Ponad 1/3 Europejczyków nie używa ochrony podczas korzystania z hotspotów Wi-Fi

Kategoria: Aktualności
Opublikowano: piątek, 18, październik 2013 10:01
Rafał Rudka

Chyba każdy lubi oderwać się na moment od rzeczywistości, gdy ma w zasięgu jakiś hotspot Wi-Fi. Ale łączenie się z internetem w takim wydaniu może nieść ze sobą ukryte zagrożenia. Mimo to ponad jedna trzecia użytkowników z Europy nie stosuje żadnych dodatkowych środków ochrony podczas logowania się przy wykorzystaniu publicznych sieci Wi-Fi. Tak wynika z badania "Kaspersky Consumer Security Risks" przeprowadzonego przez Kaspersky Lab oraz B2B International latem 2013 roku.

Obecnie bardzo łatwo jest być online - poza sieciami komórkowymi i dostępem szerokopasmowym istnieją również hotspoty, dzięki którym można połączyć komputer czy urządzenie mobilne z internetem.

Jednak wiele z takich punktów dostępowych nie zapewnia ochrony surfującym online, którzy są albo nieświadomi, albo obojętni na potencjalne problemy, jakie mogą z tego wyniknąć. W badaniu Kaspersky Lab 34% Europejczyków przyznało, że nie stosuje żadnych specjalnych środków bezpieczeństwa podczas korzystania z hotspotów, a 17% używa takich połączeń do obsługi bankowości i zakupów online. Jedynie 15% respondentów z Europy poświęciło swój czas na sprawdzenie metody szyfrowania. Czy stosowanie takich dodatkowych środków ostrożności ma sens podczas korzystania z publicznych sieci Wi-Fi, czy jest to raczej przesada?

Użytkownik, strona internetowa i...

Jak wiadomo, ostrożności nigdy za wiele. Nigdy nie wiadomo, co robi osoba z laptopem przy stoliku obok. Być może tak jak my sprawdza swoją pocztę lub czatuje z przyjaciółmi. Ale być może szpieguje działania w internecie każdego, kto znajduje się w zasięgu. Umożliwia to tzw. atak Man-in-the-Middle. Każdy punt dostępowy jest jak okno do internetu dla wszystkich podłączonych urządzeń. Każde żądanie najpierw przechodzi przez punkt dostępowy, a następnie dociera do stron, które użytkownik chce odwiedzić. Jeżeli komunikacja między użytkownikiem a punktem dostępowym nie będzie szyfrowana, cyberprzestępca z łatwością może znaleźć się w samym środku (stąd nazwa ataku - Man-in-the-Middle) i przechwycić wszystkie wprowadzanie dane. Mogą to być na przykład dane wysyłane do banku lub sklepu internetowego. Co więcej, tego typu atak można przeprowadzić nawet wtedy, gdy hotspot jest chroniony hasłem i ustanowione jest bezpieczne połączenie https między żądaną stroną a przeglądarką.

Jakimi danymi interesują się cyberprzestępcy? Takimi, z których mogą mieć pożytek - najczęściej danymi logowania i hasłami do poczty elektronicznej, bankowości, systemów płatności i portali społecznościowych.

Źródło: Kaspersky Lab