Security Risks with Smart Homes and IOT

Everyday objects that are connected to the Internet — widely known as the Internet of Things (IOT) — can help residents with a variety of tasks throughout their home. IOT devices include certain security systems, door locks, lights, garage door openers, sprinkler systems, thermostats, pet feeders, and baby monitors, to name a few. While the usefulness and efficiency of the IOT devices may be well-known, something that is not highlighted in the marketing of this technology is that every device that is added to the home Wi-Fi network opens up potential risks. Following smart security practices can help protect both property and personal information.

While IOT devices are intended to make life easier, the security risks that arise can be complicated. Smart devices may have limited security, so it is important for individuals to take precautions with their home network. A misconfigured or unpatched device can result in a network breach, or an instance resulting in unauthorized access to data, applications, or services. A network breach can make breaking into devices and data snooping possible. Once a hacker has access to one device on the network, it can be used as a gateway to other devices on the same network, leaving the owner vulnerable to physical and informational risks. For example, if hackers get into a network, they could potentially unlock doors remotely or gain access to account logins or sensitive information through the compromised device.

Many home IOT systems have an app, which could be breached if hackers get access to phones or tablets. Even personal devices that are connected to the home Wi-Fi network, such as fitness bands and smart watches, are also possible gateways for criminals. Fitness bands can provide information about the homeowner's location and daily patterns, enabling a burglar to plan an attack when the property owner is not home.

There are several "best practices" to secure home networks and devices. The following tips can help increase security:

- **Secure the network.** Home wireless networks should be secured by Wi-Fi Protected Access II (WPA2) as well as a firewall or secure router.

- **Use multiple networks.** Using multiple networks that do not communicate with each other will help protect personal information. Allowing others to access the networks puts devices at risk. For example, a three-network model could be very effective, with one network for the homeowner's computers, phones, and tablets, a separate network for guest usage, and a third designated for IOT devices. Also, consider creating a network ID that is not visible to Wi-Fi users as an extra layer of security. For visible networks, change the default username, and be sure that the name of the Wi-Fi network does not provide any personal information—even your name. Weigh the benefits and risks of connecting each smart device to the network.

- **Check the security on all devices.** Some manufacturers provide better security than others, so be sure to research the security offered on all devices (including routers) when purchasing. Individuals should check the default settings and services on all devices to determine which features are appropriate for their usage and to disable ones that are not necessary. It is also wise to have a strong passcode on your mobile device in order to protect smart devices.

- **Be diligent about updates.** Manufacturers regularly post firmware updates on their websites and apps. It is very important to regularly update IOT devices to ensure the highest level of security.

- **Plan Ahead.** Understand how a power outage will affect some of your IOT devices such as door locks, security systems and security cameras. Make sure that key devices have a backup mechanism or a power backup.

- **Create complex passwords.** Be sure to change the default usernames and passwords for all IOT devices. Each device should also have its own unique password that contains a variety of letters, numbers and symbols. It is recommended to change these passwords regularly. A password manager can be helpful for storing all passwords. Use multifactor or two-factor authentication when available to protect IOT devices and accounts.

- **Keep current location private.** Posting whereabouts on social media alerts potential intruders that the home is vacant. Be sure to check settings on accounts and make sure that locations are not made public.

As more home devices are added to the IOT, the need for security continues to increase. To discuss concerns, potential risks and smart security practices, contact your Anchin Relationship Partner or a member of Anchin Private Client at 212.840.3456 or info@anchin.com.

ANCHIN
Private Client

Ehud "Udi" Sadan, CPA, CGMA
Leader
ehud.sadan@anchin.com

Jared Feldman, CPA
Leader
jared.feldman@anchin.com

1375 Broadway, New York, NY 10018 • 212.840.3456 • www.anchinprivateclient.com