

DZIECKO BEZPIECZNE W INTERNECIE



TRZY FILARY BEZPIECZEŃSTWA

01 / RELACJA

Dziecko może powiedzieć prawdę nawet wtedy, gdy złamało wcześniejszą zasadę.

02 / ZABEZPIECZENIA

Limity czasu i treści, akceptowanie pobrań, ograniczenia kontaktów i zakupów.

03 / REAKCJA

Gdy pojawia się szantaż, groźba lub przemoc – zbierz dostępne informacje, zgłoś i szukaj pomocy.

I. MAPA ZAGROZEŃ: CO MOŻE SPOTKAĆ DZIECKO?

KONTAKT Z NIEZNAJOMYM

„Mam 11 lat, gramy razem.” W rzeczywistości może to być dorosły, który buduje zaufanie i prosi o tajemnicę.

→ **REAKCJA:** rozmowa o kontaktach, ograniczenie czatu, wspólne zgłoszenie.

OSZUSTWA W GRACH

„Darmowe Robuxy”, fałszywy sklep, link do logowania, prośba o kod SMS.

→ **REAKCJA:** nie klikać, zmienić hasło po ujawnieniu, włączyć 2FA, sprawdzić płatności.

CYBERPRZEMOC

Obrażliwe grupy, wykluczanie, publikowanie nagrań bez zgody, podszywanie się.

→ **REAKCJA:** wsparcie dziecka, zgłoszenie platformie i szkole, nie rozpowszechniać.

SZANTAŻ I NAKŁANIANIE

„Wyślij zdjęcie, inaczej pokażę rozmowę”, „zrób to niebezpieczne zadanie”.

→ **REAKCJA:** przerwać kontakt, zapewnić bezpieczeństwo, Policja przy podejrzeniu przestępstwa.

NIEODPOWIEDNIE TREŚCI

Przemoc, pornografia, samookaleczenia, niebezpieczne wyzwania, „patostreamy”.

→ **REAKCJA:** ustawienia treści i rozmowa o emocjach, w razie potrzeby specjalista.

NADUŻYWANIE EKRANÓW

Utrata snu, wycofanie, narastające konflikty, brak czasu na ruch.

→ **REAKCJA:** ustalić ramy dnia; nie traktować samej liczby minut jako diagnozy.

AI I DEEPAKE

Fałszywy głos znajomego, przerobione intymne zdjęcie, „dowód” wygenerowany przez AI.

→ **REAKCJA:** nie udostępniać, zweryfikować innym kanałem, zgłosić nadużycie.

DANE I LOKALIZACJA

Adres, plan lekcji, geotagi, szkolne zdjęcie z nazwą placówki, publiczny profil.

→ **REAKCJA:** wyłączyć lokalizację dla zbędnych aplikacji i ukryć dane.

II. MANIPULACJA I SZANTAŻ: JAK TO DZIAŁA?

Od pierwszej miłej rozmowy do presji – poznaj schemat, który może wyglądać bardzo niewinnie.

1	Pierwszy kontakt: wspólna gra lub miła rozmowa na czacie.
2	Budowanie relacji: pochwały, „tylko ja Cię rozumiem”, obietnice prezentów.
3	Izolowanie: zaproszenie na prywatny komunikator, żądanie tajemnicy.
4	Przekraczanie granic: prośby o zdjęcia, dane, zadania, udowodnienie lojalności.
5	Szantaż: groźby rozpowszechnienia treści lub skrzywdzenia, wymuszanie kolejnych zachowań.

NIE OCENIAJ PO SAMEJ NAZWIE GRY

Roblox, Minecraft, Fortnite, Discord, TikTok, Telegram, Steam czy Twitch nie są automatycznie niebezpieczne. Znaczenie ma to, KTO kontaktuje się z dzieckiem i CZEGO żąda.

