Cyberbezpieczeństwo Twojego dziecka 5-17 lat

Jak chronić dziecko w Internecie (5-17 lat)

☑ ustawienia ☑ rozmowy ☑ zasady
☑ ochrona

Radosław Wilmański

SPIS TREŚCI

Wstęp

Drodzy Rodzice,

Ten e-book nie powstał w laboratorium ekspertów ani z zimnych danych statystycznych. Powstał z rozmów, które słyszymy codziennie: „Nie wiem, co moje dziecko robi w internecie", „Nie chcę być tym złym, który zabiera telefon", „Boje się, że coś przegapię". Każdy z nas chce dobrze – ale świat cyfrowy rozwija się szybciej, niż potrafimy nadążyć.

Dlatego nie chodzi tu o zakazy, aplikacje czy filtry. Chodzi o relację. O rozmowę, która zastępuje kontrolę. O zaufanie, które daje bezpieczeństwo. O obecność – nawet wtedy, gdy nie rozumiemy wszystkiego.

Nie musisz być ekspertem od technologii, by być przewodnikiem swojego dziecka w sieci. Wystarczy, że będziesz blisko – z pytaniem, ciekawością, a czasem tylko z milczeniem i otwartym sercem.

Ten e-book to przewodnik po cyfrowym świecie dzieci – bez moralizowania, bez straszenia. Z przykładami, rozwiązaniami i dialogami, które pomogą ci być obok, nie nad. Jeśli po przeczytaniu chociaż raz porozmawiasz z dzieckiem o internecie – to już będzie sukces.

Z serdecznością,
Radosław Wilmański
(autor i tata, który też czasem się gubi – ale zawsze wraca do rozmowy)

Rozdział 1: Świat dziecka online

Jeszcze kilkanaście lat temu dzieci spędzały większość czasu poza domem – na boisku, na podwórku, wśród rówieśników.
Dzisiejsze dzieci też mają swoje „podwórko", ale jest ono wirtualne. To tam spotykają się z kolegami, przeżywają emocje, śmieją się i kłócą.
Internet nie jest dla nich dodatkiem do rzeczywistości – on jest rzeczywistością.

Rodzic, który patrzy na dziecko z telefonem w ręku, często myśli: „On tylko siedzi w internecie".
Tymczasem dziecko naprawdę tam żyje – tak, jak my kiedyś żyliśmy na trzepaku czy w szkolnym korytarzu.

Najpopularniejsze przestrzenie online

YouTube – niekończąca się telewizja

Dla wielu dzieci to podstawowe źródło rozrywki i wiedzy.
Oglądają tam bajki, tutoriale, vlogi rówieśników.
Jednak algorytmy YouTube potrafią prowadzić z filmiku na filmik – coraz dalej od treści odpowiednich dla dziecka.

⚠ **Uwaga:** Dziecko zaczynające od niewinnych bajek może po kilku kliknięciach trafić na przerażające lub brutalne treści.

TikTok – świat krótkich filmików

Dynamiczne, krótkie nagrania tworzą niekończący się strumień zabawy. TikTok wciąga dzieci, bo każdy film trwa kilka sekund, a kolejny jest tylko jednym przesunięciem palca.

💡 **Wskazówka:** Jeśli dziecko korzysta z TikToka, warto ustawić tryb „Parental Controls" – ogranicza dostęp do części treści i pozwala włączyć limity czasu.

Roblox i Minecraft – gry społeczne

Dla rodziców to „gry w klocki". Dla dzieci – światy równoległe. Tam tworzą budowle, rozmawiają z innymi, a czasem spotykają ludzi, których nie znają w realnym życiu.

📌 **Checklista –** pytania do dziecka grającego w Roblox/Minecraft:
Z kim grasz?
Czy wiesz, kim naprawdę są Twoi znajomi w grze?
Co robicie, gdy gracie razem?
Czy ktoś kiedyś prosił Cię o zdjęcie albo prywatne informacje?

Discord – komunikator dla graczy

Discord powstał jako aplikacja do rozmów w grach, ale szybko stał się miejscem tysięcy grup tematycznych. Dzieci spędzają tam godziny – często poza wiedzą rodziców.

⚠ **Uwaga:** Na Discordzie łatwo natrafić na grupy z treściami dla dorosłych.

Instagram i Snapchat – świat wizerunku

Dla nastolatków to podstawowe przestrzenie budowania swojego wizerunku. Zdjęcia, relacje, lajki – wszystko to daje satysfakcję,
ale też presję: „muszę być idealny, muszę mieć followersów".

💡 **Wskazówka:** Porozmawiaj z dzieckiem o tym, że zdjęcia w internecie często są „podrasowane" i nie pokazują prawdziwego życia.

Scenariusze wiekowe

- 7-latek – korzysta głównie z YouTube i gier edukacyjnych. Łatwo ufa nieznajomym
- 10-latek – gra online, dołącza do grup, zaczyna samodzielnie szukać treści.
- 14-latek – intensywnie używa social mediów, porównuje się z innymi, ukrywa aktywność przed rodzicami.

📌 **Checklista –** na co zwrócić uwagę:
7 lat – treści wideo i reklamy.
10 lat – kontakty online.
14 lat – presja społeczna i uzależnienie od social mediów.

Historie z życia wzięte

(Opartena prawdziwychsytuacjach z doświadczeń rodziców i terapeutów dziecięcych)

👧 Historia Kasi (7 lat) – “Bajka, która nie była bajką”

Kasia była radosną siedmiolatką. Uwielbiała kotki, kolorowe bajki i YouTube’a.
Rodzice często pozwalali jej oglądać filmy na tablecie, żeby mieć chwilę spokoju po pracy.
Pewnego dnia, podczas oglądania bajki o pieskach, filmik automatycznie przełączył się na „związaną” animację.
Tyle że zamiast śmiechu – był **krzyk, krew i brutalne sceny**.
Kasia **zamarła**. Nie rozumiała, co się dzieje.
Płakała, ale bała się wyłączyć tablet – nie wiedziała jak.
Wieczorem miała koszmary. Rano powiedziała tylko: „Nie chcę już oglądać bajek”.
Rodzice zorientowali się dopiero, gdy zaczęła unikać tabletu i spała przy włączonym świetle.
Po rozmowie okazało się, że **Kasia myślała, że to jej wina**, że obejrzała coś złego.
Rodzice włączyli **YouTube Kids**, omówili z nią całą sytuację i ustalili zasadę: **„Oglądamy tylko razem albo w salonie”**.
Dziś Kasia znów ogląda bajki – ale zawsze z rodzicem obok.

⚠ *Automatyczne rekomendacje na YouTube potrafią prowadzić do nieodpowiednich treści. Nawet niewinne bajki mogą przerodzić się w coś, co dziecko zapamięta na długo – z lękiem.*

👧 Historia Oli (10 lat) – "Zaufany kolega z gry"

Ola uwielbiała Minecrafta. Budowała zamki, ogrody i prowadziła własne „królestwo" na serwerze.
Wieczorami logowała się na **Discorda**, żeby rozmawiać z „kolegą z gry" – kimś, kto zawsze ją chwalił i pomagał budować.
Rozmowy szybko przeszły z budowania zamku do prywatnych tematów: szkoły, rodziny, wyglądu.
„Jesteś taka fajna, nie mów rodzicom, że piszemy. Dorośli i tak nic nie rozumieją" – napisał któregoś wieczoru.
Ola zaczęła kasować rozmowy, by nikt ich nie zobaczył. Czuła się wyjątkowa.
Kilka dni później „kolega" poprosił o zdjęcie, „żeby wiedzieć, jak wygląda jego najlepsza przyjaciółka".
Ola się przestraszyła, ale też nie wiedziała, co zrobić.
Zaczęła **unikać rozmów z rodzicami**, spała niespokojnie.
Dopiero po tygodniu przyznała się mamie – z płaczem.
Rodzice byli w szoku. Na szczęście zareagowali spokojnie, zgłosili profil i porozmawiali z Olą o bezpieczeństwie.
Ola wróciła do gry, ale **zrozumiała, że nie każdy w sieci jest tym, za kogo się podaje.**

⚠ *Grooming często zaczyna się niewinnie – od pochwał, gier i przyjaźni. Najlepszą ochroną jest rozmowa i nauka reagowania, gdy dziecko czuje się niekomfortowo.*

👦 Historia Michała (14 lat) – "Lajki zamiast pewności siebie"

Michał zawsze był uśmiechniętym chłopakiem. Lubił sport, śmiał się z kolegami.

Kiedy dostał nowy telefon, założył konto na Instagramie – z początku wrzucał zabawne filmiki z treningu.
Szybko przybyło mu obserwujących.
Ale z każdym tygodniem coraz bardziej przejmował się tym, ile osób zareaguje na jego zdjęcia.
Kiedy jedno ze zdjęć zebrało tylko kilka lajków, Michał spędził wieczór w pokoju, przeglądając profile rówieśników.
Zaczął porównywać się z innymi: ich ubraniami, ciałem, popularnością.
Z dnia na dzień wycofywał się z rozmów w domu, spędzał czas tylko online.
Mama zauważyła, że unika kontaktu wzrokowego, nie wychodzi z pokoju, usuwa kolejne posty.
Po kilku tygodniach zgodził się na rozmowę z psychologiem szkolnym.
Okazało się, że rozwinęły się u niego objawy obniżonej samooceny i lęku społecznego.
Dziś Michał ogranicza media społecznościowe do 30 minut dziennie.
Zaczął z powrotem chodzić na treningi.
Rodzice wspólnie z nim wprowadzili zasadę: “Nie wszystko, co widzimy w sieci, jest prawdziwe”.

⚠ *Porównywanie się z nierealnymi wzorcami z internetu może prowadzić do zaburzeń emocjonalnych, depresji i poczucia niskiej wartości.*

Wnioski dla rodziców

Każda z tych historii pokazuje coś innego, ale mają wspólny mianownik:
➡ dziecko nie miało narzędzi, żeby samo zareagować.
Dlatego:

- Rozmawiajmy **zanim** coś się wydarzy.
- Obserwujmy **zmiany w zachowaniu dziecka** – wycofanie, lęk, unikanie rozmów, utratę zainteresowań.
- Reagujmy **bez krzyku i ocen**. Strach dziecka zamieni się w zaufanie tylko wtedy, gdy wie, że może przyjść po pomoc.

💡 **Wskazówka:** Włącz na YouTube tryb „Ograniczony” (Restricted Mode), aby odfiltrować część treści.

Kluczowe przesłanie rozdziału

Twoje dziecko nie „siedzi w telefonie” – ono tam żyje.
Internet to jego szkoła, plac zabaw i korytarz szkolny w jednym.
Twoim zadaniem nie jest zakaz, ale mądre towarzyszenie.
Im lepiej zrozumiesz świat online, tym łatwiej pomożesz dziecku się w nim poruszać.

