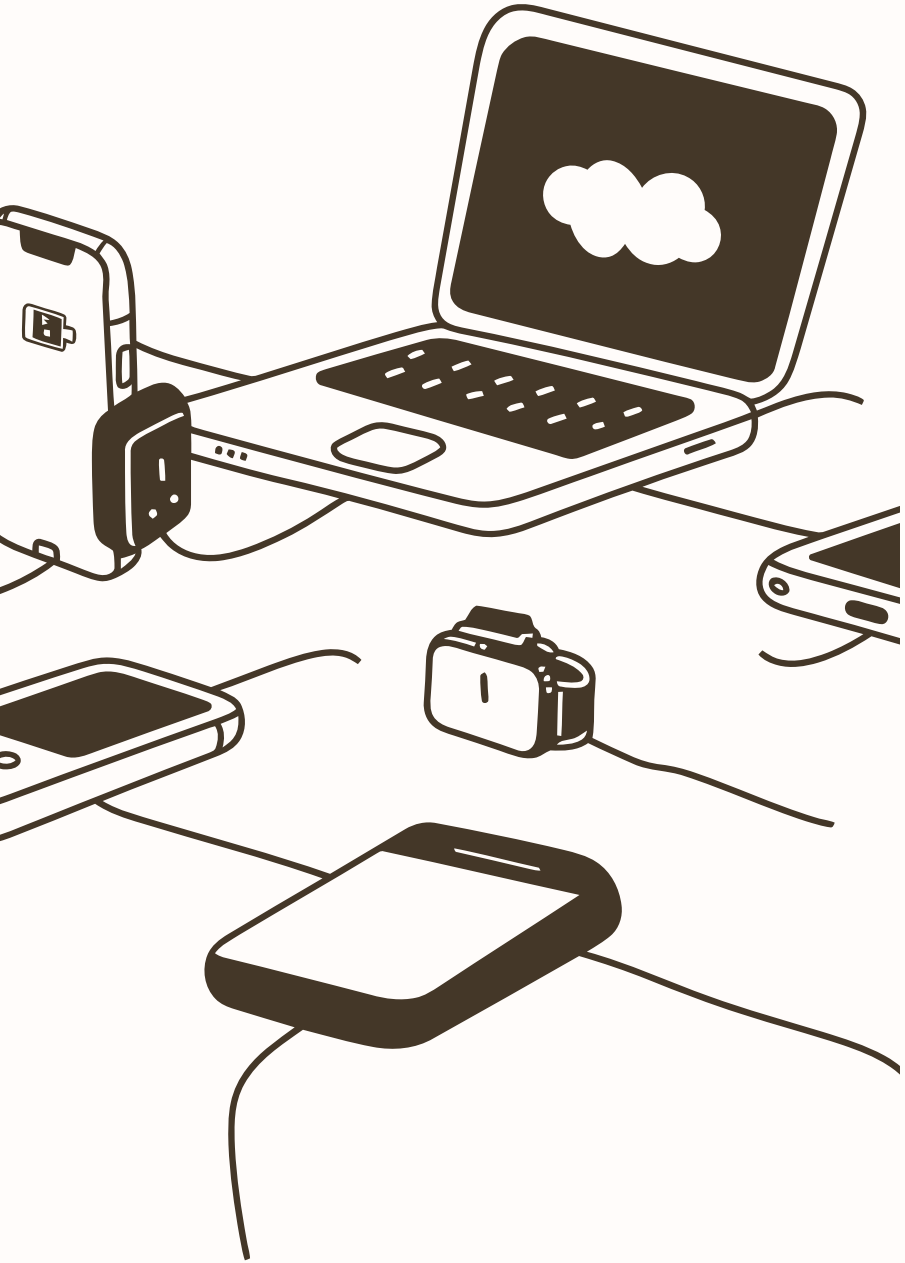


Bezpieczeństwo urządzeń mobilnych - zagrożenia i środki ochrony

Ochrona tych urządzeń jest kluczowa, towarzyszą nam w różnych miejscach, co zwiększa ryzyko ich utraty poprzez kradzież lub zagubienie. Cyberprzestępcy wiedzą, że wartość danych zgromadzonych w urządzeniu mobilnym może znacznie przekraczać wartość samego sprzętu.

