MERRILL
A BANK OF AMERICA COMPANY

CYBER SECURITY

Be Cyber-Secure: Password Protection

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

Your passwords are your first line of defense against cyber crime. If attackers gain access, they can take over your accounts, steal your identity and use your contacts to reach out to family and friends and steal their information, too. The good news is that protecting your passwords is relatively easy — for example, by using a password manager or password vault, which is a software program that stores all of your passwords in a secure digital location that you can access with one master password.

How to Protect Yourself

Be proactive:

- **When you buy stuff online,** don't open an account — check out as a guest user.
- **Avoid writing down your passwords** or storing them on your computer. Use a password manager to keep passwords secure.
- **Use unique passwords** for your banking accounts — and remember that a long password is harder to steal.
- **Use multifactor authentication** when possible. Multifactor authentication requires two or more types of identification to gain access to an account.
- **Lock mobile devices** with a strong password or biometric protection (such as a fingerprint scanner) and avoid all public Wi-Fi networks.
- **Use a pin number** for tax submissions and government benefits.
- **Don't leave devices unattended.**

If you suspect you've been targeted:

- **Don't delay**. Act quickly if you think your passwords have been stolen, if you receive a changed password notification from providers, or if your account access changes on apps.
- **Call your bank** and freeze financial and credit accounts, and your children's financial and credit accounts (Bank of America's number for stolen or lost cards is 800-432-1000). Also, inform credit bureaus.
- **Call the police and file reports** with the relevant local authorities.
- **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

10%

Number of IT managers who admit using "password" or "qwerty" as their password.[1]

300 billion

Estimated number of passwords that will be in use by 2020.[2]

<10%

Number of active Google accounts that use two-factor authentication.[3]

[1] https://www.sailpoint.com/blog/world-password-day-2018/

[2] https://cybersecurityventures.com/300-billion-passwords/

[3] https://www.usenix.org/node/208154

Be Cyber-Secure: Password Protection

MERRILL
A BANK OF AMERICA COMPANY

Why It's Important

Passwords are the gateways to your life.

You use them to protect your email, your online bank accounts and your accounts at online retailers, as well as on dozens of other sites.

By using your passwords to access 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 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.ml.com/privacy-and-security-center/privacy-and-security-center.html