With Wi-Fi available almost everywhere, it is now quite easy to connect while on the go — and multitask wherever you are. But using public or unsecured networks could expose your private information to cyber criminals who steal your passwords when you’re using public Wi-Fi. Or they may 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.

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.”

- **Only use wireless networks that are secured** and require a password.

- **Install a virtual private network,** or VPN, on your devices to encrypt and protect your internet traffic and passwords even when using public Wi-Fi.

- **Stay constantly aware** of your surroundings and use privacy screens when you can.

- **Avoid visiting** sites that are unsecure (secure sites have a padlock icon in the address bar). Also, don’t download files or apps from unfamiliar sites.

- **Avoid replying** to emails or texts from unknown senders and keep your personal information on mobile devices to a minimum.

If you suspect you’ve been targeted:

- **Don’t delay.** Acting quickly after an attack can minimize its impact.

- **Call your bank** and freeze financial accounts that may be affected (Bank of America’s number for stolen or lost cards is 800-432-1000) and inform credit bureaus.

- **Change all passwords** that may have been breached.

- **Call the police** and file reports with the relevant local authorities if you suspect your identity has been stolen.

- **Document everything** about the attack. 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 attacks.
Why It’s Important

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
- **Go “phishing.”** 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 that work 24/7 to keep data and information safe.

For more information, go to: [www.bankofamerica.com/privacy/overview](http://www.bankofamerica.com/privacy/overview)