# Asy Internetu.

## Trening bezpieczeństwa w sieci dla całej rodziny

**Program Asy Internetu ma na celu przekazanie dzieciom umiejętności, dzięki którym będą mogły korzystać z zasobów sieci w przyjemny i bezpieczny sposób. Broszura zawiera pomysły na zajęcia rodzinne przygotowane w oparciu o kodeks Asów Internetu:**

| | |
|---|---|
| **Rozsądek** | Udostępniaj z głową, czyli co można, a czego lepiej nie udostępniać w internecie. |
| **Uważność** | Nie daj się nabrać, czyli jak dostrzec, czy coś jest prawdziwe czy nie, co jest kłamstwem, a co oszustwem internetowym. |
| **Siła** | Chroń swoje sekrety, czyli jak tworzyć silne hasła oraz zapewnić bezpieczeństwo. |
| **Życzliwość** | Życzliwość jest fajna, czyli co to znaczy być uprzejmym online i szanować prywatność innych osób. |
| **Odwaga** | Rozmawiaj o wątpliwościach, czyli jak w trudnych sytuacjach poprosić o pomoc rodzica lub inną zaufaną osobę dorosłą. |

**Znajdziesz tu zestaw aktywności poświęconych zagadnieniom związanym z obecnością dzieci w internecie. Każde ćwiczenie zostało uzupełnione o zwięzłe porady, jak przeprowadzić ważne rozmowy w gronie rodzinnym. Na ostatnich stronach publikacji zamieściliśmy słowniczek kluczowych pojęć związanych z cyberbezpieczeństwem.**

**Przeprowadzenie w domu ćwiczeń zawartych w broszurze ułatwi twoim dzieciom zdobycie umiejętności potrzebnych do rozsądnego i bezpiecznego funkcjonowania w internecie.**

Google | SZKOŁA Z KLASĄ FUNDACJA

# Udostępniaj z głową: zadanie dla rodziny

Dzieci, podobnie jak niektórzy dorośli, uwielbiają dzielić się online. Udostępniają wszystko, od zdjęć swojego kota po zabawne filmiki, które chcą pokazać wszystkim znajomym. Problem polega jednak na tym, że młodsze dzieci czasami nie rozumieją, że to, co dziś publikują w internecie, ktoś będzie mógł zobaczyć w odległej przyszłości, lub że niektóre rzeczy najlepiej zachować w tajemnicy.

**Za pomocą tego ćwiczenia nauczysz dziecko decydować, czym można się dzielić w internecie, a czym nie.**

## „Kciuk w górę, kciuk w dół, kciuk w bok”

### Opisy przypadków

Przeczytaj głośno poniższe opisy przypadków. Poproś każdego członka rodziny, aby skierował kciuk w górę, jeśli uzna, że daną informacją można się dzielić z innymi; kciuk w dół, jeśli nie należy udostępniać; kciuk w bok, jeśli „to zależy”.

Za każdym razem poproś jedną osobę o wyjaśnienie swojego wyboru pozostałym członkom rodziny.

1. Udostępnienie w mediach społecznościowych zdjęcia swojego najlepszego przyjaciela, na którym głupio wyszedł.
2. Udostępnienie filmiku, który twoim zdaniem jest bardzo zabawny, ale okazuje się, że ludziom wydaje się złośliwy i w rezultacie komuś zrobiło się przykro.
3. Podczas gry nieznajomy na czacie prosi o twój telefon komórkowy i adres domowy.
4. Twoja najlepsza przyjaciółka przyjeżdża w odwiedziny na kilka dni, ale zapomniała twojego adresu i w wiadomości prywatnej prosi, żebyś go jej podał/a.
5. Przypadkowo udostępniłeś/aś nieznajomemu zbyt wiele informacji osobistych o sobie, teraz się tym przejmujesz. Czy powinieneś komuś o tym powiedzieć?
6. Udostępnienie zabawnego filmiku kota na czacie ze znajomymi.
7. Zamieszczenie swojego zdjęcia w szkolnej bluzie/mundurku z widocznym logiem i nazwą szkoły.
8. Publikowanie adresu domowego w grupie osób, których nigdy osobiście nie spotkałeś/aś.

