Cybersecurity experts say device makers have 'duty to keep users safe' from hacking

March 20 2018, by Caroline Brogan

Credit: Imperial College London

Well-connected smart devices at home and in healthcare are currently vulnerable to hacking, warn two new reports.

The reports, led by Professor Nick Jennings, artificial intelligence expert and Vice Provost at Imperial College London, were published by the Royal Academy of Engineering.

The cyber security experts who authored the reports, said although taking personal responsibility for safety is important, many smart device users don't necessarily know the best way to do so.

Manufacturers and the government therefore have a greater duty to protect device users from hacking, and the burden of cyber security should not lie solely with device users, the reports said.

Genuine harm

The authors highlighted several ways hackers could harm people and their homes.

Pacemakers, which regulate heartbeat, use wireless signals to give doctors medical data without surgery. A hacker could take control and alter the signal or switch it off completely, with major health implications.

Other vulnerable devices include MRI machines and medical pumps like those used to treat diabetes – potentially allowing remotely based wrongdoers to cause fatal overdoses.

In the home, smart home devices such as smart thermostats learn home occupiers' schedules to know when to turn on and off. In the wrong hands, this could tell burglars when the home will be empty.

Voice activated light bulbs could be used to spy on conversations, and smart plug sockets could be turned on remotely, potentially causing fires.

Professor Jennings warned: "If the government and manufacturers

don't keep on top of smart technology, wrongdoers could cause people genuine harm, and even death in extreme circumstances."

How can manufacturers protect us?
The reports suggest using a kitemark-style system to guarantee security to users from hacking. This would also act as a promise that the software will be updated regularly as and when threats change.

They also recommend that governments impose regulations on manufacturers to ensure legal compliance with modern cyber security standards. The authors also say good cyber security practices, or cyber hygiene, should also be taught from primary school.

How can we keep ourselves safe from hacking?
Professor Jennings and colleagues recommend practicing good cyber hygiene, which includes turning off smart assistants when they're not in use, keeping separate 'Home' and 'Guest' WiFi connections, and ensuring any updates are regularly installed.

They said: "Internet enabled devices are and can be hugely beneficial, particularly to the elderly or disabled. However, we are now in a transitional period where manufacturers must take responsibility, or be made to by the government."

"Internet of Things: realising the potential of a trusted smart world", by PETRAS & the Royal Academy of Engineering.

More information: Cyber safety and resilience: www.raeng.org.uk/publications/ … afety-and-resilience

Provided by Imperial College London