BANK OF AMERICA

CYBER SECURITY

Be Cyber Secure: Recognizing Ransomware

How to protect yourself — and respond if you have been targeted

A fusion of social engineering and malware, ransomware 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. In the last quarter of 2019, the average cost of recovery from a ransomware incident was $84,116, more than double the average of the quarter before.[1]

Here are some tips to help you protect yourself from ransomware:

How to Protect Yourself

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 scan newly downloaded software for malware.
- **Update your applications and operating systems regularly** and turn on automatic updates.
- **Never plug unknown storage devices,** like thumb drives, into your computer as they may contain ransomware.
- **Create strong passwords** with at least eight characters.
- **Do not share** personal information with unknown or untrusted sources in phone conversations, emails or texts.

If you detect ransomware:

- **Disconnect your devices,** backups and networks from the internet.
- **Contact your technology** providers for assistance.
- **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.

The Growing Threat, Measured

2,047

Identified ransomware complaints received by the FBI in 2019, with adjusted loss of $8.9 million.[2]

235%

Increase in ransomware attempts directed at enterprises and small businesses between 2018 and 2019.[3]

11 seconds

Estimated interval between ransomware incidents on businesses in 2021.[4]

[1] Coveware Q4 Ransomware Marketplace report, 2019.

[2] FBI IC3 Report, 2019.

[3] Malwarebytes: Cybercrime Tactics and Techniques, Ransomware Retrospective, August 2019.

[4] Cybercrime Magazine, October 21, 2019.

Be Cyber Secure: Recognizing Ransomware

How to Protect Yourself Continued

Be proactive:

- **Back up your important data.** Use an external drive or cloud backup, and make sure to perform updates at regular intervals.
- **Freeze your credit report** if you're not applying for a new loan any time soon. That way, even if your identity is stolen, criminals can't request your credit details to open new lines of credit in your name.

If you detect ransomware:

- **Document everything.** The more information you can provide, the more you can help any investigation — and decrease the likelihood of a future breach.
- **Think carefully before you decide to pay** the ransom. Consider reaching out to local or federal law enforcement agencies before settling on any plan of action.

Why It's Important

Ransomware enables cyber criminals to lock up or steal your data, as well as gain control of your devices and use them to perform malicious actions.

Once in control, cyber criminals may be capable of:

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

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

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.

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, 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

© 2020 Bank of America Corporation. All rights reserved.

3114148