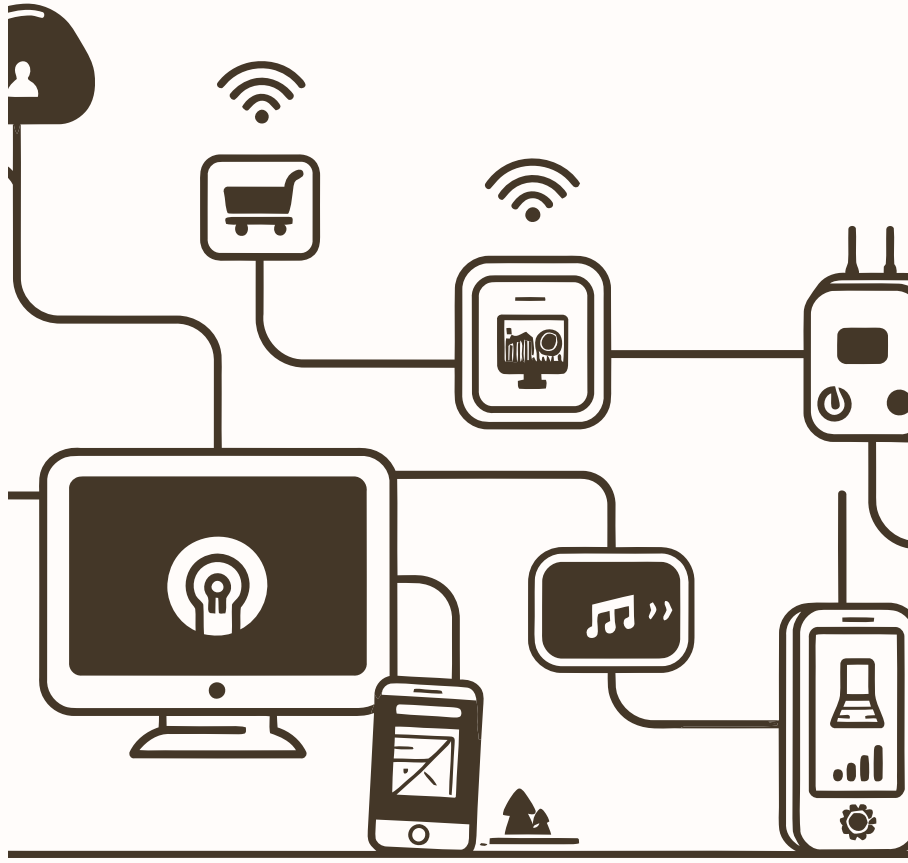
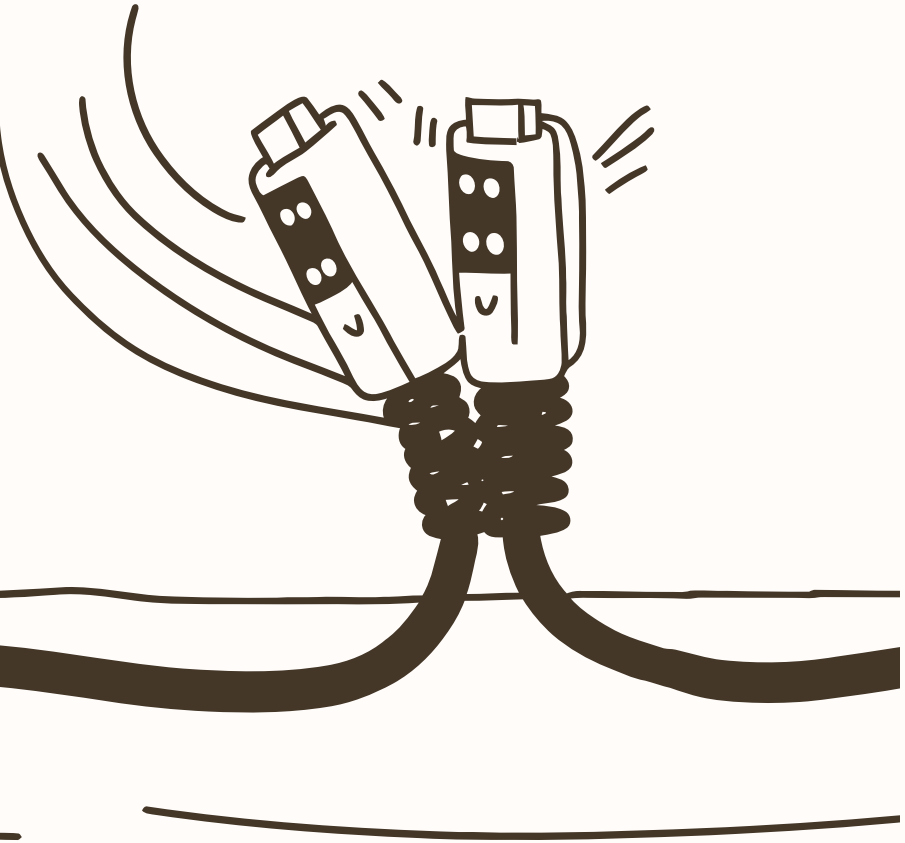
Sieci bezprzewodowe - zagrożenia związane z Wi-Fi

