

# Ochrona aktywności dziecka w Internecie

przewodnik dla rodziców ze  
scenariuszami







Patrycja Żarska Cynk

# Ochrona aktywności dziecka w Internecie

przewodnik dla rodziców ze scenariuszami

W rozległym oceanie cyfrowych informacji, gdzie fale danych przypływają bez przerwy, nasze dzieci stają na brzegu, zafascynowane i gotowe na eksplorację. Jako specjalista ds. ochrony danych osobowych dostrzegam zarówno potencjał, jaki niesie za sobą Internet – dostęp do nieograniczonej wiedzy, rozwijanie kreatywności czy budowanie sieci społecznych – jak i ciemne prądy: nie tylko cyberprzemoc czy phishing, ale także ryzyka związane z naruszeniami RODO, profilowaniem behawioralnym czy drapieżnymi praktykami

marketingowymi skierowanymi do bezbronnych nieletnich.

Niniejszy przewodnik nie ma na celu całkowitego odizolowania dziecka od sieci – to byłaby strategia równie nierealistyczna, co nieskuteczna. Zamiast tego w oparciu również o osobiste doświadczenie z moim 13-letnim synem, który właśnie wkracza świadomie do krainy mediów społecznościowych, proponuję podejście oparte na trzech filarach: wiedzy, komunikacji z dzieckiem i narzędziach.



**Po pierwsze**, uzbroimy się w zrozumienie mechanizmów działania zagrożeń – od ataków socjotechnicznych, przez nieświadome udostępnianie danych w aplikacjach mobilnych, aż po nielegalne gromadzenie danych osobowych i ich niekontrolowane rozpowszechnianie.



**Po drugie**, spojrzymy oczami dziecka na ten świat i na relacje, jakie generuje w środowisku rówieśniczym – nie chcemy wyłączyć przysłowiowego „dziecka z kąpielą” a wspierać młodych cyfrowych podróżników dobrą radą.



**Po trzecie**, zapoznamy się z praktycznymi środkami ochrony – od konfiguracji kontroli rodzicielskich, przez audyt prywatności ustawień w mediach społecznościowych, aż po metody weryfikacji wiarygodności źródeł informacji.



W kolejnych rozdziałach znajdziesz autentyczne scenariusze, zgodne z wytycznymi NASK czy PUODO. Pokazują one, jak łatwo można paść ofiarą cyberprzemocy na forach dyskusyjnych, w jaki sposób drapieżcy online wykorzystują techniki inżynierii społecznej, jakie dane o naszym dziecku gromadzą popularne aplikacje edukacyjne i co z nimi robią. Każdy przypadek opisuję krok po kroku: od przyczyny i przebiegu zdarzenia, przez analizę potencjalnych skutków (np. wyciek wrażliwych danych, permanentny ślad cyfrowy), aż po zestaw narzędzi prewencyjnych i możliwych działań naprawczych.

Moim celem jest nie tylko zwiększyć Twoją czujność, ale przede wszystkim wzmocnić kompetencje – Twoje i Twojego dziecka – w krytycznej ocenie treści online i świadomym zarządzaniu własnymi danymi. Nauczymy się, jak korzystać z przepisów prawa na co dzień, kiedy i jak zgłaszać incydenty bezpieczeństwa oraz jak wdrożyć proste procedury bezpieczeństwa w domu (szyfrowanie rozmów, silne hasła, autoryzacja dwuskładnikowa). Dzięki temu cyfrowa podróż Twoich pociech będzie nie tylko ekscytująca, ale też bezpieczna oraz zgodna z najlepszymi praktykami cyfrowego savoir-vivre.

**Opracowanie przygotowane zostało m.in. na podstawie materiałów i inspiracji Center for Internet Security, Inc. (CIS®) co pokazuje jak międzynarodowy i globalny charakter ma społeczność internetowa.**

**Niech ten przewodnik stanie się dla Ciebie kompasem i mapą po nieznanych wodach Internetu – narzędziem, które z jednej strony pozwoli skorzystać z pełni cyfrowych możliwości, a z drugiej zabezpieczy przed ukrytymi rafami i wirami. To nie tylko nauka ostrożności, ale przede wszystkim budowanie pewności siebie w roli rodzica i opiekuna w erze cyfrowej. Zauważ, że w każdym scenariuszu istotną rolę odgrywają rodzice!**

**Przy naszym współudziale w ich kolejnych krokach w cyberświecie sprawimy, że podróże i komunikacja online naszych dzieci będzie bezpieczna, świadoma i rozwijająca.**







# Scenariusz 1

niebezpieczeństwa związane z udostępnianiem danych osobowych online

**Maciek**, dociekliwy 12-latek, lubi eksplorować media społecznościowe i fora dla graczy. Pewnego dnia zaprzyjaźnia się z Frytkiem75, innym graczem, na forum internetowym. Często dyskutują o grach, a Maciek czuje, że znalazła pokrewną duszę. Podekscytowany dzieli się swoimi doświadczeniami związanymi z grami, szkolnymi historiami i ulubionymi miejscami. Stopniowo Frytek75 wypytywał go o bardziej osobiste szczegóły, takie jak lokalizacja jego szkoły, a ostatecznie jego adres domowy, obiecując wysłać mu grę, o której marzył. Ufny i nieświadomy ryzyka Maciek dzieli się swoim adresem.

Tydzień później rodzice Maćka otrzymują podejrzaną paczkę zaadresowaną do niego. Zaniepokojeni pytają o to Maćka a on podekscytowany opowiada o swoim nowym internetowym przyjacielu – Frytku75, choć sam niewiele może o nim powiedzieć, poza tym w jakiej grze online nawiązał z nim znajomość. Zaniepokojeni rodzice wyjaśniają niebezpieczeństwa związane z udostępnianiem danych osobowych w Internecie. Maciek uświadamia sobie swój błąd i czuje się przerażony, zdając sobie sprawę, że Frytek75 może nie być tym, za kogo się podawał.

## Porady dla Maćka



Poinformuj rodzica lub zaufaną osobę dorosłą, jeśli ktoś poprosi Cię o podanie danych osobowych.



Pamiętaj, że ludzie online mogą nie być tymi, za których się podają.



Nigdy nie udostępniaj danych osobowych, takich jak adres czy numer telefonu, osobom poznanym online.



## Porady dla rodziców



### Otwarty dialog

regularnie rozmawiaj z dzieckiem o działaniach online jego i znajomych.



### Edukuj na temat zagrożeń

wyjaśnij niebezpieczeństwa związane z udostępnianiem danych osobowych w Internecie, w tym adresów, numerów telefonów i informacji o szkole.



### Nadzoruj interakcje online

monitoruj, z kim Twoje dziecko wchodzi w interakcje online i omawiaj wszelkie nowe kontakty.



### Ustawienia prywatności

upewnij się, że profile w mediach społecznościowych i grach są prywatne.



### Odgrywaj scenki

wykorzystaj hipotetyczne sytuacje, aby nauczyć dziecko, jak reagować na prośby o podanie danych osobowych.



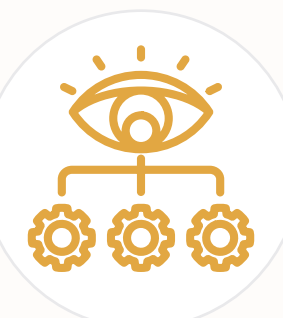
### Nauka krytycznego myślenia

zachęcaj swoje dziecko do kwestionowania intencji znajomych online i weryfikowania ich autentyczności.



### Zgłaszanie podejrzanych zachowań

poinstruuuj dzieci, aby natychmiast zgłaszały Ci wszelkie nietypowe lub niewygodne interakcje online.



### Regularnie kontroluj

sprawdzaj urządzenia i konta internetowe dziecka pod kątem nietypowej aktywności.



### Korzystaj z kontroli rodzicielskiej

wdrożenie oprogramowania do kontroli rodzicielskiej w celu monitorowania i ograniczania komunikacji z nieznanymi osobami.





## Scenariusz 2

ustalanie zasad i granic dotyczących czasu spędzanego przed ekranem i korzystania z Internetu

**Paweł**, 13-letni uczeń szkoły podstawowej, jest coraz bardziej pochłonięty swoim smartfonem, często spędzając godziny w mediach społecznościowych i serwisach streamingowych wideo. Rodzice zauważają, że jego oceny spadają, a on sam wydaje się zmęczony i rozdrażniony przez większość poranków. Zaniepokojeni, zdają sobie sprawę, że muszą ustalić granice czasu spędzanego przez niego przed ekranem, zwłaszcza w nocy, aby upewnić się, że ich dziecku pozostaje wystarczająco dużo czasu na sen i skupienie się na nauce.

Rodzice Pawła zapraszają go na rozmowę. Ten początkowo się opiera, argumentując, że wszyscy jego przyjaciele są online późno w nocy. Jednak jego rodzice wyjaśniają znaczenie równowagi i wpływ nadmiernego czasu spędzanego przed ekranem na jego zdrowie i wyniki w nauce.

### Porady dla Pawła



Równoważ aktywność online z hobby i zainteresowaniami offline.



Przestrzegaj zasad dotyczących czasu spędzanego przed ekranem ustalonych przez rodziców.



Zrozum, że te zasady służą Twojemu dobremu samopoczuciu.



## Porady dla rodziców



### Ustal jasne zasady

określ konkretne godziny korzystania z urządzenia, zwłaszcza wieczorami i w godzinach nauki.



### Wyjaśnij reguły

pomóż dziecku zrozumieć, dlaczego obowiązują te zasady, koncentrując się na zdrowiu i wynikach w nauce.



