BANK OF AMERICA

CYBER SECURITY

Be cyber secure: phishing

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

Phishing is a way that cyber criminals will try to trick you into revealing confidential or sensitive company information. Phishing occurs through several channels; emails, text messages, phone calls, and social media. When attempting to phish cyber criminals will often create a sense of urgency to trick you into clicking a link or open an attachment which will infiltrate your devices and/or email to steal passwords and bank account information.

How to protect yourself

Be proactive:

- **Be careful** when posting personally identifiable information on social media. Be compliant with your company's social media policies.
- **Download app updates.** Unpatched software can expose you to threats.
- **Invest in antivirus software** and other cyber security software that can flag suspicious emails and sites.
- **Double check sender information.** Check domain name of sender to ensure they are not spoofing the email address.
- **Never trust** unknown individuals. Verify everything they claim and do not send sensitive information to anyone whose identity you can't verify.

If you suspect you've been targeted:

- **Don't delay.** Acting quickly after an event can minimize damage to you or your company.
- **Contact your bank's servicing desk** or support staff to report a fraudulent transaction as soon as you can.
- **Know and follow your local laws** and guidelines for cyber incidents.
- **Report the threat** to the platform on which it occurred.
- **Document everything** about the event. The more information you have, the better armed you will be to assist an investigation by your company, bank and law enforcement officials, and the better prepared you will be against future cyber crime attempts.

The growing threat, measured

241,342

Number of reported incidents in the phishing category.[1]

814%

Percentage increase in reported incidents in the phishing category from 2018 to 2020.[1]

$54.2 million

Estimated loss in 2020 from incidents in the phishing category.[1]

[1] FBI IC3 Report, 2020

Be cyber secure: phishing

BANK OF AMERICA

Why it's important

Phishing is a common social engineering threat, where seemingly legitimate messages are sent via email or messaging platforms.

- **Vishing** is the phone version of phishing, and **smishing** is the SMS or messaging app version.
- **Spear phishing**: highly targeted phishing campaign designed for specific individuals.
- **Spoofing**: disguises communications in order to appear to be from someone else, including legitimate businesses or employees. Cyber criminals can spoof emails, phone numbers and websites.
- Remember that Bank of America, like many companies, will never ask you for account or CashPro® details unless you call us first.

Cyber criminals will try to illicit a strong emotional reaction in you to by-pass processes and get you to click or send items you should not. Social engineering relies on greed, curiosity, urgency, helpfulness and fear. Some ways they may attempt to phish are:

1. **Contacting you** through fraudulent, spoofed or compromised email accounts or accounts for messaging apps.
2. **Encouraging you to click** a link that downloads malware onto your computer and gives criminals access to your device and information.
3. **Providing an urgent pretext** for why you must send confidential or financial 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.business.bofa.com/en-us/content/fraud-prevention-and-cyber-security-solutions.html