Niepokojące sygnały u dziecka

- Lęk przed powiadomieniami, silny niepokój po odebraniu telefonu, ukrywanie kontaktów.
- Nagły spadek nastroju, izolowanie się, bezsenność, znaczne zmiany zachowania.
- Przelewy, zakupy lub prośby o pieniądze bez wyjaśnienia; pojawienie się nowych kont.
- Wypowiedzi o obowiązku wykonania „zadań”, szantażu, krzywdzeniu siebie lub innych.
- Konkretnie groźby, wskazanie celu, terminu lub przygotowań do przemocy.

Żaden pojedynczy objaw ani zainteresowanie kryminalistyką nie dowodzą udziału w niebezpiecznej grupie. Istnieją społeczności wykorzystujące dzieci, czasem opisywane nazwami „764” lub podobnymi. Kluczowe są konkretne zachowania i kontekst, nie samo słowo czy grafika.

Pytania, które można zadać bez przesłuchiwania

- „ Czy ktoś z gry chce rozmawiać z Tobą poza grą? Znasz tę osobę naprawdę?”
- „ Czy ktoś proponował Ci prezent za zdjęcie, hasło, wykonanie zadania albo milczenie?”
- „ Co byś zrobił(a), gdyby ktoś zagroził publikacją Twojego zdjęcia?”
- „ Czy widziałeś(-aś) treści, które straszą Cię albo zachęcają do przemocy?”

III. Słownik zagrożeń w sieci

Określenia, które mogą pojawić się w rozmowach, grach i mediach społecznościowych.

764

Nazwa sieci internetowej opisywanej w kontekście wykorzystywania, szantażowania i krzywdzenia dzieci oraz młodzieży.

NLM

Skrót pojawiający się w niektórych kontekstach internetowych. Jego znaczenie i związek z działalnością propagującą przemoc należy każdorazowo weryfikować na podstawie kontekstu i wiarygodnych źródeł.

**Cutting /
self-harm**

Określenia dotyczące samookaleczania lub innego celowego wyrządzania sobie krzywdy.

Doxxing

Ujawnianie lub rozpowszechnianie prywatnych danych osobowych bez zgody danej osoby, często w celu jej zastraszenia, nękania lub narażenia na niebezpieczeństwo.

Swatting

Wywoływanie nieuzasadnionej interwencji służb ratunkowych lub porządkowych poprzez fałszywe zgłoszenie poważnego zagrożenia, np. informacji o rzekomym ataku lub podłożeniu bomby.

Sextortion

Szantaż polegający na groźeniu ujawnieniem materiałów intymnych lub o charakterze seksualnym w celu wymuszenia określonego zachowania, uzyskania kolejnych materiałów albo osiągnięcia innych korzyści.

Lootbox

Wirtualna skrzynka w grze zawierająca losowo przyznawane przedmioty lub nagrody. Sam termin jest neutralny i nie świadczy o zagrożeniu. Warto jednak zachować czujność, gdy ktoś wykorzystuje obietnicę otrzymania takich nagród, aby zdobyć zaufanie dziecka, nakłonić je do prywatnego kontaktu lub wymusić określone zachowanie.

PAMIĘTAJ

Żaden z tych terminów nie jest jednoznacznym dowodem zagrożenia. Liczą się okoliczności, treść rozmów i zachowanie uczestników.

IV. KONTROLA RODZICIELSKA NA TELEFONIE

Dwa najpopularniejsze systemy i ustawienia, od których warto rozpocząć.

ZANIM ZACZNIESZ

Nadzór działa najlepiej na koncie dziecka z prawidłowym wiekiem, a nie na koncie dorosłego. Rodzic powinien znać konfigurację, ale nie udostępniać dziecku hasła administracyjnego ani kodu ograniczeń.

Android / Chromebook – Google Family Link

- 1 Zainstaluj Family Link na urządzeniu rodzica i utwórz lub połącz nadzorowane konto Google dziecka.
- 2 W aplikacji wybierz profil dziecka → „Czas korzystania z urządzenia” → „Limity czasu”; ustaw dzienny limit i harmonogram.
- 3 Wejdź do „Limity korzystania z aplikacji”: ogranicz konkretne gry lub komunikatory.
- 4 W ustawieniach usług Google skonfiguruj ograniczenia Chrome, wyszukiwania, YouTube i Google Play oraz zgodę na instalacje / zakupy.
- 5 Sprawdź raport użycia aplikacji i porozmawiaj o najbardziej używanych usługach.

