BANK OF AMERICA

CYBER SECURITY

Be cyber secure: smishing

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

Smishing is a way that cyber criminals will try to trick you into revealing confidential or sensitive company information. Smishing occurs when text messages, SMS, or other messaging platforms are used to send a fraudulent or deceptive message to gain access to sensitive information. Cyber criminals when they reach out will often create a sense of urgency to trick you into clicking a link or open an attachment which will infiltrate your devices 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.
- **Don't reply, click or answer from unknown sources** or click on their links or attachments.
- **Invest in antivirus software** and other cyber security software that can flag suspicious sites.
- **Don't fall for the bait.** If an offer sounds too good to be true, it probably is. Or if a text looks strange, look up the sender and call them (don't use the number they provide).
- **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.
- **Change all passwords** that may have been compromised.
- **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 events.

The growing threat, measured

241,342

Number of reported incidents in the smishing category in 2020.[1]

814%

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

$54.2 million

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

[1] FBI, IC3 Report, 2020

Be cyber secure: smishing

BANK OF AMERICA

Why it's important

A common phishing method is called smishing, where seemingly legitimate messages are sent via text, SMS messages or other messaging applications. Cyber criminals smish by:

- **Claiming suspicious activity** has been detected on an account or suspicious log-in, including posing as your company's help desk.
- **Claiming there is a problem** with your account or your payment information.
- **Asking you to click** on a link to make a payment.
- **Trick you to bypass your company's procedures** to provide them with data or money that you ordinarily would not.
- Remember that Bank of America, like many companies, will never ask you for account or CashPro® details unless you call us first.

Cyber criminals go smishing by:

1. **Contacting you** through fraudulent, spoofed or compromised phone numbers or accounts for messaging apps.
2. **Encouraging you to click** a link that downloads malware onto your mobile device 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