Publiczne sieci Wi-Fi – Jak chronić swoje dane?

Posted on 2024-10-31

Jak działają publiczne sieci Wi-Fi, jakie zagrożenia mogą wynikać z ich użytkowania oraz jak można chronić swoje dane przed nieautoryzowanym dostępem?

Jednym z kluczowych elementów, które ułatwiają nam korzystanie z internetu, są publiczne sieci Wi-Fi. Spotykamy je np. kawiarniach, na lotniskach, w hotelach, a nawet w parkach. Dzięki nim możemy bez problemu przeglądać strony internetowe, sprawdzać pocztę elektroniczną, korzystać z mediów społecznościowych czy wykonywać transakcje online. Jednak korzystanie z publicznych sieci Wi-Fi wiąże się z pewnymi zagrożeniami, zwłaszcza w kontekście ochrony danych osobowych.

Jak działają publiczne sieci Wi-Fi?

Publiczne sieci Wi-Fi to bezprzewodowe sieci lokalne, które umożliwiają użytkownikom łączenie się z internetem na zasadzie radiowej transmisji danych. Sygnał przesyłany jest za pośrednictwem fal radiowych. Sieci te często są otwarte, co oznacza, że każdy, kto znajduje

się w zasięgu sygnału, może się do nich podłączyć, często bez potrzeby wprowadzania hasła. Wi-Fi jest technologią opartą na standardzie IEEE 802.11, która zapewnia różne poziomy bezpieczeństwa, zależnie od konfiguracji sieci i zastosowanych metod szyfrowania. Publiczne sieci Wi-Fi są zazwyczaj mniej zabezpieczone niż sieci prywatne, co czyni je bardziej podatnymi na ataki cybernetyczne. Niska jakość zabezpieczeń wynika z kilku czynników, w tym z potrzeby łatwego i szybkiego dostępu dla użytkowników oraz z braku kontroli nad tym, kto korzysta z sieci.

Zagrożenia związane z korzystaniem z publicznych sieci Wi-Fi

1. Ataki typu Man-in-the-Middle (MITM)

Jednym z najpoważniejszych zagrożeń, na które narażeni są użytkownicy publicznych sieci Wi-Fi, są ataki typu Man-in-the-Middle. Cyberprzestępca przechwytuje i modyfikuje dane przesyłane między użytkownikiem a serwerem. Przejęcie sesji internetowej może prowadzić do kradzieży poufnych informacji, takich jak dane logowania, hasła czy numery kart kredytowych. Ataki MITM mogą być szczególnie niebezpieczne, ponieważ użytkownik często nie jest świadomy, że jego połączenie zostało przechwycone. Cyberprzestępca może podszywać się pod znaną witrynę internetową, co sprawia, że ofiara czuje się bezpiecznie,

wprowadzając swoje dane osobowe.

2. Fałszywe punkty dostępu (Evil Twin)

Innym popularnym zagrożeniem jest tzw. Evil Twin, czyli fałszywy punkt dostępu. Cyberprzestępca tworzy sieć Wi-Fi o nazwie identycznej lub bardzo podobnej do legalnej sieci dostępnej w danym miejscu, np. „Free_Cafe_WiFi". Gdy użytkownik podłącza się do takiej sieci, wszystkie jego dane są przechwytywane przez atakującego. W ten sposób cyberprzestępca może uzyskać dostęp
do wrażliwych informacji, takich jak dane bankowe czy hasła do różnych kont.

Nowo odkryta luka w standardzie Wi-Fi IEEE 802.11, nazwana „SSID Confusion" (CVE-2023-52424), pozwala atakującym na przechwytywanie ruchu sieciowego poprzez przekonanie ofiary do połączenia się z fałszywą, mniej bezpieczną siecią Wi-Fi. Atak wpływa na wszystkie systemy operacyjne i typy sieci, w tym domowe i korporacyjne.

Przebieg Ataku

1. Wykrywanie sieci: Atakujący modyfikuje pakiety Wi-Fi, aby zamienić identyfikatory SSID prawdziwej i fałszywej sieci, co wprowadza ofiarę w błąd.
2. Przejęcie uwierzytelnienia: Ofiara uwierzytelnia się do fałszywej sieci myśląc, że jest to zaufana sieć.
3. Trwający MitM: Atakujący przechwytuje ruch ofiary, zmieniając identyfikatory SSID w czasie rzeczywistym.

Skutki

Atak może dezaktywować VPN w przypadku połączenia się z „zaufaną” siecią, co naraża ruch ofiary na ryzyko. Zaleca się uniknięcie ponownego używania danych uwierzytelniających w różnych sieciach oraz stosowanie unikalnych haseł.

3. Brak szyfrowania danych

Większość publicznych sieci Wi-Fi korzysta z nowoczesnych protokołów szyfrowania, takich jak WPA2 lub WPA3, które oferują wysoki poziom ochrony. Protokół WEP (Wired Equivalent Privacy), który był powszechny kilkanaście lat temu, jest już praktycznie nieużywany ze względu na jego słabe zabezpieczenia. Mimo to, w niektórych przypadkach można jeszcze natrafić na sieci korzystające z WEP lub WPA, co może wynikać z nieaktualizowanego oprogramowania routera lub zaniedbań
w konfiguracji sieci.

