

Be cyber secure: smishing



Smishing is a way that cyber criminals will try to trick you into revealing confidential or sensitive company information. Smishing occurs when text messages 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.

→ Cyber criminals smish by:

- **Claiming suspicious activity** has been detected on an account or suspicious log-in, including posing as your bank or 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.

→ 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 have been targeted:

- **Don't delay.** Acting quickly after you have been targeted 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 and the better prepared you will be against future attempts.

Visit www.bankofamerica.com/security to learn how to help protect yourself and your business.

Be cyber secure: smishing



Cyber criminals go smishing by:

- **Contacting you** through fraudulent, spoofed or compromised phone numbers or accounts for messaging apps.
- **Providing an urgent pretext** for why you must send confidential or financial information.
- **Encouraging you to click** a link that downloads malware onto your mobile devices and gives criminals access to your devices and information.

IMPORTANT INFORMATION

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

"Bank of America" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.

Investment products offered by Investment Banking Affiliates:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value
----------------------	-------------------------	----------------

© 2022 Bank of America Corporation. All rights reserved. 5237116