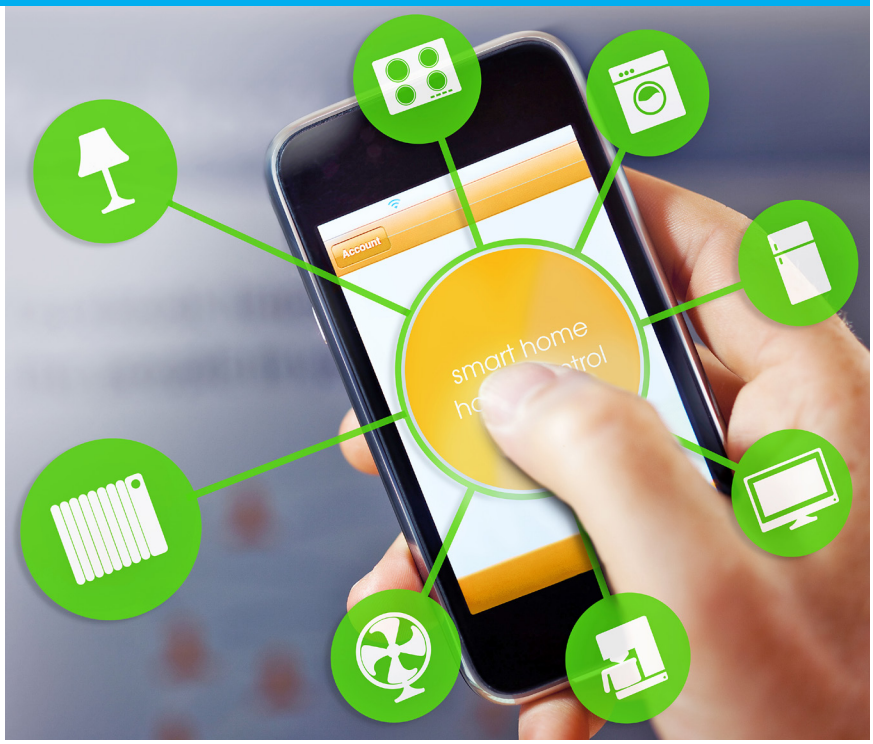
Rethinking Security in the Internet of Things Era

"Alexa, wake me at 7 in the morning."

While consumers love that connected devices make everyday tasks easy, they may not enjoy the potential fraud risks that come with it. The growing number of connected "things" in consumers' lives means the threat from unsecured devices grows as well.



By their very nature, Internet of Things (IoT) devices are easy for hackers to find. In fact, there is an entire search engine built specifically to find these gadgets. Called Shodan, it allows users to determine which devices are connected to the Internet, where they are located and who is using them. One researcher, curious to see how long it would take for a hacker to find his smart toaster, discovered an attacker on his device less than a day after plugging it in.

Fortunately, there are a number of measures consumers and community banks alike can take to keep their IoT technology secure. They include:

- ✔ **Securing devices in layers** – Using multiple factors for authentication, where one of the factors is biometric in nature, is gaining traction as a best practice.
- ✔ **Changing passwords and installing updates** – It's increasingly important for device owners to change the default passwords that come with their IoT devices. Just as important is installing device updates, which often contain patches for known security vulnerabilities, as they become available.
- ✔ **Thinking beyond the device** – The IoT dictates we think about the security not only of the gadget, but also of the apps loaded to it, the network powering it, the servers connected to it and the technology driving it (e.g., cloud-based solutions).
- ✔ **Remember the basics** – Connected devices are only as safe as the router and/or WiFi network they're attached to. IoT technology users have to practice basic WiFi and network connection security, such as good passwords, solid encryption and frequent software updates..

A connected world in which devices and artificial intelligence make everyday decisions for consumers is within view – and that extends to financial transactions and banking choices. Community banks are right to explore the technology's potential to improve experiences and deepen relations – so long as that exploration includes the security and controls consumers expect.

Source: Ashley McAlpine – Cbinsight.com