

Czy darmowe Wi-Fi w hotelu jest bezpieczne? Poradnik dla podróżujących



Planując wyjazd – niezależnie od pory roku – skupiamy się zwykle na kierunku, aktywnościach czy noclegach. Raczej niewiele osób myśli o potencjalnych zagrożeniach w sieci, a to błąd. Kiedy podróżujemy, może zdarzyć się nam np. korzystanie z publicznych sieci Wi-Fi, co niestety może narażać nas na liczne zagrożenia.



Jakie nawyki warto wdrożyć i z jakich narzędzi korzystać, by zwiększyć bezpieczeństwo online? Jak

uniknąć przykrych niespodzianek? Odpowiedzi na te pytania mogą pomóc nam uchronić się przed wieloma przykrościami, które czyhają w sieci. Nie należy ich lekceważyć. To właśnie w trakcie wyjazdów jesteśmy szczególnie narażeni na nieczne działania internetowych przestępców. Dobrze więc zadbać o odpowiednią profilaktykę, aby zawsze być o co najmniej jeden krok przed hakerami.

Bez Wi-Fi ani rusz - jak korzystamy z internetu w podróży

Korzystanie z lokalnych punktów Wi-Fi w podróży jest niemal nieodzowne. Kiedy jesteśmy w hotelu, chcemy sprawdzić nasze portale społecznościowe, pogodę na kolejny dzień, zaplanować trasę czy chociażby przejrzeć najnowsze informacje ze świata. Korzystamy też z komunikatorów internetowych, a niekiedy także z bankowości online. Wszystko to, rzecz jasna, możemy zrobić poprzez internet, ale może to wiązać się ze sporymi kosztami, które dodatkowo obciążą budżet naszej podróży.

Internet w trakcie urlopu może też służyć zwykłemu zabijaniu czasu. Czasami musimy gdzieś dojechać. Czasami siadamy w przyjemnej kawiarni tylko po to, aby poczekać na towarzysza podróży lub też na rozpoczęcie wydarzenia znajdującego się w naszym programie wyjazdu. Bez słowa przesady można stwierdzić, że korzystanie z Wi-Fi jest niemal niemożliwe do uniknięcia. Jednak wszelkie publiczne sieci dostępu do internetu oznaczają ekspozycję naszych danych na różne niebezpieczeństwa.

Zagrożenia związane z publicznymi sieciami - czego nie widać gołym okiem

Potencjalnych problemów, z jakimi może wiązać się korzystanie z publicznych sieci w trakcie podróży, jest całe mnóstwo. Wystarczy wspomnieć, że każde publiczne Wi-Fi - w hotelu, w restauracji, w pociągu, na lotnisku - jest w tym samym czasie użytkowane przez dziesiątki, a nieraz nawet setki osób. Każda z nich ma hasło dostępu. Posiadając zaś hasło, zdolny cyberprzestępca tak naprawdę bez większych trudności jest w stanie wymyślić jakieś skuteczne [oszustwo internetowe](#), które narazi na szwank nasze dane osobowe, a nieraz także pieniądze.

Statystyki są jednoznaczne: to właśnie w trakcie korzystania z publicznych Wi-Fi najczęściej dochodzi do wycieku danych, zwłaszcza jeśli nie towarzyszy nam VPN. W takich warunkach po prostu znacznie łatwiej jest namierzyć nasze IP, śledzić nasz ruch w internecie, a następnie np. uzyskać dostęp do naszych haseł.

□ [Najlepsze hotele na Zakynthos dla rodzin z dziećmi i dorosłych](#)

Jakie dane są narażone na przejęcie?

Pierwszą „ofiara” korzystania z Wi-Fi w hotelu na ogół jest IP, a więc coś w rodzaju naszego internetowego adresu. W dalszej kolejności przestępcy są jednak w stanie pozyskać o wiele dokładniejsze informacje. Należą do nich w szczególności:

- historia przeglądania internetu,
- używane przez nas sklepy online, banki, portale społecznościowe,
- hasła,
- dane osobowe,
- numery kart płatniczych,
- historia korespondencji, np. e-mail.

Jak łatwo się domyślić, takie informacje w niepowołanych rękach mogą przyczynić się do naprawde poważnych szkód. Zwłaszcza że na ogół cyberprzestępcy stosują więcej niż jedną metodę, a więc np. internetowy „podsluch” dopełniają kierunkowymi atakami phishingowymi, które, w przypadku braku ostrożności, są w stanie zainfekować nasz komputer, telefon czy tablet.

5 prostych zasad bezpiecznego korzystania z Wi-Fi podczas podróży

Czytając o zagrożeniach związanych z publicznymi sieciami Wi-Fi oraz o możliwych konsekwencjach przechwycenia wrażliwych danych, mimo wszystko nie należy popadać w panikę. Zastosowanie się do określonych zasad bezpieczeństwa powinno skutecznie uchronić nas przed zakusami internetowych przestępców. Trzeba jednak pamiętać o tym, aby do wszystkich tych zasad stosować się stale, nie pozwalając sobie nawet na moment nierozwagi.

