

Bezpieczeństwo uczniów w sieci – o czym musisz pamiętać, będąc online?

Obcy w internecie to wciąż obcy. Osoba, z którą piszesz na czacie albo grasz w grze online, może podawać się za Twojego rówieśnika, a w rzeczywistości być kimś zupełnie innym. Zdjęcie profilowe, wiek i imię można łatwo zmyślić.

Chroń swoje prywatne dane. Nigdy nie podawaj osobom poznanym w sieci swojego prawdziwego imienia, nazwiska, adresu domowego, numeru telefonu ani nazwy naszej szkoły. Te informacje powinny zostać tylko dla Ciebie i Twoich bliskich.

Nie wysyłaj swoich zdjęć ani filmów. Raz wrzucone do sieci zdjęcie nigdy z niej nie znika. Nigdy nie przysyłaj swoich fotografii (ani zdjęć swojego pokoju czy rodziny) osobom, których nie znasz osobiście.

Nigdy nie umawiaj się na spotkania na żywo. Jeśli ktoś poznany w grze lub na TikToku/Instagramie proponuje spotkanie w świecie rzeczywistym, natychmiast powiedz o tym rodzicom. Nigdy nie idź na takie spotkanie sam!

Uważaj na linki i pobieranie plików. Nie klikaj w nieznane linki i nie pobieraj gier lub załączników od obcych osób – mogą zawierać wirusy lub służyć do włamania na Twoje konto.

Ustaw profil jako prywatny. W aplikacjach takich jak TikTok czy Instagram zmień ustawienia konta na prywatne. Dzięki temu Twoje materiały będą widzieć tylko prawdziwi znajomi, a nie przypadkowi ludzie z całego świata.

Zasada ograniczonego zaufania do influencerów. Nie wierz we wszystko, co znani YouTuberzy czy TikTokerzy reklamują w swoich filmach. Często dostają za to pieniądze, a polecane przez nich strony lub produkty mogą być niebezpieczne lub bardzo drogie.

Wirtualne zakupy tylko z rodzicami. Nigdy nie kupuj niczego w grach ani sklepach internetowych samodzielnie. Podpięcie karty płatniczej rodziców bez ich wiedzy może skończyć się utratą wszystkich oszczędności z konta.

Nie wierz we wszystko, co widzisz (Fake News). W internecie łatwo stworzyć kłamstwo, które wygląda jak prawda (np. zmontowane zdjęcia, zmyślane wiadomości). Zawsze sprawdzaj sensacyjne informacje u dorosłych lub w sprawdzonych źródłach.

Reaguj na hejt i niemiłe wiadomości. Jeśli ktoś w sieci Cię obraża, wyśmiewa lub pisze rzeczy, przez które czujesz się źle, nie odpisuj mu. Zrób zrzut ekranu (screena), zablokuj tę osobę i od razu powiedz o tym dorosłemu.

Mów o wszystkim rodzicom lub nauczycielom. Jeśli zobaczysz w sieci coś, co Cię wystraszy, zaniepokoi albo sprawi, że poczujesz się nieswojo, nie zamykaj się w sobie. Opowiedz o tym komuś dorosłemu – oni zawsze Ci pomogą!

Nigdy nie używaj prostych haseł: Zapomnij o „123456”, „hasło”, „qwerty” czy Twoim imieniu z datą urodzenia (np. „Kasia2015”). Robot hakerski złamie takie hasło w ułamku sekundy!

Zasada 4 żywiołów (stwórz hasło-potwora): Dobre hasło musi mieć **co najmniej 10-12 znaków** i składać się z: wielkich liter (A, B, C), małych liter (a, b, c), cyfr (1, 2, 3), znaków specjalnych (!, @, #, \$, *).

Różne hasła: Nigdy nie używaj tego samego hasła do wszystkiego. Jeśli ktoś pozna Twoje hasło do jednej gry, od razu włamie się też na Twoją pocztę i inne konta.

Hasło to TAJEMNICA: Nie podawaj swoich haseł nikomu – nawet najlepszemu koledze czy koleżance ze ławki. Przyjaźnie się zmieniają, a dostęp do konta powinien być tylko Twój. Jedynymi osobami, które mogą (i powinny) znać Twoje hasła, są Twoi rodzice.