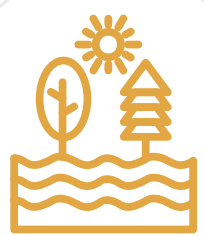
### Stwórz strefy wolne od technologii

wyznacz obszary, takie jak sypialnie i stoły jadalne, jako wolne od urządzeń, aby zachęcić rodzinę do interakcji i lepszej higieny snu.



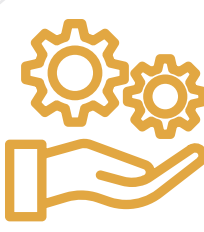
### Dawaj dobry przykład

modeluj zrównoważone zachowanie w czasie spędzanym przed ekranem.



### Zachęcaj do alternatywnych aktywności

promuj hobby i zajęcia, które nie wymagają korzystania z ekranów.



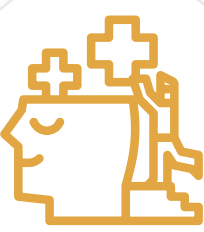
### Korzystaj z pomocy technologicznych

aby egzekwować zasady, wdrażaj blokady aplikacji lub aplikacje monitorujące czas spędzany przed ekranem.



### Regularnie przeglądaj i dostosowuj zasady

bądź otwarty na dostosowywanie zasad wraz z rozwojem dziecka i zmianą jego obowiązków.



### Nagradzaj pozytywne zachowania

uznaj i nagradzaj przestrzeganie zasad dotyczących czasu spędzanego przed ekranem.



### Otwarta komunikacja

prowadzenie otwartego dialogu na temat wpływu czasu spędzanego przed ekranem na codzienne życie i obowiązki.



### Spójność jest kluczowa

stosuj zasady konsekwentnie i sprawiedliwie, unikając wyjątków, chyba że jest to konieczne.





## Scenariusz 3

monitorowanie aktywności online i przeglądanie historii przeglądarki

10-letnia **Natalia** zaczęła ostatnio częściej korzystać z Internetu w ramach projektów szkolnych i w czasie wolnym. Jej rodzice chcą zapewnić jej dostęp do treści odpowiednich dla jej wieku. Postanawiają regularnie monitorować jej aktywność online, w tym przeglądać historię przeglądarki.

Pewnego wieczoru, podczas sprawdzania komputera Natalii, mama Natalii zauważyła kilka wyszukiwanych haseł, które prowadzą do stron nieodpowiednich dla wieku Natalii. Zaniepokojona, zdaje sobie sprawę, że musi porozmawiać z Natalią o bezpieczeństwie w Internecie i wprowadzić bardziej rygorystyczne środki monitorowania.

### Porady dla Natalii



Zwracaj uwagę na odwiedzane strony internetowe i upewnij się, że są one odpowiednie.



Pamiętaj, że Twoi rodzice mogą sprawdzić historię Twojej przeglądarki, aby zapewnić Ci bezpieczeństwo.



Jeśli natkniesz się na coś nieodpowiedniego, natychmiast poinformuj o tym rodziców.



## Porady dla rodziców



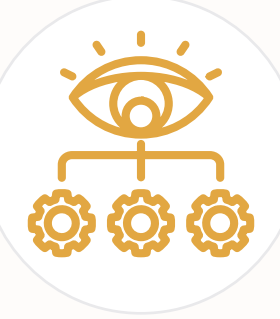
### Otwarta dyskusja

zaczynij od spokojnej rozmowy na temat bezpieczeństwa w Internecie i powodów monitorowania aktywności dziecka w sieci.



### Odpowiednie wytyczne

ustal jasne wytyczne dotyczące tego, jakie rodzaje stron internetowych są odpowiednie dla wieku dziecka.



### Regularnie kontroluj

przeglądaj historię przeglądarki, aby zrozumieć zainteresowania i nawyki dziecka w Internecie.



### Korzystaj z narzędzi

monitorujących wdrożenie oprogramowania do kontroli rodzicielskiej w celu filtrowania treści i monitorowania aktywności.



### Naucz odpowiedzialnego korzystania

poinformuj swoje dziecko o znaczeniu odpowiedzialnego korzystania z Internetu i potencjalnych zagrożeniach związanych z niektórymi witrynami.



### Zachęcaj do otwartości

wspieraj środowisko, w którym Twoje dziecko czuje się komfortowo omawiając swoje doświadczenia online.



### Korzystanie z funkcji bezpieczeństwa przeglądarki

używaj ustawień bezpiecznego wyszukiwania w przeglądarkach i wyszukiwarkach, to funkcja SafeSearch, która uruchomisz np. w ustawieniach przeglądarki Google, funkcję tą możesz też uruchomić z poziomu aplikacji Family Link.



### Utwórz bezpieczną listę

stwórz listę zatwierdzonych stron internetowych dla swojego dziecka.



### Bądź na bieżąco

z najnowszymi trendami online i związanymi z nimi potencjalnymi zagrożeniami.



### Zaangażowanie rodziców

zaangażuj się w działania online swojego dziecka, sugerując strony internetowe i zasoby online, z których może korzystać.





# PARENTAL CONTROL ON

## Scenariusz 4

włączanie kontroli rodzicielskiej na urządzeniach i w aplikacjach

Rodzice dziewięcioletniej **Kasi**, są zaniepokojeni jej ekspozycją na nieodpowiednie treści w Internecie. Postanowili włączyć kontrolę rodzicielską na jej urządzeniach i aplikacjach, aby zapewnić jej dostęp tylko do materiałów odpowiednich dla wieku. Zauważyli, że Kasia spędza dużo czasu na swoim tablecie, często pobierając nowe aplikacje bez zrozumienia ich treści.

Po skonfigurowaniu kontroli rodzicielskiej rodzice odkrywają, że Kasia próbuje pobrać grę nieodpowiednią dla jej wieku. Zdają sobie sprawę, że jest to doskonała okazja, aby nauczyć ją, jak ważne jest zachowanie ostrożności przy pobieraniu aplikacji i treści.

### Porady dla Kasi



Zrozum, że kontrola rodzicielska ma na celu ochronę przed szkodliwymi treściami.



Pytaj o zgodę przed pobraniem aplikacji lub dokonaniem zakupów w aplikacji.



Przestrzegaj granic określonych przez te kontrole.



## Porady dla rodziców



### **Wybierz odpowiednie zabezpieczenia**

wybierz narzędzia rodzicielskie, które odpowiadają potrzebom Twojej rodziny i wiekowi Twojego dziecka.



### **Wyjaśnij ich cel**

omów z dzieckiem, dlaczego te kontrole są konieczne i w jaki sposób pomagają je chronić.



### **Regularnie aktualizuj ustawienia**

w miarę jak dziecko rośnie, dostosuj elementy sterujące, aby odzwierciedlały jego poziom dojrzałości.



### **Monitoruj pobieranie aplikacji**

śledź nowe pobrane aplikacje i omawiaj ich zawartość.



### **Zachęcanie do świadomych wyborów**

naucz swoje dziecko podejmowania świadomych decyzji dotyczących tego, co pobiera i ogląda.



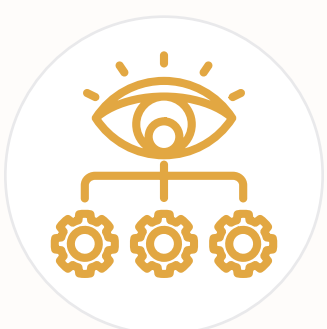
### **Bezpieczne przeglądanie**

upewnij się, że ustawienia bezpiecznego przeglądania są włączone na wszystkich urządzeniach.



### **Zaangażuj swoje dziecko**

zaangażuj dziecko w konfigurację tych elementów sterujących, angażując je w proces nauki o bezpieczeństwie.



### **Sprawdzanie zgodności**

regularnie sprawdzaj, czy kontrola rodzicielska działa zgodnie z przeznaczeniem.



### **Równowaga między zaufaniem a bezpieczeństwem**

choć zaufanie do dziecka jest niezbędne, zapewnienie mu bezpieczeństwa w Internecie jest również kluczowe.



### **Bądź na bieżąco**

z nowymi funkcjami kontroli rodzicielskiej i trendami bezpieczeństwa online.





## Scenariusz 5

uczenie dzieci rozpoznawania i unikania oszustw internetowych oraz ataków phishingowych

Sprytny 13-latek **Darek** często otrzymuje e-maile dotyczące jego aktywności w grach online. Pewnego dnia otrzymuje wiadomość e-mail pochodzącą rzekomo z popularnej platformy do gier, w której zawarto prośbę o kliknięcie linku w celu odebrania darmowej gry. Podekscytowany Darek klika link i nieświadomie instaluje złośliwe oprogramowanie na swoim komputerze.

Rodzice Darka zauważają dziwne zachowanie komputera i odkrywają jego źródło. Zdają sobie sprawę, że Darek potrzebuje wskazówek dotyczących identyfikowania i unikania oszustw internetowych i ataków phishingowych.

### Porady dla Darka



Podchodź sceptycznie do ofert, które wydają się zbyt piękne, by mogły być prawdziwe.



Nigdy nie klikaj podejrzanych linków ani nie pobieraj załączników z nieznanych wiadomości e-mail.



Poinformuj rodzica, jeśli otrzymasz dziwną wiadomość lub e-mail.



## Porady dla rodziców



### **Edukuj na temat oszustw**

naucz swoje dziecko o typowych oszustwach internetowych, w tym o wiadomościach phishingowych i fałszywych witrynach internetowych.



