BANK OF AMERICA

CYBER SECURITY

Be Cyber Secure: Connecting on the Go

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

With Wi-Fi available almost everywhere, it is now easy to connect while on the go and multitask wherever you are. But using public or unsecured Wi-Fi could expose your private information to cyber criminals who may steal your passwords via malware, or watch your keystrokes as you type out a PIN number or a password — a practice called shoulder surfing. Once these criminals have your sensitive information they can potentially gain access to your entire virtual world, so it is important to follow best practices to keep your information safe.

How to Protect Yourself

Be proactive:

- **Disable remote and automatic connection** to Wi-Fi and Bluetooth on your devices. Use Bluetooth in "hidden" mode, rather than "discoverable."
- **Avoid public Wi-Fi networks whenever possible,** especially in airports, hotels and cafes, and never use those networks to access financial accounts. Instead, use a network you trust or your cellular network.
- **Research and install** a virtual private network, or VPN, on your devices to encrypt and protect your internet traffic and passwords, especially when using public Wi-Fi. Be aware, you may have difficulty accessing some financial websites through a VPN due to anti-fraud protections.
- **Stay constantly aware** of your surroundings, and use privacy screens when you can.
- **Keep** personal information stored on mobile devices to a minimum.

If you suspect you've been targeted:

- **Don't delay.** Acting quickly after an event can minimize its impact.
- **Call your bank** and freeze financial accounts that may be affected) and inform credit bureaus.
- **Change all passwords** that may have been compromised.
- **Call the police** and file reports with the relevant local authorities if you suspect your identity has been stolen.
- **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

3:1

Ratio of connected devices to humans by 2023.[1]

$160 million

Reported losses to identity theft in 2019[2]

3.4

Average number of pieces of personally identifying information (birth dates, credit card numbers, etc.) consumers share online.[3]

[1] https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490

[2] https://pdf.ic3.gov/2019_IC3Report.pdf

[3] https://www.experian.com/blogs/ask-experian/survey-findings-are-consumers-making-it-easier-for-identity-thieves/

Be Cyber Secure: Connecting on the Go

Why It's Important

Using secure Wi-Fi and maintaining good spacial awareness is important to keeping your information and data safe. With your passwords or other stolen information, 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.

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