BANK OF AMERICA
美国银行

GLOBAL INFORMATION SECURITY

Be Cyber Secure: Cyber Security Best Practices for Businesses Navigating Volatile Times

Tips and best practices to help you protect yourself and your business

With cyber criminals more active and attempting to capitalize on the coronavirus, make sure you know how to protect your company's information and assets. It's times like these that good cyber security best practices are more important than ever.

How to Protect Yourself

Be Proactive:

- **When working from home, only use wireless networks that are secured** and require a password. Avoid public Wi-Fi networks, and never conduct any financial or confidential work over a public Wi-Fi connection.
- **Conduct all business matters on company approved devices,** even when working remotely.
- **Never trust unknown individuals.** Verify everything they claim and do not send sensitive information to anyone whose identity you can't verify.
- **Do not discuss confidential information** around other people when working remotely. As much as is practically possible, conduct your work in a private space.
- **Ensure communication validation steps** are followed when working remotely to ensure company information and data stays secure.

If you suspect you've been targeted:

- **Don't delay.** Acting quickly after an incident can minimize damage to your business.
- **Monitor all transactions** for suspicious activity in the aftermath of an incident.
- **Know and follow your local laws** and guidelines for cyber incidents.
- **Document everything about the incident.** The more information you have, the better armed you will be to assist an investigation by your company and law enforcement officials, and the better prepared you will be against future attacks.
- **Change all passwords** that may have been breached.
- **Contact your bank's servicing desk** or support staff to report a fraudulent transaction as soon as you can.

Are you prepared for these potential remote work risks?

Data Loss
due to unsecured Wi-Fi networks and devices

Phishing
and vishing scams

Unauthorized
system access enabled by insecure passwords and the use of non-approved software

Malware
including ransomware risks

Be Cyber Secure: Cyber Security Best Practices for Businesses Navigating Volatile Times

Threat Vectors:

Watch out for some common threat vectors cyber criminals are using:

- **Phishing:** do not reply to or click on links in emails, even when they appear to be from a legitimate source. Cyber criminals are able to spoof email domains to make their phishing attempts appear as if they originate from credible sources. They are also using scare tactics that reference the coronavirus as a means to gain access to your data by directing you to click on links that can install malware onto your device.

- **Vishing:** cyber criminals utilize vishing techniques, such as impersonating a trusted source or robocalls, to scam people out of data and money over the phone. Criminals will create a sense of urgency to incite quick responses out of their targets.

- **Apps:** downloading news apps can help you keep up to date with latest developments, but when downloading apps, ensure they come from a reliable source and follow your company's guidelines on what is acceptable to install on your work devices.

- **Websites:** ensure that the information you are reading is coming from a legitimate source. Check the URLs of the websites you are visiting carefully, and be sure not to click on anything that looks suspicious. Follow your company's guidelines on what websites are safe to surf when using work devices.

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.go