Rozdział 2: Zagrożenia w sieci

Internet sam w sobie nie jest ani dobry, ani zły. To narzędzie – tak jak samochód. Może zawieźć nas do szkoły czy pracy, ale w nieodpowiednich rękach staje się zagrożeniem. Dla dziecka internet to miejsce zabawy i nauki, ale też przestrzeń, w której łatwo o krzywdę.

Każdy rodzic powinien znać najczęstsze zagrożenia, aby móc szybko reagować i uczyć dziecko świadomego korzystania z sieci.

Cyberprzemoc i hejt

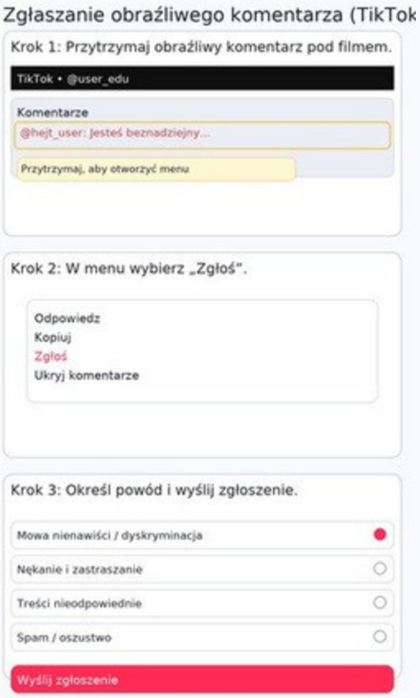
Cyberprzemoc to jedno z największych wyzwań w świecie online. Występuje tam, gdzie dzieci komunikują się ze sobą – na Messengerze, TikToku, Discordzie, w grach online.

Formy cyberprzemocy:

- obraźliwe komentarze i przezwiska,
- tworzenie fałszywych profili ośmieszających dziecko,
- rozsyłanie kompromitujących zdjęć lub filmików,
- wykluczanie z grup czy rozmów online.

⚠ **Sygnały ostrzegawcze:**

- dziecko nagle przestaje korzystać z ulubionej aplikacji,
- boi się sprawdzić wiadomości lub reaguje lękiem na powiadomienia,
- staje się wycofane i niechętnie rozmawia o relacjach z rówieśnikami.



💡 **Wskazówka dla rodzica:** Pokaż dziecku, jak działa „blokuj i zgłoś". To naturalna reakcja na hejt, a nie oznaka słabości.

📌 **Checklista –** jak reagować na cyberprzemoc:

- Zapewnij dziecko, że nie jest winne temu, co się stało,
- Zrób zrzuty ekranu obraźliwych treści (dowód),
- Zgłoś sytuację do szkoły, jeśli dotyczy rówieśników,
- Jeśli sprawa jest poważna – nie bój się zawiadomić policji.

Grooming i niebezpieczne kontakty

„Grooming" to proces, w którym dorosły zdobywa zaufanie dziecka, udając rówieśnika, a następnie próbuje je wykorzystać. Zaczyna się niewinnie – od wspólnej gry, rozmów o szkole, zainteresowania pasjami dziecka. Dopiero później pojawiają się prośby o zdjęcia, sekrety, a nawet propozycje spotkań.

⚠ **Sygnały ostrzegawcze:**

- dziecko spędza dużo czasu na prywatnych czatach,
- ma „nowego przyjaciela", o którym nic nie mówi,
- nagle zaczyna mieć sekrety w internecie,
- ktoś wysyła mu prezenty online (np. płatne skiny w grze).

💡 **Wskazówka:** Naucz dziecko zasady „nigdy nie wysyłaj zdjęcia obcej osobie" i że przyjaciel online ≠ przyjaciel w realu.

📌 **Checklista –** jak reagować na grooming:

- Zawsze rozmawiaj z dzieckiem bez oceniania („chcę ci pomóc, nie ukarać"),
- Zapisz rozmowy (dowód),
- Zablokuj kontakt i zgłoś konto,
- W przypadku poważnych podejrzeń – zgłoś sprawę na policję lub do organizacji zajmujących się bezpieczeństwem dzieci online.

Grooming – przykład 1: hobby → wiek → prywat

Przykład edukacyjny: brak treści wrażliwych.

Hej! Super profil. Grasz w Minecrafta?

Tak, czasem gram.

Ile masz lat? Ja 13 ☺

12.

Czerwona flaga: dopytywanie o wiek na początku rozmowy.

Przenieśmy się na WhatsApp — tu słabo działa. Daj numer.

Uwaga: próba przeniesienia rozmowy poza platformę omija moderację i raportowanie.

Grooming – przykład 2: prezenty → dane → tajer

Przykład edukacyjny: brak treści wrażliwych.

Mogę Ci kupić skina. Mam kody premium.

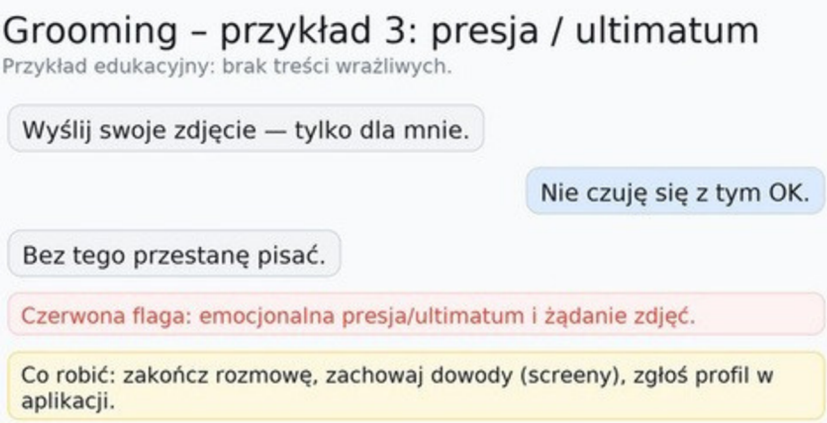
Serio?

Podaj mail/telefon — wyślę tylko Tobie.

Czerwona flaga: oferowanie prezentów w zamian za dane kontaktowe.

Tylko nie mów rodzicom — nie zrozumieją.

Czerwona flaga: prośba o tajemnicę i izolowanie od dorosłych.



Fake newsy i dezinformacja

Internetpełen jest informacji – niestety nie wszystkie są prawdziwe. Dzieci łatwo wierzą w fake newsy, bo często widzą je w atrakcyjnej formie: filmiku, memie czy grafice. Przykłady fake newsów:

- „Popularny youtuber umarł" – a tak naprawdę to chwyt klików,
- „Jeśli udostępnisz ten post, wygrasz iPhone'a",
- „Szczepionki zawierają chipy" – informacje powielane nawet przez dorosłych.

⚠ **Sygnały ostrzegawcze:**

- dziecko powtarza dziwne informacje znalezione w sieci,
- zaczyna się bać rzeczy, które nie mają sensu (np. końca świata).

💡 **Wskazówka:** Naucz dziecko trzech pytań kontrolnych:

1. Kto to napisał?
2. Skąd ta osoba ma informacje?
3. Czy inne źródła to potwierdzają?

📌 **Ćwiczenie z dzieckiem:**
Razem znajdźcie w internecie sensacyjny nagłówek i spróbujcie sprawdzić, czy to prawda.

⚠ **Schemat powtarza się niemal zawsze:**

- Sensacyjny nagłówek: „Nie żyje…”, „Tragiczny wypadek…”, „Cała Polska w szoku…”.
- Brak źródeł: brak odwołania do wiarygodnych mediów (PAP, Onet, TVP, Polsat News itp.).
- Czarno-białe zdjęcie celebryty – często używane jako sugestia żałoby.
- Link do zewnętrznej strony – po kliknięciu często wymagane jest logowanie (wyłudzanie haseł).
- Wpis pojawia się tylko w social media / podejrzanych portalach, nie ma go w poważnych mediach.
- Presja emocjonalna – „Kliknij, by dowiedzieć się więcej”, „Zobacz nagranie”.

💡 **Wskazówka dla rodziców i nastolatków:** zanim udostępnisz lub uwierzysz w taką informację:
1. Sprawdź w Google News lub dużych portalach, czy temat jest potwierdzony.
2. Wejdź na oficjalne profile osoby (Instagram, Facebook) – zwykle szybko dementują plotki.
3. Nie klikaj w podejrzane linki – mogą prowadzić do phishingu.

Uzależnienie od gier i social mediów

Nie każde korzystanie z internetu jest złe. Problem pojawia się, gdy dziecko nie potrafi już funkcjonować bez telefonu czy komputera.

Mechanizmy uzależnienia:

- „nagrody dnia" w grach,
- powiadomienia z aplikacji,
- presja lajków i komentarzy.

⚠ **Objawy uzależnienia:**

- dziecko rezygnuje z innych pasji, żeby grać,
- jest rozdrażnione, gdy trzeba odłożyć telefon,
- spędza noce online, a rano nie ma siły na szkołę,
- kłamie, ile czasu spędziło w internecie.

💡 **Wskazówka:** Wprowadź zasadę „technologia z przerwami" – np. co 45 minut obowiązkowa przerwa od ekranu.

📌 **Checklista –** jak zapobiegać uzależnieniu:

- Wprowadź limity czasu (np. 2 godziny rozrywki dziennie).
- Ustal godziny offline (np. brak internetu po 21:00 w dni szkolne).
- Zadbaj o alternatywy: sport, spotkania, pasje offline.
- Razem twórzcie domowe zasady ekranowe (i wszyscy ich przestrzegają – także rodzice!).

Kluczowe przesłanie rozdziału

Internet to narzędzie – może uczyć i rozwijać, ale może też krzywdzić. Twoim zadaniem nie jest zabronić dziecku dostępu, ale nauczyć je rozpoznawać zagrożenia i reagować. Pamiętaj: dziecko nie powie Ci wprost „mamo, tato, mam problem z cyberprzemocą" – ono po prostu zmieni swoje zachowanie. To, czy to zauważysz i odpowiednio zareagujesz, może zadecydować o jego poczuciu bezpieczeństwa.

Rozdział 3: Phishing i oszustwa „na wiadomość”

Phishing to próby wyłudzenia danych lub pieniędzy przez fałszywe wiadomości: e-mail, SMS, komunikator, a nawet telefon. Dla dzieci i nastolatków szczególnie groźne są oszustwa podszywające się pod szkołę, gry, sklepy z doładowaniami lub „znajomych”.

