**Czy można zhakować.... lodówkę?**

**Urządzenia mobilne ze stałym dostępem do Internetu nikogo już nie zaskakują, ale lodówka czy pralka podłączona do Wi-Fi to nadal coś nowego. Urządzenia takie cieszą się coraz większą popularnością.**

Czy można zhakować… lodówkę?

Urządzenia mobilne ze stałym dostępem do Internetu nikogo już nie zaskakują, ale lodówka czy pralka podłączona do Wi-Fi to nadal coś nowego. Urządzenia takie cieszą się coraz większą popularnością.

**Internet of Things**

Zjawisko gromadzenia i wymiany danych przez różne przedmioty za pośrednictwem sieci komputerowej określamy pojęciem “**Internet of Things**” (IoT). Pojęcia to określa jedną z możliwych wizji niedalekiej przyszłości, w której nawet najprostsze urządzenia są połączone z Internetem i bez przerwy przesyłają dane. Zaczynając od smart-watchy, przez inteligentne lodówki i kończąc na inteligentnych wagach, które znajdą dla Ciebie odpowiednią dietę w Internecie na podstawie Twojej wagi.

**Czy można włamać się do pralki lub lodówki?**

Na zachodzie inteligentne telewizory, lodówki, pralki cieszą się coraz większą popularnością. Jak każdą rzecz elektroniczną – również te można zhakować, tym bardziej, że bardzo szerokie grono producentów kwestie bezpieczeństwa produkowanych przez siebie urządzeń zdaje się mocno lekceważyć.

Warto pamiętać, że wyciek danych z takich urządzeń może być równie groźny, jak włamanie do komputera czy smartfona.

**Router WiFi – klucz do bezpieczeństwa**

*- Ponieważ konfiguracja każdego z inteligentnych urządzeń może być bardzo trudna i skomplikowana, sugeruję, by zacząć od kluczowej rzeczy, czyli odpowiednich ustawień domowego routera Wi-Fi, który może stać się pierwszym, potencjalnym celem ataku* – przestrzega Arkadiusz Zakrzewski, specjalista pomocy technicznej antywirusa AVG – *Warto pamiętać o trzech prostych, ważnych sprawach: Po pierwsze zmień dane logowania (login i hasło) z domyślnych ustawień fabrycznych routera na własne, po drugie skonfiguruj listę urządzeń, które będą miały dostęp i będą mogły łączyć się z Twoją siecią, a po trzecie upewnij się, że zapora firewall w Twoim urządzeniu sieciowym działa i chroni Cię przed atakami z zewnątrz.*