# Jak zabezpieczyć urządzenie

**Dowiesz się:**

• Dlaczego warto chronić urządzenia dziecka przed złośliwym oprogramowaniem.

• Jakie narzędzia skutecznie zabezpieczają urządzenia.

• Jak rozpoznać infekcję urządzenia i jak zareagować.

Każde urządzenie podłączone do internetu jest narażone na kontakt ze złośliwym oprogramowaniem. Może ono zainfekować komputer, smartfon lub tablet dziecka, powodując szkody lub umożliwiając dostęp do danych osobom nieuprawnionym.

Bardzo często oprogramowanie tego typu jest nieświadomie uruchamiane i instalowane przez samych użytkowników, w tym dzieci, np. poprzez otwieranie załączników z poczty elektronicznej lub klikanie w linki.

**Czym jest złośliwe oprogramowanie i jak działa?**

Złośliwe oprogramowanie (malware) to wszystkie aplikacje stworzone po to, by uszkodzić urządzenie lub ukraść poufne dane użytkownika. Do najczęściej spotykanych należą:

• Wirusy i robaki – uszkadzają pliki i programy, spowalniają działanie urządzenia lub rozprzestrzeniają się na inne sprzęty.

• Trojany (konie trojańskie) – ukrywają się pod postacią pozornie bezpiecznych aplikacji, w rzeczywistości umożliwiając atakującym przejęcie kontroli nad urządzeniem.

• Programy szpiegujące (spyware) – zbierają poufne dane (np. hasła, loginy, dane bankowe), które mogą być później wykorzystane przez cyberprzestępców.

• Ransomware – blokuje dostęp do danych lub całego urządzenia, żądając zapłaty okupu za przywrócenie dostępu.

**Jak skutecznie zabezpieczyć urządzenie dziecka?**

Warto zadbać o kilka podstawowych elementów bezpieczeństwa urządzeń, z których korzysta dziecko:

• Regularne aktualizacje systemu operacyjnego, aplikacji oraz przeglądarek.

• Program antywirusowy – instalowany zarówno na komputerze, jak i na urządzeniach mobilnych dziecka (np. Avast, Norton, Kaspersky).

• Zapora sieciowa (firewall) – chroni przed próbami nieautoryzowanego dostępu z internetu.

• Ograniczenie uprawnień użytkownika – ustawienie konta dziecka bez uprawnień administratora, co uniemożliwia instalację niebezpiecznych aplikacji.

• Zabezpieczenia wbudowane w platformy – np. Netflix Kids, YouTube Kids, Google SafeSearch, które zmniejszają ryzyko przypadkowego kontaktu ze złośliwymi aplikacjami lub niebezpiecznymi treściami.

**Ochrona urządzeń mobilnych (smartfonów, tabletów):**

• Pobieraj aplikacje tylko z oficjalnych sklepów (Google Play, AppStore).

• Zabezpiecz urządzenie hasłem, kodem PIN lub metodą biometryczną.

• Aktywuj opcję kontroli rodzicielskiej na urządzeniu mobilnym, np. Chroń dzieci w sieci.

• Włącz automatyczne aktualizacje systemu oraz aplikacji.

• Regularnie sprawdzaj aplikacje zainstalowane przez dziecko.

**Dodatkowym zabezpieczeniem działającym w sieci Orange jest mechanizm wykrywania zagrożeń - CyberTarcza.**

Jak rozpoznać infekcję urządzenia dziecka?

Typowe objawy infekcji malware to:

• wolniejsze działanie urządzenia lub częste zawieszanie się systemu,

• pojawianie się niechcianych reklam i wyskakujących okien,

• nowe, nieznane aplikacje pojawiające się w systemie,

• nagłe zmiany ustawień przeglądarki lub innych programów,

• szybkie rozładowywanie się baterii urządzenia mobilnego,

• zwiększone zużycie danych mobilnych bez wyraźnego powodu.

**Co zrobić, gdy urządzenie dziecka zostało zainfekowane?**

Jeżeli zauważysz objawy infekcji malware na urządzeniu dziecka:

1. Odłącz sprzęt od internetu, aby ograniczyć dalsze szkody.

2. Przeskanuj urządzenie aktualnym programem antywirusowym.

3. Usuń lub przenieś do kwarantanny wykryte zagrożenia.

4. W przypadku poważnej infekcji rozważ przywrócenie ustawień fabrycznych lub reinstalację systemu operacyjnego (po wcześniejszym zabezpieczeniu ważnych danych).

5. Zmień hasła do kont, z których korzystało dziecko na zainfekowanym urządzeniu.

**Ostrożność w publicznych sieciach Wi-Fi**

Dziecko powinno zachować ostrożność, korzystając z publicznych sieci Wi-Fi:

• unikać logowania się na ważne konta (bankowość, poczta e-mail, profile społecznościowe),

• upewnić się, że odwiedzane strony mają zabezpieczenia HTTPS (symbol kłódki na pasku adresu),

• wyłączyć automatyczne łączenie się urządzenia z publicznymi hotspotami,

• w razie potrzeby korzystać z bezpiecznego połączenia VPN.

**Edukacja dziecka na temat bezpieczeństwa online**

Zabezpieczenia techniczne najlepiej działają, gdy towarzyszy im edukacja dziecka na temat bezpiecznego korzystania z internetu. Rozmawiaj regularnie z dzieckiem o zagrożeniach online. Ucz je ostrożności podczas klikania w linki oraz pobierania aplikacji. Zachęcaj dziecko, by zgłaszało Ci wszelkie niepokojące sytuacje związane z działaniem urządzenia.

**Pamiętaj:**

• Złośliwe oprogramowanie to realne zagrożenie dla urządzeń dzieci.

• Podstawą ochrony są: aktualizacje, program antywirusowy i zapora sieciowa.

• Dzieci powinny korzystać tylko z oficjalnych sklepów z aplikacjami.

• Warto ograniczyć prawa użytkownika na urządzeniu dziecka.

• Infekcję można rozpoznać po nietypowym zachowaniu urządzenia – warto reagować szybko.

• Ochrona techniczna to nie wszystko – kluczowa jest rozmowa i edukacja dziecka.

**Zobacz:**

• Aplikacja „Chroń dzieci w sieci” (Orange)

• Poznaj nowoczesną aplikacje kontroli rodzicielskiej

• Sprawdź jak dzięki niej możesz zadbać o bezpieczeństwo dziecka.