Witaj w prezentacji poświęconej bezpieczeństwu sieci bezprzewodowych. Poznasz najczęstsze niebezpieczeństwa związane z sieciami bezprzewodowymi oraz praktyczne wskazówki, jak zabezpieczyć swoje dane podczas korzystania z Wi-Fi zarówno w miejscach publicznych, jak i w domu.





Co to jest sieć bezprzewodowa?

Łączność bez kabla

Sieć internetowa, z którą łączysz się bezprzewodowo przez router Wi-Fi w domu, telefon, hotelu, kawiarni czy na dworcu.

Wygoda użytkowania

Możliwość korzystania z internetu w dowolnym miejscu w zasięgu sieci.

Potencjalne ryzyko

Sieci bezprzewodowe niosą ze sobą duże ryzyko, jeśli nie są odpowiednio zabezpieczone.

Dlaczego Wi-Fi może być niebezpieczne?

Publiczne sieci są otwarte dla każdego

Nikt nie sprawdza, kto się do nich podłącza, co stwarza idealne warunki dla cyberprzestępców.

Łatwo podszyć się pod "prawdziwą" sieć

Nazwa "FreeAirportWiFi" może być stworzona przez cyberprzestępcę, aby wyłudzić Twoje dane.

Brak zabezpieczeń prowadzi do zagrożeń

Twoje dane mogą być przechwycone, możesz być śledzony, a nawet ktoś może przejąć połączenie z aplikacją lub stroną.

Przykładowe zagrożenia

Przechwycenie danych logowania

Cyberprzestępcy mogą zdobyć Twoje dane dostępowe do poczty, portalu firmowego czy banku.

Podsłuchiwanie połączeń

Tzw. "sniffing" - wszystko, co wpisujesz w niezabezpieczonej sieci, może zostać zapisane przez atakującego.

Fałszywe strony logowania

Po kliknięciu np. w Facebooka możesz trafić na podrobioną stronę, która wykradnie Twoje dane.

Atak "man in the middle"

Ktoś pośredniczy między Tobą a internetem, kontrolując całą komunikację i przechwytując wrażliwe informacje.

Jak się chronić podczas korzystania z Wi-Fi?

Unikaj ryzykownych połączeń

Nie łącz się automatycznie z otwartymi sieciami. Unikaj darmowych sieci bez hasła - szczególnie w miejscach publicznych.

Chroń wrażliwe dane

Nie loguj się do konta bankowego ani służbowego przez publiczne Wi-Fi. Używaj sieci komórkowej (LTE/5G) lub VPN, jeśli musisz skorzystać z internetu poza domem.

Kontroluj ustawienia urządzeń

Wyłącz automatyczne łączenie z zapamiętanymi sieciami w telefonie i laptopie. Sprawdź, czy strona ma szyfrowane połączenie (adres zaczyna się od Https://).