### **Pokaż przykłady**

wiadomości phishingowych i wyjaśnij, jak je wykryć.



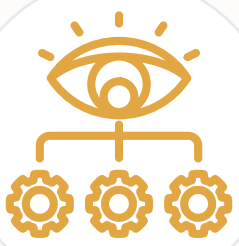
### **Nigdy nie klikaj podejrzanych linków**

poinstruuuj dziecko, aby nigdy nie klikało linków ani nie pobierało załączników z nieznanych źródeł.



### **Weryfikacja autentyczności**

naucz swoje dziecko weryfikować autentyczność e-maili lub wiadomości, porównując je z oficjalną komunikacją.



### **Regularne aktualizacje i bezpieczeństwo**

upewnij się, że komputer ma zaktualizowane oprogramowanie antywirusowe i omów znaczenie cyberbezpieczeństwa.



### **Zachęcanie do komunikacji**

zachęcaj dziecko do konsultowania się z Tobą w przypadku otrzymania podejrzanych wiadomości e-mail lub ofert.



### **Ochrona danych osobowych**

podkreśl znaczenie nieudostępniania danych osobowych online.



### **Krytyczne myślenie**

kultywuj krytyczne myślenie w przypadkach, gdy dziecko otrzymuje oferty, które wydają się zbyt piękne, aby mogły być prawdziwe.



### **Nauczaj i praktykuj bezpieczne nawyki przeglądania**

nauczanie i praktykowanie bezpiecznych nawyków przeglądania.



### **Zgłaszanie podejrzanych działań**

poinstruuuj dziecko, aby zgłaszało podejrzane działania online.





## Scenariusz 6

silne hasła i bezpieczeństwo online

15-letni **Aleksander** lubi gry i kontakty towarzyskie online. Dla wygody używa prostych haseł do swoich kont online. Pewnego dnia odkrywa, że jego konto do gier zostało zhakowane i zmanipulowane.

Rodzice, zauważając jego frustrację, dowiadują się o incydencie i zdają sobie sprawę, jak ważne jest edukowanie Aleksandra w zakresie solidnych praktyk dotyczących haseł i bezpieczeństwa w Internecie.

### Porady dla Aleksandra



Używaj złożonych haseł składających się z liter, cyfr i symboli.



Nigdy nie udostępniaj swoich haseł znajomym.



Regularnie zmieniaj hasła, zwłaszcza do ważnych kont.



## Porady dla rodziców



### **Edukuj na temat bezpieczeństwa haseł**

wyjaśnij znaczenie używania silnych, unikalnych haseł dla każdego konta.



### **Używaj złożonych haseł**

zachęcaj do używania w hasłach kombinacji wielkich i małych liter, cyfr i symboli.



### **Menedżery haseł**

używaj menedżerów haseł do bezpiecznego przechowywania i generowania silnych haseł.



### **Regularna zmiana haseł**

opowiadaj się za regularną zmianą haseł i nie używaj ich ponownie na różnych platformach.



### **Uwierzytelnianie dwuskładnikowe**

włącz uwierzytelnianie dwuskładnikowe (2FA) na kontach w celu zwiększenia bezpieczeństwa.



### **Omówienie zagrożeń**

porozmawiaj o zagrożeniach związanych ze słabymi hasłami, takich jak włamania i kradzież tożsamości.



### **Ćwicz tworzenia haseł**

poproś dziecko, aby poćwiczyło tworzenie solidnych haseł i wyjaśniło, dlaczego każdy element hasła jest ważny.



### **Monitorowanie bezpieczeństwa kont**

okresowo sprawdzaj ustawienia zabezpieczeń kont internetowych swojego dziecka.



### **Dawaj dobry przykład**

używając solidnych haseł.





DEEPFAKE

## Scenariusz 7

AI, deepfake'y i nowe zagrożenia

Ewa, 14-latka, korzysta z popularnego czatu głosowego w grze. Spotyka tam osobę, która podszywa się pod rówieśnika, używając deepfake'owego głosu. Przekonuje Ewę do udostępnienia swojego wideo.

### Porady dla Ewy



Zweryfikuj tożsamość rozmówcy – poproś o wspólne granie przy wideo, porównaj głos na żywo.



Nigdy nie klikaj podejrzanych linków ani nie pobieraj załączników z nieznanymi wiadomości e-mail.



Poinformuj rodzica, jeśli otrzymasz dziwną wiadomość lub e-mail.

### Porady dla rodziców



#### Omów

na czym polega technologia deepfake i jak ją rozpoznać.



#### Zainstaluj narzędzie do analizy głosu lub obrazu

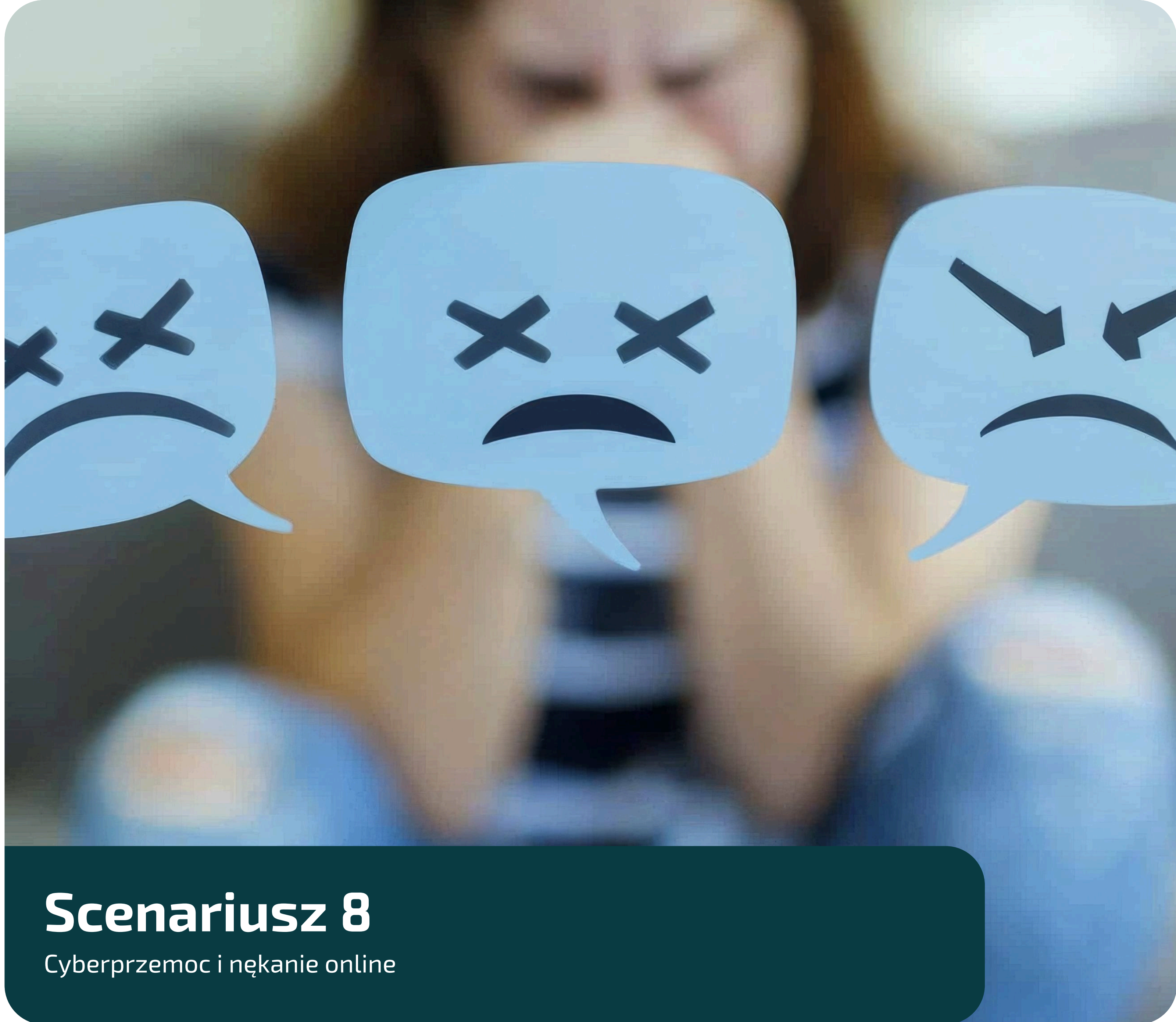
np. aplikację do detekcji deepfake



#### Ustal zasady

rozmów wideo tylko z zaufanymi osobami i w obecności dorosłego





## Scenariusz 8

Cyberprzemoc i nękanie online

13-letnia **Patrycja** staje się celem cyberprzemocy ze strony grupy uczniów z jej szkoły. Umieszczają oni obraźliwe komentarze na jej postach w mediach społecznościowych i wysyłają obraźliwe wiadomości. Początkowo Patrycja próbuje ignorować zastraszanie, ale zaczyna to wpływać na jej samoocenę i nastrój.

Rodzice Patrycji zauważają jej wycofane zachowanie, a po zbadaniu sprawy odkrywają trwającą cyberprzemoc. Zdają sobie sprawę, że muszą zająć się tą poważną sprawą i zapewnić Patrycji bezpieczeństwo i dobre samopoczucie.

### Porady dla Patrycji



Zachowuj uprzejmość i szacunek we wszystkich interakcjach online.



Jeśli jesteś prześladowany online, zapisz dowody i natychmiast poinformuj o tym osobę dorosłą.



Przeciwstawiaj się nękaniam i wspieraj znajomych, którzy mogą być jego ofiarami.