## Krótki poradnik

**Przypadek 1:** Dzieci czasami nie zdają sobie sprawy, że to, co uważają za zabawne, może ich przyjaciołom wydać się wstydliwe lub irytujące. Przypomnij im, aby zawsze pytały osobę, która jest na zdjęciu/filmie, zanim je udostępnią innym.

**Przypadek 2:** Przypomnij, że niektóre rzeczy mogą zdenerwować innych, zwłaszcza młodszych kolegów i koleżanki. Zachęć dzieci, aby pomyślały o zawartości filmiku i o tym, czy jego udostępnianie może kogoś obrazić lub zdenerwować.

**Przypadek 3:** Można wyłączyć funkcję czatu w grach online. Upewnij się, czy twoje dziecko wie, że łatwo jest blokować i zgłaszać osoby, które nękają lub wysyłają nieodpowiednie wiadomości.

**Przypadek 4:** Ten scenariusz dotyczy sytuacji, w której twoje dziecko chce umówić się na wspólne nocowanie z osobą, którą zna. Niezbędne będzie przekazanie tej osobie waszego adresu. Przypomnij dziecku, jak bezpiecznie udostępniać swoje dane osobowe. Może na przykład poprosić, żebyś zadzwonił/a do rodziców zaproszonej osoby.

**Przypadek 5:** Przypomnij dziecku, aby przyszło do ciebie lub innej zaufanej osoby dorosłej, jeśli coś poszło nie tak, abyś mógł/mogła szybko zadziałać. Możesz pomóc mu zablokować, usunąć i zgłosić innych użytkowników.

**Przypadek 6:** Porozmawiaj ze swoim dzieckiem o rzeczach, którymi bez wątpliwości można się dzielić online, np. zabawnym, nieobraźliwym filmikiem z kotem wysłanym do przyjaciół. Zachęcanie do właściwego zachowania w internecie jest naprawdę ważne. Pozytywne wykorzystanie technologii to jedna z rzeczy, które gwarantują bezpieczeństwo dzieci w internecie.

**Przypadek 7:** Logo szkoły widoczne na zdjęciu może ujawnić, do której szkoły chodzi Twoje dziecko. Przed udostępnieniem takiego zdjęcia upewnij się, że logo i nazwa szkoły nie są widoczne. Wykorzystaj okazję i porozmawiaj z dzieckiem o przypadkowym udostępnieniu.

**Przypadek 8:** Przypomnij dziecku, że istnieją lepsze sposoby na udostępnianie adresu, jeśli ktoś naprawdę tego potrzebuje. Patrz przypadek 4.

Zagrajcie razem w grę **Interlandia**. Odwiedź **Górę Uważności**, gdzie informacja podróżuje z prędkością światła, a wśród znajomych internautów jest ktoś, kto ma tendencję do nadmiernego udostępniania – notoryczny udostępniacz.

Otwórz przeglądarkę internetową na pulpicie lub urządzeniu mobilnym (np. tablecie) i odwiedź stronę **https://beinternetawesome.withgoogle.com/pl_all/interland/gora-uwaznosci**.

# Nie daj się nabrać: zadanie dla rodziny

Nie wszystko, na co twoje dziecko natknie się w internecie, jest prawdziwe lub wiarygodne. Największa trudność polega na dostrzeganiu różnic. Uczenie się, jak rozpoznać wskazówki dotyczące tego, co jest prawdziwe, a co fałszywe, co jest kłamstwem lub oszustwem internetowym, pomoże dziecku pewnie poruszać się online i uważać na to , co zobaczy i przeczyta.

**Ta aktywność pomoże twojemu dziecku dostrzec kluczowe wskazówki, dzięki którym będzie mogło sprawdzić, czy może zaufać temu, na co natrafiło w sieci.**

## Wyszukaj , Oceń , Sprawdź wynik

### Wyszukaj

1. Usiądźcie razem, weź tablet lub inne urządzenie i przejdź do swojej ulubionej wyszukiwarki.
2. Sprawdź, czy funkcja bezpiecznego wyszukiwania jest włączona.
3. Wybierz temat, którym twoje dziecko się żywo interesuje albo o którym dużo wie (np. piłka nożna, przyroda, ulubiony aktor) i wpisz go w polu wyszukiwania.
4. Kliknij różne wyniki na górze wyszukiwarki, przewiń kilka stron w dół i tam także kliknij kilka wyników.
5. Sprawdź punkty na poniższej liście kontrolnej i oceń, czy możesz dostrzec jakieś wskazówki.

