Jak korzystać z sieci Wi-Fi?

Kategoria: Styl życia
Opublikowano: poniedziałek, 28, luty 2011 00:00
Odsłony: 2874

Portal eGospodarka.pl podaje, że na świecie jest około 750 000 hotspotów, z których codziennie korzystają miliony ludzi. Za specjalistami z firmy ESET wskazuje, że potrzeba dostępu do informacji i sieci jest obecnie tak ogromna, że coraz więcej użytkowników stara się podłączyć do pierwszej napotkanej i najlepiej niezabezpieczonej sieci Wi-Fi - bardzo często do sieci sąsiada.

Pożyczanie niezabezpieczonej sieci dla niektórych wydaje się, mimo oczywistego nadużycia, czymś naturalnym i zupełnie bezpiecznym. W rzeczywistości niezabezpieczone Wi-Fi to zagrożenie zarówno dla dostarczającego takie połączenie z siecią, jak i dla osób korzystających z sieci. ESET przypomina, że za sprawą takich narzędzi jak Firesheep osoby niepowołane mogą w łatwy sposób uzyskać dostęp do połączenia internetowego i przechwytywać wszystkie dane, które użytkownik wprowadza podczas korzystania z sieci. Należy przy tym pamiętać, że Firesheep nie wymaga dużej wiedzy i może z niego skorzystać właściwie każdy internauta. O skali zagrożenia świadczyć może fakt, że od chwili pojawienia się tego niebezpiecznego rozszerzenia dla Firefoxa zostało ono pobrane z sieci ponad milion razy.

"Dzięki Firesheep prawie każdy może przejąć nasze konto na Facebooku, Twitterze czy innym serwisie społecznościowym" – mówi Randy Abrams, dyrektor ds. edukacji technicznej firmy ESET, producenta rozwiązań antywirusowych. - *"Niemal wszyscy mają umiejętności wystarczające do skorzystania z Firesheepa i zabawienia się we 'wścibskiego' sąsiada"* – dodaje Abrams.

Pozostawienie domowej sieci Wi-Fi bez jakiegokolwiek zabezpieczenia specjaliści z firmy ESET przyrównują do przekazania nieznajomemu kluczy do własnego domu. I choć otwartość i życzliwość są cechami pożądanymi, to jednak w wypadku sieci Wi-Fi zalecane jest postawienie na zasadę ograniczonego zaufania i skorzystanie z opcji ochrony swojej sieci protokołem WPA2.

Brak dbałości o odpowiednie zabezpieczenie domowej sieci Wi-Fi to według analityków zagrożeń firmy ESET jeden problem. Drugi dotyczy coraz częstszego korzystania z sieci bezprzewodowych za pośrednictwem publicznych hotspotów. Oferują je na przykład lotniska czy popularne sieci kawiarni i restauracji. Aby ułatwić swoim klientom dostęp do Internetu, nie wprowadzają one żadnych zabezpieczeń swoich hotspotów. Użytkownicy ulegają w takich miejscach złudnemu poczuciu bezpieczeństwa, które hipotetycznie zapewnia im międzynarodowa korporacja, oferująca bezpłatny dostęp do sieci. W rzeczywistości istnieje jednak ryzyko zainfekowania komputera wirusem lub utraty cennych danych. Dlatego w takich miejscach korzystanie z Wi-Fi powinniśmy ograniczyć do przeglądania serwisów informacyjnych.

Trzy kroki do bezpiecznego korzystania z Wi-Fi według firmy ESET:

1. Dla sieci domowej należy włączyć w ustawieniach swojego routera protokół WPA2 (Wi-Fi Protected Access® 2), który zapewni należytą ochronę połączenia z Internetem. Należy przy tym pamiętać, że o faktycznym poziomie bezpieczeństwa domowej sieci Wi-Fi decyduje jej najsłabszy element np. starszy laptop, nie obsługujący WPA2.
2. Dostęp do własnej sieci i jej ustawień należy zabezpieczyć silnym hasłem, które powinno składać się z co najmniej 8 znaków. Powinno również zawierać duże i małe litery, cyfry oraz znaki specjalne (!@#$% itd.). „JanKowalski" czy „Kasia18" to przykłady tego, jak hasło wyglądać nie powinno.
3. Korzystając z publicznej sieci Wi-Fi, należy kierować się przede wszystkim rozsądkiem.

Zagrożenia nie stanowi przeglądanie za pośrednictwem takiej sieci stron internetowych, czytanie najnowszych doniesień prasowych czy przeszukiwanie sklepów internetowych. Ryzyko pojawia się wtedy, gdy dana strona wymaga logowania lub podawania prywatnych informacji. Takie serwisy lepiej odwiedzać wyłącznie za pośrednictwem bezpiecznego, szyfrowanego połączenia.

Źródło: www.eset.pl / eGospodarka.pl / fot. www.morguefile.com