## Porady dla rodziców



### **Słuchaj i wspieraj**

wysłuchaj doświadczeń dziecka bez oceniania i zaoferuj pełne wsparcie.



### **Dokumentowanie nękania**

prowadź rejestr wszystkich wiadomości i postów dotyczących nękania.



### **Zgłoszenie nękania**

zgłoś cyberprzemoc odpowiednim platformom mediów społecznościowych i, jeśli to konieczne, władzom szkoły.



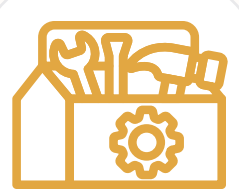
### **Nauczanie etykiety online**

omów znaczenie uprzejmości i szacunku w sieci.



### **Zachęcaj do pozytywnych interakcji**

zachęcaj swoje dziecko do angażowania się w pozytywne społeczności i działania online.



### **Omówienie narzędzi do blokowania i raportowania**

naucz dziecko, jak blokować i zgłaszać użytkowników na platformach mediów społecznościowych.



### **Profesjonalna pomoc w razie potrzeby**

poszukaj profesjonalnej pomocy, jeśli nękanie wpływa na zdrowie psychiczne twojego dziecka.



### **Wzmacniaj poczucie własnej wartości**

i odporność dziecka



### **Edukuj na temat konsekwencji prawnych**

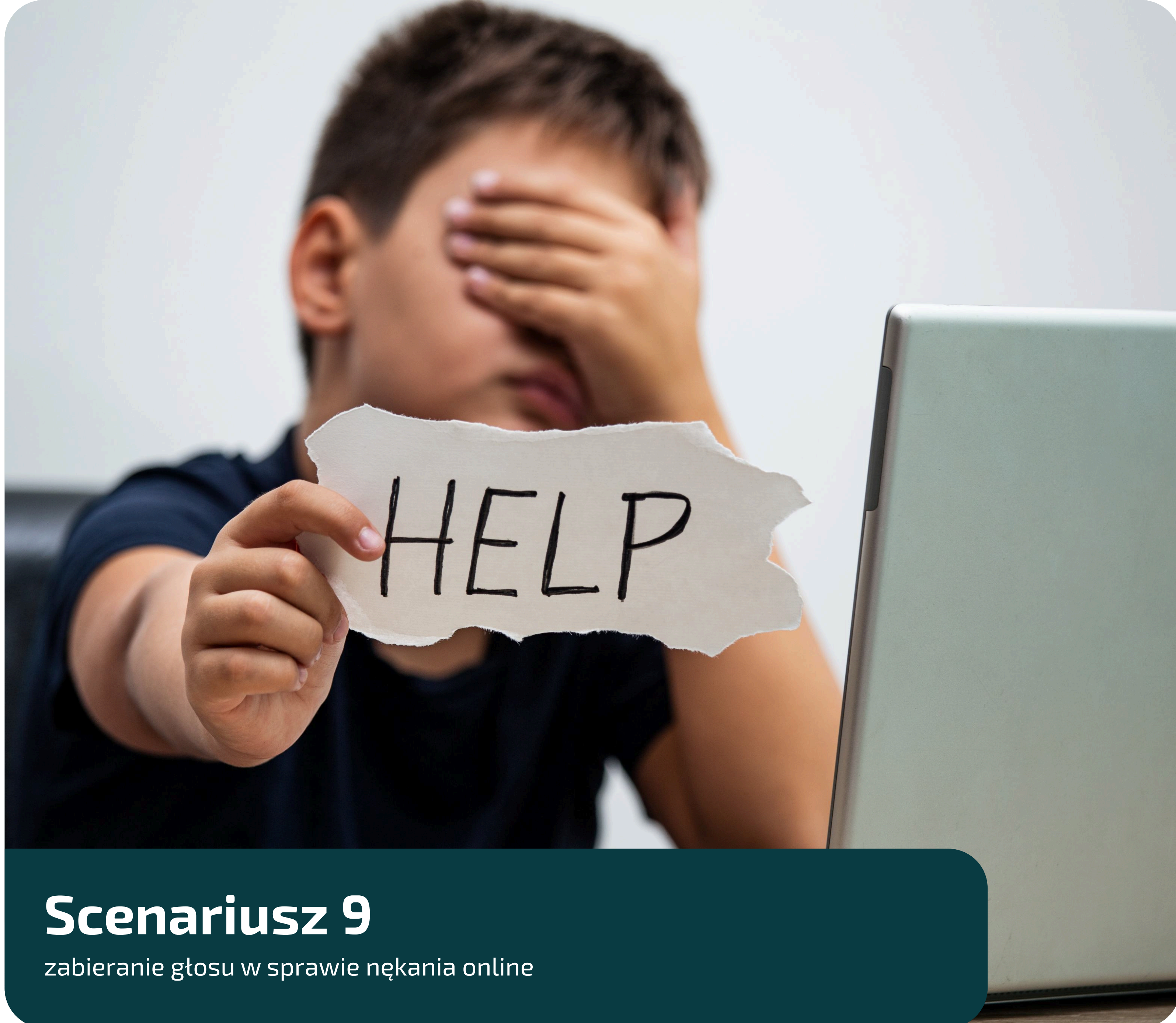
omów konsekwencje prawne cyberprzemocy zarówno dla ofiar, jak i sprawców.



### **System wsparcia rodzinnego**

stwórz rodzinny system wsparcia, w którym dziecko czuje się bezpieczne i doceniane.





## Scenariusz 9

zabieranie głosu w sprawie nękania online

**Jakub**, 14-letni gracz, często wchodzi w interakcje z graczami online. Ostatnio otrzymał wrogie i pełne gróźb wiadomości od anonimowego gracza. Początkowo lekceważył to jako część kultury gier, ale wkrótce odkrywa, że wiadomości są coraz bardziej niepokojące i przykre.

Nie chcąc o tym rozmawiać, Jakub zachowuje niepokojące wiadomości dla siebie, dopóki jego starsza siostra nie zauważy jego niepokoju i nie zachęci go do otwarcia się. Następnie pomaga mu porozmawiać z rodzicami o zaistniałej sytuacji.

### Porady dla Patrycji



Nigdy nie odpowiadaj na groźby lub nieprzyjemne wiadomości.



Powiedz rodzicowi, rodzeństwu, nauczycielowi lub zaufanej osobie dorosłej, jeśli czujesz się nękany w Internecie.



Blokuj i zgłaszaj użytkowników, którzy sprawiają, że czujesz się niebezpiecznie.



## Porady dla rodziców



### Zachęcaj do otwartego dialogu

wspieraj środowisko, w którym Twoje dziecko może dzielić się swoimi doświadczeniami online.



### Traktuj poważnie obawy dziecka

nie bagatelizuj nękania, nawet jeśli ma miejsce "tylko" w cyfrowym świecie.



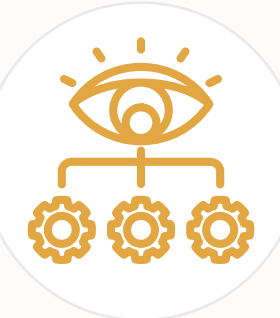
### Zrozumienie sytuacji

uzyskaj jasne zrozumienie nękania, w tym tego, kto jest w nie zaangażowany i co zostało powiedziane.



### Zgłoś i zablokuj napastnika

poprowadź swoje dziecko w zgłaszaniu i blokowaniu napastnika na platformie.



### Przegląd praktyk bezpieczeństwa online

omów praktyki w zakresie bezpieczeństwa i prywatności w sieci.



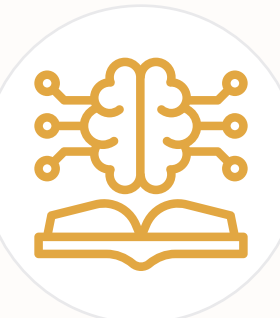
### Wsparcie emocjonalne

zapewnij wsparcie emocjonalne i otuchę.



### Profesjonalne doradztwo

rozważ profesjonalne doradztwo, jeśli nękanie ma znaczący wpływ emocjonalny.



### Edukuj na temat cyfrowego śladu

ucz o cyfrowych śladach i o tym, jak działania online mogą mieć konsekwencje w świecie rzeczywistym.



### Bądź na bieżąco z platformami internetowymi

bądź świadomy platform internetowych i społeczności, których częścią jest Twoje dziecko.



### Omówienie odpowiednich reakcji

naucz odpowiednich reakcji na nękanie online, w tym nieangażowania się w kontakt z osobą nękającą.





## Scenariusz 10

monitorowanie mediów społecznościowych i aplikacji do przesyłania wiadomości

**Justyna**, 16-letnia uczennica szkoły średniej, jest aktywna na wielu platformach mediów społecznościowych. Szanując jej prywatność, rodzice są zaniepokojeni jej interakcjami online i treściami, na które może być narażona.

Rodzice Justyny postanawiają porozmawiać z nią o znaczeniu odpowiedzialnego korzystania z mediów społecznościowych. Wspólnie ustalają plan okresowego przeglądu jej aktywności w mediach społecznościowych, zapewniając bezpieczeństwo i odpowiedzialność w obecności online.

### Porady dla Justyny



Pomyśl, zanim opublikujesz. Czy czujesz się komfortowo, gdy wszyscy to widzą?



Zachowaj prywatność swoich profili i akceptuj zaproszenia do znajomych tylko od osób, które znasz.



Porozmawiaj z rodzicami o tym, co należy udostępniać online.