### Oceń

Czy strona ma zakładkę: „O Nas”?

Czy widać, kto jest autorem strony? Jeśli tak, czy jest to ktoś znany?

Czy język na stronie jest wyraźnie emocjonalny?

Czy jest to strona sponsora albo fana (więc może jest głównie pozytywna)? Jeśli informacje są negatywne, czy możesz dowiedzieć się więcej o samej witrynie i źródle krytyki?

Czy to subiektywna opinia / blog tylko jednej osoby czy raczej wydaje się neutralna?

Jeśli to witryna z wiadomościami (serwis informacyjny), to czy jest ci dobrze znana i możesz jej zaufać, czy raczej chcesz dowiedzieć się więcej na jej temat albo sprawdzić, czy inni czytelnicy sądzą, że próbuje przedstawić informacje w bezstronny sposób?

Czy adres WWW strony jest prawidłowy (np. czy nie zawiera literówki lub jest w innej domenie krajowej niż ta, którą znasz)?

Jeśli jest to strona służąca do logowania, czy ma adres zaczynający się od https://?

### Sprawdź wynik

**Przyznaj każdej stronie jeden z trzech poziomów wiarygodności:**

🙂 3 = dość wiarygodna

😐 2 = najlepiej sprawdzić z osobą dorosłą

☹️ 1 = nie należy polegać na tej stronie

## Krótki poradnik

Razem z dzieckiem przejrzyj wyniki wyszukiwania i przedyskutuj pytania z sekcji „Oceń”, aby sprawdzić, czy potraficie dostrzec jakieś wskazówki.
Zachęcaj dziecko, żeby mówiło ci o stronach, które według niego/niej są godne zaufania, czyli wiarygodne i bezpieczne. Czy potrafi wymienić cechy godnej zaufania (czyli wiarygodnej i bezpiecznej) strony internetowej?

Porozmawiaj z dzieckiem o uprzedzeniach – ustal, czy potrafi określić pobudki, jakimi kieruje się autor. Sprawdź, czy potrafi dostrzec błędy ortograficzne i gramatyczne, które mogą świadczyć o nierzetelności strony internetowej.
Porozmawiaj z dzieckiem o elementach, które świadczą o tym, że strona jest bezpieczna od strony technicznej. Ustal, czy wie, kiedy może podać swoje dane podczas logowania.

Zagrajcie razem w grę **Interlandia**. Odwiedź **Rzekę Rzeczywistości**, gdzie nie wszystko jest zawsze takie, jak się wydaje na pierwszy rzut oka. Kieruj się swoją krytyczną oceną, aby zdecydować, co jest faktem, a co fikcją.

Otwórz przeglądarkę internetową na pulpicie lub urządzeniu mobilnym (np. tablecie), i odwiedź stronę **https://beinternetawesome.withgoogle.com/pl_all/interland/rzeka-rzeczywistosci**.

# Chroń swoje sekrety: zadanie dla rodziny

Wiemy, że niektóre informacje muszą pozostać prywatne. Dla młodszych dzieci to może być trudne do zrozumienia. Może im się wydawać, że dzielenie się hasłami z najlepszymi przyjaciółmi jest w porządku. Prawdopodobnie nie będą wiedzieć, że w internecie niektórzy ludzie działają na szkodę innych i próbują wykraść ich informacje.

**To ćwiczenie pomoże twojemu dziecku zrozumieć, jak zapewnić poufność i bezpieczeństwo swoich prywatnych informacji online.**

## Przepis na silne hasło

Zacznij od swobodnej rozmowy. Zapytaj swoje dziecko, czy uważa, że hasło „123” jest mocne (bezpieczne). Porozmawiajcie o tym, dlaczego ważne jest posiadanie takiego hasła, które tobie jest łatwo zapamiętać, ale nikt inny go nie zgadnie.

Napiszcie razem przepis na silne hasło i zawrzyjcie w nim wszystkie składniki potrzebne do stworzenia bezpiecznego hasła do kont online i konkretne instrukcje, jak je ułożyć.

Przykładowe składniki:

3 wielkie litery

4 lub więcej małych liter

2 symbole

1 cyfra

## Krótki poradnik

Spróbuj utworzyć inne hasło dla każdego konta online, aby nie używać wszędzie jednakowych.

