

Oddasz swe dziecko za darmowy dostęp do Wi-Fi?

7 października 2014

Z eksperymentu, który F-Secure przeprowadził wspólnie z Europolem, wynika, że konsumenci beztrąsko narażają swoje dane osobiste i lekkomyślnie akceptują absurdalne warunki korzystania z sieci.

Niezależne badanie, wspierane przez Europol, zostało przeprowadzone w imieniu F-Secure przez angielski Cyber Security Research Institute oraz SySS, niemiecką firmę zajmującą się testami penetracyjnymi. W ramach projektu zbudowano przenośny router Wi-Fi z komponentów wartych ok. 200 euro, który nie wymagał zaawansowanej znajomości zagadnień IT, aby go obsługiwać. Badacze ulokowali urządzenie w tych rejonach Londynu, gdzie odbywają się ważne wydarzenia polityczne i ekonomiczne. Następnie obserwowali, jak ludzie łączą się z siecią.

W ciągu 30 minut do hotspota podłączyło się 250 urządzeń, większość z nich najpewniej automatycznie i bez świadomości użytkowników. 33 osoby aktywnie korzystały z sieci, wyszukując witryny internetowe i wysyłając pliki oraz e-maile. Przechwycono (i błyskawicznie usunięto) 32 MB ruchu sieciowego.

Przez krótki czas badacze wyświetlali użytkownikom stronę z warunkami korzystania z sieci, która musiała być zaakceptowana, aby można było skorzystać z hotspota. Warunki zawierały niedorzeczny zapis, w którym użytkownik w zamian za dostęp do sieci zobowiązywał się do oddania pierwotnego dziecka lub ukochanego zwierzątka. W sumie na warunki zgodziło się 6 osób, zanim strona została wyłączona.

Zapis ten wyraźnie pokazuje, jak mało uwagi użytkownicy poświęcają takim dokumentom, które zazwyczaj są zbyt długie i

napisane nieprzystępnym językiem. W Dzienniku Internautów kilkakrotnie sygnalizowaliśmy już istnienie tego problemu.

Generalnie z eksperymentu wynika, że konsumenci lekkomyślnie korzystają z otwartych hotspotów, nie myśląc o ochronie swojej prywatności. Rozwiązanie? Można trzymać się z daleka od publicznych sieci Wi-Fi albo korzystać z odpowiednich zabezpieczeń, które sprawiają, że połączenie będzie niewidoczne, a dane niemożliwe do odczytania dzięki silnemu szyfrowaniu. Poniżej można zapoznać się z pełnym raportem z badania.

Źródło: [Dziennik Internautów](#)