A) Czym jest phishing? (warianty)

- E-mail phishing — fałszywe maile podszywające się pod znane firmy, szkołę, platformy.
- Smishing — SMS/MMS z linkiem („dopłata do paczki”, „blokada konta”).
- Vishing — telefon od „konsultanta banku/policjanta”.
- Phishing w komunikatorach (Messenger, WhatsApp, Discord) — „Wyślij mi kod / pilnie wejdź w link”.
- Spear-phishing — wiadomość szyta pod konkretną osobę (np. wychowawca, trener).
- Clone-phishing — skopiowana prawdziwa wiadomość z podmienionym linkiem/załącznikiem.
- QR-phishing (QRishing) — naklejki z kodem QR prowadzącym do fałszywych stron.
- MFA fatigue — „zalew” powiadomień 2FA, aby wymusić potwierdzenie logowania.

💡**Jak to działa:** Atak wywołuje emocje (pilność, strach, nagroda), kieruje na spreparowaną stronę i prosi o dane (login, karta, BLIK). Często podszywa się pod prawdziwą domenę, używając podobnych liter lub dodatkowych poddomen.

B) Czerwone flagi (naucz tego dziecko)

1. Pilność/termin („ostatnie 15 minut”).
2. Straszenie blokadą, karą lub utratą konta.
3. Prośba o dane poufne (hasła, kody, BLIK, numery kart).
4. Link ukryty pod przyciskiem („Zweryfikuj”, „Potwierdź”).
5. Domena (np.support-konto-twojbank.com.example.ru).
6. Literówki, brak polskich znaków, słaba jakość logo.
7. Załączniki .zip/.exe/.apk do „instalacji zabezpieczeń”.
8. „Znajomy” prosi o szybki przelew/kod, nie odbiera telefonu.
9. Propozycje „łatwych pieniędzy”, konkursy „dla pierwszych 50 osób”.
10. Prośba o wyłączenie 2FA lub instalację „narzędzia do zdalnej pomocy”.

📌 **Zasada STOP**

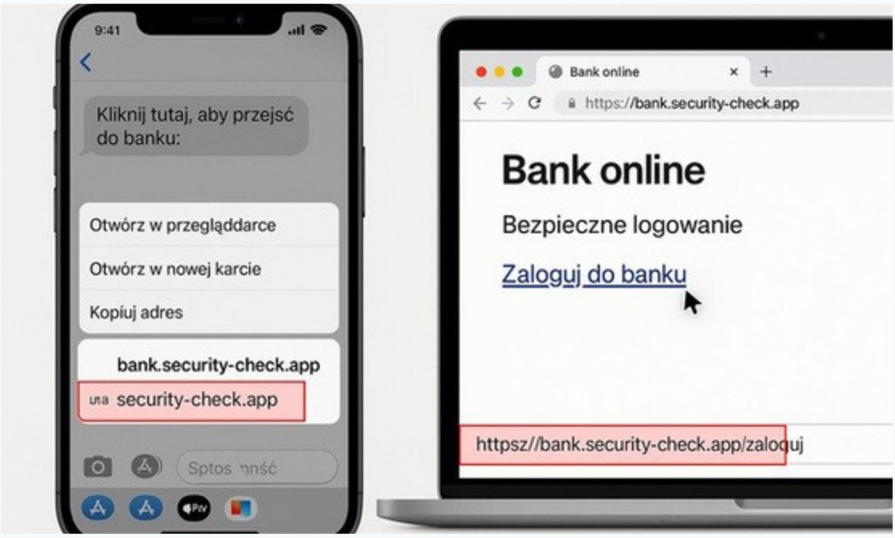
S — Stań (nie klikaj). T — Tchnij (weź oddech). O — Oceń (domena, nadawca). P — Potwierdź innym kanałem (zadzwoń, zapytaj w aplikacji).

C) Test 10 sekund — mini-procedura

1. Kto prosi i dlaczego? (czy to normalne?)
2. Nadawca: adres e-mail/telefon (dokładny, nie tylko nazwa).
3. Domena linku: prawdziwa czy „look-alike”?
4. Czy wymaga podania danych/płatności „natychmiast”?
5. Potwierdź: otwórz aplikację/usługę niezależnie, bez kliknięcia w link.

D) Jak bezpiecznie sprawdzić link (komputer i telefon)

- Komputer: najedź myszką na link i zobacz adres w lewym dolnym rogu przeglądarki.
- Telefon: przytrzymaj link dłużej → podgląd adresu (nie wchodź!).
- Sprawdzaj główną domenę: to, co bezpośrednio przed „/” i najwyżej przed ostatnią kropką.
- HTTPS/kłódka ≠ zaufanie. Fałszywe strony też mają certyfikaty.
- Skracacze linków mogą ukrywać prawdziwy adres — zachowaj podwyższoną czujność.



💡 **Pro tip**
Menedżer haseł (np. wbudowany w przeglądarkę) nie wypełni hasła na fałszywej domenie. To dodatkowa warstwa ochrony.

E) Co zrobić, jeśli kliknąłeś link lub podałeś dane:

- Natychmiast zmień hasło do danego konta (i wszędzie, gdzie było takie samo). Włącz 2FA,
- Wyloguj wszystkie sesje u→rządzeń (Ustawienia konta Bezpieczeństwo → Urządzenia).
- Jeśli podałeś dane karty/BLIK — skontaktuj się z bankiem (zablokuj kartę, odwołaj transakcję),
- Obserwuj skrzynkę: maile o resetach haseł, alerty logowania,
- Na komputerze: skan antywirusem, usuń podejrzane rozszerzenia. Na telefonie: usuń nieznane aplikacje,
- Reaguj od razu.

📌 **Wspólna rozmowa**
„Kliknęłam/-em w link" nie kończy się karą. Dziękujemy za szczerość, razem naprawiamy. Błędy się zdarzają — ważne, by szybko działać.

F) Jak zgłaszać oszustwo i blokować nadawcę

- Gmail: Otwórz wiadomość → ⋮ Więcej → „Zgłoś phishing".
- Outlook/Hotmail: Otwórz → „Zgłoś wiadomość" → „Phishing".
- Apple Mail (iCloud): Przekaż do skrzynki raportującej lub
- oznacz jako „Zgłoś niechcianą" w aplikacji.
- SMS: Zablokuj numer w telefonie i zgłoś jako spam (Android: Wiadomości → Szczegóły → Zablokuj i zgłoś; iPhone: Informacje → Zablokuj).
- Media społecznościowe (Instagram/TikTok/Discord): wejdź w profil → „Zgłoś" (Impersonation/Scam) → zablokuj.
- W firmach/szkołach: przekaż próbkę do administratora IT/wychowawcy (bez klikania linków).

⚠ **Uwaga**
Nie odpisuj, nie dyskutuj z oszustem. Każda interakcja potwierdza, że adres/telefon „żyje".

G) Scenariusze rozmów z dzieckiem (skrypty)

- „Dopłata do paczki": „Pokaż mi tę wiadomość. Zróbmy test 10 sekund. Sprawdźmy adres nadawcy i domenę."
- „Ktoś prosi o BLIK": „Zadzwońmy do tej osoby. Jeśli nie odbiera — nie wysyłamy żadnych kodów."
- „Kod z gry/skin": „Sprawdźmy, czy to oficjalny sklep/platforma. Nie logujemy się przez link z wiadomości."

📌 **Ćwiczenie 5 minut**
Raz na tydzień pokaż dziecku 2–3 przykłady (zrzuty ekranów z internetu). Niech wskaże czerwone flagi i powie, co zrobi.

H) Szablony do skopiowania

- Do znajomego (na prośbę o BLIK): „Hej, dla bezpieczeństwa zawsze dzwonię, zanim wyślę kod. Oddzwonię do ciebie za chwilę."
- Do szkoły/administratora: „Otrzymałem/-am podejrzanego maila podszywającego się pod [nazwa]. Przesyłam nagłówki/zrzut (bez wchodzenia w link)."

I) Zasady domowe „anty-phishing" (do wydruku)

- Nigdy nie wysyłamy kodów/hasła przez czat/SMS,
- Nigdy nie logujemy się z linku w wiadomości — zawsze przez aplikację lub wpisując adres ręcznie.

- Jeśli coś jest PILNE w wiadomości — tym bardziej zatrzymaj się i zadzwoń,
- Jeśli nie wiemy — pytamy. Brak pewności = brak kliknięcia.

💡 **Plakat do domu**
„Zatrzymaj się. Oddychaj. Sprawdź. Potwierdź w innym kanale.” — wydrukuj i powieś obok biurka.

J) Jednostronicowa ściąga — Phishing

• 10-sek. test
• 10 czerwonych flag
• Co robić po kliknięciu
• Gdzie zgłaszać
• Zasady domowe. Wydrukuj i trzymaj przy komputerze/na lodówce.

Rozdział 4: Podstawy edukacji cyfrowej w domu

Najlepszym zabezpieczeniem dziecka w internecie nie jest blokada, hasło czy aplikacja. To **świadomy rodzic i rozmowa**. Technologie się zmieniają – TikTok dziś, jutro coś nowego – ale zasady, które dziecko wyniesie z domu, pozostaną z nim na zawsze.

Dlaczego edukacja cyfrowa jest tak ważna?

Dziecko, które rozumie, jak działa internet, potrafi samodzielnie chronić się przed wieloma zagrożeniami. To jak nauka jazdy na rowerze: najpierw trzymamy za siodełko, potem puszczamy – a dziecko samo wie, jak utrzymać równowagę.

📌 Porównanie:

- W świecie realnym uczymy: „Nie rozmawiaj z obcymi".
- W świecie cyfrowym uczymy: „Nie ufaj każdemu, kto pisze w internecie".

Jak rozmawiać z dzieckiem o internecie

Rozmowa powinna być codzienną częścią życia – naturalna, spokojna i oparta na zaufaniu. Zamiast wykładu – krótkie dialogi, ciekawość i pytania otwarte. Nie oceniaj – pytaj, słuchaj, tłumacz.

👶 Dziecko 4–6 lat — pierwsze bajki i filmy online

Cel: nauczyć rozpoznawania bezpiecznych treści i proszenia o pomoc.
Rodzic: „Co lubisz oglądać w telefonie?”
Dziecko: „Świnka Peppa i kotki.”
Rodzic: „Super! A wiesz, że nie wszystkie bajki w internecie są prawdziwe? Czasem ktoś udaje Peppę, ale pokazuje coś brzydkiego. Jak zobaczysz coś dziwnego, od razu przyjdź do mnie.”

💬 **Dlaczego to działa:** rodzic nie straszy, tylko tłumaczy i uczy reakcji („przyjdź do mnie”).

👧 Dziecko 7–9 lat — pierwsze gry i reklamy

Cel: zrozumienie, że nie wszystko w internecie jest prawdą, a reklamy mają swój cel.
Rodzic: „W tej grze trzeba oglądać reklamy, żeby dostać punkty, prawda?”
Dziecko: „Tak, tam pokazują nową grę.”
Rodzic: „A wiesz, że reklamy chcą, żebyś coś kupił? Dlatego pokazują rzeczy, które ci się podobają.”
Dziecko: „To trochę oszukane.”
Rodzic: „Dokładnie. Dlatego warto się zastanowić, zanim klikniesz.”

