Jak bezpiecznie korzystać z publicznych sieci Wi-Fi

Publiczne hotspoty Wi-Fi cieszą się dużą popularnością i dobrą opinią ale nie powinno się im nadmiernie ufać, dlatego warto wiedzieć, jak bezpiecznie z nich korzystać.

1. Unikanie podawania danych i używania jednakowych haseł

Szczególnie niebezpiecznym krokiem przy korzystaniu z publicznej niesprawdzonej sieci jest używanie podczas sesji haseł do różnych kont. Mogą one zostać przechwycone przez hakerów. Co więcej, jeżeli do kilku różnych profili ma się ustawione jednakowe hasło, zagrożenie może wzrosnąć. Wszędzie powinniśmy więc ustalić inne ciągi szyfrów.
W żadnym wypadku nie należy podawać nikomu danych do własnych kont. Nawet jeżeli jest to warunek konieczny do tego, by uzyskać dostęp do połączenia z Internetem.

2. Antywirus na laptop i telefon

Z publiczną siecią Wi-Fi użytkownicy łączą się za pomocą różnych urządzeń.
Każdy sprzęt, z którego zamierzamy się logować na różne konta, powinien być odpowiednio zabezpieczony. Ma to znaczenie, szczególnie jeśli dokonuje się z niego zakupów, a przy tym korzysta z bankowości i wprowadza dane kart kredytowych.

Podstawą jest nieustanna aktualizacja systemu danego urządzenia. Wraz z nią dostawca wprowadza często wiele nowych zabezpieczeń, które mają sprostać wyzwaniu cyberprzestępczości. Poza tym, na komputerze oraz telefonie powinien być zainstalowany antywirus, który ochroni użytkownika przed różnymi atakami hakerskimi, a nawet utratą tożsamości. Istotne jest również zainstalowanie specjalnej ochrony bankowej w postaci wtyczki do przeglądarki czy dodatku do oprogramowania antywirusowego.

3. Sprawdzenie certyfikatu SSL na stronie logowania do publicznego Wi-Fi

Przed wykonaniem jakiegokolwiek ruchu w danej witrynie należy sprawdzić jej certyfikat SSL. Większe bezpieczeństwo zachowa się, dokonując tego samego na stronie logowania do publicznej sieci Wi-Fi. Posiadanie przez dany serwis takiego certyfikatu, daje gwarancję poufności danych. Potwierdza to kłódka widniejąca obok paska z adresem URL (https://)

4. Wyłączenie udostępniania plików i drukarek

Niemal za każdym razem, gdy użytkownik łączy się z nowym Wi-Fi, pojawia się komunikat z zapytaniem o udostępnianie plików i drukarek dla urządzeń w sieci. W zależności od systemu niżej może pojawić się sugestia mówiąca o tym, że zaleca się włączenie tej opcji jedynie w sieci domowej lub służbowej, ale nie w publicznej. Warto się do tego zastosować i samemu zdecydować komu da się dostęp do danych, bo nawet w warunkach zawodowych czy rodzinnych nie zawsze muszą być one bezpieczne.

By pliki z komputerów nie trafiły w niepowołane ręce, warto sprawdzić, czy ustawienia komputera i sieci są odpowiednio skonfigurowane. Wówczas należy odwiedzić Panel sterowania, a następnie przejść ścieżkę: Sieć i Internet → Centrum sieci i udostępniania. Po lewej stronie klikamy w zakładkę „Zmień zaawansowane ustawienia udostępniania" i wybrane pola z udostępnianiem plików i drukarek oznaczamy statusem „wyłączone".

5. Bezpieczne VPN do szyfrowania danych

Sieci Wi-Fi w wielu wypadkach są dość ryzykownym rozwiązaniem do wykonywania różnych działań w sieci, szczególnie tych, podczas których podaje się wrażliwe dane osobowe czy numery kart płatniczych. Łącząc się z publicznym Wi-Fi, użytkownik nie ma na ogół pojęcia, kto otrzymuje wówczas dostęp do jego danych. Pojawia się więc ryzyko przechwycenia informacji przez osoby niepożądane np. hakerów.
W takim wypadku jednym z zabezpieczeń może być użycie VPN (ang. Virtual Private Network), czyli prywatnej wirtualnej sieci. Dzięki niej dane zostaną zaszyfrowane i przekierowane do zdalnego serwera dostawcy VPN, ukrywając IP i chroniąc tym samym tożsamość użytkownika. Najlepiej zainwestować czas i pieniądze w płatne rozwiązania od sprawdzonych firm

Podsumowanie

Nierozważne korzystanie z publicznych sieci Wi-Fi naraża użytkownika na utratę danych, szpiegowanie, zainstalowanie na urządzeniu niechcianych programów, a nawet podsłuchów tzw. ataków Man-in-the-Middle (MitM). Należy więc zadbać o odpowiednie zabezpieczenie każdego urządzenia, instalując na nim program antywirusowy i ochronę bankową. Istotnym czynnikiem jest też ustawienie silnych i odmiennych dla każdego konta haseł. Warto również zwrócić uwagę na obecność certyfikatów SSL na stronach logowania do sieci, a także rozważyć zakup VPN.