BANK OF AMERICA

CYBER SECURITY

Be Cyber Secure: Internet of Things (IoT)

Tips for maintaining security in the age of connected devices

If you have installed a thermostat, doorbell or refrigerator with internet connectivity, you have accessed the rapidly expanding world of connected devices, also known as the Internet of Things, or IoT. While these devices allow you to remotely monitor conditions within your home, their convenience also carries risk. Any device connected to the internet is a potential target for cyber threats.

How to Protect Yourself

Be proactive:

- **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.

If you suspect you've been targeted:

- **Disconnect devices** from the internet to prevent cyber criminals from controlling them.
- **Scan devices and networks** using the latest security protection tools to find any infected files or malicious programs.
- **Apply any available sofware patches,** firmware or security patches after scanning and cleaning your system. Reset or reboot devices, if necessary.
- **Change all passwords** associated with the affected accounts.
- **Recover corrupted files** from backups whenever possible.
- **Call law enforcement** and file reports with the relevant local authorities if you suspect sensitive information has been stolen or financial loss has occurred.
- **Contact a cyber security expert** if more assistance is necessary.

The IoT Landscape, Measured

29 billion

Estimated number of network connected devices by 2023[1]

6.2 billion

Estimated global devices in use in 2021[2]

80%

Percent of hacking-related breaches of devices caused by weak or compromised passwords.[3]

[1] Cisco Annual Internet Report (2018-2023), updated March 9, 2020.

[2] Gartner Gartner Forecasts Global Devices..., 2021.

[3] Verizon Data Breach Investigation Report, 2019.

Be Cyber Secure: Internet of Things (IoT)

How to Protect Yourself (*Continued*)

Be proactive:

- **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.

If you suspect you've been targeted:

- **Document everything** about the incident. The more information you have, the better armed you will be to assist an investigation, and the better prepared you will be against future incidents.

Why It's Important

IoT technology and devices bring more intelligence and convenience to daily and working life. But each device is potentially an open door to your networks and systems that a cyber criminal may be able to exploit.

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.
- **Access or deactivate your networks or devices** (such as home alarms) in order to harvest your personal information.
- **Launch attacks** on other connected endpoints.

Due diligence and effective cyber security practices, however, can minimize the risks posed by these threats without sacrificing the best features of your connected devices.

Global Information Security at Bank of America

The GIS team is made up of information security professionals staffing multiple security operations centers across the globe who work 24/7 to keep data and information safe.

For more information, go to: www.bankofamerica.com/privacy/overview.go

3573242