CYBER SAFETY

Keeping your Internet of Things (IoT) and smart devices secure*

"Internet of things (IoT)" devices are rapidly connecting our homes, businesses, and cities to the internet to improve efficiency, communication and convenience. IoT can include smart devices that help control lighting, security cameras, climate and entertainment in a home, along with personal items such as mobile devices, fitness trackers, gaming consoles, "nanny cams," baby monitors and digital assistants. Even some of our home appliances such as refrigerators and dishwashers can come outfitted with Wi-Fi.

The added convenience of connected devices can also make a home an easy target for cyber criminals. Poorly designed and outdated connected devices, and their associated accounts, can allow unauthorized access to your home network along with all the devices and information on it. Additionally, most smart devices are collecting usage data, and manufacturers may sell or share information with third parties. Your fitness and health data, home entertainment and energy usage, voice recordings, the entertainment you watch and sites you access can all be used to build a profile on you and your family.

Smart and IoT devices that can put you and your family at risk, if not set up securely, include:

- Smart device apps configured to share data
- Digital assistants (e.g., Alexa, Google, etc.)
- Gaming consoles
- Wi-Fi printers
- Personal fitness trackers and equipment
- Webcams, Nanny cams, and security cameras
- Climate, lighting, and home security controls
- Home appliances with Wi-Fi access (e.g., refrigerators, microwaves)
- Home entertainment systems with Wi-Fi access (e.g., TVs, smart sound systems)

Consider the following best practices to ensure that your smart devices are set up securely, and you are aware of the information being collected and shared, or make the necessary adjustments.

Best practices to secure your personal and home smart devices:

- **Ensure that your smart device is from a reputable manufacturer that provides the ability to set a secure password, turn off features** not needed or wanted, and **offers control of how data is collected** on the device.
- **Keep your smart devices connected on a separate network** from the one on which you handle sensitive transactions, work remotely, etc. Devices like gaming consoles, home entertainment systems, and security cameras should not be on the same network as the devices on which you do your financial transactions, as cybercriminals can potentially compromise a smart device not secured properly.

(continued)

Keeping your Internet of Things (IoT) and smart devices secure*

- **Set up smart devices with an email login account that is not also used for financial and other sensitive accounts.**
- **Change the default passwords of your IoT and smart devices. Set them up with passwords that are unique** (not the same password for other important accounts) **and complex,** using numbers, special characters, and upper and lower-case letters. **Consider implementing a reputable password manager** to help securely manage your usernames and passwords.

  Implement two-factor authentication (2FA), if offered, to increase the security of your IoT device accounts.
- **Update your smart devices and related control apps to the latest software versions,** which often contain important fixes to remove known bugs or vulnerabilities. If offered, turn on the auto-update feature.
- **Consider the privacy settings** and the type of data your devices are collecting, how it is being used, and with whom it may be shared or sold. Home energy usage, entertainment selections, health data, and voice recordings may all be stored in your accounts. **Limit or disable features you don't use** via the app used to monitor or control the device. Consider contacting the manufacturer, or review the device's support documentation, often published online, to better understand the how your data might be used, shared, or sold.
- **Turn off Wi-Fi/Bluetooth when not in use,** as these can also be leveraged to gain access to an IoT or smart device.
- **Protect your video-capable devices with a webcam cover,** to ensure the view is blocked when the camera is not in use, when you are not attending a video meeting or when using your fitness equipment.

*This document is provided for educational and informational purposes only and is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The information provided in this document is intended to help clients protect themselves from cyber fraud. It does not provide a comprehensive listing of all types of cyber fraud activities and it does not identify all types of cybersecurity best practices. You, your company or organization is responsible for determining how to best protect itself against cyber fraud activities and for selecting the cybersecurity best practices that are most appropriate to your needs. Any reproduction, retransmission, dissemination or other unauthorized use of this document or the information contained herein by any person or entity is strictly prohibited.