BANK OF AMERICA

CYBER SECURITY

Be Cyber Secure: Mobile Devices

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

Shopping, banking, donating to your favorite charity — you can now do almost everything with the click of a button. While enjoying these conveniences, make sure you aren't sharing sensitive information on apps or on online accounts, which could make your mobile devices a prime target for cyber criminals, and ensure you are utilizing simple best practices to minimize your risk.

How to Protect Yourself

Be proactive:

- **Act immediately** if you receive a changed password notification, an attempted log in alert from providers or if your account access changes on apps that you did not initiate.
- **Lock your mobile device** with a strong password and use biometric protection. Use a unique and different password across all of your apps and accounts.
- **Install or activate anti-theft software or apps** that can lock down your phone remotely, and apps that will help you locate your device.
- **Only download apps from official app stores,** and regularly update both your apps and your operating system to protect your devices.
- **Only access** mobile or online banking through a secured Wi-Fi connection.
- **Minimize the amount of personal information** you store on your devices or share online.
- **Educate your children** on best practices when using their mobile devices, inluding an explanation of their digital footprint.

If you suspect you've been targeted:

- **Don't delay.** Acting quickly after an event can minimize its impact.
- **Report stolen devices** to your service provider. If you provide the unique device identification number, they may be able to disable it.
- **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.
- **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

3.4

Average number of personally identifying information (birth dates, credit card numbers, etc.) consumers share online.[1]

3:1

Ratio of connected devices to humans by 2023.[2]

10.3

Average age that children get their first smartphone.[3]

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

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

[3] https://staysafeonline.org/press-release/stay-cyber-aware-internet-safety-month/

Be Cyber Secure: Mobile Devices

BANK OF AMERICA

Why It's Important

Cyber criminals know that many mobile users don't take adequate security precautions.

By stealing your phone, tablet, laptop or wearable device, they may gain more than just your confidential information. They might be able to access your entire virtual world, including your financial, social and email accounts.

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 real information and use it to apply for new credit cards or even apply for loans.
- **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