BANK OF AMERICA

CYBER SECURITY

Be cyber secure: recognizing ransomware

Ransomware is a type of malware that typically spreads through phishing emails, fraudulent websites and SMS messaging. Once it is installed on a system or network, it encrypts files and holds them hostage until a ransom is paid. Cyber criminals are directing ransomware campaigns at individuals and many types of businesses and government services, and successful attempts are becoming increasingly sophisticated and costly.

→ Once in control, cyber criminals may be capable of:

- **Disrupting** your personal and business activities.
- **Destroying critical information** stored on your systems.
- **Ransom payment** to support other criminal activities.

→ Be proactive:

- **Be wary of any unsolicited emails,** and don't click on links or attachments inside them. This includes emails from companies you know or from friends.
- **Invest in a robust security software package** that can flag suspicious emails and websites and check newly downloaded software programs for malware.
- **Update your applications and operating systems regularly** and turn on automatic updates.
- **Verify website credentials.** Since URLs can be spoofed, suspicious address links in messages should be confirmed by the message sender through another means of contact.
- **Never plug unknown storage devices,** like thumb drives, into your computer as they may contain ransomware.
- **Contact your technology** providers for assistance.

→ If you suspect you have been targeted:

- **Disconnect your devices** and network from the internet.
- **Change all passwords** that may have been compromised.
- **Check all financial accounts.** If you see any signs of fraudulent activity or a financial loss, contact your bank and law enforcement. File reports with relevant authorities if you suspect compromise or theft of data.
- **Report any infected device** that is your employer's property to the company's IT department.
- **Consider reaching out** to local or federal law enforcement agencies before settling on any plan of action.

Visit www.bankofamerica.com/security to learn how to help protect yourself and those closest to you.

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.

Merrill Lynch, Pierce, Fenner & Smith Incorporated (also referred to as "MLPF&S" or "Merrill") makes available certain investment products sponsored, managed, distributed or provided by companies that are affiliates of Bank of America Corporation ("BofA Corp."). MLPF&S is a registered broker-dealer, registered investment adviser, Member SIPC, and a wholly-owned subsidiary of BofA Corp.

Bank of America Private Bank is a division of Bank of America, N.A., Member FDIC, and a wholly-owned subsidiary of BofA Corp.

Banking products are provided by Bank of America, N.A., and affiliated banks, Members FDIC, and wholly-owned subsidiaries of BofA Corp.

Investment products:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value