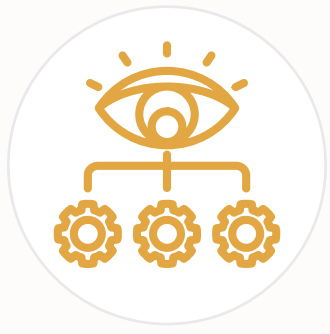


## Porady dla rodziców



### Ustal podstawowe zasady

korzystania z mediów społecznościowych, w tym co należy publikować i udostępniać.



### Regularne spotkania kontrolne

regularnie sprawdzaj aktywność w mediach społecznościowych.



### Szanuj prywatność

zrównoważ monitorowanie z poszanowaniem prywatności dziecka.



### Omówienie reputacji online

omów, w jaki sposób zachowanie dziecka w Internecie może wpłynąć na jego reputację i przyszłe możliwości.



### Edukuj w zakresie ustawień prywatności

naucz, jak korzystać z ustawień prywatności na różnych platformach.



### Zachęcanie do pozytywnej obecności w sieci

zachęcaj do budowania pozytywnej i pełnej szacunku obecności online.



### Zagrożenia związane z nadmiernym udostępnianiem

omów ryzyko związane z nadmiernym udostępnianiem danych osobowych.



### Modeluj właściwe zachowanie

dawaj przykład, korzystając z mediów społecznościowych.



### Bądź na bieżąco

z najnowszymi trendami i potencjalnymi zagrożeniami związanymi z platformami mediów społecznościowych, śledź monity CERT czy organizacji zaangażowanych w edukację cyfrową dzieci jak Cyfrowy Skaut, Dajemy Dzieciom Siłę.



### Otwarta komunikacja

utrzymuj otwarte linie komunikacji na temat interakcji i doświadczeń dziecka w Internecie.





# Scenariusz 11

konsekwencje publikowania nieodpowiednich treści online

**Włodek**, lat 17, jest popularnym uczniem, aktywnym w mediach społecznościowych. Pewnego wieczoru na imprezie z przyjaciółmi publikuje kilka zdjęć i filmów na swoich kontach w mediach społecznościowych, z których niektóre zawierają nieodpowiednie treści i język.

Następnego dnia spotyka się z reakcją społeczności szkolnej i otrzymuje ostrzeżenie od dyrektora szkoły dotyczące jego zachowania w Internecie. Rodzice Włodka dowiadują się o nieodpowiednich wpisach w mediach społecznościowych. Zgadza się usiąść z Włodkiem i porozmawiać o tym, jak odpowiedzialnie publikować w Internecie

## Porady dla Włodka



Zrozum, że to, co publikujesz online, może być widoczne dla wielu osób, w tym dla przyszłych pracodawców.



Unikaj udostępniania treści, które mogłyby zawstydzić Ciebie lub inne osoby.



Pomyśl o tym, jak Twoje posty wpływają na Twój osobisty wizerunek i reputację.



## Porady dla rodziców



### Omów wpływ

wyjaśnij, w jaki sposób działania online mogą mieć konsekwencje w świecie rzeczywistym, które wpływają na reputację, relacje i przyszłe możliwości.



### Rola cyfrowego śladu

naucz o pojęciu cyfrowego śladu i o tym, jak raz opublikowana treść może pozostać online przez czas nieokreślony.



### Zachęcaj do odpowiedzialnego publikowania

zachęcaj do zastanowienia się dwa razy przed opublikowaniem posta i rozważenia jego potencjalnego wpływu.



### Sprawdź ustawienia prywatności

przejrzyj ustawienia prywatności na platformach społecznościowych, aby kontrolować, kto może zobaczyć posty.



### Studia przypadków

podziel się przykładami z życia wziętymi, jak nieodpowiednie treści negatywnie wpływają na innych.



### Zachęcaj do empatii

omów znaczenie empatii i szacunku dla innych w Internecie.



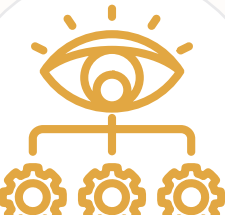
### Przedstaw konsekwencje prawne

poinformuj dziecko o konsekwencjach prawnych publikowania szkodliwych lub obraźliwych treści.



### Buduj świadomość

informuj swoje dziecko na bieżąco o zasadach obowiązujących w szkole i normach społecznych dotyczących zachowań online.



### Monitoruj korzystanie z mediów społecznościowych

regularnie sprawdzaj, w jaki sposób dziecko korzysta z mediów społecznościowych, jednocześnie szanując jego prywatność.



### Promuj pozytywną obecność

zachęcaj do budowania pozytywnej i konstruktywnej obecności online.





# Scenariusz 12

krytyczne myślenie o informacjach online

**Magda**, 13-letnia uczennica, niedawno ukończyła szkolny projekt oparty na informacjach, które znalazła w Internecie. Jednak jej nauczyciel zwraca uwagę na kilka nieścisłości w swojej pracy, powołując się na niezetelne źródła.

Rodzice Magdy, zdając sobie sprawę, że może ona nie być wystarczająco wnikliwa, jeśli chodzi o wiarygodność informacji online, decydują się poprowadzić ją w ocenie i weryfikacji treści online.

## Porady dla Magdy



Nie wszystko, co przeczytasz w Internecie, jest prawdą. Naucz się kwestionować i weryfikować informacje.



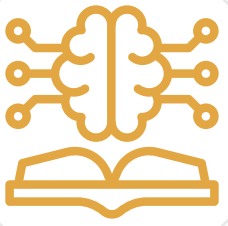
Sprawdzaj fakty, korzystając z wiarygodnych źródeł.



Omów z osobą dorosłą wszelkie mylące lub kontrowersyjne informacje znalezione w Internecie.



## Porady dla rodziców



### **Naucz oceny**

pokaż, jak ocenić wiarygodność strony internetowej lub źródła online.



### **Omów sprawdzanie faktów**

zachęcaj do podwójnego sprawdzania faktów w wielu renomowanych źródłach.



### **Zrozumienie stronniczości**

naucz swoje dziecko, jak rozpoznawać stronniczość i odróżniać opinie od faktów.



### **Zachęcaj do zadawania pytań**

promuj postawę zadawania pytań w odniesieniu do informacji znalezionych online.



### **Korzystaj z renomowanych źródeł**

poprowadź swoje dziecko w kierunku uznanych, renomowanych źródeł wiadomości i stron edukacyjnych.



### **Przykłady z życia wzięte**

użyj rzeczywistych przykładów, aby zilustrować konsekwencje dezinformacji.



### **Ucz krytycznego myślenia**

wspieraj podstawowe umiejętności myślenia, w tym analizy i rozumowania.



### **Zaangażuj się**

w projekty badawcze swojego dziecka i prowadź je w poszukiwaniu i ocenie źródeł.



### **Edukuj w zakresie umiejętności cyfrowych**

zapewnij zasoby i narzędzia w zakresie umiejętności cyfrowych.



### **Techniki bezpiecznego wyszukiwania**

naucz dziecko skutecznych i bezpiecznych technik wyszukiwania informacji.





## Scenariusz 13

zgłaszanie zagrożeń lub incydentów online

**Mariusz**, 15-letni gracz, otrzymuje serię wiadomości z pogrózkami od innego gracza online. Wiadomości nasilają się, sprawiając, że Mariusz czuje się zaniepokojony i przestraszony. Waha się, czy powiedzieć o tym rodzicom, obawiając się, że mogą oni ograniczyć jego granie.

Kiedy jego rodzice zauważają zmiany w jego zachowaniu, pytają i dowiadują się o sytuacji. Zdają sobie sprawę, jak ważne jest nauczanie Mariusza, jak radzić sobie z zagrożeniami online i jak ważne jest zgłaszanie takich incydentów.

### Porady dla Mariusza



Nie kontaktuj się z nikim, kto grozi Ci lub straszy Cię w Internecie.



Zachowaj wszelkie wiadomości z pogrózkami i pokaż je zaufanej osobie dorosłej.



Pamiętaj, że to nie Twoja wina, jeśli ktoś Ci grozi. Poszukaj pomocy u zaufanej osoby dorosłej.



## Porady dla rodziców



### **Stwórz bezpieczne środowisko**

upewnij się, że Twoje dziecko czuje się bezpiecznie i jest wspierane w omawianiu doświadczeń online.



### **Traktuj zagrożenia poważnie**

potwierdź powagę zagrożeń online i zapewnij swoje dziecko o jego bezpieczeństwie.



### **Dokumentowanie gróźb**

poinstruuuj dziecko, aby zapisywało zrzuty ekranu lub nagrania wiadomości z pogróżkami.



### **Zgłaszanie**

poinstruuuj dziecko, jak zgłaszać zagrożenia w grze administratorom gry i, w razie potrzeby włączyć się w ten proces szczególnie w ramach zgłaszania zagrożeń organom ścigania.



### **Przegląd praktyk bezpieczeństwa online**

omów bezpieczne praktyki online, w tym ustawienia prywatności i wybór osób, z którymi dziecko chce wchodzić w interakcje.



### **Otwarta komunikacja**

prowadź otwarty dialog na temat interakcji online dziecka.



### **Monitoruj aktywności online**

monitoruj aktywność online swojego dziecka, szanując jego prywatność.



### **Naucz mechanizmów raportowania**

ustal i poinformuj swoje dziecko o funkcjach raportowania dostępnych na większości platform do gier.