Ważne: Family Link nie nadzoruje całego iPhone’a dziecka ani każdej aktywności w przeglądarce czy komunikatorach. Lokalizacja zależy od urządzenia i jego konfiguracji. Oficjalna pomoc: support.google.com/families.

iPhone / iPad – Chmura rodzinna + „Czas przed ekranem”

- 1 Na swoim urządzeniu Apple otwórz „Ustawienia” → „Rodzina” i dodaj konto dziecka.
- 2 Wybierz dziecko → „Czas przed ekranem”; skonfiguruj limity aplikacji i harmonogram czasu bez urządzenia.
- 3 Włącz „Ograniczaj treść i prywatność” oraz odpowiedni poziom treści internetowych i aplikacji.
- 4 Ustaw „Poproś o zakup”, limity komunikacji i – jeśli dostępne – funkcje bezpieczeństwa komunikacji.

- 5 Ustaw osobny kod „Czasu przed ekranem”, inny niż kod odblokowania telefonu; nie podawaj go dziecku.

CO ZOBACZY RODZIC?

Zwykle czas użycia, aplikacje, prośby o instalacje i część ustawień, a nie pełną treść wszystkich wiadomości. Regularne wspólne przeglądanie listy kontaktów i rozmowa są nadal potrzebne.

V. KOMPUTERY, KONSOLE I DOMOWA SIĘĆ

Ustawienia telefonu to za mało — dziecko może korzystać również z komputera, konsoli i domowego Wi-Fi.

Windows / Xbox — Microsoft Family Safety

- 1 Utwórz grupę rodzinną na family.microsoft.com; konto dziecka powinno być kontem członka rodziny.
- 2 Połącz komputer z Windows lub konsolę Xbox z właściwym kontem dziecka.
- 3 W ustawieniach profilu włącz harmonogram i limity czasu dla urządzenia oraz konkretnych aplikacji / gier.
- 4 Skonfiguruj ograniczenia wiekowe gier, zakupów i raportowanie aktywności.
- 5 Jeśli filtrujesz strony, pamiętaj, że filtry Family Safety działają z obsługiwaną przeglądarką Microsoft Edge i kontem Microsoft.

PlayStation / Nintendo Switch — ustawienia rodzinne

- Utwórz konto dziecka w grupie rodzinnej konsoli i użyj oficjalnej aplikacji / panelu rodzicielskiego producenta.
- Ogranicz gry według wieku, czat lub interakcje z obcymi oraz zakupy, jeśli konsola oferuje te funkcje.
- Dodaj limit czasu i kod nadzorczy; sprawdź też ustawienia w samych grach.

Wi-Fi w domu i przeglądarki

- Zmień domyślne hasło administratora routera, włącz aktualizacje i silne zabezpieczenie Wi-Fi.
- Jeśli router pozwala: osobny profil dziecka, harmonogram dostępu, filtr rodzinny DNS.

- Włącz SafeSearch i odpowiednie ustawienia YouTube, pamiętając, że filtr nigdy nie jest stuprocentowy.
- Sprawdź, czy dziecko nie używa innych urządzeń lub transmisji danych komórkowych, które omijają ustawienia routera.

NIE INSTALUJ NARZĘDZI SZPIEGUJĄCYCH

Nie polecamy potajemnych aplikacji do śledzenia treści rozmów ani łamania haseł. Ustal jawne, proporcjonalne do wieku zasady nadzoru; przy podejrzeniu krzywdzenia działaj zdecydowanie i włącz odpowiednie służby.

VI. GRY I KOMUNIKATORY – CO SPRAWDZIĆ?

W większości usług ważniejsze od samej nazwy jest to, kto może pisać do dziecka i na jakich zasadach.

