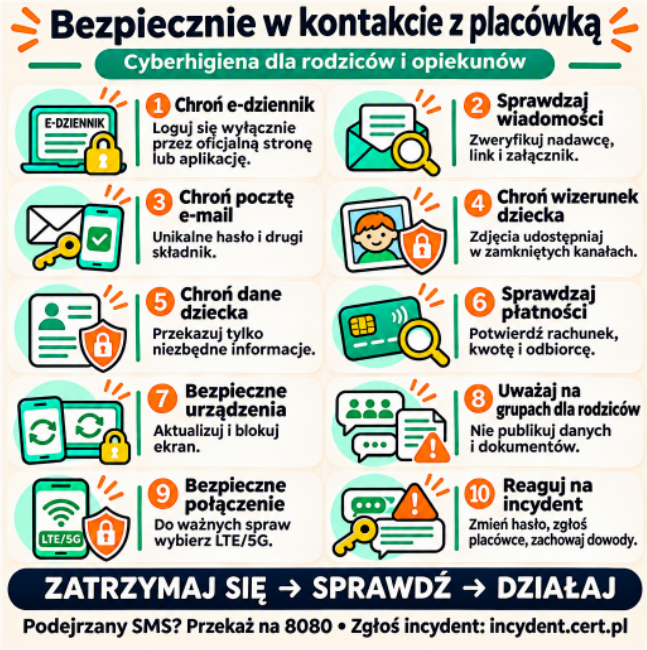




Skontaktuj się z placówką

[numer telefonu] |

[adres e-mail] |

[adres strony]

Podejrzany SMS: przekaż na numer 8080

Zgłoszenie podejrzanej strony lub wiadomości:

incydent.cert.pl

BEZPIECZNIE W KONTAKCIE Z PLACÓWKĄ

Podstawowe zasady cyberhigieny dla klientów i odbiorców Przedszkola

Cyfrowe narzędzia ułatwiają codzienny kontakt z placówką, sprawdzanie informacji o dziecku i wymianę ważnych wiadomości. Warto jednak pamiętać, że konto e-dziennika, poczta, dane osobowe oraz zdjęcia dziecka wymagają odpowiedniej ochrony. Poniższe zasady pomagają korzystać z tych rozwiązań bezpiecznie i świadomie.

Materiał wytworzony przy wsparciu sztucznej inteligencji.

PLACÓWKA • CYBERHIGIENA 1/10

Chroń e-dziennik i aplikację placówki



Po utracie telefonu, zmianie numeru lub adresu e-mail zgłoś placówce potrzebę zmiany albo odebrania dostępu.



Loguj się wyłącznie przez oficjalną stronę lub aplikację wskazaną przez placówkę.



Używaj unikalnego hasła i włącz dodatkowe uwierzytelnianie, jeśli jest dostępne.



Nie przekazuj loginu, hasła ani kodu aktywacyjnego innym osobom.

ZATRZYMAJ SIĘ → SPRAWDŹ → DZIAŁAJ

PLACÓWKA • CYBERHIGIENA 2/10

Uważaj na fałszywe wiadomości



Pilna dopłata, zmiana planu lub prośba o dane? Nie działaj pod presją.



Sprawdź adres nadawcy, link i nazwę załącznika.



Informację potwierdź w e-dzienniku, aplikacji placówki lub telefonicznie.



Nie instaluj aplikacji ani certyfikatów z linku w wiadomości.

ZATRZYMAJ SIĘ → SPRAWDŹ → DZIAŁAJ

PLACÓWKA • CYBERHIGIENA 3/10

Chroń pocztę e-mail



Do poczty używaj długiego, unikalnego hasła.



Włącz uwierzytelnianie wieloskładnikowe.



Nie przesyłaj hasła ani kodu logowania w odpowiedzi na wiadomość.



Sprawdzaj reguły przekazywania i nierozpoznane logowania.

ZATRZYMAJ SIĘ → SPRAWDŹ → DZIAŁAJ

PLACÓWKA • CYBERHIGIENA 4/10

Chroń wizerunek dziecka



Zdjęcia i nagrania udostępniaj w uzasadnionych przypadkach na zamkniętych kanałach.



Nie publikuj zdjęć innych dzieci bez odpowiedniej podstawy i uzgodnienia.



Nie przesyłaj materiałów z dziećmi do przypadkowych grup i komunikatorów.



Przed publikacją sprawdź tło, identyfikatory, lokalizację i dane widoczne na zdjęciu.

ZATRZYMAJ SIĘ → SPRAWDŹ → DZIAŁAJ

CYBERHIGIENA • DLA RODZICÓW 5/10

Chroń dane dziecka



Przekazuj placówce tylko dane potrzebne do konkretnej sprawy.



Dokumenty wysyłaj oficjalnym kanałem wskazanym przez placówkę.



Nie publikuj PESEL-u, diagnoz, informacji zdrowotnych ani dokumentów dziecka w grupach rodziców.



Przed wysłaniem załącznika sprawdź odbiorcę i zawartość pliku.

ZATRZYMAJ SIĘ → SPRAWDŹ → DZIAŁAJ

CYBERHIGIENA 6/10

Sprawdzaj płatności



Numer rachunku sprawdź w e-dzienniku, aplikacji lub oficjalnej wiadomości placówki.



Przed przelewem zweryfikuj odbiorcę, rachunek, kwotę i tytuł.



Nie płać przez link z niespodziewanego SMS-a lub e-maila.



Zmianę rachunku zawsze potwierdź telefonicznie z placówką.

ZATRZYMAJ SIĘ → SPRAWDŹ → DZIAŁAJ

CYBERHIGIENA 7/10

Dbaj o urządzenia



Aktualizuj system, przeglądarkę, e-dziennik i aplikację placówki.



Blokuj ekran kodem PIN, hasłem lub biometrią.



Nie pozostawiaj zalogowanego urządzenia bez nadzoru.



Pobieraj aplikacje wyłącznie z oficjalnych sklepów i linków placówki.

ZATRZYMAJ SIĘ → SPRAWDŹ → DZIAŁAJ

CYBERHIGIENA • DLA RODZICÓW 8/10

Uważaj na grupy rodziców



Nie publikuj danych dzieci, dokumentów ani kodów dostępu.



Nie przesyłaj dalej zdjęć i informacji poza cel, dla którego je udostępniono.



Ważne ustalenia potwierdzaj w oficjalnym kanale placówki.



Usuń z grupy osoby, które nie powinny już mieć dostępu.

ZATRZYMAJ SIĘ → SPRAWDŹ → DZIAŁAJ

CYBERHIGIENA 9/10

Łącz się bezpiecznie



Unikaj otwartych sieci Wi-Fi bez hasła.



Wyłącz automatyczne łączenie z Wi-Fi.



Do e-dziennika, poczty i płatności wybierz internet komórkowy.



Jeśli to możliwe, korzystaj z własnego hotspotu LTE/5G.

ZATRZYMAJ SIĘ → SPRAWDŹ → DZIAŁAJ