Nie udostępniaj haseł nikomu, nawet najlepszemu przyjacielowi.

Słabe hasło to takie, które łatwo odgadnąć, jak imię twojego zwierzaka.

Pomieszaj wielkie i małe litery.

Unikaj używania imion i nazwisk, imienia swojego zwierzaka, daty urodzenia i innych oczywistych informacji, które mogą ułatwić innym odgadnięcie hasła.

Dołącz liczby i symbole, aby utrudnić odgadnięcie lub zhakowanie (złamanie) hasła (haker to ktoś, kto próbuje uzyskać dostęp do czyichś informacji bez pozwolenia).

Używaj krótkiego zdania zamiast jednego słowa, które dla innych będzie trudne do odgadnięcia, a dla ciebie łatwe do zapamiętania.

Teraz zagrajcie razem w grę **Interlandia**. Odwiedź **Wieżę Skarbów**, w której musisz wyprzedzić hakera i zbudować fortecę z silnymi hasłami, żeby chronić swoje sekrety.

Otwórz przeglądarkę internetową na pulpicie lub urządzeniu mobilnym (np. tablecie), i odwiedź stronę **https://beinternetawesome.withgoogle.com/pl_all/interland/wieza-skarbow**.

# Życzliwość jest fajna: zadanie dla rodziny

Młodsze dzieci często nie zdają sobie sprawy, że niektóre wiadomości w sieci mogą zostać zrozumiane inaczej, niż chciał ich autor. Jeśli są świadkami nieuprzejmych zachowań, powinny zareagować. Czasami to, co nam wydaje się udostępnionym publicznie nieszkodliwym żartem, może zawstydzić i zdenerwować innych użytkowników internetu, a nawet naszych przyjaciół

**To zadanie pomoże twojemu dziecku zrozumieć, co to znaczy traktować innych użytkowników internetu z szacunkiem.**

## Gra w „A co, jeśli...”

Przeczytaj opisy sytuacji, a następnie poproś każdego członka rodziny, aby powiedział, co by zrobił/a w każdej z nich.

**Sytuacja 1:** Twój przyjaciel jest zmartwiony, ponieważ ktoś wysyła mu nieprzyjemne wiadomości online. Zauważyłeś/aś, też że ludzie dodają złośliwe komentarze do zdjęć, które opublikował twój przyjaciel.

**Sytuacja 2:** Podczas grania w grę online ktoś publikuje na czacie niegrzeczne dowcipy, które tobie wcale nie wydają się zabawne, a raczej denerwujące.

**Sytuacja 3:** Znajomy wysyła ci jego zdaniem zabawny film przedstawiający sytuację, gdy ktoś dręczy kolegów z klasy. Uważasz, że to wcale nie jest śmieszne, czujesz się zaniepokojony/a.

**Sytuacja 4:** W prywatnej wiadomości do przyjaciela napisałaś/eś, że w nowej fryzurze wygląda inaczej. Mimo że twój komentarz miał zabrzmieć pochlebnie, masz wrażenie, że przyjaciel czuje się urażony.

## Dyskusja w gronie rodzinnym:

Dlaczego to ważne, aby być życzliwym dla innych, zarówno online, jak i offline?

## Krótki poradnik

To naturalne, że poszczególni członkowie rodziny mogą mieć odmienne zdanie na temat każdej z opisanych sytuacji. Różne odpowiedzi sprzyjają rodzinnej dyskusji.

**Sytuacje 1 i 3:** Jeśli w internecie spotyka kogoś coś złego, nawet dziecko może aktywnie się przeciwstawić, zidentyfikować niepokojącą sytuację i zadziałać – najważniejsze, by nie pozostawać obojętnym. Odpowiedzialność społeczna naszych dzieci kształtuje się, gdy stają w obronie tego, co słuszne i próbują chronić innych, gdy dzieje się im krzywda.

**Scenariusz 2:** Nawet jeśli nie czujesz się ekspertem w dziedzinie technologii, możesz pomóc dzieciom rozwiązać ich problemy. Wytłumacz dziecku, że powinno przyjść do ciebie lub innej zaufanej osoby dorosłej, jeśli cokolwiek wzbudza jego niepokój.

**Scenariusz 4:** Wyjaśnij, że często błędnie rozumiemy wiadomości tekstowe, które nie są wypowiedziane głośno, twarzą w twarz. Możecie razem wymyślić więcej przykładów.

