HASŁO

Rodzinne hasło przeciw podrobionemu głosowi: jak je ustalić, jak go używać i co zrobić, gdy dzwoni „wnuczek”

dla was i dla rodziców · gotowa wiadomość do wysłania · gdzie zgłaszać w Polsce · stan na 11.10.2026

Dlaczego to ważne właśnie teraz

- Szybkie modele AI do klonowania głosu potrzebują dziś **od 3 do 30 sekund** nagrania (Bankier.pl, 16.09.2026). Wystarczy rolka, relacja albo powitanie na poczcie głosowej.
- W 2025 r. Policja odnotowała **5226** oszustw „na legendę” (na wnuczka, na policjanta, na wypadek). Pokrzywdzonych było **5409** osób, straty: **158,7 mln zł**. Rok wcześniej: 3825 oszustw.
- Nie każde takie oszustwo używa AI. Często dzwoni zwykły człowiek, który gra rolę. Hasło działa w obu przypadkach.
- Rodzinne hasło zaleca polska Policja („hasło klucz”) i amerykańskie FBI („secret word or phrase”).

Jak wybrać dobre hasło

☐ **Czegoś takiego nie ma w internecie.** Nie imię psa, nie data urodzin, nie nazwa ulicy, nie drużyna, której kibicujecie.

☐ **2 słowa, które do siebie nie pasują**, np. „zielony kalafior”, „tramwaj w piżamie”. Łatwo zapamiętać, trudno zgadnąć.

☐ **Ustalcie je na żywo** albo przez telefon, a nie w czacie rodzinnym. Jeśli ktoś przejmie konto na Messengerze czy WhatsAppie, przeczyta hasło.

☐ **Wszyscy znają to samo:** rodzice, dziadkowie, rodzeństwo, nastoletnie dzieci. Seniorom zapiszcie je na kartce w portfelu, bez podpisu „hasło”.

☐ **Zmieńcie je**, gdy ktoś je wypowie przy obcych albo gdy raz posłużyło do sprawdzenia podejrzanego telefonu.

☐ **Dodatkowo pytanie kontrolne:** coś, co wiecie tylko wy („co jedliśmy na weselu u Kaśki?”). Uwaga: odpowiedź nie może być w waszych zdjęciach na Facebooku.

Co zrobić, gdy dzwoni „bliski w kłopotach”

1. **Nie mówcie imion jako pierwsi.** Oszust czeka, aż powiecie „Tomek, to ty?”. Zapytajcie: „Kto mówi?”.
2. **Poproście o hasło.** „Podaj nasze hasło”. Prawdziwy wnuczek je zna. Wymówki („nie mam czasu”, „zapomniałem”) to sygnał do rozłączenia.
3. **Rozłączcie się** i **sami zadzwońcie** na numer, który macie zapisany od dawna, albo do kogoś z rodziny.
4. **Telefon stacjonarny:** odłóżcie słuchawkę i odczekajcie **30 sekund** albo zadzwońcie z innego telefonu. Oszust potrafi nie zwolnić linii i „odebrać” wasz telefon na policję (zalecenie Policji).
5. **Nic nie przelewajcie**, nie podawajcie kodu BLIK, nie oddawajcie pieniędzy „kurierowi”, nie instalujcie żadnej aplikacji.

Czerwone flagi w rozmowie

1 **Nagły wypadek, areszt, porwanie, szpital.** Do tego płacz i „nie mów nikomu, nawet mamie”.

2 **Nowy numer albo nowe konto.** „Zepsuł mi się telefon, piszę z numeru kolegi”.

3 **Pośpiech.** „Musisz teraz, inaczej pójdę do więzienia". Presja „tu i teraz" to znak rozpoznawczy oszustwa.

4 **„Policjant", „prokurator", „pracownik banku"** prosi o pieniądze, BLIK albo o udział w „akcji". Policja nigdy nie prosi o przekazanie pieniędzy ani kodu BLIK.

5 **Głos brzmi dobrze, ale rozmowa jest dziwna.** Krótkie zdania, unikanie pytań, cisza przy pytaniu o szczegóły. Klon AI odtwarza głos, nie wspomnienia.

Mniej waszego głosu w sieci (warto rozważyć)

- Powitanie na poczcie głosowej: standardowe z sieci zamiast nagrania waszym głosem.
- Konto prywatne albo mniej długich nagrań, na których mówicie, jeśli nie prowadzicie profilu zawodowo.
- Nie odpowiadajcie długo na głuche telefony z nieznanych numerów („halo, halo, słyszy mnie pan?").

Gdy coś się już stało: gdzie dzwonić w Polsce

Sytuacja	Co zrobić
Oszust jest w trakcie, np. jedzie „kurier" po pieniądze	Dzwońcie na **112**.
Przelew, BLIK albo dane karty poszły	**Od razu bank** (numer z odwrotu karty albo z aplikacji): blokada, próba zatrzymania przelewu. Potem zawiadomienie na policji.
Podejrzany SMS	Przekażcie go bez zmian na **8080** (CERT Polska, bezpłatnie).
Podejrzany link, strona, wiadomość	Zgłoszenie na **incydent.cert.pl**.
Wyciekły dane (dowód, PESEL)	Zastrzeżcie PESEL w aplikacji **mObywatel** albo w urzędzie gminy.

Wiadomość do wysłania rodzicom (skopiujcie):
„Mamo, tato, oszuści potrafią już podrobić mój głos z krótkiego nagrania z internetu. Ustalmy hasło: **[wasze hasło]**. Powiem je wam przez telefon, nie piszę go tutaj. Jeśli ktoś zadzwoni, że jestem w kłopotach i potrzebuję pieniędzy, poproś o to hasło. Jeśli go nie poda, rozłącz się i zadzwoń do mnie na mój stary numer. Nic nie przelewaj, nie podawaj kodu BLIK i nie dawaj pieniędzy żadnemu kurierowi, nawet jeśli głos brzmi dokładnie jak mój. Policja nigdy nie prosi o pieniądze. Kocham was, wolę 10 telefonów za dużo niż 1 za mało."

Źródła (11.10.2026): policja.pl, „Zwalczanie przestępczości kryminalnej", 16.01.2026 (5226 oszustw, 5409 pokrzywdzonych, 158 676 710 zł) · policja.pl, „Uwaga! BLIK i oszustwa z wykorzystaniem sztucznej inteligencji", 17.10.2025 (hasło klucz, 30 sekund, inny telefon) · policja.pl, „Bankowcy dla cyberedukacji: Metoda na wnuczka w nowej odsłonie", 13.03.2025 · bankier.pl, „AI sklonuje każdy głos…", 16.09.2026 (3–30 s próbki) · FBI IC3 PSA I-120324-PSA, 3.12.2024 (secret word) · cert.pl (8080, incydent.cert.pl) · gov.pl/web/mobywatel (zastrzeżenie PESEL).