJ SIĘ NABRAĆ!

Wydawcą poradnika jest Fundacja e-nergia ul. Trzebnicka 10D 55-095 Domaszczyn KRS 0000882948



SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI – CENTRUM
ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO W RAMACH RZĄDOWEGO PROGRAMU
WSPARCIA ORGANIZACJI POZARZĄDOWYCH MOC MAŁYCH SPOŁECZNOŚCI

PRAKTYCZNY PORADNIK

FUNDACJI E-nergia

NIE DAJ SIĘ NABRAĆ NA DEZINFORMACJĘ



Dezinformacja to celowe publikowanie fałszywych informacji. Jest szkodliwa i niebezpieczna. Może wywoływać strach, panikę, wrogość do grup społecznych i narodowościowych, osłabiać instytucje publiczne, czy wpływać na wynik wyborów...

1. SPRAWDZAJ ŹRÓDŁO

Upewnij się, że informacja pochodzi z **wiarygodnego źródła** np. komunikatu policji. Uważaj na fałszywe adresy (np. facebo0k.com).

2. WERYFIKUJ

Sprawdź **inne źródła informacji** (znane portale, strony instytucji państwowych). Sprawdź czy ktoś jeszcze o tym pisze. Jeżeli w innych miejscach **nie ma takiej informacji, może być ona fałszywa**.

3. UWAŻAJ NA EMOCJE

Krzykliwe nagłówki mające na celu wywołanie złości, strachu i innych skrajnych emocji. To częsty **podstęp dezinformatorów**.

4. NIE UFAJ ZDJĘCIOM I FILMOM

W dobie sztucznej inteligencji (AI) **zdjęcia, a nawet filmy** (obraz i głos) można **łatwo zmanipulować**. Przyjrzyj się dokładnie czy elementy na zdjęciu lub filmie są realne. Zwracaj uwagę na **szczególności**.

5. NIE DZIAŁAJ POCHOPNIE

Udostępnienia, komentarze i reakcje (np. emotką pod wpisem na Facebooku) **zwiększają zasięg informacji, która może być fałszywa**.

6. ZASTANÓW SIĘ

Zachowaj rozsądek i bądź krytyczny wobec informacji, szczególnie tych emocjonalnych. Zadaj sobie pytanie „**kto na tym zyskuje?**”. Dezinformacja ma zwykle konkretny cel - np. skłócenie społeczeństwa.

7. SIĘGAJ PO POMOC

Istnieją specjalne **strony weryfikujące informacje**. Możesz do nich także wysłać konkretną informację w celu weryfikacji. Adresy znajdziesz na ostatniej stronie tego poradnika.

DBAJ O SVOJE BEZPIECZEŃSTWO



1. CHROŃ SVOJE DANE

Nigdy nikomu nie podawaj swoich **hasła**, numeru **PIN**, czy kodu **BLIK**. Zastrzeż swój **PESEL** w aplikacji **mObywatel**. Uważaj z podawaniem numeru **dowodu osobistego**, czy numeru **karty bankowej**.

2. STOSUJ BEZPIECZNE HASŁA

Nie ustawiaj hasła, które łatwo odgadnąć. Kluczowe są: **e-mail**, **portale społecznościowe** oraz **bankowość elektroniczna**. Korzystaj z **dwuetapowego uwierzytelniania** np. hasło + SMS / aplikacja.

3. NIE KLIKAJ W OTRZYMANE LINKI

Zawsze loguj się (np. do banku) przez **oficjalną stronę** lub **aplikację**. Uważnie wpisuj adres strony, **uważaj na literówki** (np. „allegro0.pl” zamiast „allegro.pl”). Oszuści podrabiają wygląd prawdziwych stron.

4. ZACHOWAJ OSTROŻNOŚĆ

Jeżeli ktoś kontaktuje się, podając za np. pracownika banku, urzędu, czy policjanta i **prosi o Twoje hasła lub kody** - nie rób tego! **Natychmiast przerwij rozmowę**, skontaktuj się z tą instytucją i powiadom ją o tym.

5. „CO NAGLE TO PO DIABLE”

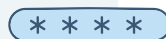
Jeśli ktoś kontaktuje się i przekonuje, że „**musisz natychmiast coś zrobić**” (np. przestać pieniądze BLIKiem albo zweryfikować swoje konto na Facebooku) **to zapewne oszustwo!** Nie działaj pochopnie!

6. UWAŻAJ NA OKAZJE

Zanim coś kupisz, sprawdź sklep – zobacz opinie, adres i numer kontaktowy. **Zbyt atrakcyjna cena** (znacznie poniżej rynkowej) może oznaczać fałszywy sklep i **próbę wyłudzenia**.

7. ZGŁASZAJ PODEJRZANE SYTUACJE

Zgłaszaj podejrzone sytuacje. Skontaktuj się ze swoim bankiem, policją, lub zgłoś do CERT. Numery i adresy znajdziesz **na kolejnej stronie**.



Wraz z rozwojem cyfryzacji stale obserwujemy **wzrost zagrożeń płynących z sieci**. Pojawiają się nowe i przebiegłe metody oszustw, a ich ofiarami padają najczęściej osoby starsze.