Zastosowanie przestarzałego protokołu niesie ze sobą poważne ryzyko, gdyż dane przesyłane w takiej sieci mogą być łatwo przechwycone przez osoby trzecie. Nawet jeśli sieć korzysta z WPA2 lub WPA3, warto pamiętać, że publiczne sieci Wi-Fi mogą być podatne na różnego rodzaju ataki, takie jak MITM. Dlatego zawsze warto zachować ostrożność i łączyć się tylko z zaufanymi sieciami, szczególnie przy przesyłaniu poufnych informacji.

4. Sniffing

Sniffing to technika polegająca na przechwytywaniu danych przesyłanych przez sieć. W publicznych sieciach Wi-Fi, gdzie transmisja danych jest często nieszyfrowana, sniffing staje

się bardzo prostym narzędziem do wykradania informacji. Sniffery mogą przechwycić takie dane, jak hasła, wiadomości e-mail, a nawet zawartość przeglądanych stron internetowych. Dlatego tak ważne jest korzystanie z usługi VPN, ponieważ szyfruje on cały ruch internetowy, tworząc bezpieczny tunel między urządzeniem użytkownika a serwerem. Dzięki temu nawet jeśli dane zostaną przechwycone, będą one zaszyfrowane i niemożliwe do odczytania przez osoby trzecie.

5. Złośliwe oprogramowanie

Korzystanie z publicznych sieci Wi-Fi może również zwiększyć ryzyko zainfekowania urządzenia złośliwym oprogramowaniem. W otwartych sieciach cyberprzestępcy mogą wprowadzać złośliwe oprogramowanie na urządzenia użytkowników poprzez różnego rodzaju techniki, takie jak drive-by download (automatyczne pobieranie plików bez wiedzy użytkownika) czy fałszywe aktualizacje oprogramowania. Zainfekowane urządzenie może stać się bramą do wykradania danych osobowych lub innych cennych informacji.

Jak chronić swoje dane podczas korzystania z publicznych sieci Wi-Fi?

1. Unikanie przesyłania poufnych informacji

Jednym z najprostszych sposobów na ochronę swoich danych w publicznych sieciach Wi-Fi jest unikanie przesyłania poufnych informacji, takich jak loginy, hasła czy dane bankowe. Dla takich danych należy lepiej skorzystać z sieci mobilnej lub połączyć się z zaufaną, zabezpieczoną siecią prywatną.

2. Używanie VPN (Virtual Private Network)

Wirtualna sieć prywatna jest jednym z najskuteczniejszych narzędzi do ochrony danych w publicznych sieciach Wi-Fi. Szyfruje wszystkie dane przesyłane między urządzeniem użytkownika a serwerem VPN, co znacznie utrudnia ich przechwycenie przez osoby trzecie. Dzięki temu, nawet jeśli cyberprzestępca przechwyci zaszyfrowane dane, nie będzie mógł ich odczytać.

3. Korzystanie z HTTPS

Przy korzystaniu z publicznych sieci Wi-Fi warto zwracać uwagę na to, czy odwiedzane strony internetowe korzystają z protokołu HTTPS, który zapewnia szyfrowanie danych przesyłanych między przeglądarką a serwerem. Adresy stron korzystających z HTTPS zaczynają się od „https://” zamiast „http://”. Obecność ikony kłódki w pasku adresu

przeglądarki jest również sygnałem, że połączenie jest szyfrowane.

4. Wyłączanie udostępniania plików i drukarek

W publicznych sieciach Wi-Fi zaleca się wyłączenie funkcji udostępniania plików i drukarek, która może umożliwić nieautoryzowany dostęp do danych przechowywanych na urządzeniu. W systemie Windows można to zrobić w ustawieniach sieci, natomiast na urządzeniach Apple opcje te znajdują się w preferencjach systemowych.

5. Aktualizacja oprogramowania

Aktualizacje często zawierają poprawki bezpieczeństwa, które naprawiają wykryte luki w zabezpieczeniach. Korzystając z najnowszych wersji oprogramowania, minimalizujemy ryzyko, że nasze urządzenie stanie się ofiarą cyberprzestępcy.

6. Wyłączenie automatycznego łączenia z

sieciami Wi-Fi

Wielu użytkowników nie zdaje sobie sprawy, że ich urządzenia mogą automatycznie łączyć się z sieciami Wi-Fi, które wcześniej były używane. Może to prowadzić do sytuacji, w której urządzenie połączy się z fałszywym punktem dostępu, stworzonym przez cyberprzestępcę. Dlatego warto wyłączyć funkcję automatycznego łączenia się z sieciami Wi-Fi i ręcznie wybierać te, do których chcemy się podłączyć.

Podsumowując, korzystanie z publicznych sieci Wi-Fi, choć wygodne, wiąże się z istotnymi zagrożeniami dla prywatności i bezpieczeństwa naszych danych. Świadomość tych zagrożeń oraz stosowanie odpowiednich środków ostrożności, takich jak korzystanie z VPN, zwracanie uwagi na protokół HTTPS, czy regularne aktualizacje oprogramowania, mogą znacząco zmniejszyć ryzyko. Pamiętajmy, że dbanie o bezpieczeństwo naszych informacji w sieci to nasza wspólna odpowiedzialność, a podejmowanie prostych kroków może uchronić nas przed poważnymi konsekwencjami cyberataków.