BANK OF AMERICA

CYBER SECURITY

Be Cyber Secure: Recognizing Ransomware

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

A type of 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.

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

How to Protect Yourself

Be proactive:

- **Do not reply to emails or texts,** or click on links from unknown senders — they may be phishing attempts.
- **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.
- **Back up your important data.** Use an external drive or cloud backup, and make sure to perform updates at regular intervals.

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.
- **Document everything.** The more information you can provide, the more you can help any investigation — and decrease the likelihood of a future breach.

The Growing Threat, Measured

2474

Reported victims of ransomware in 2020.[1]

$29.1MM

Ransomware losses reported to the FBI in 2020.[1]

11 seconds

Estimated interval between ransomware incidents on businesses in 2021.[2]

[1] FBI, IC3 Report, 2020.

[2] Cybercrime Magazine, October 21, 2019.

Be Cyber Secure: Recognizing Ransomware

How to Protect Yourself Continued

Be proactive:

- **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:

- **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 who work 24/7 to keep data and information safe.

For more information, go to: www.bankofamerica.com/privacy/overview.go

3596683