



Bezpieczny Internet

**Przewodnik dla
dzieci i rodziców**

Prywatność, bezpieczeństwo, relacje i dobre cyfrowe nawyki

Czym właściwie jest Internet?

Internet to ogromna sieć połączonych urządzeń, usług i stron. Dzięki niej możemy się uczyć, rozmawiać, grać, oglądać filmy i załatwiać codzienne sprawy.

INTERNET W PROSTYCH SŁOWACH

Telefon, komputer, konsola czy telewizor łączą się z innymi urządzeniami i usługami. Korzystając z tego aplikacje, komunikatory, gry, poczta i strony internetowe. Internet daje dostęp do ludzi i informacji, ale nie sprawdza, czy treść, reklama albo osoba po drugiej stronie są wiarygodne.

APLIKACJA TO NIE CAŁY INTERNET

Możesz świetnie znać swoją ulubioną grę, aplikację czy komunikator, a mimo to trafić na fałszywy profil, podejrzaną reklamę albo próbę wyłudzenia danych. Dlatego warto wiedzieć nie tylko, jak korzystać z Internetu, ale też jak rozpoznawać sytuacje, które powinny wzbudzić czujność.

ZANIM ZALOGUJESZ SIĘ LUB PODASZ DANE

Sprawdź, czy jesteś we właściwym miejscu. Zwróć uwagę na:

1. ADRES

Sprawdź pełną nazwę domeny. Uważaj na literówki i dodatkowe słowa.

2. HTTPS

HTTPS oznacza, że dane przesyłane między Twoim urządzeniem a stroną są szyfrowane. Nie oznacza jednak, że sama strona jest uczciwa lub bezpieczna.

3. ŹRÓDŁO

Do e-dziennika, gry czy aplikacji wchodź przez oficjalną stronę lub aplikację, a nie z przypadkowego linku.



DLA DZIECKA

Nie podawaj hasła, kodu ani danych płatniczych tylko dlatego, że strona wygląda znajomo. Jeśli coś budzi Twoje wątpliwości, pokaż ekran dorosłemu.



DLA DOROSŁEGO

Nie musisz znać każdej aplikacji. Ważne, żeby rozmawiać z dzieckiem o tym, gdzie podaje dane, komu je udostępnia i dlaczego ktoś ich potrzebuje.



ZRÓBCIE TO RAZEM

Znajdźcie oficjalną stronę szkoły, e-dziennika albo często używanej usługi. Sprawdźcie jej adres i dodajcie ją do zakładek.

Prywatność i cyfrowy ślad

Prywatność to świadome decydowanie o tym, jakie informacje o sobie udostępniasz i kto może je zobaczyć.

UWAŻAJ, KOMU UDOSTĘPNIASZ TE INFORMACJE:

- pełne imię i nazwisko, adres, numer telefonu i nazwę szkoły;
- bieżącą lokalizację i informacje o tym, że nikogo nie ma w domu;
- prywatne zdjęcia, rozmowy i wizerunek innych osób.

Hasła i kodów logowania nie przekazuj innym osobom. Dane płatnicze i zdjęcia dokumentów udostępniaj tylko wtedy, gdy jest to konieczne i za wiedzą rodzica lub opiekuna.



CYFROWY ŚLAD

Cyfrowy ślad powstaje podczas korzystania z Internetu – gdy publikujesz, komentujesz, wyszukujesz informacje lub korzystasz z aplikacji i stron. Część tego śladu tworzysz sam, a część powstaje automatycznie, na przykład przez historię odwiedzanych stron, wyszukiwania, lokalizację czy informacje zapisywane przez aplikacje.

Zanim coś opublikujesz, pomyśl: czy chcę, żeby zobaczył to nauczyciel, rodzina albo ja sam za kilka lat?



DLA DZIECKA

Zatrzymaj się na chwilę i sprawdź, czy zdjęcie, film albo wpis nie pokazują informacji, których nie chcesz udostępniać obcym.

