MERRILL
A BANK OF AMERICA COMPANY

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. But that convenience comes with a trade-off: Having your credit card and other sensitive information saved in apps or in online accounts makes your mobile devices a prime target for cyber criminals.

How to Protect Yourself

Be proactive:

- **Keep a record** of every device's make, model number and serial number.
- **Act immediately** if you receive a changed password notification from providers, or if your account access changes on apps.
- **Lock your mobile device** with a strong password or use biometric protection, such as a fingerprint lock. Never re-use passwords.
- **Install anti-theft software** that can, say, lock down your phone remotely, and apps that will help you locate your device.
- **Download apps only from official app stores** and regularly update both your apps and your operating system.
- **Only access** mobile or online banking through your bank's site. In fact, don't visit any sites that are not secure (check for a padlock icon in the address bar).
- **Never reply** to text messages or emails from unfamiliar senders, especially if they contain links.
- **Keep the personal information** you store or share online to a minimum.

If you suspect you've been targeted:

- **Don't delay.** Acting quickly after an attack 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 (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.

The Growing Threat, Measured

3.4

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

20 *to* 30 billion

Number of connected devices expected to be in use by 2020.[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.mckinsey.com/featured-insights/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age

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

Be Cyber-Secure: Mobile Devices

MERRILL
A BANK OF AMERICA COMPANY

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 info. They might be able to access your entire virtual world, including social and email accounts.

With your passwords and access to your social and financial accounts, cyber attackers 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
- **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.ml.com/privacy-and-security-center/privacy-and-security-center.html