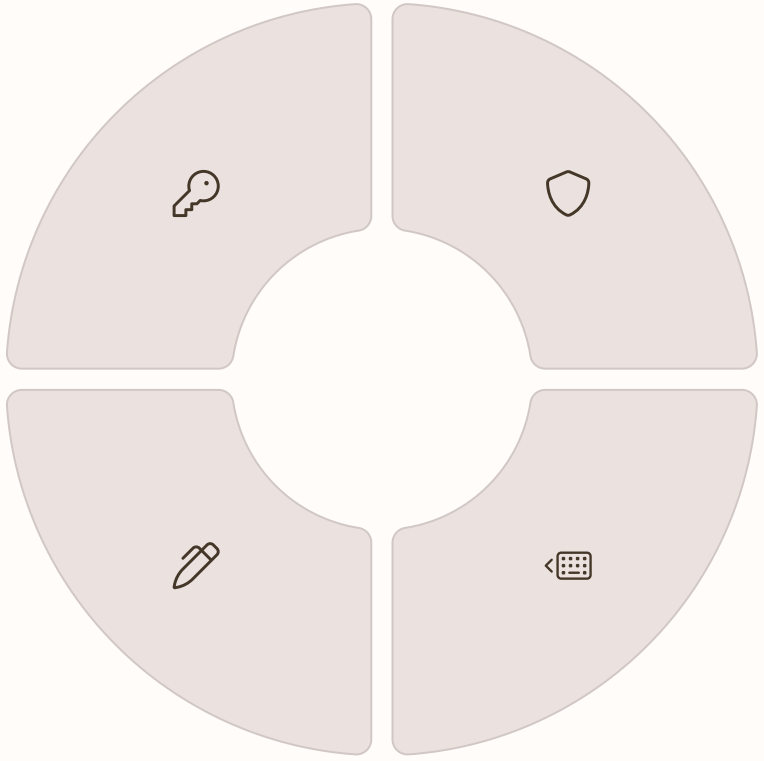
Co z Wi-Fi w domu?

Zmień domyślne hasła

Nie zostawiaj ustawień "admin/admin" w routerze. Ustaw silne hasło do sieci Wi-Fi (minimum 12 znaków, z literami, cyframi i znakami specjalnymi).

Aktualizuj oprogramowanie

Regularnie aktualizuj oprogramowanie routera, aby chronić się przed nowymi zagrożeniami.



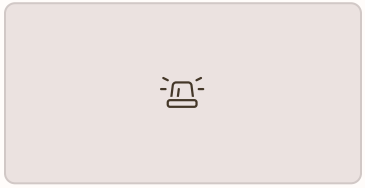
Włącz szyfrowanie

Korzystaj z szyfrowania WPA2 lub WPA3, które zapewnia wysoki poziom bezpieczeństwa.

Ukryj nazwę sieci

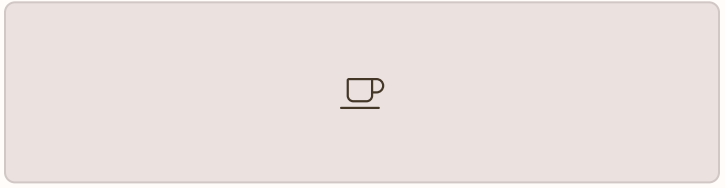
Ukryj nazwę sieci (SSID), jeśli nie chcesz, by była publicznie widoczna.

Zapamiętaj!



Dostępność ≠ Bezpieczeństwo

To, że możesz się połączyć z Wi-Fi, nie znaczy, że powinieneś.