Jeśli nie masz pewności, czy coś warto wrzucić do sieci – zapytaj dorosłego.



DLA DOROSŁEGO

Zwróć uwagę, jakie informacje dziecko udostępnia o sobie w aplikacjach, grach i serwisach społecznościowych. Porozmawiajcie o tym, które dane powinny pozostać prywatne i dlaczego.



ZRÓBCIE TO RAZEM

Wybierzcie jedną aplikację i sprawdźcie, jakie ma uprawnienia: np. do lokalizacji, aparatu, mikrofonu lub kontaktów. Wyłączcie te, które nie są potrzebne.

Hasła i bezpieczne logowanie

Dobre hasło to podstawa, ale bezpieczeństwo konta zależy także od dodatkowych zabezpieczeń logowania i ochrony urządzenia.

4 ZASADY OCHRONY KONTA

**Silne i unikalne
hasło**

Wybierz długie, trudne do odgadnięcia hasło i nie używaj go na kilku kontach.

2FA/MFA

Włącz dodatkowe potwierdzenie logowania, jeśli jest dostępne.

Blokada ekranu

Zabezpiecz telefon, tablet i komputer kodem, hasłem lub biometrią.

Aktualizacje

Regularnie aktualizuj telefon, tablet, komputer i używane aplikacje.

CO TO 2FA I MFA?

2FA (uwierzytelnianie dwuskładnikowe) oznacza, że podczas logowania potwierdzasz swoją tożsamość na dwa sposoby, np. hasłem i jednorazowym kodem otrzymanym w telefonie.

MFA (uwierzytelnianie wieloskładnikowe) działa podobnie, ale może wykorzystywać więcej niż dwa sposoby potwierdzenia.

Kodu logowania nie podawaj nikomu.



DLA DZIECKA

Nie używaj jednego hasła wszędzie i nie przekazuj go kolegom ani osobom poznanym w Internecie. Jeśli dostaniesz kod logowania, o który sam nie prosisz, nie podawaj go nikomu i powiedz dorosłemu.



DLA DOROSŁEGO

Pomóż dziecku korzystać z menedżera haseł – narzędzia, które bezpiecznie przechowuje hasła i ułatwia używanie innego hasła do każdego konta. Zadbajcie też o blokadę urządzeń.



ZRÓBIE TO RAZEM

Wybierzcie kilka najważniejszych kont dziecka i sprawdźcie, czy każde ma inne hasło oraz czy można włączyć dodatkowe potwierdzenie logowania.

Podejrzane wiadomości i linki

Phishing i inne oszustwa próbują skłonić odbiorcę do szybkiego kliknięcia, podania danych albo zapłaty.

Najważniejsze jest zatrzymać się i sprawdzić, z czym mamy do czynienia.



PRESJA

„Natychmiast”, „ostatnia szansa”, „konto zablokowane”.

NAGRODA

Darmowe skiny, monety, doładowanie czy informacja o wygranej w konkursie, w którym nie brałeś udziału.

ADRES

Literówka, dziwna końcówka albo adres, który tylko przypomina prawdziwą stronę.

DANE

Prośba o hasło, kod, kartę, BLIK lub szybki przelew.

STOP

Sprawdź, zanim klikniesz!

**ZATRZYMAJ
SIĘ**

**SPRAWDŹ
NADAWCĘ
I ADRES**

**NIE PODAWAJ
DANYCH**

**ZAPYTAJ
DOROSŁEGO**



DLA DZIECKA

Jeśli po kliknięciu linku trafisz na podejrzaną stronę, niczego nie wpisuj ani nie instaluj. Poproś dorosłego o pomoc. Jeśli podałeś hasło, jak najszybciej je zmień. Jeśli podałeś inne dane, od razu powiedz o tym dorosłemu.



DLA DOROSŁEGO

Rozmawiajcie o przykładach z gier, komunikatorów i sklepów. Pokaż dziecku, by zwracało uwagę na nadawcę, adres strony i to, o co ktoś prosi. Zachęcaj, by od razu mówiło Ci, gdy kliknie podejrzaną link, poda dane lub coś wzbudzi jego niepokój.