Teraz zagrajcie razem w grę **Interlandia**. Odwiedź **Królestwo Życzliwości**, gdzie musisz powstrzymać rozprzestrzenianie się niemiłej atmosfery i pomóc szerzyć życzliwość.

Otwórz przeglądarkę internetową na pulpicie lub urządzeniu mobilnym (np. tablecie) i odwiedź stronę **https://beinternetawesome.withgoogle.com/pl_all/interland/krolestwo-zyczliwosci**.

# Słowniczek

**Od phisherów do hakerów - trudno nadążyć za cyfrowym żargonem. Oto kilka przydatnych pojęć.**

## Udostępniaj z głową...

| | |
|---|---|
| **Cyfrowy ślad** | Twój cyfrowy ślad to wszystko, co składa się na wizerunek twojej osoby w internecie. Tworzą go zdjęcia, nagrania audio, wideo, teksty, posty na blogach i wiadomości, które piszesz na stronach znajomych. |
| **Granice osobiste** | Zasady, które ustalasz, aby dać innym do zrozumienia, jak powinni się wobec ciebie zachowywać w bezpieczny i akceptowalny sposób. |
| **Informacje osobowe** | Informacje o konkretnej osobie. Informacje o tobie mogą być mniej lub bardziej publiczne/ prywatne w zależności od stopnia ich wrażliwości. |
| **Ustawienia** | Obszar w dowolnej usłudze cyfrowej, aplikacji, witrynie internetowej itp., w którym można zdefiniować lub dostosować zakres udostępnianych im informacji i określić zasady obsługiwania konta. |

## Nie daj się nabrać...

| | |
|---|---|
| **Zaszyfrowany** | Informacje lub dane przekształcone w kod. |
| **Zapora / Firewall** | Program, który chroni komputer przed większością oszustw i włamań dokonywanych przez hakerów. |
| **Złośliwe oprogramowanie** | Termin odnoszący się do różnych form wrogiego lub niepożądanego oprogramowania, takiego jak wirusy komputerowe i inne szkodliwe programy. |
| **Phishing** | Atak phishingowy ma miejsce, gdy ktoś próbuje nakłonić użytkownika do udostępnienia danych osobowych online. Wyłudzanie informacji odbywa się zazwyczaj za pośrednictwem e-maila, reklam lub witryn, które wyglądają podobnie do stron, z jakich już korzystasz. |
| **Scam** | Nieuczciwa próba zarobienia pieniędzy lub zdobycia czegoś wartościowego na drodze oszustwa. |
| **Phishing profilowany (spear phishing)** | Wyrafinowana forma oszustwa, w której cyberprzestępca wykorzystuje wszelkie dostępne w sieci informacje na temat ofiary, żeby obniżyć jej czujność i zainfekować komputer lub wykraść dane. |

## Chroń swoje sekrety...

| | |
|---|---|
| **Haker** | Osoba korzystająca z komputera w celu uzyskania dostępu do prywatnych informacji bez zezwolenia. |
| **Prywatność** | Ochrona informacji o tobie i innych osobach. |
| **Bezpieczeństwo** | Poleganie na dobrych nawykach w celu zabezpieczania sprzętu i oprogramowania. |
| **Scammer** | Ktoś, kto oszukuje lub podstępem przekonuje kogoś innego, by ujawnił swoje prywatne informacje albo nawet oddał pieniądze. |
| **Weryfikacja dwuetapowa** | Forma zabezpieczenia, w której logowanie do usługi wymaga dwóch kroków. Na przykład może być konieczne wprowadzenie hasła i kodu wysłanego w wiadomości SMS. |

## Życzliwość jest fajna...

| | |
|---|---|
| **Blokowanie (kogoś)** | Sposób na ograniczenie komuś dostępu do twojego profilu, możliwości wysyłania wiadomości itp. |
| **Bierny obserwator** | Ktoś, kto ma prawo interweniować lub zgłaszać złe zachowanie, ale nie robi nic, by je powstrzymać. |
| **Dokuczanie** | Powodowanie nieprzyjemnych lub wrogich sytuacji w rozmowie lub działaniu, aby celowo sprawić komuś przykrość. |
| **Aktywny obserwator** | Ktoś, kto interweniuje, aby powstrzymać i/lub zgłosić nieodpowiednie zachowanie. |