👧 Dziecko 9–10 lat — rozmowy online i czaty

Cel: wytłumaczyć różnicę między znajomym a obcym w internecie.
Rodzic: „Widzę, że w grze można pisać z innymi. Z kim najczęściej rozmawiasz?”
Dziecko: „Z kimś, kto ma nick ‘SpeedNinja’. Fajnie się gra.”
Rodzic: „A wiesz, czy to dziecko, czy dorosły?”
Dziecko: „Nie wiem.”
Rodzic: „W internecie nie zawsze wiadomo, kto jest po drugiej stronie. Lepiej nie mówić, gdzie mieszkasz i jak masz na imię, dobrze?”

👦 Dziecko 11–12 lat — memy, żarty, fake newsy

Cel: nauczyć krytycznego myślenia i rozpoznawania nieprawdziwych informacji.
Rodzic: „Widziałem, że udostępniłeś mema o gwieździe, która podobno umarła. Skąd wiedziałeś, że to prawda?”
Dziecko: „Bo dużo osób to udostępniło.”
Rodzic: „W internecie łatwo ktoś może wymyślić historię, żeby zdobyć lajki. Zawsze warto sprawdzić w wiadomościach albo zapytać mnie, zanim się uwierzy.”

👧 Dziecko 13–14 lat — media społecznościowei samoocena

Cel: rozmowa o presji lajków i prywatności.
Rodzic: „Wrzuciłaś super zdjęcie! Dużo komentarzy?”
Dziecko: „Tak, ale jedna osoba napisała coś niemiłego.”
Rodzic: „To przykre. W internecie ludzie czasem piszą, co im ślina na język przyniesie. Ale to nie znaczy, że mają rację. Pamiętaj – ty decydujesz, kto cię obserwuje i co pokazujesz.”

👦 Dziecko 15–16 lat — prywatność, sexting, granice

Cel: rozmowa o odpowiedzialności i zaufaniu.
Rodzic: „Słyszałem ostatnio, że w szkołach krążą zdjęcia uczniów z prywatnych rozmów. Co o tym myślisz?”
Dziecko: „To głupie, ale wszyscy czasem coś wysyłają.”
Rodzic: „Wiem, że to kuszące, ale zdjęcia w sieci mogą zostać tam na zawsze. Lepiej pomyśleć, czy nie zrobi ci to problemu za rok albo pięć.”

👦Nastolatek 17+ — odpowiedzialność, praca, dane osobowe

Cel: nauczyć świadomego zarządzania reputacją cyfrową.

Rodzic: „Masz konto na LinkedIn? To dobry moment, żeby je założyć – tam pokazujesz, co umiesz, nie tylko co wrzucasz na Insta."
Dziecko: „Serio? To dla dorosłych."
Rodzic: „Nie, właśnie dla młodych, którzy chcą się rozwijać. Internet to nie tylko zabawa – to też twoja wizytówka."

💬 Sytuacje „nagłe" – jak reagować, gdy dziecko zobaczy coś niepokojącego

Rodzic: „Jeśli zobaczysz coś, co cię przestraszy lub zawstydzi – film, zdjęcie, wiadomość – nie bój się przyjść do mnie. Nie będę zły. Chcę tylko pomóc, żebyś czuł się bezpiecznie."

💬 Dlaczego to ważne: **dziecko zapamięta, że może przyjść bez strachu przed karą.**

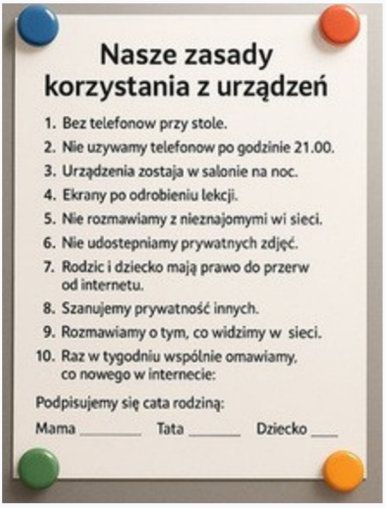
💡 Jak rodzic może zacząć rozmowę „z niczego"

- „Widziałem dziś ciekawy film o bezpieczeństwie w sieci, chcesz zobaczyć razem?"
- „Słyszałem, że dzieci w szkole dostają dziwne wiadomości – czy też to zauważyłeś?"
- „Czy ktoś w grze prosił cię kiedyś o numer telefonu albo zdjęcie?"
- „Jak myślisz, dlaczego ludzie czasem udają kogoś innego w internecie?"
- „Zastanawiam się, czy ja bym potrafił odróżnić fałszywą wiadomość. Może mnie nauczysz?"

🎯 Zasady dobrego dialogu:

1. **Nie oceniaj – pytaj.** Zamiast: „Znowu siedzisz w telefonie!”, powiedz: „Co ci się w tej grze podoba?”
2. **Nie wyśmiewaj.** Nawet jeśli coś wydaje ci się błahe, dla dziecka to ważne.
3. **Dziel się własnym doświadczeniem.** Pokaż, że też popełniasz błędy.
4. **Rozmawiaj przy okazji.** W samochodzie, przy kolacji, przed snem – nie tylko „na poważnie”.
5. **Wspólne odkrywanie.** Poproś dziecko, by nauczyło cię obsługi nowej aplikacji.

Ustalanie zasad korzystania z urządzeń



Dzieci potrzebują granic, bo granice dają im poczucie bezpieczeństwa. Zasady najlepiej ustalać wspólnie – wtedy dziecko czuje się ich współautorem.

📌 Przykładowa lista zasad rodzinnych:

- Telefon zostaje w salonie na noc (ładowanie poza sypialnią).
- Zero telefonów przy posiłkach.
- Limit: 2 godziny dziennie rozrywki online (czas różny w zależności od wieku).
- Brak internetu po godzinie 21:00 w dni szkolne.
- Dodajemy do znajomych tylko osoby, które znamy osobiście.

Najczęstsze błędy rodziców

⚠ **Uwaga:**

- Zakazy bez rozmowy („Bo ja tak mówię”).
- Brak konsekwencji (raz pozwalamy, raz zabraniany).
- Brak własnego przykładu (rodzic mówi: „Nie używaj telefonu przy stole”, a sam scrolluje Facebooka).
- Reagowanie karą zamiast rozmową („Zabieram ci telefon na tydzień”).

💡 **Wskazówka:** Zamiast zabierać dziecku telefon, lepiej razem ustalić zasady i konsekwencje.

Umowa cyfrowa rodzic–dziecko

Dobrym narzędziem jest stworzenie prostej umowy rodzinnej. To może być kartka papieru, na której spiszecie wspólnie zasady korzystania z internetu.

📌 Przykład umowy:

- Rodzic zobowiązuje się, że nie będzie zaglądał w telefon dziecka bez powodu.
- Dziecko zobowiązuje się, że nie będzie rozmawiać z obcymi w internecie.
- Wszyscy zobowiązują się, że odkładają telefony na czas posiłków.

💡 **Wskazówka:** Podpiszcie się pod umową i powieście ją w widocznym miejscu.

Co daje edukacja cyfrowa w domu?

- Buduje zaufanie między dzieckiem a rodzicem.
- Uczy dziecko, że może przyjść z problemem bez obawy o karę.
- Daje mu poczucie bezpieczeństwa – wie, że nie jest samo w świecie online.
- Przygotowuje je na sytuacje, gdy rodzica nie ma obok.

Kluczowe przesłanie rozdziału

Najlepszym „programem antywirusowym" dla dziecka jest świadomy rodzic. Zasady, rozmowy i przykład są ważniejsze niż jakakolwiek aplikacja. To Ty jesteś pierwszym przewodnikiem swojego dziecka w świecie online.

Rozdział 5 — Instrukcje krok po kroku (wersja dla początkujących)

Poniższe instrukcje zostały przygotowane tak, aby każdy rodzic — nawet bez doświadczenia technicznego — mógł samodzielnie włączyć blokady i filtry.

A) Android — Google Family Link (darmowe)

0) Co przygotować

1. Telefon rodzica (Android lub iPhone) z kontem Google.
2. Telefon dziecka (Android) z własnym kontem Google.
3. Połączenie z internetem (Wi-Fi)

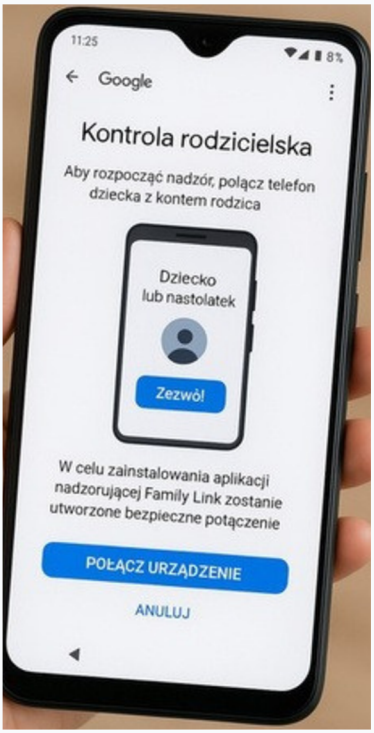
1) Instalacja i start na telefonie rodzica

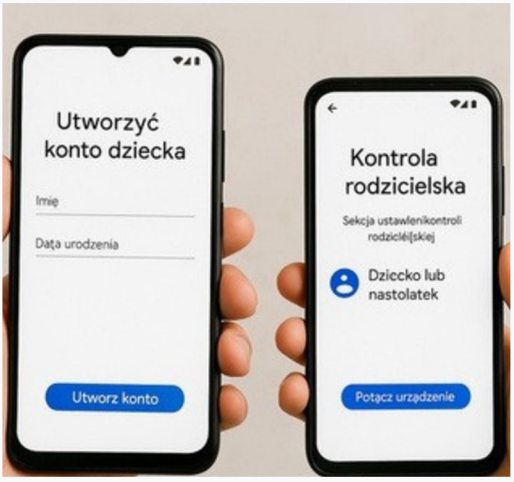
1. Otwórz Sklep Play (na iPhonie – App Store).
2. Wyszukaj „Google Family Link (dla rodziców)” i zainstaluj.
3. Uruchom aplikację → Zaloguj się na swoje konto Google.
4. Wybierz „Zarządzaj rodziną” → „Dodaj dziecko”.

2) Powiązanie telefonu dziecka

Opcja A — dziecko ma już konto Google na telefonie:

1. Na telefonie dziecka: Ustawienia → Google → Kontrola rodzicielska.
2. Stuknij „Rozpocznij” → „Dziecko lub nastolatek” → „Dalej”.
3. Zeskanuj kod/połącz według instrukcji w Family Link na telefonie rodzica lub zaloguj konto dziecka i zaakceptuj nadzór.
4. Przejdź kolejne kroki: „Połącz urządzenie” → „Zezwól”.