### **Profesjonalna pomoc w razie potrzeby**

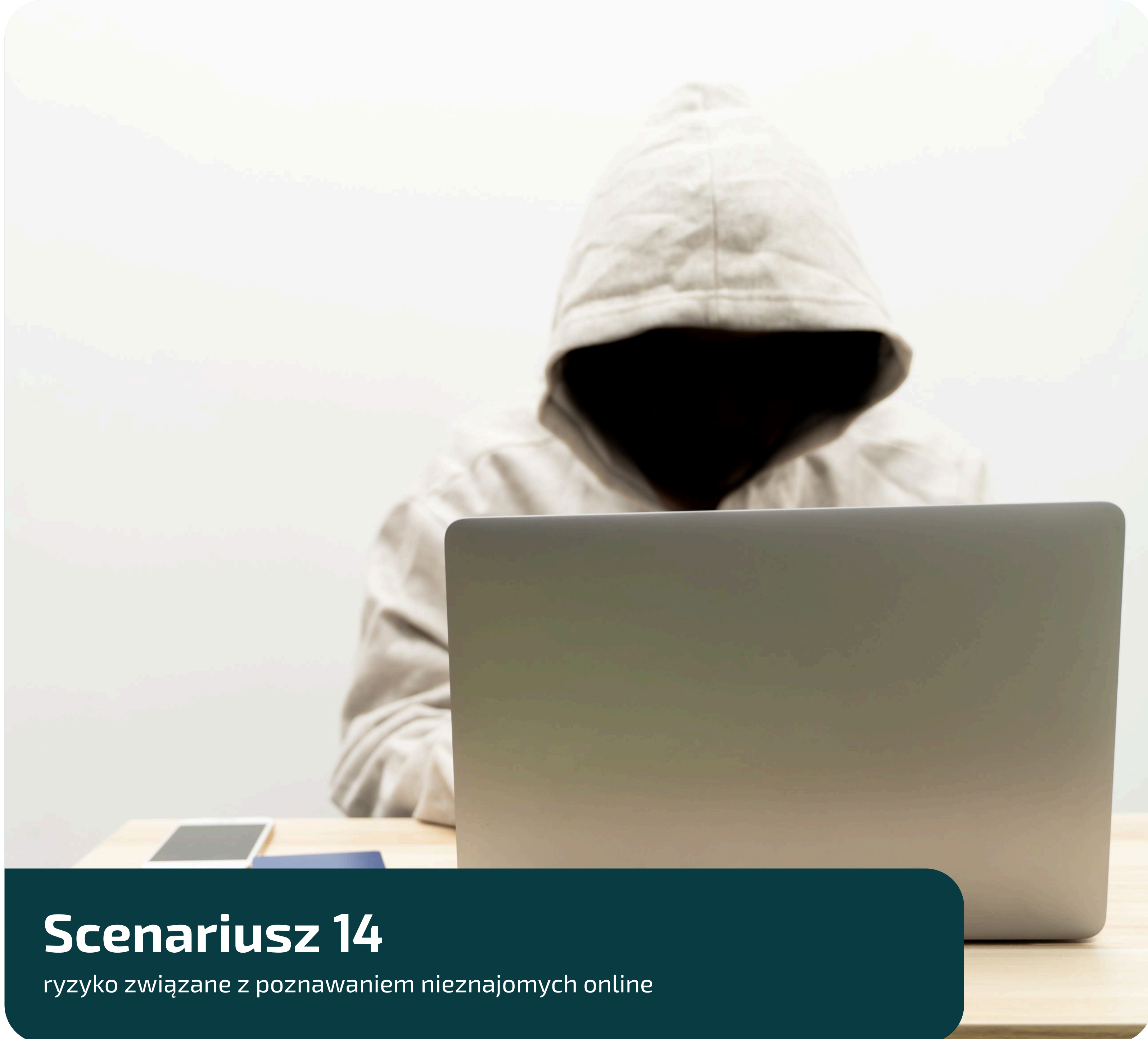
zasięgnij porady, jeśli incydent ma wpływ na zdrowie psychiczne dziecka.



### **Wsparcie rodziny**

oferuj ciągłe wsparcie i zrozumienie.





## Scenariusz 14

ryzyko związane z poznawaniem nieznajomych online

15-letnia **Olga** zaprzyjaźnia się z osobą poznaną na czacie online. Po tygodniach czatowania osoba ta sugeruje, by spotkali się osobiście. Podekscytowana Olga zgadza się i planuje spotkanie w lokalnej kawiarni, nie informując o tym rodziców.

Starszy brat Olgi podsłuchuje jej rozmowę telefoniczną i powiadamia rodziców. Zaniepokojeni rodzice Olgi usiedli z nią, aby omówić potencjalne niebezpieczeństwa związane z osobistym spotkaniem z kimś online.

### Porady dla Olgi



Nigdy nie zgadzaj się na osobiste spotkanie z kimś, z kim rozmawiałeś tylko online.



Poinformuj rodziców o wszelkich zaproszeniach na spotkania ze znajomymi online.



Pamiętaj, że ludzie online mogą nie być tymi, za których się podają.



## Porady dla rodziców



### **Omów niebezpieczeństwo**

podkreśl ryzyko związane z osobistymi spotkaniami ze znajomymi online.



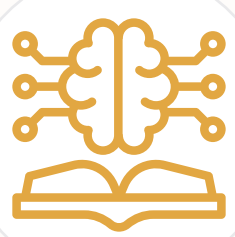
### **Zero spotkań sam na sam**

poinstruuuj, aby nigdy nie spotykać się z internetowym znajomym sam na sam lub prywatnie.



### **Otwarta komunikacja**

zachęcaj dziecko do omawiania znajomych i aktywności online.



### **Edukuj w zakresie zabezpieczeń**

naucz dziecko środków bezpieczeństwa, takich jak spotykanie się w miejscach publicznych i informowanie zaufanej osoby dorosłej.



### **Odgrywaj scenki scenek**

wykorzystaj odgrywanie ról, aby przećwiczyć radzenie sobie z zaproszeniami na spotkania.



### **Monitoruj interakcji online**

miej oko na interakcje online swojego dziecka, szanując jego prywatność.



### **Buduj zaufanie**

zbuduj relację opartą na zaufaniu, w której Twoje dziecko czuje się komfortowo omawiając działania online.



### **Zrozum perspektywę dziecka**

wysłuchaj powodów, dla których dziecko chce spotykać się z przyjaciółmi online i zajmij się wszelkimi błędnymi przekonaniem.



### **Ustal granice**

ustal jasne zasady dotyczące relacji online i spotkań osobistych.



### **Nadzór rodzicielski**

zaoferuj, że będziesz towarzyszyć swojemu dziecku, jeśli kiedykolwiek rozważane jest spotkanie ze znajomym online.





## Scenariusz 15

zasady dotyczące gier online i czatów

**Michał**, lat 10, spędza dużo czasu grając w gry online z funkcjami czatu. Jego rodzice zauważyli, że staje się coraz bardziej niespokojny po sesjach grania i podsłuchali, jak używa nieodpowiedniego języka podczas czatów w grze.

Rodzice Michała ustalili zasady dotyczące jego gier online i korzystania z pokoi rozmów, aby zapewnić zdrowsze środowisko gier.

### Porady dla Michała



Zachowaj szacunek dla innych podczas grania w gry lub czatowania online.



Nie udostępniaj danych osobowych graczom poznanym online.



Jeśli ktoś sprawia, że czujesz się niekomfortowo, przerwij rozmowę i powiedz o tym osobie dorosłej.



## Porady dla rodziców



### Ustal limity czasowe

aby zapobiec nadmiernemu graniu.



### Monitoruj czaty

zwracaj uwagę na język i zachowanie dziecka na czatach.



### Omów odpowiednie zachowanie

porozmawiaj o pełnej szacunku komunikacji i zachowaniu online.



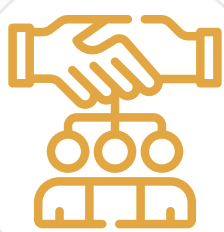
### Wybór gier

wybierz gry odpowiednie dla wieku i poziomu dojrzałości dziecka.



### Zachęcaj do przerw

promuj robienie przerw, aby ograniczyć czas spędzany przed ekranem i stres.



### Naucz etykiety online

naucz swoje dziecko cyfrowej etykiety i wpływu słów.



### Kontrola rodzicielska

użyj kontroli rodzicielskiej, aby ograniczyć dostęp do określonych funkcji czatu.



### Zrównoważone działania

zachęcaj do zrównoważenia aktywności online i offline.



### Otwarty dialog

utrzymuj otwartą komunikację na temat doświadczeń i uczuć dziecka związanych z grami.



### Dawaj dobry przykład

sam modeluj odpowiednie zachowanie w sieci.



# Scenariusz 16

ustawienia prywatności w mediach społecznościowych i aplikacjach do przesyłania wiadomości

**Kaśka**, 16-letnia licealistka, lubi kontaktować się z przyjaciółmi i dzielić się swoim życiem w mediach społecznościowych. Często publikuje zdjęcia swoich codziennych aktywności, nieświadoma tego, że jej profil jest publicznie widoczny. Pewnego dnia otrzymuje wiadomości od nieznanych osób, które komentują jej posty, co wprawia ją w zakłopotanie.

Jej rodzice, zauważając jej niepokój, sprawdzają jej konta w mediach społecznościowych i zdają sobie sprawę, że jej posty są widoczne dla każdego online. Decydują, że kluczowe jest edukowanie Kaśki na temat znaczenia ustawień prywatności i bezpieczniejszego zarządzania jej obecnością w Internecie.

