

Be cyber secure: IoT



Thermostats, doorbells and refrigerators with internet connectivity are all part of a network known as the Internet of Things (IoT). Any device connected to the internet is a potential target for cyber threats.



Once a device is compromised, criminals may:

- **Take advantage of the permissions you give your device** to make online purchases in your name, listen to your conversations using a device microphone or collect data about your device usage.
- **Compromise** other devices connected to your network.
- **Access or deactivate your networks or devices** (such as home alarms) in order to protect your personal information.
- **Launch attacks** on other connected endpoints.



Here are some tips that can help protect you from potential IoT cyber incidents or prevent you from taking action that could be costly:

- **Create strong, unique passwords** of at least eight characters for each of your accounts. If you reuse passwords, a criminal who discovers one of them could use it to access another device or account.
- **Change the manufacturer's default settings.** Connected devices often come with default usernames and passwords that are published on internet. Change them to something unique as soon as you can.
- **Update your devices and applications regularly.** If a connected device or its application has an auto-update feature, turn it on. This often requires only a few clicks to set up.
- **Check your privacy settings.** You may be sharing information through your device or its applications. Review your privacy settings to see if you are unintentionally sending information to social media accounts, for example.
- **Turn encryption on.** Some devices let you use encrypted communications, but the setting isn't always turned on by default.
- **Make your home network more secure.** Turn off any internet-enabled features on your device when it is not in use. This will limit its exposure to online threats.
- **Report** the incident to local law enforcement immediately and contact your bank.

Visit www.bankofamerica.com/security to learn how to help protect yourself and those closest to you.

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.