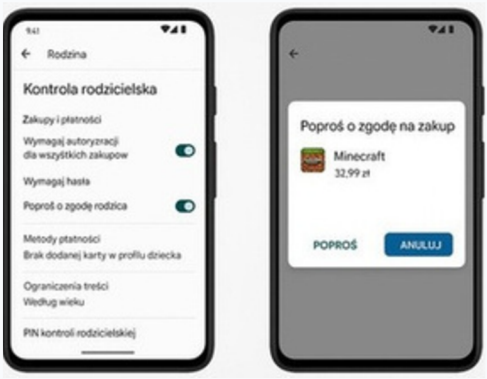




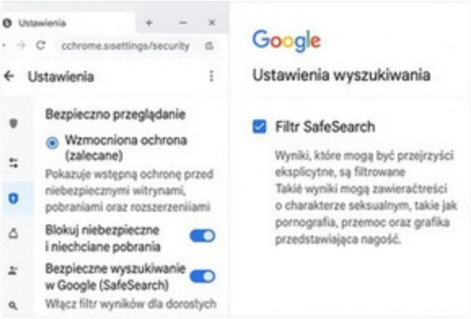
Opcja B — tworzysz nowe konto dla dziecka:

1. W Family Link (u rodzica) wybierz „Utwórz konto dla dziecka” → wpisz dane (imię, data urodzenia).
2. Po utworzeniu konta zaloguj je na telefonie dziecka.
3. Powtórz kroki z opcji A, aby włączyć nadzór.

3) Zgody i filtry w Google Play



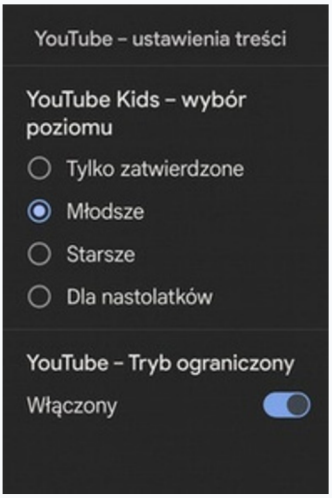
1. Family Link (telefon rodzica) → [Imię dziecka] → „Zarządzanie ustawieniami”.
2. „Kontrola na Google Play”:
   - „Zatwierdzanie zakupów/instalacji” → „Wymagaj zatwierdzenia dla wszystkich”.
   - „Klasyfikacje wiekowe treści” → ustaw odpowiedni wiek (np. 7–12).



4) Filtry stron + bezpieczne wyszukiwanie

1. Family Link → „Ustawienia” → „Filtry w Google Chrome” → włącz „Zatrzymuj nieodpowiednie witryny” lub „Zezwalaj tylko na wybrane witryny”.
2. Family Link → „Ustawienia” → „Bezpieczne wyszukiwanie (SafeSearch)” → „Włącz”.

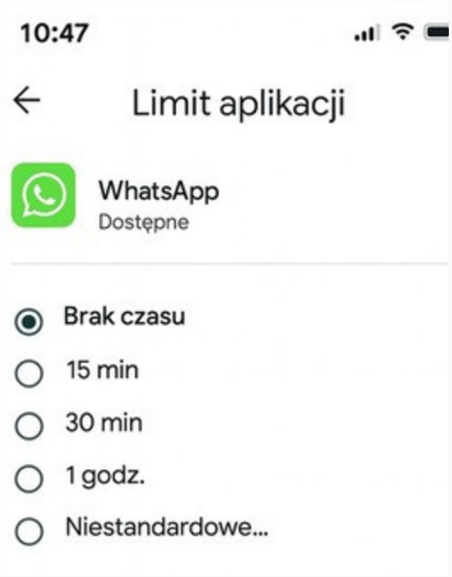
5) YouTube / YouTube Kids



Wariant 1 — YouTube Kids (zalecane dla młodszych):
1. Na telefonie dziecka zainstaluj YouTube Kids i zaloguj konto dziecka.
2. Ustaw profil i poziom treści (Młodsze/Starsze).
3. Włącz „Zatwierdzanie treści przez rodzica", jeśli chcesz ręcznie akceptować kanały.

Wariant 2 — zwykły YouTube z ograniczeniami:
1. W aplikacji YouTube: Profil → Ustawienia → Tryb ograniczony
2. FamilyLink:Ustawienia → YouTube → wybierz poziom ograniczeń → Włącz.

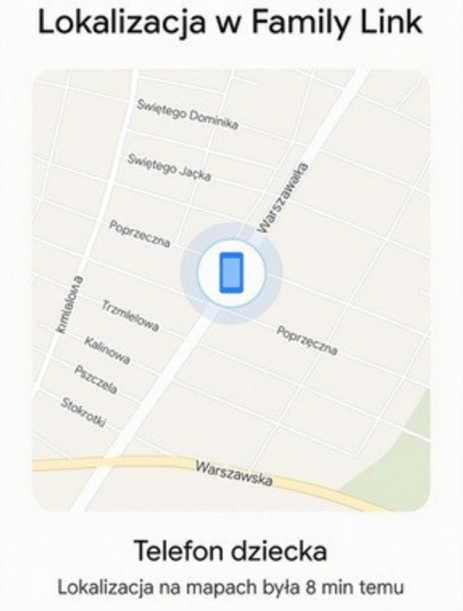
6) Limity czasu i godziny snu



1. Family Link → [Imię dziecka] → „Limity aplikacji" → wybierz aplikację → ustaw dzienny limit (np. 30–60 min).
2. „Czas w urządzeniu" → „Godziny snu" → ustaw przedział (np. 21:00–7:00).
3. (Opcja) Dodaj przerwy w ciągu dnia (nauka/posiłki).

7) Lokalizacja i zdalna blokada

1. Family Link → „Lokalizacja” → „Włącz udostępnianie lokalizacji”.
2. W razie potrzeby użyj „Zablokuj urządzenie” (w razie zgubienia telefonu).



8) Zabezpieczenia przed omijaniem

- Ustaw PIN/hasło na telefonie dziecka.
- Ustawienia → Aplikacje → Specjalny dostęp → Instalowanie nieznanych aplikacji→ Wyłącz dla przeglądarek/menedżerów plików.
- Wytłumacz dziecku powód zasad — to zwiększa akceptację.

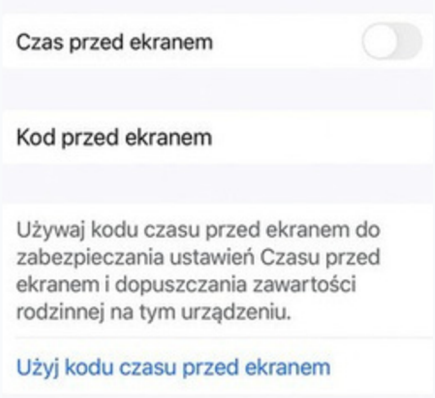
B) iPhone / iPad — Czas przed ekranem

0) Dwie metody konfiguracji

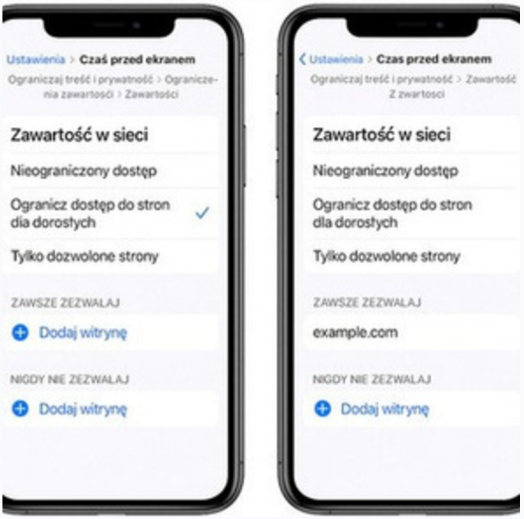
- Na urządzeniu dziecka (najprościej).
- Zdalnie przez Chmurę Rodzinną (Family Sharing) z Twojego iPhone’a.

1) Włącz Screen Time na iPhonie/iPadzie dziecka

1. Ustawienia → Czas przed ekranem → „Włącz”.
2. Wybierz „To iPhone/iPad mojego dziecka”.
3. Ustaw Kod Czasu przed ekranem (inny niż kod blokady).
4. W kreatorze ustaw: „Przerwa” (np. 21:00–7:00), „Limity aplikacji” (Gry/Social — np. 1 h/dzień), „Zawsze dozwolone” (Telefon, Wiadomości).

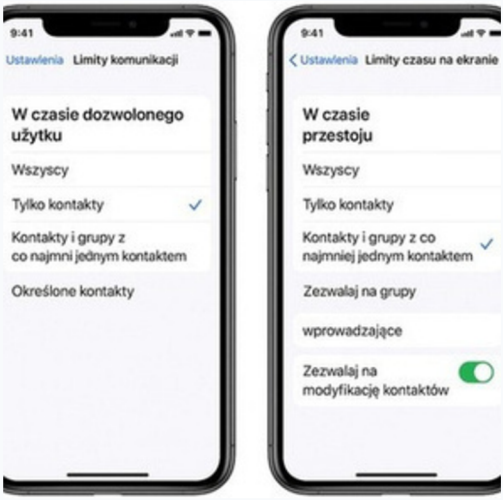


2) Ograniczenia treści i prywatności



1. Ustawienia → Czas przed ekranem → „Ograniczenia dot. treści i prywatności” → Włącz.
2. „Ograniczenia zawartości”: Treści web → „Ograniczaj strony dla dorosłych” lub „Dozwolone tylko wybrane strony”; Filmy/Programy/Muzyka → klasy wiekowe; Aplikacje → 9+/12+.
3. „Zakupy i pobieranie”: Instalowanie/Usuwanie aplikacji → „Nie zezwalaj”; Zakupy w aplikacji → „Nie zezwalaj”.

3) Limity komunikacji (opcjonalnie)

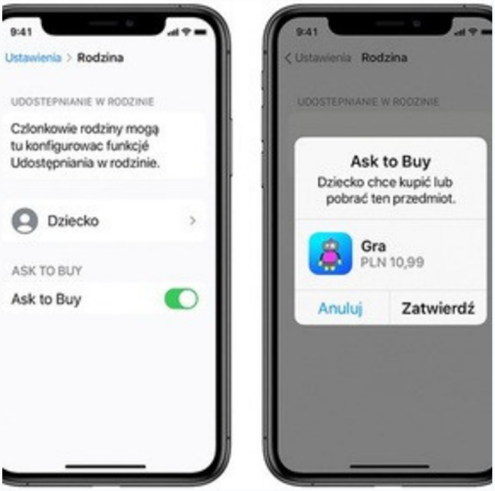


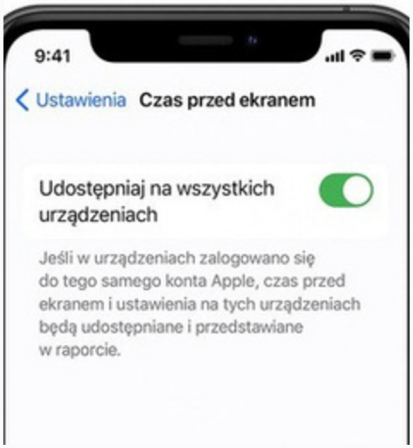
Ustawienia → Czas przed ekranem → „Limity komunikacji” → zdefiniuj kontakty dozwolone podczas Przerwy i poza nią.