## Porady dla Kaśki



Zachowaj prywatność swoich profili w mediach społecznościowych i udostępniaj je tylko osobom, które znasz.



Pomyśl, zanim opublikujesz. Gdy coś znajdzie się w sieci, może być trudne do usunięcia.



Regularnie sprawdzaj ustawienia prywatności z rodzicem.

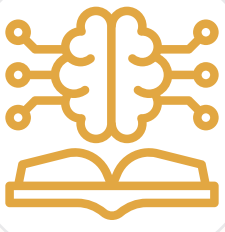


## Porady dla rodziców



### Wspólny przegląd ustawień prywatności

przejrzyj ustawienia prywatności na każdej platformie mediów społecznościowych z dzieckiem, upewniając się, że ich profile są ustawione jako prywatne.



### Edukuj w zakresie udostępniania informacji

omów, jakiego rodzaju informacje nie powinny być udostępniane publicznie, takie jak lokalizacja, dane kontaktowe i plany osobiste.



### Zachęcaj do regularnych aktualizacji

przypominaj dziecku o regularnym sprawdzaniu i aktualizowaniu ustawień prywatności.



### Omów zagrożenia

związane z nadmiernym udostępnianiem danych osobowych, w tym niechcianą uwagę i obawy dotyczące prywatności danych.



### Naucz świadomości śladu cyfrowego

wyjaśnij, w jaki sposób zachowanie dziecka w Internecie może wpłynąć na jego reputację i przyszłe możliwości.



### Modeluj właściwe zachowanie

zademonstruj odpowiedzialne korzystanie z mediów społecznościowych.



### Monitoruj korzystania z mediów społecznościowych

upewniając się, że jest ona zgodna z rodzinnymi wytycznymi dotyczącymi bezpieczeństwa online.



### Promuj pozytywną obecność

zachęcaj swoje dziecko do pozytywnego i kreatywnego korzystania z mediów społecznościowych.



### Stwórz bezpieczne środowisko

wspieraj środowisko rodzinne, w którym Twoje dziecko czuje się komfortowo omawiając kwestie lub wątpliwości online.



### Bądź na bieżąco

bądź na bieżąco z najnowszymi trendami w mediach społecznościowych i narzędziami ochrony prywatności, aby skutecznie kierować swoim dzieckiem.





THANK  
YOU!

## Scenariusz 17

szacunek i uprzejmość w sieci

**Witek**, lat 15, aktywnie uczestniczy w różnych forach internetowych i społecznościowych. Pewnego dnia jego rodzice podsłuchali, jak odnosił się lekceważąco do innego gracza w grze online.

Zaniepokojeni tym zachowaniem rodzice Witka postanawiają zwrócić uwagę na znaczenie szacunku i uprzejmości we wszystkich interakcjach online, podkreślając, że anonimowość Internetu nie usprawiedliwia złego zachowania.

### Porady dla Witka



Traktuj innych online tak, jak sam chciałbyś być traktowany.



Unikaj mówienia krzywdzących lub złośliwych rzeczy w Internecie.



Pamiętaj, że po drugiej stronie ekranu znajduje się prawdziwa osoba.



## Porady dla rodziców



### **Omów etykietę online**

porozmawiaj o traktowaniu innych z szacunkiem, nawet w Internecie.



### **Ustal oczekiwania**

jasno określ akceptowalne i pełne szacunku zachowanie online.



### **Dawaj dobry przykład**

modeluj pozytywne i pełne szacunku interakcje online.



### **Konsekwencje za niewłaściwe zachowanie**

ustal konsekwencje za lekceważące lub nieuprzejme zachowanie online.



### **Trening empatii**

zachęcaj dziecko do empatii, pytając je, jak by się czuło, gdyby ktoś zwracał się do niego w podobny sposób.



### **Monitoruj interakcje online**

okresowo sprawdzaj komunikację online swojego dziecka, upewniając się, że jest ona zgodna z wartościami rodziny.



### **Zachęcaj do pozytywnych społeczności**

poprowadź swoje dziecko do społeczności internetowych promujących pozytywne nastawienie i szacunek.



### **Omów wpływ słów**

porozmawiaj o tym, jak słowa mogą wpływać na innych, nawet jeśli są przekazywane cyfrowo.



### **Promuj autorefleksję**

zachęcaj swoje dziecko do zastanowienia się nad jego zachowaniem online i jego wpływem na innych.



### **Naucz rozwiązywania konfliktów**

oferuj strategię radzenia sobie z nieporozumieniami online w sposób pełen szacunku.





## Scenariusz 18

monitorowanie zakupów i subskrypcji online

14-letnia **Joasia** ma dostęp do rodzinnego tabletu z połączoną kartą kredytową w celu dokonywania zakupów aplikacji. Rodzice ufają jej osądowi, ale zauważają opłaty za kilka subskrypcji i gier online, których nie akceptują.

Zdając sobie sprawę z potrzeby bardziej precyzyjnych wytycznych i monitorowania, rodzice usiedli z Joanną, aby omówić odpowiedzialne wydatki online i znaczenie uzyskania zgody na zakup.

### Porady dla Joanny



Przed zakupem czegokolwiek online zapytaj o zgodę.



Pamiętaj o zakupach w aplikacjach i subskrypcjach.



Naucz się wartości pieniędzy i rozsądnego ich wydawania.

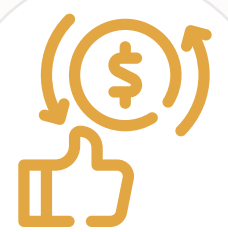


## Porady dla rodziców



### Ustal limity wydatków

ustal jasne zasady dotyczące kwoty, jaką dziecko może wydać i jakie rodzaje zakupów są dozwolone.



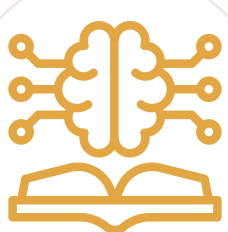
### Wymagaj zgody na zakupy

nalegaj, aby dziecko pytało o zgodę przed zakupem lub subskrypcją.



### Wspólne przeglądanie zakupów

regularnie sprawdzaj historię zakupów z dzieckiem, aby zrozumieć jego nawyki związane z wydatkami.



### Edukuj na temat oszustw internetowych

ostrzeż swoje dziecko o oszustwach i znaczeniu weryfikacji legalności witryn i aplikacji przed zakupem.



### Połączenie z ograniczonym kontem

rozważ połączenie tabletu/smartfona z kontem z ograniczonymi środkami, aby kontrolować wydatki.



### Omów wartość pieniądza

i odpowiedniego budżetowania.



### Nagradzaj swoje dziecko

wdrażaj system, w którym dziecko może zdobywać kredyty lub dodatki na zakupy poprzez obowiązki domowe lub dobre zachowanie.



### Korzystaj z kontroli rodzicielskiej

aby zatwierdzać lub odrzucać żądania zakupu.



### Zachęcaj do szukania informacji przed zakupem

naucz swoje dziecko wyszukiwania informacji i czytania recenzji przed dokonaniem zakupu online.



### Wzorowa odpowiedzialność finansowa

demonstruj odpowiedzialne zachowania finansowe podczas zakupów online.





## Scenariusz 19

obywatelstwo cyfrowe i odpowiedzialne zachowanie w sieci

**Ania**, 13-latka, chętnie korzysta z mediów społecznościowych i platform internetowych. Jej rodzice, zauważają, że chociaż Ania jest obeznana z technologią, nie jest w pełni świadoma tego, co robi. Rodzice obserwują, jak Ania od czasu do czasu

udostępnia posty swoich znajomych bez ich zgody i angażuje się w gorące debaty online. Zaniepokojeni, decydują, że nadszedł czas, aby nauczyć Ani cyfrowego obywatelstwa i odpowiedzialnego zachowania w sieci.

### Porady dla Ani



Twoje działania online wpływają na innych. Bądź dobrym cyfrowym obywatelem.



Szanuj prywatność i opinie innych osób w Internecie.



Uświadom sobie długoterminowe skutki swojego zachowania online.



## Porady dla rodziców



### **Definicja obywatelstwa cyfrowego**

wyjaśnij pojęcia obywatelstwa cyfrowego i jego znaczenia w dzisiejszym cyfrowym świecie.



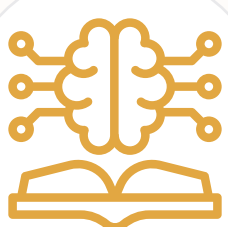
### **Omów obowiązki**

porozmawiaj o obowiązkach związanych z korzystaniem z Internetu, w tym o poszanowaniu prywatności i opinii innych osób.



### **Zachęcaj do komunikacji opartej na szacunku**

naucz swoje dziecko, aby komunikowało się z szacunkiem i konstruktywnie online, nawet w przypadku nieporozumień.



### **Edukuj w zakresie prywatności i bezpieczeństwa**

omówienie znaczenia prywatności i bezpieczeństwa online.



### **Modeluj pozytywne zachowania**

demonstruj pozytywne i odpowiedzialne zachowania cyfrowe.



### **Nauczaj o zgodzie**

podkreśl potrzebę uzyskania zgody przed udostępnieniem treści innych osób.



### **Omów wpływ działań online**

zwłaszcza konsekwencje w prawdziwym życiu.



### **Równowaga między życiem online i offline**

zachęcaj do zachowania zdrowej równowagi między działaniami online a relacjami i działaniami offline.



### **Wspieraj krytyczne myślenie**

o treściach, które dziecko konsumuje i udostępnia.



### **Otwarty dialog**

utrzymuj otwarty i ciągły dialog na temat doświadczeń i nauki dziecka w cyfrowym świecie.