Czym są urządzenia mobilne?

Charakterystyka

Urządzenia mobilne to przenośne urządzenia elektroniczne umożliwiające przetwarzanie i przesyłanie danych bez konieczności podłączania przewodem sieciowym. Wyróżniają się niewielkimi rozmiarami i wagą, co ułatwia ich przenoszenie.

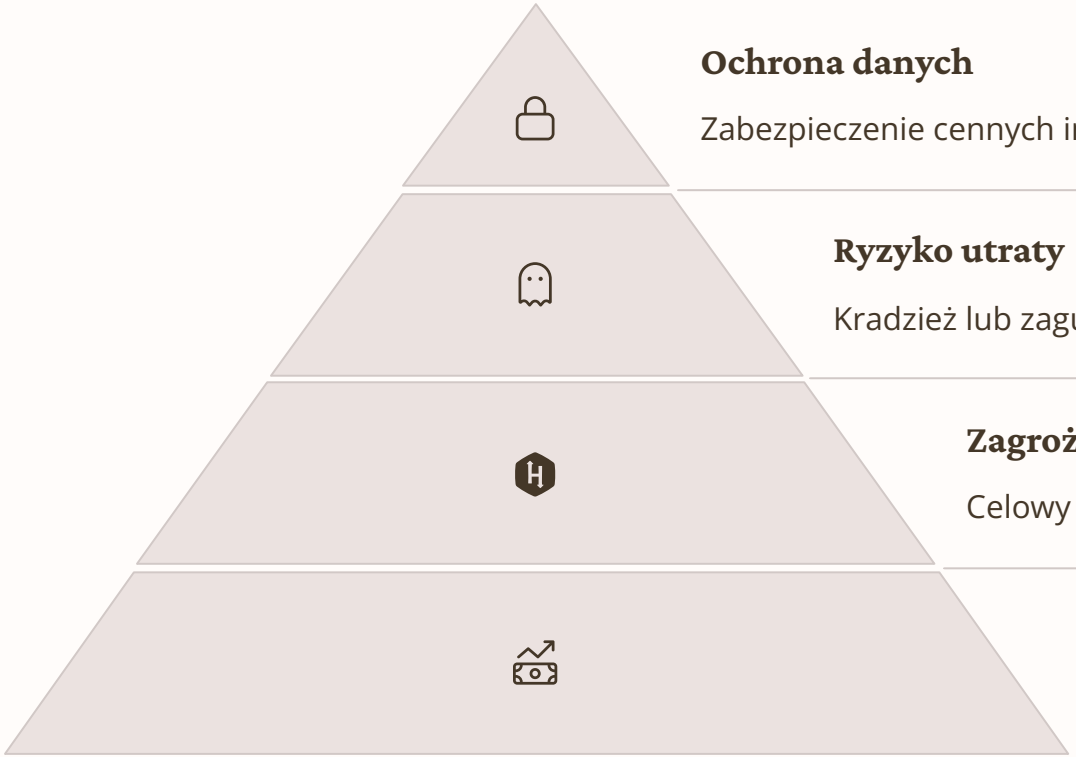
Funkcjonalność

Pozwalają na odbieranie i wysyłanie poczty, korzystanie z internetu oraz utrzymywanie stałego kontaktu z innymi użytkownikami lub firmą z różnych lokalizacji. Są stale "pod ręką", co zwiększa ich użyteczność w codziennym życiu.

Przykłady

Do najpopularniejszych urządzeń mobilnych zaliczamy smartfony, tablety oraz laptopy. Każde z nich oferuje różny poziom mobilności i funkcjonalności, dostosowany do potrzeb użytkownika.

Dlaczego ochrona urządzeń mobilnych jest tak istotna?