4) Family Sharing — „Poproś o zakup” (Ask to Buy)

1. Ustawienia (na iPhonie rodzica) → [Twoje imię / Apple ID] → „Rodzina”.

2. Dodaj konto dziecka lub wybierz istniejące.
3. Włącz „Poproś o zakup (Ask to Buy)”.





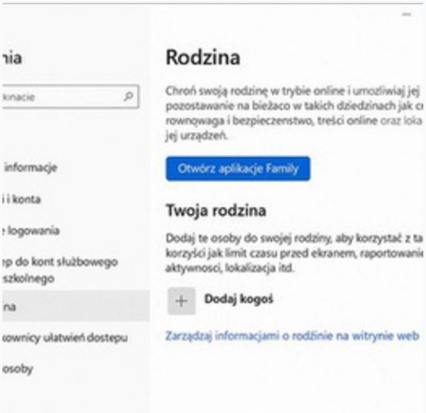
5) Zabezpieczenia przed omijaniem

- Nie ujawniaj kodu Screen Time; ustaw inny niż blokada ekranu.
- Włącz „Udostępniaj na wszystkich urządzeniach”, jeśli dziecko ma kilka sprzętów Apple.

C) Windows 10/11 — Microsoft Family Safety

0) Co przygotować

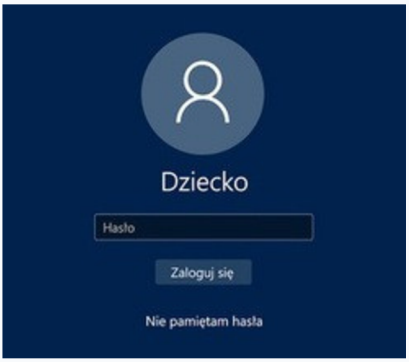
- Komputer z Windows 10/11.
- Konto Microsoft rodzica i osobne konto dziecka.



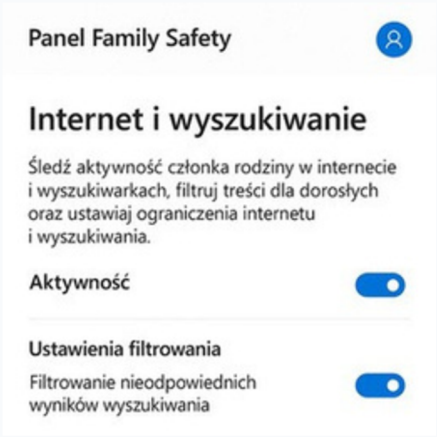
1) Dodaj dziecko do rodziny Microsoft

1. Windows: Ustawienia → Konta → „Rodzina i inni użytkownicy”.
2. „Dodaj członka rodziny” → „Dodaj dziecko” → e-mail dziecka lub „Utwórz konto”.
3. Wyślij zaproszenie i zaakceptuj je na koncie dziecka.

2) Zaloguj dziecko na jego konto w Windows



1. Wyloguj bieżącego użytkownika → zaloguj się jako dziecko (pierwsze logowanie może potrwać).

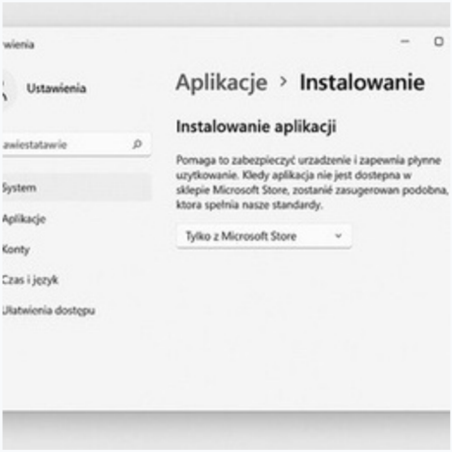


3) Ustaw filtry i limity w panelu rodzica

1. Otwórz przeglądarkę: family.microsoft.com → wybierz profil dziecka.
2. „Czas przed ekranem” → ustaw harmonogram (dni/godziny) i limity dzienne dla komputera.
3. „Aplikacje i gry” → ustaw limity lub zablokuj wybrane programy (np. gry).
4. „Witryny i wyszukiwanie” → włącz filtr nieodpowiednich stron; rozważ tryb „Tylko dozwolone witryny”. (Najpewniej działa w Edge — rozważ zablokowanie Chrome/Firefox).
5. „Wydatki” → włącz zgody na zakupy w Microsoft Store.

4) Dodatkowe wzmocnienia w Windows

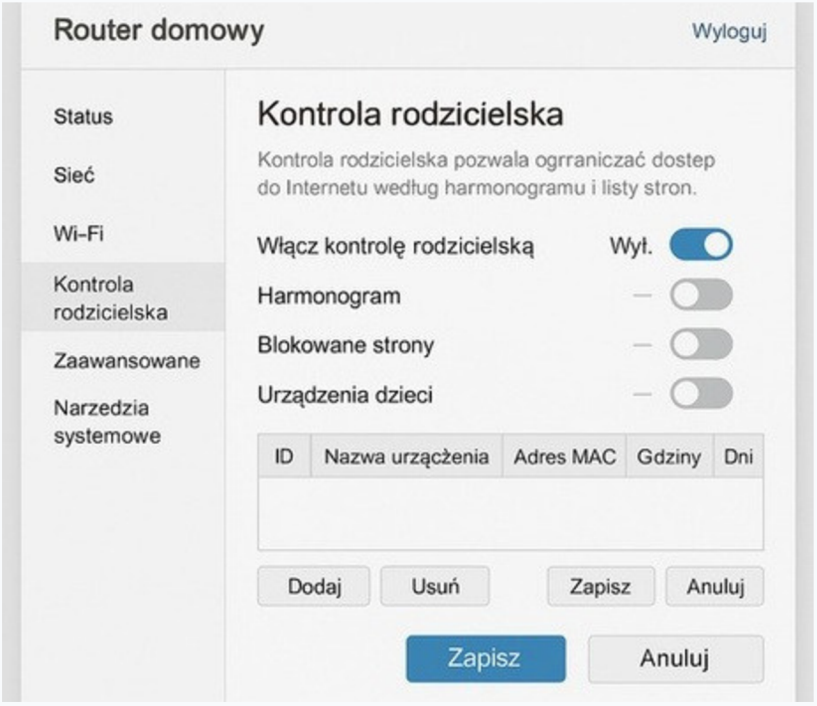
- Ustaw Edge jako przeglądarkę domyślną.
- (Opcja) Ogranicz instalowanie aplikacji do Microsoft Store: Ustawienia → Aplikacje → Instalowanie aplikacji → „Tylko z Microsoft Store”.



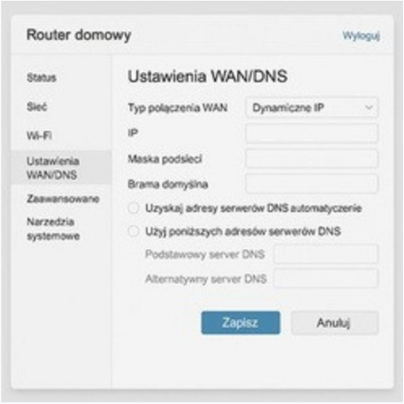
D) Router domowy — filtr dla całego domu

Metoda 1: Wbudowana „Kontrola rodzicielska” w routerze

1. Połącz się z Wi-Fi routera i wejdź w przeglądarce na 192.168.1.1 lub 192.168.0.1.
2. Zaloguj się (login/hasło na naklejce routera lub od operatora).
3. Odszukaj „Parental Controls / Kontrola rodzicielska”.
4. Wybierz urządzenie dziecka (nazwa/adres MAC).
5. Ustaw harmonogram (np. blokada od 21:30 do 7:00) oraz kategorie stron do blokady (18+, hazard).
6. (Opcja) Zdefiniuj białą listę dozwolonych witryn.
7. Zapisz/Zastosuj; jeśli trzeba, zrestartuj router.



Metoda 2: Filtr DNS (szybko i darmowo)



1. W panelu routera: Ustawienia internetu/WAN/DNS.
2. Ustaw ręcznie serwery DNS (rodzinne):

- OpenDNS FamilyShield: 208.67.222.123 i 208.67.220.123
- Cloudflare Family: 1.1.1.3 i 1.0.0.3

3. Zapisz/Zastosuj; uruchom ponownie router.
4. Na urządzeniu dziecka: rozłącz i połącz Wi-Fi (odśwież DNS).

Uwaga praktyczna

- Ustaw silne hasło do panelu routera i wyłącz WPS.
- Dodatkowo włącz filtry w samych urządzeniach (Family Link / Screen Time), aby utrudnić omijanie blokad.

Rozdział 6: Monitorowanie i bezpieczeństwo urządzeń

Celem monitoringu nie jest podglądanie dziecka, lecz szybkie wychwycenie sygnałów ryzyka i wsparcie w budowaniu zdrowych nawyków. Zawsze mów dziecku wprost, jakie raporty są włączone i po co — zaufanie to podstawa.

A) Higiena cyfrowa — fundament bezpieczeństwa

1) Aktualizacje systemu i aplikacji — włącz automatyczne aktualizacje na każdym urządzeniu.

2) Blokada ekranu — ustaw PIN/hasło/biometrię i krótki czas automatycznej blokady (30–60 sek.).

3) Silne hasła + 2FA — włącz uwierzytelnianie dwuskładnikowe dla Google/Apple/Microsoft, poczty i social mediów.

4) Kopie zapasowe — włącz iCloud/Google One/OneDrive; testowo przywróć plik, by mieć pewność, że kopia działa.

💡 **Wskazówka**
Zasada 3×Z: Zaktualizowane urządzenia, Zablokowany ekran, Zapas (kopie).

B) Co monitorować (i gdzie to znaleźć)

- Czas przed ekranem i użycie aplikacji — raporty: Family Link (Android), Screen Time (iOS), Family Safety (Windows).
- Historia przeglądania — Chrome/Safari/Edge (z kontem dziecka i filtrami).
- Historia YouTube / YouTube Kids — ostatnio oglądane; w Kids można zatwierdzać kanały.
- Powiadomienia z aplikacji społecznościowych — sygnał przeciążenia, jeśli są aktywne nocą.

