BANK OF AMERICA

CYBER SECURITY

Be Cyber Secure: Protect Your Home Network

Tips to protect yourself, and how to respond if you think you have been targeted.

Wireless networks — and the other technologies that make up the Internet of Things (IoT), like voice assistants, smart appliances and other connected devices, including phones — are turning most homes into digital hubs. While these devices can increase productivity and convenience, they can also carry risks, leaving your home network susceptible to cyber threats. You can help protect your home network and devices by following these best practices:

How to Protect Yourself

Be proactive:

- **Strengthen your home network.** Change your router's default password and your network name (service set identifier, or SSID), and use an SSID that doesn't contain your address, name or other things that are easy to identify.
- **Use the highest security settings** on your router and turn on encryption to make it hard for cyber criminals to get access.
- **Update all operating systems, apps and security software** — including antivirus programs and firewalls. Regularly reboot your devices to remove potentially harmful files or programs.
- **Turn off your network** when you're away for an extended period of time.
- **Do not reply to emails or texts,** or click on links from unknown senders — they may be phishing attempts.
- **Avoid websites that aren't secure** and don't download files or apps from unfamiliar sites.

If you suspect you've been targeted:

- **Don't delay.** Act quickly if you think you are the target of an identity theft or a phishing scam.
- **Call your bank** and freeze financial accounts that may be affected, and inform credit bureaus.
- **Change all passwords** that cyber criminals may have stolen.
- **Call the police** to report if your device or information has been stolen.
- **File reports** with the relevant local law enforcement officials.
- **Document everything** about the event. The more information you have, the better armed you will be to assist an investigation by your company, your bank and law enforcement officials, and the better prepared you will be against future events.

The Growing Threat, Measured

17

Average number of connected devices in US households[1]

467,361

Number of cyber security complaints reported to IC3 with losses exceeding $3.5 billion. [2]

20 *to* 30 billion

Number of connected devices expected to be in circulation by 2020, up from 10 to 15 billion in 2015.[3]

[1] https://enterprise.verizon.com/verizon-insights-lab/dbir/tool/

[2] https://pdf.ic3.gov/2017_IC3Report.pdf

[3] https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age

Be Cyber Secure: Protect Your Home Network

BANK OF AMERICA

Why It's Important

The more computers, phones, wearable and smart devices that are connected to your home network, the more possible ways cyber criminals can gain access to your confidential data.

Default router settings are often easy to obtain, and cyber criminals will exploit this to gain access to your network. Once on your network, they can gain access to all of your accounts and information.

With your passwords and access to your social and financial accounts, cyber criminals can:

- **Transfer funds** out of your accounts or charge purchases to them.
- **Steal your identity** and claim your tax refund or government benefits.
- **Create a fake identity** with some of your information and use it to open a new credit card or apply for a loan.
- **Phish** using your email address or social media accounts to reach out to your contacts and convince them to share confidential information.
- **Gain access to your company's network** when connecting via your home Wi-Fi.

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