

Cyberbezpieczeństwo rodziny i szkoły

Rodzice i opiekunowie · Czas warsztatu prowadzonego: 45 minut

Cel: Przeprowadzić rozmowę z dzieckiem o ryzykach, zbudować plan pomocy i chronić prywatność.

Bez wymuszania dostępu do prywatnych rozmów dziecka i bez zbierania obrazów intymnych. Czas warsztatu jest rozplanowany na zadania i wymaga udziału prowadzącego. Ten materiał nie jest certyfikatem ukończenia ani opinią prawną. Przykłady są fikcyjne.

Scenariusz zajęć — 45 minut

1. **5 min** — Bezpieczna rozmowa jest ważniejsza niż kontrola
2. **10 min** — Phishing i przejmowanie kont
3. **10 min** — Cyberprzemoc: jak zareagować
4. **10 min** — Wizerunek i prywatność
5. **10 min** — Domowy plan pomocy

Rezultat uczestników: Plan rozmowy rodzinnej, checklista kont i reagowania na cyberprzemoc.

Materiały i organizacja: konspekt, kartki, długopisy, neutralne opisy sytuacji, tablica. Ustal zasady szacunku i możliwości odstąpienia od ćwiczenia. Nie pobieraj autentycznych danych uczestników.

Bezpieczna rozmowa jest ważniejsza niż kontrola

Dziecko częściej szuka pomocy, gdy spodziewa się wysłuchania, a nie natychmiastowej kary. Warto rozmawiać o zwykłych doświadczeniach w sieci i ustalać granice korzystania z urządzeń, a nie tylko reagować w kryzysie. Rodzic powinien dać do zrozumienia, że opowiedzenie o trudnej sytuacji nie oznacza automatycznej utraty telefonu.

Ćwiczenie / polecenie

Zaproponuj trzy pytania otwierające spokojną rozmowę bez oceniania.

Notatki prowadzącego:

Phishing i przejmowanie kont

Wiadomości wymuszające pośpiech, prośby o kod logowania, niewiarygodne linki i podszywanie się pod znajome osoby mogą prowadzić do utraty dostępu do kont. Unikalne hasła, aktualizacje i uwierzytelnianie dwuskładnikowe zwiększają bezpieczeństwo. Rodzina powinna mieć jasny plan zgłoszenia podejrzanej wiadomości.

Ćwiczenie / polecenie

Na fikcyjnym ekranie znajdź pięć sygnałów oszustwa; nie pokazuj rzeczywistych kont.

Notatki prowadzącego:

Cyberprzemoc: jak zareagować

Wysłuchaj dziecka, oceń pilność i zadbaj o bezpieczeństwo. Nie rozsyłaj kompromitujących treści, nawet w intencji dowodowej. Działaj wraz ze szkołą według odpowiedniej procedury, a w poważnych przypadkach rozważ kontakt z właściwymi służbami. Materiały intymne dzieci wymagają szczególnej ostrożności.

Ćwiczenie / polecenie

Ułóż trzyetapową odpowiedź rodzica na fikcyjne zgłoszenie hejtu.

Notatki prowadzącego:

Wizerunek i prywatność

Publikowanie zdjęć dzieci może ujawniać miejsce pobytu, zwyczaje lub dane innych uczniów. Zanim cokolwiek udostępnisz, oceń potrzebę i wpływ na prywatność. Prośba o „zgode całej klasy” nie zastępuje właściwych zasad ochrony danych. Warto nauczyć dzieci poszanowania granic własnych i cudzych.

Ćwiczenie / polecenie

Wybierz spośród fikcyjnych postów te, które są zbędnie ujawniające.

Notatki prowadzącego:

Domowy plan pomocy

Ustalcie, do kogo dziecko może zwrócić się w domu i w szkole, co zrobić po utracie konta, jak zatrzymać krążenie szkodliwych treści i kiedy szukać specjalistycznej pomocy. Plan należy aktualizować i pozostawić możliwość rozmowy bez zawstydzania.

Ćwiczenie / polecenie

Napisz na papierze trzy kroki pomocy, kanał zgłoszenia i zasadę niepublikowania materiałów.

Notatki prowadzącego:

Praca na przypadkach

STUDIUM PRZYPADKU 1

Przemoc na czacie

Dziecko przyznaje, że ktoś wysłał mu poniżające wiadomości, i boi się odebrania telefonu.

Jak reaguje rodzic?

1. Spokojnie wysłuchuje, ocenia bezpieczeństwo, pomaga uruchomić procedurę
2. Oskarża dziecko i publikuje rozmowy

Omówienie dla prowadzącego: Budowanie zaufania jest podstawą skutecznego wsparcia.

STUDIUM PRZYPADKU 2

Kod „od nauczyciela”

Dorosły otrzymuje SMS z prośbą o kod logowania do rzekomej platformy szkolnej.

Co zrobić?

1. Podać kod
2. Zweryfikować prośbę innym kanałem i nie podawać kodu

Omówienie dla prowadzącego: Kod logowania nie służy do przekazywania niezweryfikowanym nadawcom.

Pytania kontrolne i klucz dla prowadzącego

1. Jak przyjąć zgłoszenie cyberprzemocy?

Możliwe odpowiedzi: Spokojnie, bez oceniania / Karą za samo zgłoszenie

Klucz: Spokojnie, bez oceniania. Zaufanie pomaga dziecku szukać wsparcia.

2. Kody uwierzytelniania...

Możliwe odpowiedzi: Należy chronić / Można wysłać nieznajomemu

Klucz: Należy chronić. To poufne dane dostępu.

3. Materiały intymne małoletnich...

Możliwe odpowiedzi: Rozsyłamy do rodziców / Nie kopiujemy i nie rozpowszechniamy

Klucz: Nie kopiujemy i nie rozpowszechniamy. Należy ograniczyć krzywdę.

4. Dobre hasła...

Możliwe odpowiedzi: Są unikalne / Są wspólne dla wszystkich

Klucz: Są unikalne. Niepowtarzalność ogranicza ryzyko.

5. Po publikacji zdjęcia dziecka...

Możliwe odpowiedzi: Trzeba liczyć się z utratą kontroli nad zasięgiem / Ma je tylko najbliższy znajomy

Klucz: Trzeba liczyć się z utratą kontroli nad zasięgiem. Materiał może zostać skopiowany.

6. Rodzinny plan obejmuje...

Możliwe odpowiedzi: Osobę wsparcia i zasady reagowania / Wyłącznie zakazy

Klucz: Osobę wsparcia i zasady reagowania. Dziecko potrzebuje dostępu do pomocy.

Plan zastosowania w placówce

Plan rozmowy rodzinnej, checklista kont i reagowania na cyberprzemoc.

Dokumentację osobową i opis rzeczywistego zdarzenia prowadzi się poza DSS w uprawnionych systemach placówki. Sprawdź aktualność procedur oraz rozdziel obowiązki prawny od dobrej praktyki.

Źródła do weryfikacji

- NASK: Jak reagować na cyberprzemoc
- MEN: Wiedza moją Tarczą — materiały z 8.10.2026

Autorski materiał edukacyjny Fundacji WHITE-RED · aktualizacja redakcyjna 12.10.2026 · W razie bezpośredniego zagrożenia życia lub zdrowia dzwoń 112. Fundacja WHITE-RED