

WSPÓLNIE W SIECI:

„Jak dbać o cyberbezpieczeństwo w Szkole Podstawowej”

Bezpieczeństwo dzieci w Internecie to wspólna misja uczniów, rodziców i nauczycieli, która wymaga otwartości, czujności oraz znajomości podstawowych zasad cyfrowej higieny. Współczesna szkoła podstawowa nie istnieje bez technologii. Internet pomaga w nauce, pozwala rozwijać pasję i ułatwia kontakt z rówieśnikami. Cyfrowy świat niesie jednak realne zagrożenia, takie jak wyłudzenie danych, złośliwe oprogramowanie czy cyberprzemoc.

Sekcja dla ucznia:

Twój cyfrowy plecak bezpieczeństwa

Internet jest jak wielkie miasto – pełen ciekawych miejsc, ale też zakamarków, w których trzeba uważać. Zastosuj te zasady, aby surfować bez strachu:

- Zasada ograniczonego zaufania: Nie każda osoba w sieci jest tym, za kogo się podaje. Nigdy nie spotykaj się na żywo z kimś poznanym przez Internet bez wiedzy rodziców.
- Ochrona prywatności: Nie podawaj swojego nazwiska, adresu domowego, numeru telefonu ani nazwy szkoły na publicznych czatach, forach czy w grach.
- Klucz do zamka: Twórz silne hasła (używaj dużych liter, cyfr i znaków specjalnych) i nikomu ich nie zdradzaj – nawet najlepszemu przyjacielowi.
- Stop cyberprzemocy: Traktuj innych tak, jak sam chcesz być traktowany. Nie wyzywaj, nie wyśmiewaj i nie rozsyłaj screenów bez zgody innych.
- Podejrzane wiadomości: Nie klikaj w dziwne linki i nie otwieraj załączników od nieznajomych, nawet jeśli obiecują darmowe „skiny” do gier lub wirtualną walutę.
- Reaguj i zgłaszaj: Jeśli zobaczysz coś, co Cię wystraszy, zawstydzi lub zaniepokoi, natychmiast powiedz o tym rodzicom lub nauczycielowi.

Sekcja dla rodzica:

Jak być mądrym przewodnikiem w sieci

Technologia zmienia się szybko, ale fundamentem bezpieczeństwa dziecka pozostaje relacja z rodzicem. Zamiast całkowitych zakazów, warto postawić na edukację i wsparcie.

Rozmowa zamiast kontroli

- Interesuj się tym, co dziecko robi na smartfonie czy komputerze, tak samo jak pytasz o przebieg dnia w szkole.
- Stwórz atmosferę, w której dziecko nie będzie bało się przyjść do Ciebie, gdy popełni błąd w sieci (np. kliknie w zły link).

Narzędzia i techniczna ochrona

- Zasady ekranowe: Wspólnie ustalcie limity czasu przed ekranem i zasady stref wolnych od technologii (np. zakaz używania telefonów podczas posiłków i przed snem).
- Kontrola rodzicielska: Zainstaluj aplikacje filtrujące treści dostosowane do wieku dziecka, zwłaszcza u uczniów młodszych klas.
- Aktualizacje systemowe: Regularnie dbaj o instalowanie poprawek bezpieczeństwa i programu antywirusowego na domowych urządzeniach.

Edukacja o cyfrowym śladzie

- Uświadom dziecko, że wszystko, co trafia do Internetu (zdjęcia, komentarze), zostaje tam na zawsze i może zostać skopiowane.
- Naucz dziecko krytycznego myślenia – fake newsy i internetowe manipulacje są powszechne.
- Ściągawka domowa: Kodeks Bezpiecznego Internetu

Warto wydrukować te krótkie zasady i powiesić w widocznym miejscu w domu:

Sytuacja	Co robi uczeń?	Co robi rodzic?
Logowanie	Tworzy unikalne hasła i wylogowuje się na szkolnych komputerach.	Pomaga dziecku zarządzać hasłami i uczy dwuskładowego uwierzytelnienia.
Prywatność	Nie publikuje zdjęć z widocznym adresem lub logo szkoły	Kontroluje ustawienia prywatności na profilach dziecka i pyta o zgodę przed wrzuceniem jego zdjęć.
Komunikacja	Zgłasza rodzicom każdą próbę nękania lub zaczepki od obcych	Reaguje, nie ocenia emocjonalnie i w razie potrzeby zabezpiecza dowody – np.: zrzuty ekranu.
Pobieranie	Pyta o zgodę przed instalacją nowej aplikacji lub gry.	Pobiera oprogramowanie wyłącznie z oficjalnych sklepów – np. :Google Play

Gdzie szukać pomocy

Jeśli podejrzewasz, że dziecko padło ofiarą cyberprzestępstwa lub cyberprzemocy, skorzystaj z bezpłatnego wsparcia ekspertów:

- Telefon Zaufania dla Dzieci i Młodzieży: 116 111 (bezpłatny, całodobowy).
- Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci: 800 100 100.
- Zgłaszanie nielegalnych treści w sieci: Serwis Dyżurnet.pl, który analizuje zgłoszenia o cyberzagrożeniach.
- Materiały edukacyjne: Oficjalne poradniki i kompendia znajdziesz na stronie SaferInternet.pl.