Ochrona danych

Zabezpieczenie cennych informacji

Ryzyko utraty

Kradzież lub zagubienie urządzenia

Zagrożenie cyberprzestępcami

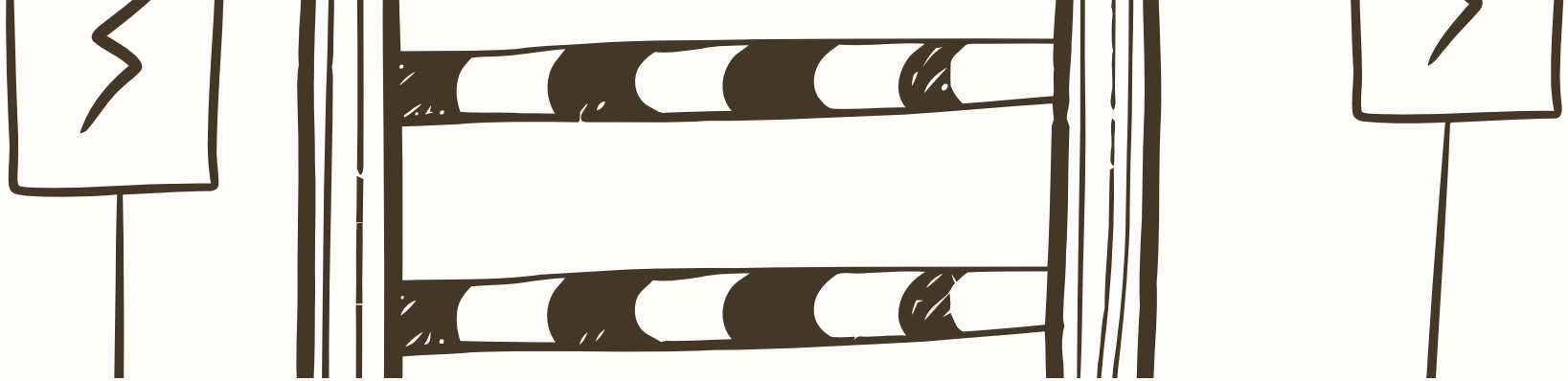
Celowy dostęp do danych

Wartość zgromadzonych danych

Często przewyższa wartość urządzenia

W przypadku dostępu osób postronnych do urządzenia, istnieje zagrożenie uzyskania przez nie dostępu do zgromadzonych danych - wiadomości, dokumentów, zdjęć, notatek, a także loginów i haseł.

Używanie prywatnych urządzeń mobilnych do celów służbowych powinno być zabronione lub znacznie ograniczone, firma nie jest w stanie kontrolować ani zagwarantować odpowiedniego poziomu bezpieczeństwa urządzenia użytkownika.



Czego należy unikać?

Przetwarzanie służbowych danych na prywatnych urządzeniach

Odbieranie służbowej poczty, edytowanie dokumentów firmowych czy logowanie do serwisów firmy na prywatnych urządzeniach stwarza poważne ryzyko wycieku danych.

Pozostawianie urządzeń bez nadzoru

Nigdy nie zostawiaj urządzenia mobilnego bez opieki w miejscach publicznych, takich jak restauracje, samochody czy środki transportu publicznego.

Korzystanie z niezaufanych sieci

Unikaj łączenia się z niezabezpieczonymi sieciami Wi-Fi w miejscach publicznych, które mogą być wykorzystywane przez cyberprzestępców do przechwytywania danych.

Instalowanie niezaufanego oprogramowania

Nie instaluj aplikacji z nieznanych źródeł lub takich, których przeznaczenie i sposób działania nie są jasno określone.

Na co zwrócić uwagę?

Szyfrowanie danych

Wszystkie dane firmowe na urządzeniach mobilnych powinny być właściwie zaszyfrowane przy użyciu sprawdzonych narzędzi i trudnych do odgadnięcia haseł.

Zaufane sieci

Istotne jest, by sieć przez którą transmitowane są dane była zaufana, a urządzenie nie łączyło się automatycznie z niezabezpieczonymi sieciami.

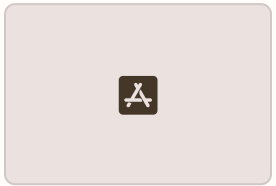
Zabezpieczenie nośników

Pamiętaj, że sam kod PIN nie chroni danych na kartach pamięci - należy zadbać o szyfrowanie danych na wszystkich nośnikach.

