BEZPIECZEŃSTWO W PUBLICZNYM WI-FI [OPINIA]

Podczas wakacji często wyjeżdżamy i korzystamy z Internetu w miejscach publicznych. Niestety, nie zawsze pamiętamy, że publiczna sieć Wi-Fi może stanowić dla nas zagrożenie. Nie jest prawdą, że obecne systemy bezpieczeństwa są na tyle silne, że hakerzy nie są w stanie włamać się na nasz profil w portalu społecznościowym czy na konto w banku. Nie tylko są w stanie, ale my sami, logując się do publicznego Wi-Fi, znakomicie im to ułatwiamy. Jak uniknąć przykrych niespodzianek?

Sieć publiczna i co w niej widzi haker

Sieć publiczna to taka, która umożliwia każdemu użytkownikowi bezprzewodowy, niezabezpieczony hasłem dostęp do Internetu. Haker, zalogowany do takiej sieci, posługuje się tzw. snifferami. Są to programy przeznaczone do śledzenia ruchu w sieci i umożliwiające przeglądanie zawartości przesyłanych pakietów danych. Znajdują się w nich adresy IP odwiedzanych przez nas stron i w związku z czym haker może podążać naszym śladem. Szczególnie niebezpieczne jest logowanie się do kont nieszyfrowanych (bez szyfrowania SSL). W przypadku np. nieszyfrowania transmisji danych przez pocztę, nasze wiadomości mogą zostać przechwycone i odczytane. Pliki tekstowe są najłatwiejsze do odczytania, ale wprawny cyberwłamywacz poradzi sobie z każdym plikiem, także graficznym i zarchiwizowanym. Jest to kwestia bardziej zaawansowanego snippera.

Wszystko to nie oznacza jednak, że każdorazowe korzystanie z publicznego Wi-Fi zakończy się cyberatakiem i kradzieżą naszych danych lub zainfekowaniem naszego urządzenia. Istnieją sposoby zabezpieczające przed przykrymi konsekwencjami surfowania w Internecie poza domem.

Serwisy internetowe

Z zasady nie należy logować się z sieci publicznej do jakichkolwiek serwisów. Wiąże się to bowiem z koniecznością podania swoich danych. Różne serwisy wymagają do zalogowania różnych danych, w tym imienia, nazwiska, daty urodzenia, numeru PESEL, adresu e-mail, numeru telefonu. Serwisy bankowe mogą żądać dodatkowo danych dotyczących rachunku. Jest to nie lada gratka dla hakera, który może – przez naszą niefrasobliwość – wyczyścić nasze konto bankowe. Zatem nawet w nagłej sytuacji nie powinniśmy np. sprawdzać stanu konta bankowego, korzystając z darmowej sieci Wi-Fi. Znacznie bezpieczniej jest użyć transmisji komórkowej.

Podczas łączenia się z Internetem za pomocą publicznego Wi-Fi trzeba też w celach bezpieczeństwa wyłączyć opcję udostępniania plików. Można to zrobić za pomocą jednego kliknięcia w panelu sterowania, jak również, przy połączeniu z nową siecią publiczną, wybrać opcję „publiczna”.

VPN i SSL

Wirtualna sieć prywatna (Virtual Private Network, VPN) umożliwia połączenie z głównym serwerem, który może się znajdować gdziekolwiek, w każdym miejscu na świecie, i w ten sposób korzystanie z

zasobów Internetu. Jest to rozwiązanie dość kosztowne, ale gwarantuje zachowanie całkowitej anonimowości i bezpieczeństwo w sieci.

Jeżeli nie mamy możliwości zainwestowania w VPN, odwiedzajmy jedynie te strony, które posiadają certyfikat SSL (Secure Socket Layer). Adres strony zabezpieczonej tym certyfikatem rozpoczyna się od https://, a obok niego zwykle znajduje się zielona ikonka kłódki. Tak oznaczone są wszystkie strony serwisów bankowych – wymagają tego przepisy. Jest to certyfikat o najwyższym stopniu bezpieczeństwa. Adresy stron niezabezpieczonych rozpoczynają się od http:// i niekiedy obok znajduje się słowny komunikat „niezabezpieczona". Takich unikamy.

Internet komórkowy bez limitu

Zazwyczaj powodem korzystania przez posiadaczy smartfonów z publicznych sieci Wi-Fi jest darmowy dostęp, umożliwiający surfowanie w Internecie bez obaw o wysoki rachunek telefoniczny. Tymczasem urządzenia pracujące w środowisku Android są najczęściej atakowane. Rozwiązaniem jest wykupienie u swojego operatora komórkowego abonamentu z opcją nieograniczonej transmisji danych. Nie będzie wówczas potrzeby logowania się do Wi-Fi. Mając Internet bez limitu można utworzyć ze swojego smartfona lub tabletu osobisty hotspot. Takie rozwiązanie jest niewiele droższe od abonamentu z limitem gigabajtów, a na pewno urządzenie będzie bezpieczne.

Wtyczka zabezpieczająca

Użytkownik przeglądarek Mozilla Firefox, Opera i Google Chrome, używający laptopa w miejscach publicznych (hotele, restauracje, kawiarnie), ma możliwość zainstalowania w każdej z tych przeglądarek wtyczki zabezpieczającej dostęp do sieci. Można taką wtyczkę pobrać za darmo wcześniej z Internetu. Jest ich sporo, a wśród użytkowników dobrą opinią cieszy się np. HTTPS Everywhere (producent Electronic Frontier Foundation). Zapewnia ona domyślnie bezpieczne połączenie z najpopularniejszymi serwisami, jak Amazon, E-Bay czy Yahoo, ale można również ręcznie dodać własne zasoby.

Tekst sponsorowany

Autor: Konrad Bielawski, specjalista ds. odzyskiwania danych w firmie DATA Lab. Informatyk z wykształcenia. Pasjonat sportów motorowych i brytyjskiego kina.