ZRÓBcie TO RAZEM

Przyjrzyjcie się przykładowej wiadomości, która może być oszustwem. Nie otwierajcie linku. Sprawdźcie, co powinno wzbudzić Waszą czujność.

Nieznajomi i rozmowy online

Awatar, wiek, głos czy zdjęcie nie zawsze pokazują, kto naprawdę jest po drugiej stronie. Długa rozmowa czy wspólna gra nie są jeszcze dowodem, że ktoś jest godny zaufania.

SYGNAŁY OSTRZEGAWCZE

Zwróć uwagę, gdy ktoś:

- prosi o dane, lokalizację, zdjęcia albo włączenie kamery;
- szybko chce przenieść rozmowę do prywatnego komunikatora;
- prosi o zachowanie rozmowy w tajemnicy, zawstydzia lub straszy;
- daje prezent i oczekuje czegoś w zamian;
- namawia na spotkanie bez wiedzy rodzica lub opiekuna.



SPOTKANIE Z OSOBĄ POZNANĄ ONLINE

Nie umawiaj się na spotkanie bez wiedzy rodzica lub opiekuna. Jeśli chcesz spotkać osobę poznaną w sieci, ustal to razem z dorosłym. Spotkanie powinno odbyć się w miejscu publicznym i w obecności zaufanej osoby dorosłej.



DLA DZIECKA

Nie podawaj osobie poznanej w sieci swojego adresu ani nie udostępniaj lokalizacji i prywatnych zdjęć. Jeśli ktoś naciska, prosi Cię o zachowanie czegoś w tajemnicy, namawia do spotkania bez wiedzy rodzica albo sprawia, że czujesz dyskomfort, przerwij rozmowę i powiedz o tym dorosłemu.



DLA DOROSŁEGO

Rozmawiaj z dzieckiem o osobach poznanych w sieci. Zapytaj np. „Z kim lubisz grać?” albo „Czy ktoś prosił Cię o zachowanie czegoś w tajemnicy?”. Zwróć uwagę na ukrywanie rozmów, lęk, zmianę nastroju oraz prezenty lub doładowania. Jeśli coś Cię zaniepokoi, zachowaj dowody i szukaj pomocy.



ZRÓBcie TO RAZEM

Przećwiczcie, co zrobić, gdy ktoś prosi o zdjęcie, lokalizację, zachowanie czegoś w tajemnicy lub spotkanie. Ustalcie, kiedy przerwać rozmowę i powiedzieć dorosłemu.

Przemoc w sieci: jak reagować?

Krzywdzenie online może przybierać różne formy: obrażanie, wyśmiewanie, grożenie, podszywanie się pod kogoś albo rozpowszechnianie ośmieszających materiałów. Jeśli druga osoba mówi, że coś ją rani, prosi, żeby przestać albo wyraźnie czuje się z tym źle – to nie jest już żart.

GDY TO DOTYCZY CIEBIE

- nie zostawaj z tym sam;
- zachowaj wiadomości, zrzuty ekranu i inne dowody;
- powiedz o sytuacji zaufanemu dorosłemu;
- jeśli ktoś Ci grozi lub czujesz się zagrożony, poproś o pomoc od razu;
- pamiętaj, że to, że ktoś Cię krzywdzi, nie oznacza, że zrobiłeś coś złego.

GDY JESTEŚ ŚWIADKIEM

- nie reaguj polubieniem i nie udostępniaj krzywdzących treści dalej;
- okaż wsparcie osobie, która została zaatakowana;
- zgłoś treść i powiedz o niej dorosłemu;
- nie dołączaj do wyśmiewania, nawet dla żartu.

ZATRZYMAJ CYBERPRZEMOC

1. PRZERWIJ

Nie odpowiadaj agresją.

2. ZACHOWAJ

Zrób zrzuty ekranu i zapisz linki.

3. ZABLOKUJ

Zgłoś treść i zablokuj sprawcę.