Ochrona poczty

Wiadomości pocztowe wraz z załącznikami powinny być odpowiednio zaszyfrowane, uniemożliwiając odczytanie ich treści przez niepowołane osoby.

Co zwiększa bezpieczeństwo?

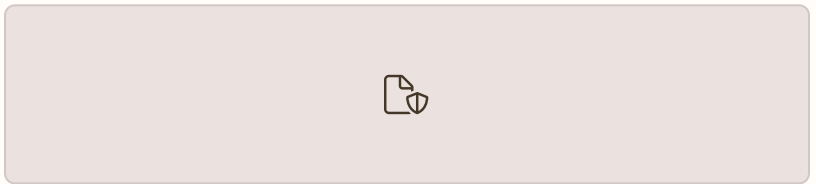


Weryfikacja aplikacji

Sprawdzaj wydawcę, ranking i opinie

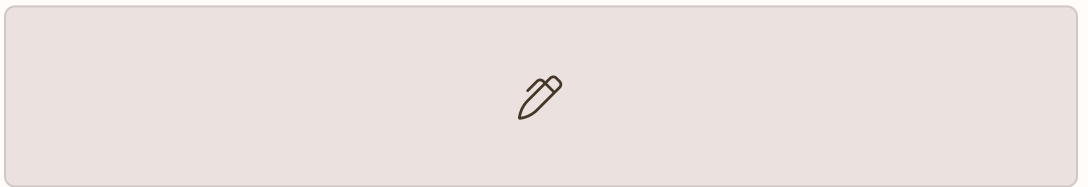
Zabezpieczenie dostępu

Używaj kodu PIN lub silnego hasła



Ochrona antywirusowa

Stosuj programy zabezpieczające



Aktualizacja oprogramowania

Dbaj o najnowsze wersje systemu

Przed instalacją aplikacji warto sprawdzić, kto jest jej wydawcą i jakie ma opinie. Istotne jest również weryfikowanie rankingu aplikacji - ilu użytkowników ją pobrało, jakie ma oceny oraz czy zgłoszono błędy. Należy zwrócić uwagę na to, do jakich obszarów aplikacja uzyskuje dostęp i jakie dane może przesyłać.

Szyfrowanie danych w urządzeniu oraz na nośnikach, które są w urządzeniu (np. karty pamięci) stanowi dodatkową warstwę ochrony. Stosowanie ochrony antywirusowej i zapory sieciowej pozwala wychwycić niepożądane oprogramowanie oraz próby przesyłania danych.

Pamiętaj o zagrożeniach

Złośliwe aplikacje

Cyberprzestępcy tworzą aplikacje, które pozornie wyglądają niewinnie i udają pożyteczne oprogramowanie (np. programy antywirusowe, gry czy przeglądarki), a w rzeczywistości służą do przeprowadzania ataków.

Nieświadoma instalacja

Złośliwe aplikacje najczęściej instalowane są przez samych użytkowników, którzy niczego nie podejrzewają. Zawsze weryfikuj źródło i uprawnienia instalowanych programów.

Ochrona przez szyfrowanie

Szyfrowanie danych na urządzeniach mobilnych zapewnia ochronę nie tylko w przypadku kradzieży lub zagubienia urządzenia, ale także może chronić dane przed działaniem niektórych złośliwych aplikacji.

Jak dbać o bezpieczeństwo urządzenia mobilnego?

Zabezpiecz urządzenie

Używaj kodu PIN, hasła lub biometrii do ochrony dostępu do urządzenia.

Włącz szyfrowanie danych

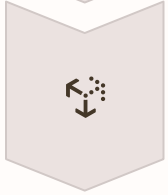
Zaszyfruj wszystkie wrażliwe dane przechowywane na urządzeniu i kartach pamięci.

Zapewnij ochronę antywirusową

Zainstaluj i regularnie aktualizuj oprogramowanie antywirusowe.

Kontroluj połączenia sieciowe

Wyłącz automatyczne łączenie się z niezaufanymi i niezabezpieczonymi sieciami.



Aktualizuj oprogramowanie

Dbaj o aktualność systemu operacyjnego i wszystkich zainstalowanych aplikacji.