Roblox

- 1 Utwórz własne konto Roblox z uprawnieniami rodzica i połącz je z kontem dziecka.
- 2 „Settings” → „Parental Controls”: ustaw poziom treści, kontakty, limity czasu, wydatki i dostępne doświadczenia.
- 3 Wspólnie przejrzyj znajomych oraz gry, w które dziecko gra najczęściej.

Uwaga: starsze instrukcje z „Parent PIN” mogą być nieaktualne — Roblox zastąpił to rozwiązanie kontem rodzica z uprawnieniami. Zakres kontroli zależy od wieku. Pomoc: en.help.roblox.com (Parental Controls Overview).

Fortnite / Epic Games

- 1 Zaloguj się na konto Epic dziecka i otwórz sekcję „Kontrola rodzicielska”.
- 2 Ustaw oddzielny 6-cyfrowy PIN i dostosuj czat głosowy / tekstowy, wiek treści oraz zakupy.
- 3 Sprawdź, czy rozmowy nie odbywają się przez czat konsoli lub inne komunikatory poza grą.

Minecraft / konta Microsoft

Sprawdź konto Microsoft dziecka, tryb multiplayer, możliwość dołączania do serwerów, zaproszenia do znajomych i czat. Przy młodszych dzieciach wybieraj serwery znane rodzicom i wspólną grę.

Discord – Centrum rodzinne

Na koncie rodzica wejdź w „Ustawienia” → „Centrum rodzinne” i połącz konta po zaakceptowaniu zaproszenia przez nastolatka. Możesz zobaczyć m.in. część ostatnich kontaktów, serwerów i aktywności, a także zarządzać wybranymi ustawieniami. Centrum rodzinne NIE pokazuje treści prywatnych wiadomości. Sprawdź również ustawienia DM, zaproszeń i prywatności.

Telegram, Steam, Twitch

Przejrzyj z dzieckiem listę grup, znajomych, prywatność profilu i to, kto może wysyłać wiadomości. Zwróć uwagę na przenoszenie znajomości z gry do innego komunikatora, podejrzane linki, prośby o pieniądze i tajemnice. Funkcje nadzoru są na tych platformach różne i ograniczone.

VII. MEDIA SPOŁECZNOŚCIOWE, AI I PRYWATNOŚĆ

TikTok i inne media społecznościowe

- Przestrzegaj minimalnego wieku danej platformy; nie zakładaj młodszemu dziecku konta z fałszywą datą urodzenia.
- Gdy nastolatek korzysta legalnie z usługi: wspólnie ustaw prywatność konta, wiadomości, komentarze i widoczność filmów.
- TikTok oferuje „Parowanie rodziny” (Family Pairing): w ustawieniach konta łączy profil rodzica i nastolatka; zakres funkcji zależy od wieku i wersji aplikacji.
- Sprawdź, czy dziecko publikuje lokalizację w czasie rzeczywistym, zdjęcia w szkolnym stroju, plan dnia lub filmy z innymi dziećmi bez zgody.

Ochrona danych i kont

- Nie podawaj kodów SMS do logowania, nawet gdy ktoś podszywa się pod znajomego lub obsługę platformy.
- Dla każdego konta używaj unikalnego hasła / menedżera haseł, włącz 2FA.
- Przeglądaj uprawnienia aplikacji: kamera, mikrofon, lokalizacja i dostęp do kontaktów.
- Nie publikuj skanów dokumentów, biletów z kodami czy danych ułatwiających namierzenie dziecka.

SZCZEGÓLNE ZAGROŻENIE: SPREPAROWANE ZDJĘCIA INTYMNE

Treści generowane przez AI mogą służyć do upokarzania i szantażu. Nie obwiniaj dziecka, nie przesyłaj ani nie kopiuj materiałów intymnych z udziałem nieletnich; zanotuj adres konta/strony i skontaktuj się z Policją i Dyżurnet.pl.

VIII. CO ZROBIĆ, GDY POJAWIA SIĘ ZAGROŻENIE?

BEZPOŚREDNIE ZAGROŻENIE – DZWOŃ 112

Jeśli pojawiają się konkretne groźby skrzywdzenia, wskazanie celu lub terminu ataku, przygotowania do przemocy, bezpośrednie ryzyko samobójcze albo zagrożenie zdrowia / życia – dzwoń 112. Nie czekaj na komplet dowodów.