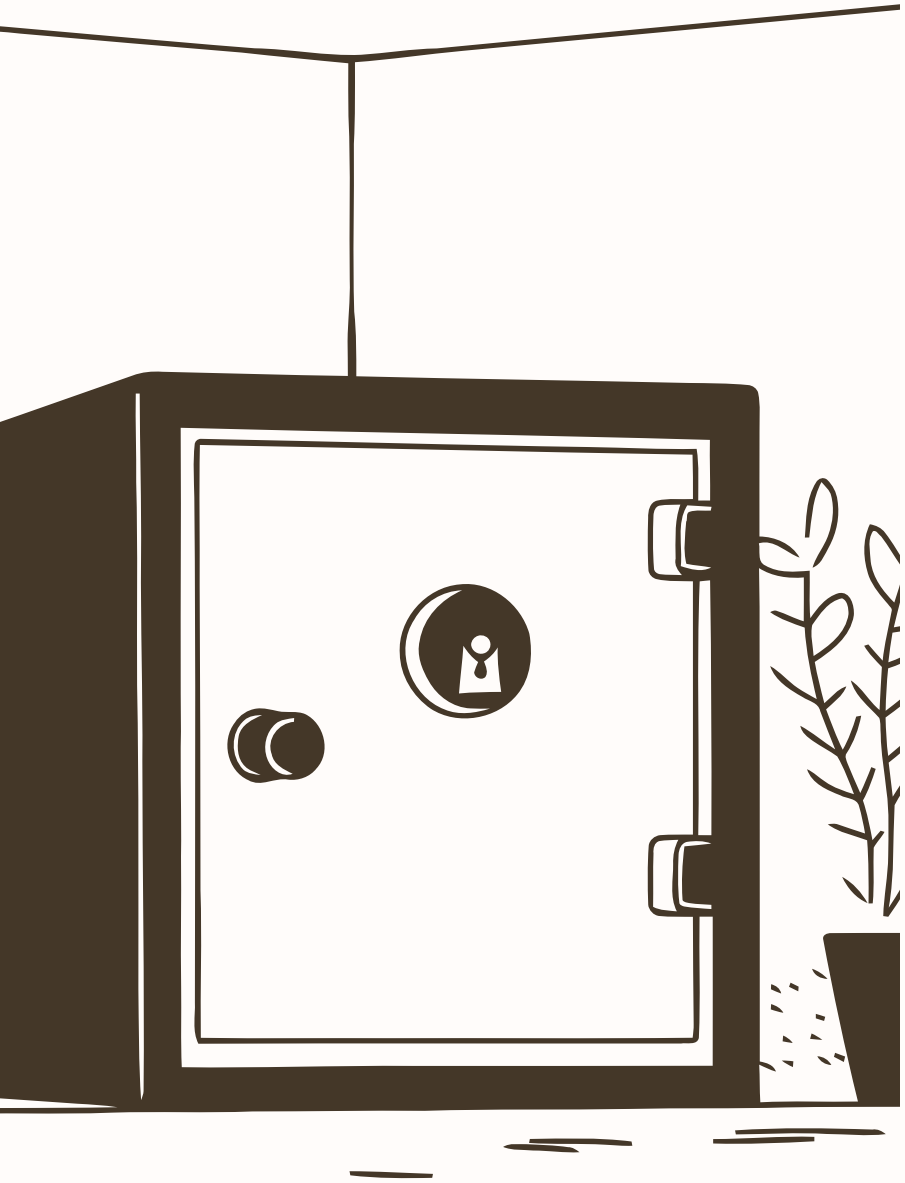


Publiczne Wi-Fi = Publiczna rozmowa

Publiczne Wi-Fi to jak rozmowa na głos w zatłoczonej kawiarni – każdy może podsłuchać.

Zawsze się wyloguj

Zawsze wyloguj się z kont i zamknij sesje, jeśli łączyłeś się przez niezaufaną sieć.



Bezpieczne zachowania

Tak ✔️	Nie ❌
Korzystaj z VPN	Logowanie do banku w galerii handlowej
Używaj danych mobilnych	Klikanie w linki z publicznej sieci
Łącz się tylko z własną siecią firmową	Zostawianie Wi-Fi włączonego na stałe
Sprawdzaj, czy strona ma "Https://"	Przesyłanie dokumentów przez publiczne Wi-Fi