⚠ **Uwaga**
Monitoruj tylko tyle, ile naprawdę potrzebujesz. Nadmierna kontrola osłabia zaufanie. Ustalcie zasady: co przeglądasz, jak często i po co.

C) Procedura 10 minut w tygodniu — szybki przegląd rodzica

1. Otwórz raport czasu przed ekranem (Family Link/Screen Time/Family Safety).

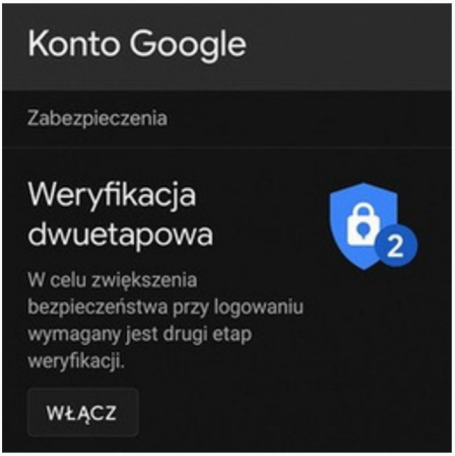
2. Sprawdź 3 najdłużej używane aplikacje i porównaj z poprzednim tygodniem.
3. Przejrzyj historię YouTube/YouTube Kids i ostatnie subskrypcje.
4. Zapytaj dziecko: „Co było fajne online? Co cię zaniepokoiło?”
5. Ustal ewentualne korekty limitów i zaplanuj wspólną aktywność offline.

📌 **Checklista (do wydruku)**

- ☐ Przejrzałem raport tygodnia
- ☐ Rozmowa: 2 pytania do dziecka
- ☐ Korekta limitów (jeśli potrzeba)
- ☐ Sprawdzona historia YouTube/Przeglądarki
- ☐ Zaplanowana aktywność offline

D) Bezpieczeństwo kont i urządzeń — krok po kroku

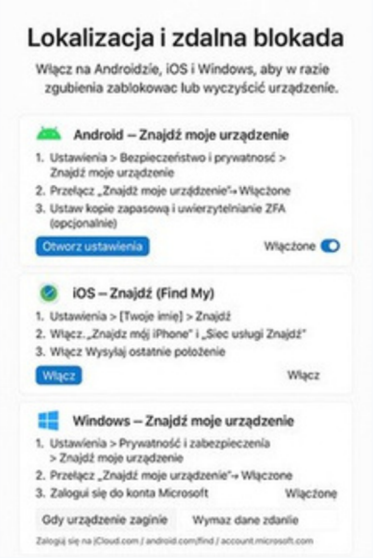
- Google (Android): konto.google.com → Zabezpieczenia → włącz 2FA (aplikacja/klucze), sprawdź logowania i urządzenia.



- Apple (iOS): Ustawienia → [Twoje imię] → Hasło i bezpieczeństwo→ włącz 2FA; sprawdź listę urządzeń i „Znajdź”.

- Microsoft (Windows): account.microsoft.com → Security → włącz 2FA; włącz „Find my device” dla laptopa dziecka.

- Lokalizacja i zdalna blokada: włącz na Androidzie/iOS/Windows, aby w razie zgubienia zablokować/wyczyścić urządzenie.



E) Gdy wydarzy się incydent — plan działania

- Spokój i rozmowa — celem jest pomoc, nie kara.
- Zabezpiecz dowody — zrzuty ekranu, linki, daty, nicki.
- Zablokuj i zgłoś — użytkownika/treści w aplikacji; rozważ zmianę haseł i włączenie 2FA.
- Urządzenie — skan antywirusem (Windows Defender), aktualizacje; w razie potrzeby przywrócenie ustawień.
- Zgłoszenia — szkoła (przy rówieśnikach), administratorzy serwisów; w poważnych sprawach policja.

⚠ **Uwaga — czerwone flagi**
• Nocne, ukrywane korzystanie • Nagłe skasowanie kont/rozmów • Prośby o zdjęcia/dane • Spadek nastroju, izolacja. Reaguj natychmiast i zapewnij wsparcie.

F) Mądre granice monitoringu (etyka i relacja)

- Transparentność: dziecko wie, co jest monitorowane i dlaczego.
- Rozwój: z wiekiem — więcej zaufania i samodzielności.
- Relacja: technologia wspiera, ale nie zastępuje rozmowy.

💡 **Przesłanie rozdziału**
Najlepszy monitoring to zaufanie + rytuał 10 minut tygodniowo + higiena cyfrowa. To zestaw, który działa w codzienności.

Rozdział 7: Umowa cyfrowa rodzic–dziecko i scenariusze rozmów

Ten rozdział daje Ci gotowe, praktyczne narzędzia: umowę cyfrową do podpisania z dzieckiem, scenariusze rozmów w trudnych sytuacjach oraz karty do wydruku. Dzięki nim wprowadzisz jasne zasady i utrzymasz dobrą relację — bez krzyków i walki z telefonem.

A) Po co umowa cyfrowa? (i dlaczego działa)

💡**Dlaczego działa:**

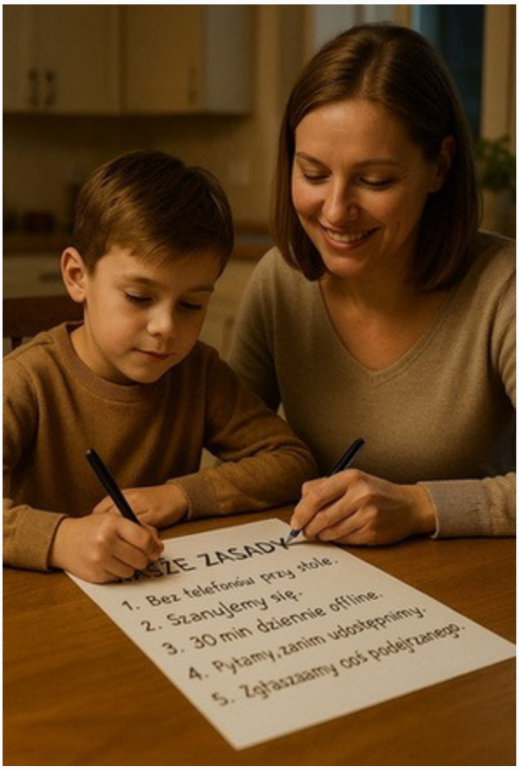
- daje dziecku poczucie sprawczości (współtworzy zasady) zamienia „zakazy" na „uzgodnienia"
- ułatwia konsekwencję (odwołujemy się do wspólnie podpisanego dokumentu)
- porządkuje oczekiwania i granice (czas, treści, prywatność, bezpieczeństwo)

Zanim podpiszecie umowę:

1) Porozmawiaj o tym, co dla dziecka w internecie jest ważne (gry, kontakt z klasą, pasje).

2) Powiedz, co jest ważne dla Ciebie (bezpieczeństwo, sen, szkoła, relacje).

3) Ustalcie cele: np. 8 h snu, nauka przed rozrywką, brak telefonu przy posiłkach.



B) Gotowa UMOWA CYFROWA — wersja podstawowa (do wydruku i podpisu)

📌 **Instrukcja**
Wydrukuj tę stronę, wstaw imię dziecka i wspólnie przejdźcie każdy punkt. Zasady zapisuj prostym językiem; dopiszcie rzeczy ważne dla Waszej rodziny.

UMOWA CYFROWA RODZIC–DZIECKO
Imię dziecka: _____ Wiek: ___ Data: _____
1) Czas i rytm:
• maks. ____ min dziennie rozrywki online (dni szkolne); ____ min (weekend)
• przerwa od tech. na min. 1 h przed snem; urządzenia ładujemy poza sypialnią
2) Strefy i chwile offline:
• zero telefonów przy posiłkach i w czasie lekcji/odrabiania zadań
3) Bezpieczeństwo i prywatność:
• nie podaję adresu, szkoły, nazwiska, haseł; nie wysyłam zdjęć obcym
• proszę rodzica o pomoc, jeśli coś mnie zaniepokoi online
4) Kontakty i publikacje:
• do znajomych dodaję osoby, które znam z realu (chyba że rodzic zaakceptuje inaczej)
• zanim opublikuję zdjęcie innych — pytam o zgodę
5) Zgody i instalacje:
• nowe aplikacje instaluję po zgodzie rodzica; zakupy w aplikacjach — tylko za zgodą
6) Narzędzia i raporty:
• zgadzam się na limity czasu i raporty (Family Link/Screen Time/Family Safety) — wiem, po co są
7) Konsekwencje i naprawa:
• jeśli złamię zasady: krótkie ograniczenie + plan naprawczy (patrz drabina konsekwencji)
Podpisy:
Rodzic/opiekun: _____
Dziecko: _____

C) Umowa cyfrowa — dopasowanie do wieku

6–8 lat (wersja prosta)

- Oglądam/gram tylko to, co wybraliśmy razem.
- Jak coś mnie przestraszy — natychmiast wołam rodzica.
- Nie rozmawiam z obcymi w grach.
- Tablet/telefon odpoczywa po kolacji.

9–12 lat (wersja rozszerzona)

- Limit dzienny: ____ min; najpierw szkoła/obowiązki, potem gry.
- Pytam o zgodę, zanim dodam kogoś do znajomych.
- Nie wysyłam zdjęć nikomu, kogo nie znam w realu.
- Jeśli widzę hejt — blokuję i zgłaszam, mówię rodzicowi.

13–16 lat (wersja partnerska)

- Sam zarządzam czasem; jeśli raport pokaże przeciążenie — ustalamy korektę.
- Uważnie dobieram znajomych i dbam o prywatność profilu.
- Nie publikuję nic, co mogłoby mnie skrzywdzić w przyszłości.
- Biorę odpowiedzialność za konsekwencje i realizuję plan naprawczy, jeśli złamię zasady.

D) Scenariusze rozmów (gotowe skrypty)

1) „Pierwsza umowa" — start bez napięcia

Rodzic: „Chciałbym, żebyśmy ustalili zasady korzystania z telefonu tak, żeby było i bezpiecznie, i przyjemnie. Co jest dla ciebie w telefonie najważniejsze?"
Dziecko: „Gry i kontakt z klasą."
Rodzic: „OK. Dla mnie ważne są sen i nauka. Ustalmy wspólnie limity i miejsca, gdzie telefon odpoczywa."

💡 **Cel rozmowy**
Połącz potrzeby dziecka z oczekiwaniami rodzica i zapisz wspólne „TAK/NIE".

2) Gdy podejrzewasz grooming/niebezpieczny kontakt

Rodzic: „Zauważyłem, że dużo piszesz z kimś nowym. Chcę mieć pewność, że to bezpieczne. Nie będę cię karać za szczerość. Powiedz — skąd się znacie?”
Dziecko: „Z gry.”
Rodzic: „Super, że mówisz. Pamiętaj — prawdziwy przyjaciel nie prosi o sekrety ani zdjęcia. Jeśli ktoś prosi — blokujemy i zgłaszamy. Pomogę ci to zrobić.”