4. POWIEDZ

Powiadom dorosłego.



DLA DOROSŁEGO

Najpierw wysłuchaj dziecka i potraktuj sytuację poważnie. Zamiast od razu odbierać urzędzenie, skup się na wsparciu i wspólnym rozwiązaniu problemu. Zabezpiecz dowody, zgłoś treść, a gdy sprawa dotyczy szkoły – skontaktuj się z wychowawcą lub pedagogiem. Jeśli pojawiają się groźby lub realne zagrożenie bezpieczeństwa dziecka, skorzystaj z odpowiedniej pomocy wskazanej na stronie 11.



ZRÓBCIE TO RAZEM

Ustalcie, do kogo dziecko może zwrócić się po pomoc w szkole i poza nią. Zapiszcie ich dane na stronie 11.

Gry, reklamy i prawda w sieci

Gra może zachęcać do zakupów, reklama wyglądać jak zwykła porada, a zdjęcie, film lub głos mogą być zmienione albo wygenerowane. Dlatego warto sprawdzać autora, źródło i cel treści.

GRY I ZAKUPY

Chroń login do gry i nie instaluj dodatków z nieznanych źródeł. Gry mogą zachęcać do szybkich zakupów przez płatne paczki, losowe nagrody i oferty ograniczone czasowo.

Zanim coś kupisz, zastanów się: czy tego potrzebujesz, ile to kosztuje i czy masz zgodę rodzica?

REKLAMA, WSPÓŁPRACA I AI

Treść sponsorowana może wyglądać jak zwykły film, recenzja lub polecenie. Szukaj oznaczeń:

- „reklama”,
- „współpraca reklamowa”,
- „materiał sponsorowany”.

Zdjęcie, film lub głos mogą być też zmienione albo wygenerowane przez AI.

Jak sprawdzić, czy treść jest prawdziwa?

KTO?

Kto to opublikował?

KIEDY?

Czy to aktualne?

DOWODY?

Czy są wiarygodne źródła?

PO CO?

Jaki jest cel tej treści?

AI I DEEPPAKE

Nienaturalny głos, niespójności obrazu lub błędy logiczne mogą być sygnałem manipulacji, ale dobrze wykonany deepfake może ich nie mieć. Dlatego zawsze sprawdź źródło i porównaj informację w innych wiarygodnych miejscach.



DLA DZIECKA

Popularny film, dużo polubień czy obietnica nagrody nie oznaczają, że treść jest prawdziwa. Gdy masz wątpliwości, sprawdź treść razem z dorosłym.



DLA DOROSŁEGO

Rozmawiaj z dzieckiem o reklamach, zakupach w grach, fake newsach i treściach tworzonych przez AI. Ucz je sprawdzać źródła i nie podejmować decyzji pod wpływem chwili.



ZRÓBCIE TO RAZEM

Wybierzcie jeden post, film lub reklamę. Sprawdźcie autora, datę, źródło i cel treści.

Higiena cyfrowa

Higiena cyfrowa to codzienne nawyki, które pomagają korzystać z urządzeń i Internetu bez przeciążenia. Chodzi o równowagę między ekranem, snem, ruchem, nauką i relacjami.

SYGNAŁY, ŻE WARTO COŚ ZMIENIĆ

- Jeśli często pojawiają się zmęczenie, ból głowy, problemy ze snem, rozdrażnienie lub trudności z koncentracją, warto przyjrzeć się także temu, ile czasu spędzasz przed ekranem i jak z niego korzystasz.
- Jeśli trudno Ci przerwać grę, scrollowanie albo odłożyć telefon, warto zrobić przerwę i przyjrzeć się swoim nawykom.



4 DOBRE NAWYKI

ODŁÓŻ EKRAN PRZED SNEM

Postaraj się nie korzystać z telefonu, tabletu ani komputera tuż przed snem.

RÓB PRZERWY I RUSZAJ SIĘ

Co jakiś czas oderwij wzrok od ekranu, wstań, przeciągnij się albo wyjdź na chwilę na zewnątrz.