# Słowniczek

W dobie nieustannych innowacji technologicznych samo nauczanie obsługi urządzeń to za mało – równie istotne są kompetencje miękkie: krytyczne myślenie, empatia online, zdolność do radzenia sobie z niepowodzeniami i troska o prywatność. Bez zintegrowanego podejścia łączącego elementy techniczne, psychologiczne i prawne, cyfrowa wyprawka dziecka będzie niepełna i narażona na luki. Warto więc systematycznie poszerzać zarówno wiedzę, jak i praktyczne umiejętności – rodzinne rytuały, wspólne sesje edukacyjne i świadome korzystanie z nowych technologii to klucz do sukcesu. W uzupełnieniu znajdziesz więc garść podstawowych pojęć ze świata cyfrowej edukacji i samoobrony. Każde hasło zawiera krótkie wyjaśnienie, dlaczego jest istotne oraz praktyczną wskazówkę.

| Pojęcie                               | Definicja                                                                                                                                | Znaczenie                                                                                            | Wskazówka                                                                                                                                            |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cyberhigiena                          | Zbiór nawyków i procedur zapewniających podstawowy poziom bezpieczeństwa cyfrowego (aktualizacje, silne hasła, regularne kopie).         | To codzienny rytuał chroniący przed większością popularnych ataków, nie tylko jednorazowe działania. | Stwórzcie „rodzinną checklistę” – cotygodniowe przypomnienie o aktualizacji systemu, sprawdzeniu kopii zapasowych i zmianie haseł co kwartał.        |
| Cyberprzemoc                          | Przemoc psychiczna lub fizyczna realizowana za pomocą narzędzi cyfrowych – wiadomości, zdjęć, filmów, forów czy gier online.             | Lęk, depresja, izolacja społeczna.                                                                   | Ustalcie kanały komunikacji: dziecko powinno od razu zgłaszać niepokojące zachowania. Regularnie rozmawiajcie o tym, co widzi i doświadczyło online. |
| Deepfake i manipulacja multimedialna  | Zaawansowane techniki generowania lub modyfikowania obrazów i audio w sposób trudny do wykrycia.                                         | Może służyć do oszustw, dezinformacji, stalkowania i szantażu.                                       | Uczcie krytycznego spojrzenia – weryfikujcie materiał u źródła, sprawdzajcie metadane zdjęcia i korzystajcie z narzędzi do detekcji deepfake’ów.     |
| Dwuskładnikowe uwierzytelnianie (2FA) | Dodatkowa warstwa bezpieczeństwa, wymagająca obok hasła także drugiego czynnika – SMS, aplikacji uwierzytelniającej, klucza sprzętowego. | Nawet jeśli hasło zostanie przejęte, dostęp nie zostanie przyznany bez drugiego czynnika.            | Włączajcie 2FA na kontach społecznościowych i edukacyjnych – większość platform (Google, Microsoft, Facebook) ją oferuje.                            |



| Pojęcie                                            | Definicja                                                                                                                                                                                   | Znaczenie                                                                                                                                              | Wskazówka                                                                                                                                                                           |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Edukacja resiliencyjna (digital resilience)</b> | Rozwijanie u dziecka umiejętności radzenia sobie z negatywnymi doświadczeniami online (trolle, hejt, niepowodzenia w grach).                                                                | Techniczne zabezpieczenia to jedno, ale odporność psychiczna minimalizuje emocjonalne skutki ataków i frustracji.                                      | Rozmawiajcie o emocjach, zachęcajcie do przerw i aktywności offline jako metody radzenia sobie ze stresem cyfrowym.                                                                 |
| <b>Grooming</b>                                    | Budowanie relacji z dzieckiem przez osobę dorosłą w celu wykorzystania seksualnego.                                                                                                         | Działa podstępnie – zaczyna się od pozornie niewinnego zainteresowania, by stopniowo przerodzić się w manipulację.                                     | Opowiadajcie o zjawisku w sposób dostosowany do wieku, ucząc, jak rozpoznawać niepokojące zachowania (nadmierne komplementy, prośby o tajne rozmowy, szybkie propozycje spotkania). |
| <b>Kontrola rodzicielska</b>                       | Narzędzia sprzętowe lub programowe służące ograniczeniu dostępu do treści i monitorowaniu aktywności online.                                                                                | Umożliwia ustawienie limitów czasowych, blokadę nieodpowiednich stron czy filtrów wiekowych w grach.                                                   | Wybierzcie rozwiązanie dopasowane do potrzeb – od narzędzi wbudowanych w system (Windows, iOS) po dedykowane aplikacje (np. Family Link).                                           |
| <b>Obywatelstwo cyfrowe (digital citizenship)</b>  | Świadome i etyczne uczestnictwo w życiu online, respektowanie praw innych użytkowników, poszanowanie własności intelektualnej i przestrzeganie zasad netykiety.                             | W epoce mediów społecznościowych dzieci często nie zdają sobie sprawy z konsekwencji – od obrażania innych po naruszanie praw autorskich.              | Wprowadźcie rodzinne zasady – np. zakaz obraźliwych komentarzy, szanowanie prywatności znajomych.                                                                                   |
| <b>Phishing (wyłudzenie danych)</b>                | Próba nakłonienia do ujawnienia wrażliwych informacji (hasła, numeru karty) poprzez fałszywe maile, wiadomości lub strony internetowe.                                                      | Dzieci mogą kliknąć link w treści, która wydaje się wiarygodna („Twoja szkoła wysłała Ci zadanie”), a w efekcie stracić dostęp do konta czy pieniędzy. | Pokażcie przykłady fałszywych maili i stron, nauczcie zawsze sprawdzać adres nadawcy i linków (hover-over URL).                                                                     |
| <b>Phygitalność</b>                                | Integracja doświadczeń fizycznych i cyfrowych (np. AR w edukacji). Połączenie świata fizycznego (physical) z cyfrowym (digital), by użytkownik otrzymał spójne, zintegrowane doświadczenie. | Wzbogaca naukę, ale otwiera nowe wektory ataku (podszywanie się pod obiekty AR) czy uzależnienia od urządzeń.                                          | Korzystajcie świadomie – oceniajcie wartości edukacyjne aplikacji AR/VR i pilnujcie przerw od ekranu.                                                                               |



| Pojęcie                                  | Definicja                                                                                                                        | Znaczenie                                                                                                                                                                                                                                                                                                                                        | Wskazówka                                                                                                                                                                            |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RODO i ochrona prywatności</b>        | Ogólne Rozporządzenie o Ochronie Danych (GDPR) – zasady przetwarzania danych osobowych w UE, w tym dzieci.                       | Zgodnie z polskim prawem dziecko, które ukończyło 13 lat, nie może samodzielnie założyć konta w grze internetowej lub profilu w mediach społecznościowych, jeśli założenie takiego konta wiąże się z przetwarzaniem danych osobowych. Wynika to z przepisów RODO (art. 8), które w Polsce ustalają tzw. „cyfrowy wiek zgody” na poziomie 16 lat. | Sprawdźcie polityki prywatności aplikacji, z których korzystacie. Upewnijcie się, że dziecko nie podaje więcej informacji niż konieczne (np. pseudonim zamiast prawdziwego imienia). |
| <b>Ślad cyfrowy (digital footprint)</b>  | Zestaw wszystkich informacji o aktywności użytkownika w sieci – posty, komentarze, zdjęcia, logowania, rekordy wyszukiwania itp. | Ślad może być trwały i widoczny dla przyszłych pracodawców, uczelni czy obcych osób.                                                                                                                                                                                                                                                             | Nauczcie dziecko, że wszystko, co trafia do sieci, może zostać „zamrożone” na zawsze. Praktykujcie wspólne przeglądanie profili i usuwanie nieodpowiednich treści.                   |
| <b>Zarządzanie tożsamością cyfrową</b>   | Świadome budowanie i ochrona wizerunku online – wybór pseudonimów, kontrola treści, unikanie deanonimizacji.                     | Chroni przed kradzieżą tożsamości i pozwala dziecku decydować, jak chce być postrzegane w sieci.                                                                                                                                                                                                                                                 | Zachęcajcie do używania pseudonimów w grach i forach. Ustalcie zasady dotyczące publikacji zdjęć – czy i jak je tagować.                                                             |
| <b>Zasada minimalnych uprawnień</b>      | Dziecku przydziela się tylko te uprawnienia, które są niezbędne do korzystania z danego systemu lub aplikacji.                   | Zmniejsza ryzyko, że dziecko niechcący zmieni ustawienia systemowe, zainstaluje niebezpieczne oprogramowanie lub udzieli dostępu do wrażliwych danych.                                                                                                                                                                                           | Zakładanie konta standardowego (bez praw administratora) na komputerze czy tablecie dziecka to proste, ale skuteczne zabezpieczenie.                                                 |
| <b>Złośliwe oprogramowanie (malware)</b> | Aplikacje tworzone z zamiarem wyrządzenia szkody – wirusy, trojany, ransomware, spyware.                                         | Ataki mogą być ukierunkowane na dziecięce konta, a rodzice często nie podejrzewają, że malware infiltrować może nawet gry edukacyjne czy rozszerzenia do przeglądarki.                                                                                                                                                                           | Zainstalujcie i aktualizujcie program antywirusowy na wszystkich urządzeniach. Ustalcie zasady instalacji – tylko za zgodą rodzica.                                                  |





Newsletter RODO

Maj 2025 nr 5/2025

# Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

[SKONTAKTUJ SIĘ Z NAMI](#)