3) Cyberprzemoc — dziecko jest ofiarą

Rodzic: „Widzę, że trudniej ci ostatnio zaglądać do telefonu. Czy ktoś był dla ciebie niemiły w sieci? Jestem po twojej stronie — razem to ogarniemy.”
→ Zrób zrzuty ekranu, zablokuj sprawcę, zgłoś w aplikacji i w szkole, wesprzyj emocjonalnie.

4) Dziecko zobaczyło treści seksualne/przemocowe

Rodzic: „To, co widziałeś, mogło być trudne. Dzięki, że mówisz. To nie twoja wina — internet czasem pokazuje rzeczy, których nie chcesz widzieć. Porozmawiajmy, co czujesz, i włączymy filtry, żeby to się nie powtarzało.”

5) Ustalanie limitów (gdy jest konflikt o czas)

Rodzic: „Raport pokazuje 3 h dziennie gier. Co możemy zmienić, żeby było zdrowiej, ale wciąż przyjemnie? Proponuję: 1,5 h dziennie + dodatkowe 30 min w weekend za odrobione obowiązki.”

6) Prośba o nową aplikację — decyzja „TAK/ZA WARUNKIEM/NIE”

Rodzic: „Pokaż mi aplikację, której chcesz używać. Przejrzymy razem, do czego służy, jakie ma oceny wiekowe i czy ma kontrolę rodzicielską. Jeśli spełnimy warunki bezpieczeństwa, dostajesz zgodę.” → TAK

📌 **Drzewko decyzji — nowa aplikacja**
- Do czego służy?
- Czy ma zgody i filtry?
- Czy możeszużywać w trybie prywatnym?
- Od jakiego wieku?

E) Drabina konsekwencji (zawsze z drogą powrotu)

1) Przypomnienie zasad → 2) Rozmowa i mini-zadanie naprawcze → 3) Krótkie ograniczenie (np. 24 h mniej gier) → 4) Tryb „pod opieką” (korzystanie tylko przy rodzicu) → 5) Pauza + plan naprawczy (pisemny).

⚠ **Ważne**
Konsekwencje muszą być krótkie, przewidywalne i uzgodnione w umowie. Zawsze daj szansę na odbudowę zaufania.

F) Tygodniowy przegląd rodziny — karta do wydruku

Co tydzień 10 minut: przegląd raportu, rozmowa (2 pytania), drobna korekta limitów, wspólny plan offline.

KARTA PRZEGLĄDU (data: _____):
• Top 3 aplikacje: _____ / _____ / _____
• Co było fajne online? _____
• Co zaniepokoiło? _____
• Ustalenia na tydzień: _____
Podpisy: Rodzic _____ Dziecko _____

💡 **Wskazówka:** Wydrukuj kilka kopii, trzymaj na lodówce i odhaczaj postępy.

G) Załączniki: plansze i listy do domu

- Lista „TAK / NIE" do publikacji w sieci (TAK: krajobrazy, prace plastyczne; NIE: adres, szkoła, prywatne zdjęcia).
- Plansza „Strefy offline" (stół, łazienka, sypialnia).
- Plakat „Pytaj, zanim klikniesz" — 3 pytania: kto? skąd to wie? czy potwierdzają to inne źródła?

📞 Gdzie szukać pomocy

Jeśli coś cię niepokoi, nie jesteś sam. W Polsce działa kilka instytucji, które pomagają rodzicom i dzieciom w sytuacjach zagrożeń online:

Instytucja	Co oferuje	Kontakt
Dyżurnet.pl	Zgłaszanie niebezpiecznych treści	dyzurnet.pl
Helpline.org.pl	Wsparcie dla rodziców	800 100 100
Telefon zaufania dla dzieci i	Pomoc i rozmowa	116 111
SaferInternet.pl (NASK)	Materiały edukacyjne	saferinternet.pl
Policja / cyber@policja.go	W sytuacjach poważnych	—

Rozdział 8: Zestaw narzędzi — linki do instrukcji wideo i polecane strony

Oficjalne przewodniki i filmy krok po kroku. Linki są klikalne, a także znajdziesz kody QR do szybkiego skanowania.

7.1 Oficjalne przewodniki

- Google Family Link — Centrum pomocy: **support.google.com/families**

- Family Link — strona produktu: **families.google/familylink**

- Apple — Screen Time: **support.apple.com/108806**

- Microsoft Family Safety — konfiguracja: **support.microsoft.com/family-safety**

- YouTube Kids — pomoc: **support.google.com/youtubekids**

> 📌 **Praktyka**
> Zawsze sprawdzaj datę aktualizacji artykułu. Interfejsy zmieniają się często; w razie wątpliwości porównaj 2–3 źródła.

7.2 Filmy instruktażowe (YouTube)

- Apple Support — oficjalny kanał: **youtube.com/AppleSupport**

- Microsoft — Family Safety (wideo): YouTube: **zUOy-NPaP6M**

- Family Link — playlista: **Playlista Family Link**

7.3 Centra bezpieczeństwa popularnych aplikacji

- TikTok — Family Pairing: **support.tiktok.com/.../family-pairing**

- Instagram — Family Center: **help.instagram.com/309877544512275**

- Snapchat — Family Center: **parents.snapchat.com/family-center**

- Discord — Family Center: **discord.com/safety-family-center**

- Roblox — Parental Controls (FAQ): **en.help.roblox.com/.../Parental-Controls-FAQ**

7.4 Filtry sieciowe (DNS/router)

- OpenDNS FamilyShield — router guide: **support.opendns.com/.../FamilyShield**
- Cloudflare 1.1.1.1 for Families — setup: **developers.cloudflare.com/1.1.1.1/setup**

7.5 Aplikacje komercyjne

- Qustodio: **qustodio.com**
- Kaspersky Safe Kids: **kaspersky.com/safe-kids**
- Norton Family: **us.norton.com/products/norton-family**

💡 **Jak korzystać z listy:**
Dodaj kluczowe linki do zakładek. Wróć do nich co 3–6 miesięcy — funkcje i nazwy opcji potrafią się zmieniać.

Załącznik A: Kody QR — szybkie skanowanie

Zeskanuj kod aparatem telefonu, by otworzyć instrukcję lub stronę pomocy. Pod każdym kodem znajdziesz też klikalny link

- Google Family Link – Centrum pomocy

https://support.google.com/families/?hl=pl

- Google Family Link – strona produktu

https://families.google/familylink/

- Apple – Czas przed ekranem (Screen Time)

https://support.apple.com/en-us/108806

- Microsoft Family Safety – konfiguracja

https://support.microsoft.com/en-us/account-billing/set-up-microsoft-family-safety-b6280c9d-38d7-82ff-0e4f-a6cb7e659344

- YouTube Kids – pomoc

https://support.google.com/youtubekids/?hl=en

- TikTok – Family Pairing
https://support.tiktok.com/en/safety-hc/account-and-user-safety/family-pairing

- Instagram – Family Center
https://help.instagram.com/309877544512275

- Snapchat – Family Center
https://parents.snapchat.com/family-center

- Discord – Family Center
https://discord.com/safety-family-center

- Roblox – Parental Controls FAQ
https://en.help.roblox.com/hc/en-us/articles/30428248050068-Parental-Controls-FAQ

- OpenDNS FamilyShield – router guide

https://support.opendns.com/hc/en-us/articles/228006487-FamilyShield-Router-Configuration-Instructions

- Cloudflare 1.1.1.1 for Families – setup

https://developers.cloudflare.com/1.1.1.1/setup/

- Qustodio – strona

https://www.qustodio.com/en/

- Kaspersky Safe Kids – strona

https://www.kaspersky.com/safe-kids

- Norton Family – strona

https://www.us.norton.com/products/norton-family

- Internet Matters – Parental Controls

https://www.internetmatters.org/parental-controls/

Zakończenie – refleksja dla rodzica

Internet to nie wróg.

To narzędzie – potężne, szybkie i często nieprzewidywalne. Twoje dziecko dorasta w świecie, którego ty nie miałeś. Ale to nie znaczy, że nie możesz go zrozumieć. Wystarczy, że **pójdziesz z nim kawałek tej drogi** – zamiast próbować zatrzymać świat.

Nie bój się rozmawiać o błędach. Nie bój się przyznać, że nie wiesz. W oczach dziecka nie musisz być wszechwiedzącym rodzicem. Wystarczy, że jesteś **obecnym rodzicem**. Bo najlepszy filtr, najskuteczniejsza aplikacja i najmocniejsze hasło, to zaufanie **między tobą a dzieckiem**.

Zrób pierwszy krok dziś – nie jutro.

- Zapytaj: „*Co dziś ciekawego widziałeś w internecie?*"
- Obejrzyj razem z dzieckiem jego ulubiony filmik.
- Powiedz: „*Nie wszystko rozumiem w tym świecie, ale chcę wiedzieć, co jest dla ciebie ważne.*"

To najprostsza i najpotężniejsza forma cyberbezpieczeństwa.

Bo bezpieczeństwo dziecka w sieci zaczyna się od twojej rozmowy.

Podziękowanie od autora

Dziękuję, że sięgnąłeś po ten e-book. Każdy rodzic, który chce zrozumieć cyfrowy świat swojego dziecka, już wykonuje ogromny krok w stronę bezpieczeństwa i zaufania.

Ten poradnik powstał z połączenia wiedzy, doświadczenia i codziennych rozmów o tym, jak technologia wpływa na nasze życie rodzinne.

Mam nadzieję, że dzięki zawartym tu wskazówkom łatwiej będzie Ci chronić swoje dziecko, a jednocześnie nauczyć je mądrego i odpowiedzialnego korzystania z Internetu.

Dziękuję wszystkim, którzy wspierali mnie w procesie tworzenia — rodzicom, nauczycielom i specjalistom, którzy podzielili się swoim doświadczeniem.

Z wyrazami szacunku,

Radek Wilmański
SafeBook Polska

Dziękuję za przeczytanie!

Masz chwilę na krótką informację zwrotną?

Jeśli w trakcie czytania coś było niejasne
albo zabrakło odpowiedzi na ważne pytanie — napisz do mnie maila: safebookpolska-kontakt@wp.pl

Czytam każdą wiadomość.
Jeśli coś będzie wymagało doprecyzowania, zaktualizuję e-booka i podeślę nową wersję mailowo.

Jeśli ten e-book był dla Ciebie pomocny

Będzie mi bardzo miło, jeśli zostawisz krótką opinię lub ocenę na stronie produktu.
To pomaga innym rodzicom podjąć dobrą decyzję.

A jeśli znasz kogoś, komu ten temat może pomóc
śmiało poleć mu tego e-booka.

Dziękuję za zaufanie

Radek Wilmański SafeBook Polska
Autor e-booka
„Cyberbezpieczeństwo Twojego dziecka”