KONTROLUJ CZAS PRZED EKRANEM

Sprawdź, ile czasu spędzasz w aplikacjach. Jeśli jest go więcej, niż planowałeś, wprowadź przerwy lub limity.

ODKŁADAJ TELEFON PODCZAS ROZMÓW I POSIŁKÓW

Niech część dnia będzie naprawdę bez ekranu.



DLA DZIECKA

Zwracaj uwagę, kiedy sięgasz po telefon z przyzwyczajenia, a nie dlatego, że naprawdę go potrzebujesz. Spróbuj sam ustalać sobie momenty bez ekranu i sprawdzaj, czy udaje Ci się ich trzymać.



DLA DOROSŁEGO

Ustalajcie zasady wspólnie i stosujcie je wobec domowników. Pomóż dziecku zauważać, kiedy ekran wypiera sen, ruch, naukę lub relacje. Kontrola rodzicielska może wspierać dobre nawyki, ale nie zastąpi rozmowy.



ZRÓBcie TO RAZEM

Sprawdźcie w telefonach tygodniowy czas korzystania z aplikacji. Zobaczcie, które z nich zajmują najwięcej czasu i wybierzcie jedną rzecz, którą warto ograniczyć lub zmienić.

Bezpieczne korzystanie z urządzeń i sieci

Domowa sieć łączy telefony, komputery, telewizory, konsole i inne urządzenia. Bezpieczeństwo zależy nie tylko od samego Internetu, ale też od ustawień urządzeń i codziennych nawyków.



PAMIĘTAJ O TYCH ZASADACH

- blokuj telefon, tablet i komputer kodem, hasłem lub biometrią;
- nie udostępniaj hasła do domowej sieci przypadkowym osobom;
- nie zmieniaj samodzielnie ustawień routera;
- na cudzym urządzeniu pamiętaj o wylogowaniu się z konta;
- nietypowe komunikaty lub prośby o zmianę ustawień pokaż dorosłemu.

PUBLICZNE Wi-Fi

Korzystając z publicznego Wi-Fi, pamiętaj o kilku prostych zasadach:

- wyłącz w urządzeniu automatyczne dołączanie do dostępnych sieci;
- przed wpisaniem danych sprawdź, czy strona korzysta z HTTPS;
- nie ignoruj komunikatów bezpieczeństwa wyświetlanych przez przeglądarkę;
- upewnij się, że wybrałeś właściwą sieć Wi-Fi.



WSKAZÓWKĄ LUKMAN

Klienci Lukman Multimedia mogą skontaktować się z naszym wsparciem technicznym w sprawach dotyczących routera, konfiguracji i działania usługi.



DLA DOROSŁEGO

Dbaj o zabezpieczenie domowych urządzeń i kontroluj dostęp do sieci. Stosuj kontrolę rodzicielską odpowiednio do wieku dziecka, pamiętając, że nie zastąpi rozmowy i wspólnych zasad.



ZRÓBcie TO RAZEM

Wybierzcie jedno urządzenie używane przez dziecko. Sprawdźcie, czy ma blokadę ekranu, aktualne aplikacje i tylko potrzebne uprawnienia.

Co zrobić, gdy coś się wydarzy?

Jeśli coś w sieci Cię zaniepokoi, nie działaj sam. Poniższe kroki pokazują, co możesz zrobić jako dziecko – a potem, jak może pomóc dorosły.

JAK ZAREAGOWAĆ?



DLA DZIECKA

• PODEJRZANY LINK LUB UJAWNIONE DANE

Niczego więcej nie wpisuj. Jeśli podałeś hasło, kod lub dane płatnicze – od razu powiedz dorosłemu.

• HEJT, SZANTAŻ LUB NIEPOKOJĄCY KONTAKT

Nie wdawaj się w kłótnię. Zachowaj wiadomości, zrób rzuty ekranu, zablokuj kontakt i powiedz o sytuacji dorosłemu.