- 1 Zadbaj o bezpieczeństwo dziecka. Odsuń je od presji, zapewnij obecność dorosłego; nie obwiniaj ani nie krzycz.
- 2 Ustal, co się stało: kto, gdzie, od kiedy, czy istnieje kontakt poza Internetem lub groźba spotkania.
- 3 W przypadku zwykłych gróźb, nękania lub oszustwa zabezpiecz wiadomości: zrzuty ekranu, nazwę użytkownika, link, datę, godzinę. Nie publikuj materiałów.
- 4 Jeśli sprawa dotyczy intymnych wizerunków osób małoletnich – nie pobieraj, nie kopiuj i nie przesyłaj ich. Zapisz adres strony/identyfikator konta, zgłoś Policji i Dyżurnet.pl.
- 5 Nie konfrontuj samodzielnie sprawcy, nie odpowiadaj groźbami, nie umawiaj spotkania „na wyjaśnienie”.
- 6 Zgłoś zdarzenie platformie; po zabezpieczeniu potrzebnych informacji zablokuj sprawcę.
- 7 Gdy mogło dojść do przestępstwa, powiadom Policję. Jeśli sprawa dotyczy rówieśników w szkole – poinformuj wychowawcę / dyrektora i współpracuj w ramach szkolnych procedur.
- 8 Zadbaj o wsparcie psychologiczne.

Gdzie szukać pomocy?

112	POLICJA	DYŻURNET.PL	SZKOŁA
zagrożenie bezpośrednie	przestępstwo, szantaż, poważne groźby	nielegalne treści online	zdarzenia związane z uczniami i bezpieczeństwem

IX. NAJWAŻNIEJSZE ZALECENIA DLA RODZICÓW

Sześć codziennych działań, które pomagają chronić dziecko w Internecie.

01 **Interesuj się aktywnością dziecka w Internecie.**

Rozmawiaj o znajomościach nawiązywanych podczas gier, korzystania z komunikatorów i mediów społecznościowych.

02 **Ustal jasne zasady korzystania z urządzeń.**

Omów zasady kontaktowania się z nieznajomymi, udostępniania treści i korzystania z prywatnych komunikatorów.

03 **Regularnie rozmawiaj o bezpieczeństwie cyfrowym.**

Wyjaśniaj, czym są manipulacja, szantaż, wywieranie presji i naruszanie prywatności.

04 **Ucz ochrony danych osobowych.**

Przypominaj, aby nie przekazywać nieznajomym haseł, adresu zamieszkania, planu dnia ani prywatnych zdjęć.

05 **Ostrzegaj przed pozornie atrakcyjnymi ofertami.**

Wirtualne prezenty, waluta w grze i obietnice nagród mogą być wykorzystywane do zdobywania zaufania dziecka.

06 **Zwracaj uwagę na niepokojące zmiany w zachowaniu.**

Mogą to być nasilony lęk, ukrywanie kontaktów, strach przed odejściem od telefonu, otrzymywanie gróźb lub wypowiedzi dotyczące skrzywdzenia siebie albo innych.

Ważne numery i miejsca pomocy

112 – numer alarmowy

116 111 – telefon zaufania dla dzieci i młodzieży (24/7)

800 12 12 12 – Dziecięcy Telefon Zaufania RPD

800 100 100 – telefon dla dorosłych w sprawie bezpieczeństwa dzieci (sprawdź bieżące godziny na 800100100.pl)

dyzurnet.pl – zgłoszenia nielegalnych treści.

MATERIAŁY ŹRÓDŁOWE:

support.google.com/families • support.apple.com/pl-pl/108806 • support.microsoft.com/pl-pl/family-safety • en.help.roblox.com • epicgames.com/help • support.discord.com • support.tiktok.com • 116111.pl • 800100100.pl • dyzurnet.pl