1. Zadbaj o aktualizacje i zabezpieczenia przed wyjazdem

Zacznijmy od rzeczy najbardziej podstawowych. Przed udaniem się w podróż dokonaj pełnej aktualizacji wszystkich swoich urządzeń, łącznie z programem antywirusowym. Takie aktualizacje dla wielu osób wydają się uciążliwe, ale mają one na celu „załatanie” potencjalnych luk w bezpieczeństwie.

2. Wyłącz automatyczne łączenie z siecią Wi-Fi

Kolejna rzecz to ustawienia kart sieciowych. Być może Twój laptop lub telefon domyślnie łączą się z każdym dostępnym Wi-Fi. Koniecznie wyłącz tę opcję, jeśli nie chcesz nieświadomie narazić się na niebezpieczeństwo.

3. Korzystaj z dwuskładnikowego uwierzytelniania i trybu prywatnego

W trakcie podróży korzystaj też z dwuskładnikowego uwierzytelniania. Logowanie się za pomocą hasła często nie wystarczy, więc taki dodatkowy poziom ochrony jest szczególnie wskazany w podróży. Nie zapisuj haseł w pamięci przeglądarki i nie korzystaj z automatycznego wypełniania. Najlepiej używaj trybu prywatnego przeglądarki.

4. Łącz się tylko przez sprawdzony VPN i unikaj bankowości internetowej

Pamiętaj o tym, aby z publicznymi sieciami łączyć się wyłącznie poprzez dobry VPN. Staraj się też nie logować do bankowości elektronicznej i zawsze sprawdzaj, czy strona internetowa, z której korzystasz, posiada protokół HTTPS. Pamiętaj też, że nie każdy VPN dobrze chroni Twoją prywatność. Zwłaszcza w podróży staraj się więc korzystać tylko z usług od sprawdzonych i zweryfikowanych operatorów.

5. Wzmocnij ochronę haseł i rozważ dodatkowe zabezpieczenia bankowe

Jeśli należysz do osób, które korzystają z tego samego hasła do wszystkich kont: zmień to przed podróżą. Jeśli zapamiętanie ich sprawia Ci trudność, możesz skorzystać z menedżera haseł. Czasami warto też rozważyć tymczasową zmianę sposobu potwierdzania transakcji w bankowości elektronicznej z SMS-ów na fizyczne karty kodów jednorazowych lub token. Jest to posunięcie dość skrajne, ale z drugiej strony bardzo utrudnia ono zadanie cyberprzestępcom.

Czy VPN to dobre rozwiązanie dla turystów?

Zagrożenie różnego rodzaju formami cyberprzestępczości w podróży powinno stanowić przedmiot ogólnej wiedzy. Nawet polska policja w specjalnym opracowaniu podaje nam bazowe zasady [bezpieczeństwa w sieci](#), jakich powinniśmy przestrzegać w trakcie wakacji, urlopu czy krótkiego wypadu.

Jednym z kluczowych zagadnień jest ochrona prywatności przed działaniami przestępców. W tym zadaniu wysoce użytecznym wsparciem powinien okazać się dobry VPN. [Jak działa VPN?](#) Połączenie z internetem za pomocą wirtualnej sieci prywatnej (VPN) jest szyfrowane. Oznacza to, że nikt nie jest w stanie namierzyć nas po IP. Łączność odbywa się poprzez tunel, który jest skutecznie chroniony przed wścibskimi spojrzeniami postronnych. Nasza aktywność przebiega pod ukrytym adresem IP, nie pozostawia po sobie śladów i jest dodatkowo zabezpieczona przeciwko wszelkim formom śledzenia.

Kiedy korzystasz z sieci np. w hotelu poprzez VPN, jesteś niemal całkowicie niewidoczny. Nawet gdyby haker chciał uzyskać dostęp do Twoich danych, wymagałoby to od niego bardzo wiele wysiłku, który niekoniecznie zakończyłby się sukcesem. Z tego powodu jakościowy VPN powinien być jednym z głównych narzędzi bezpieczeństwa w sieci, jakie zabierzesz ze sobą w podróż.

Jak podróżować mądrze i bezpiecznie w erze cyfrowej?

Nie ulegaj atmosferze terroru i miej na uwadze, że każdemu zagrożeniu w sieci można skutecznie zapobiegać. Jeżeli więc w niedalekim terminie wybierasz się w podróż, weź ze sobą przede wszystkim zdrowy rozsądek oraz kilka najważniejszych zasad dotyczących bezpieczeństwa w internecie. Nie otwieraj podejrzanych linków, nie loguj się do banku w publicznych sieciach, zawsze korzystaj z dobrego Wi-Fi. Oprócz tego, uruchom uwierzytelnianie dwuetapowe i dokonaj aktualizacji systemu. To powinno wystarczyć, aby sprawnie uniknąć czyhających w podróży sieciowych niebezpieczeństw.