FEJK

Jak sprawdzić, czy zdjęcie, film albo nagranie głosu jest z AI, i 7 sposobów na fejka bez żadnej aplikacji

SynthID Detector od Google DeepMind · dostępny dla wszystkich od 7.10.2026 · strona po angielsku

Krok po kroku: SynthID Detector

1. Wejdźcie na **synthid.com**. To oficjalna strona Google DeepMind. Uwaga na podróbki o podobnych nazwach: znaku wodnego Google nie sprawdzi żadna inna strona.
2. Zalogujcie się (konto Google, Apple albo OpenAI).
3. Wgrajcie **1 plik**: zdjęcie, film albo nagranie audio. Najlepiej oryginał zapisany z czatu lub strony, a nie zrzut ekranu.
4. Przeczytajcie wynik. Jeśli narzędzie znajdzie znak wodny, pokaże, które fragmenty pliku go mają (np. część obrazu albo odcinek nagrania).

Co to sprawdza: niewidoczny znak wodny **SynthID**, który Google dodaje do treści ze swoich modeli AI (ponad 180 mld zdjęć i filmów). Detector rozpoznaje też treści z narzędzi partnerów: **OpenAI, NVIDIA i Kakao**, a wkrótce Apple. Znak ma przetrwać przycięcie, filtry i kompresję.

Najważniejsze ograniczenie: wynik „nie znaleziono znaku" **nie znaczy, że plik jest prawdziwy**. Znaczy tylko, że nie zrobiło go narzędzie, które dodaje SynthID. Fejki z innych programów przejdą ten test. Detector to 1 z kilku kroków, a nie wyrocznia.

Szybciej, w aplikacji Gemini

Wgrajcie zdjęcie, film albo klip audio do czatu w Gemini i zapytajcie: *„Czy to zostało stworzone albo edytowane przez Google AI? Sprawdź SynthID."* Gemini (podobnie jak Wyszukiwarka i Chrome) sprawdzi znak wodny Google. Treści z innych firm sprawdzicie na synthid.com.

7 sposobów na rozpoznanie fejka bez aplikacji

1 **Pośpiech + emocje + pieniądze = stop.** „Mamo, miałem wypadek, przelej teraz", „ostatnia szansa na inwestycję". Presja czasu to typowy element oszustwa, z AI czy bez.

2 **Oddzwońcie na znany numer.** Głos da się podrobić. Rozłączcie się i zadzwońcie sami na numer, który macie zapisany od lat, albo do kogoś z rodziny.

3 **Ustalcie hasło rodzinne.** 1 słowo, które znają tylko bliscy i które nie pada w internecie. Kto dzwoni „w potrzebie", musi je podać.

4 **Szukajcie źródła.** Wyszukajcie obraz w Google Lens (wyszukiwanie obrazem). Jeśli to samo zdjęcie krąży od lat w innym kontekście albo nikt poważny go nie opublikował, to sygnał ostrzegawczy.

5 **Znana twarz poleca inwestycję?** Sprawdźcie oficjalny profil tej osoby i stronę firmy. Reklamy z celebrytami „polecającymi" szybki zysk to klasyczny przekręt.

6 **Patrzcie na detale, ale im nie ufajcie w 100%.** Napisy w tle, dłonie, biżuteria, odbicia w lustrze, cienie, mruganie i ruch ust w filmie. Nowe modele robią coraz mniej błędów, więc „wygląda dobrze" nic nie dowodzi.

7 **Sprawdźcie nadawcę.** Nowe konto, brak historii, zmieniony numer, link skrócony albo z literówką w adresie. Linku z wiadomości nie otwierajcie, wejdźcie na stronę sami.

Gdy coś jest podejrzane albo już się stało

- **Podejrzany SMS:** przekażcie go bez zmian na bezpłatny numer **8080** (CERT Polska): funkcja „Przekaż", bez dopisków i bez zrzutów ekranu.
- **Podejrzana strona, mail albo link:** zgłoście na **incydent.cert.pl**.
- **Przelaliście pieniądze albo podaliście dane karty:** od razu dzwońcie do banku (blokada karty, próba zatrzymania przelewu), potem zgłoście sprawę na policję.
- **Wyciekły wasze dane:** zastrzeżcie PESEL, np. w aplikacji mObywatel.

Wersja dla rodziców (do przesłania): „Jeśli ktoś dzwoni albo pisze, że jestem w kłopotach i potrzebuję pieniędzy, rozłącz się i oddzwoń do mnie na mój stary numer. Zapytaj o nasze hasło. Nic nie przelewaj, dopóki ze mną nie porozmawiasz. Zdjęcie albo film możesz sprawdzić na synthid.com, ale nawet jak wyjdzie »czyste«, i tak zadzwoń."

Źródła: blog.google/innovation-and-ai/models-and-research/google-deepmind/synth-id-ai-content/ (7.10.2026: dostęp dla wszystkich, partnerzy, 180 mld) · deepmind.google/models/synthid/ (odporność znaku, sprawdzanie w Gemini, Search i Chrome) · androidpure.com/synthid-detector-general-availability/ (synthid.com, logowanie, „brak znaku ≠ prawdziwe") · digitaltrends.com (7.10.2026) · cert.pl (SMS na 8080, incydent.cert.pl).