• NIELEGALNA LUB SZKODLIWA TREŚĆ

Nie przysyłaj jej dalej. Powiedz dorosłemu, gdzie ją znalazłeś. Nie zapisuj ani nie rozpowszechniaj treści.

• GDY KTOŚ JEST W NIEBEZPIECZEŃSTWIE

Natychmiast powiedz o tym dorosłemu. Jeśli istnieje zagrożenie życia lub zdrowia, zadzwoń pod numer 112.



DLA DOROSŁEGO

Najpierw wysłuchaj dziecka, nie obwiniaj go i potraktuj sytuację poważnie. Pomóż zabezpieczyć konto i zmienić ujawnione hasła. Jeśli podano dane płatnicze, jak najszybciej skontaktuj się z bankiem. W przypadku hejtu, szantażu lub niepokojącego kontaktu zachowaj dowody, pomóż dziecku zablokować sprawcę i zgłoś treść. Jeśli sytuacja jest poważna lub nie ustaje, skorzystaj z odpowiedniej pomocy.

GDZIE SZUKAĆ POMOCY?

116 111

Telefon zaufania dla dzieci i młodzieży.

800 100 100

Telefon dla dorosłych w sprawach bezpieczeństwa dzieci.

Dyżurnet.pl

Zgłaszanie treści, które mogą być nielegalne lub szkodliwe.

incydent.cert.pl

Zgłaszanie incydentów i podejrzanych stron.

8080

Przekazywanie podejrzanych SMS-ów z linkiem.

112

W sytuacji bezpośredniego zagrożenia życia lub zdrowia.

MOJE ZAUFANE OSOBY

Wpisz 2–3 osoby, do których możesz zwrócić się po pomoc, gdy coś w sieci Cię przestraszy lub zaniepokoi.
imię i nazwisko nr telefonu

Bezpieczna sieć zaczyna się od wiedzy

Lukman Multimedia jest lokalnym dostawcą usług telekomunikacyjnych. Oferujemy Internet światłowodowy, telewizję i telefonię, a jednocześnie chcemy wspierać rodziny w świadomym i bezpiecznym korzystaniu z sieci.

DODATKOWA OCHRONA W SIECI LUKMAN MULTIMEDIA

W sieci **Lukman Multimedia** korzystamy z Listy Ostrzeżeń CERT Polska, która pomaga ograniczać dostęp do stron wykorzystywanych m.in. do phishingu i wyłudzenia danych. Dzięki temu użytkownicy naszej sieci zyskują dodatkową warstwę ochrony przed wejściem na znane, niebezpieczne strony.

ŹRÓDŁA I WIĘCEJ INFORMACJI

Poradnik powstał na podstawie poniższych materiałów. Znajdziesz w nich więcej informacji i praktycznych wskazówek.

OSEhero – osehero.pl

Cyberprofilaktyka NASK – cyberprofilaktyka.pl

Safer Internet – saferinternet.pl

Ministerstwo Cyfryzacji – gov.pl/web/cyfryzacja

NASK PIB / OSE – nask.pl, ose.gov.pl

Higiena Cyfrowa – higienacyfrowa.pl

CERT Polska – cert.pl

Dyżurnet.pl – dyzurnet.pl

UODO – uodo.gov.pl

UOKiK – uokik.gov.pl

Materiał ma charakter edukacyjny i nie zastępuje indywidualnej pomocy specjalistycznej. Dołożyliśmy starań, aby treści były rzetelne i aktualne. Sposób postępowania w konkretnej sytuacji należy dostosować do jej okoliczności. Zdjęcia: Adobe Stock. Przy redakcji treści korzystano z narzędzi AI. Materiał został zweryfikowany i zatwierdzony redakcyjnie. Opracowanie 2026.

Lukman Multimedia Sp. z o.o.

+48 25 785 55 55

info@lukman.pl

www.lukman.pl



Zeskanuj i sprawdź
dostępność usług
Lukman Multimedia.



**Internet
światłowodowy**



**Telewizja
Lukman 4K**



**Telefonia
mobilna**