**2 proste sposoby na zabezpieczenie domowej sieci Wi-Fi**

**Kiedy na biurku pojawia się nowy router, większości osób wydaje się, że konfiguracja sieci jest już zakończona. Niestety, nawet po wizycie montera konieczne jest samodzielne wprowadzenie zmian zwiększających jej bezpieczeństwo.**

**Domyślnie nie znaczy dobrze**

W większości przypadków taki router działa na ustawieniach domyślnych. Hasło do niego można poznać w kilka sekund, bo... jest takie samo dla wszystkich routerów! Pierwszym krokiem jest więc jego zmiana w panelu zarządzania (strona 192.168.0.1).

Również w panelu zarządzania są informacje o szyfrowaniu połączenia. Używane standardy to WEP, WPA oraz WPA2 (ten ostatni jest najlepszy, warto go ustawić). Bezpieczeństwo zwiększy również instalacja firewalla (zapory ogniowej) broniącej dostępu z zewnątrz.

**Niespodziewani goście...**

Te dwie zmiany to absolutne podstawy domowego bezpieczeństwa, które każdy powinien wykonać zanim zacznie korzystać z sieci. To jednak nie koniec niespodzianek w domowym WiFi. Niektóre firmy umożliwiają podłączanie się innych użytkowników w ramach otwartego dostępu. W efekcie może się okazać, że ktoś inny również korzysta z naszego łącza... Informacje o polityce w tym zakresie będą zawarte w umowie z providerem.

„Zabezpieczenie sieci domowej to kilka prostych czynności, które zagwarantują nam spokój i bezpieczeństwo” - mówi Arkadiusz Zakrzewski, dyrektor pomocy technicznej AVG w Polsce. „Warto wykonać je od razu po instalacji routera by uniknąć włamań i kradzieży poufnych danych”.