

Sign in | Register Contact Us Press Room Consumers





American Bankers Association

Policy Issues

Advocacy

Compliance

Tools & Resources

Products

ABA Foundation

Overview

Home > Tools & Resources > Infographics > Ransomware Infographic

By Bank Type/Job Role

Print

E-mail Bulletins

Ransomware Infographic

Experts On Call

Online Discussion Groups

Toolboxes

Communication Tools

Infographics

Benchmarking Programs

Economic Resources

Millennials and Banking

Women's Leadership Resources

Job Bank



RANSOMWARE

Ransomware is a type of malicious software (malware) that freezes your computer or mobile device until a sum of money is paid. It can destroy personal and business files, leading to stolen data and large financial losses.

KNOW

Ransomware attacks—especially those that target small businesses—are **evolving in complexity and are on the rise.**

All devices are vulnerable, but more and more **mobile attacks** are being reported.

\$209 Million collected by criminals in the first quarter of 2016.

A projected **\$1 Billion +** in losses from ransomware attacks in 2016 alone, according to the FBI.

Ransom fees vary, from \$200 – \$10,000.

IDENTIFY

Ransomware targets a specific individual within a business, or a consumer with a link or attachment that infects your computer with malware or leads you to an infected website. Three ways ransomware can take shape are:

Spear phishing emails

- The sender appears to be someone you may know or someone relevant to your business.
- The message is often personalized, and may include your name or a reference to a recent transaction.

Advertisements or pop-up windows

- Your computer freezes, and a popup message appears.
- The message may threaten a loss of your files or information, or may also tell you that your files have been encrypted.

Downloadable Software

- Ransomware is also present in downloadable games and file-sharing applications.

Once the PC is infected, your files are encrypted and inaccessible. The fraudster demands a ransom payment in order to unlock them.

PREVENT

- Always back up your files and save them offline or in the cloud.**
- Always use antivirus software and a firewall.** Be sure they are set to update automatically.
- Enable popup blockers.**
- Don't click.** Be cautious when opening emails or attachments you don't recognize—even if the message comes from someone in your contact list.
- Only download software from sites you know and trust.**
- Alert your local law enforcement agency as soon as you encounter a potential attack.**

© 2016 American Bankers Association



Navigate Our Site

- ▶ About ABA
- ▶ Training and Events
- ▶ Policy Issues
- ▶ Advocacy
- ▶ Compliance
- ▶ Tools and Resources
- ▶ Products
- ▶ ABA Foundation
- ▶ Press Room
- ▶ Consumers

Connect with ABA

- ▶ Register for Benefits Webinar
- ▶ Subscribe to E-mail Bulletins
- ▶ Ask a Staff Expert
- ▶ Become an ABA Member
- ▶ Join an ABA Committee
- ▶ Network with Peers
- ▶ Become a Sponsor/Exhibitor
- ▶ Find Industry Providers
- ▶ Post a Job or Resume
- ▶ ABA Banking Journal News Site

Follow ABA

- Dodd-Frank Tracker Blog
- Banks and the Economy Blog
- @ABABankers
- Facebook
- LinkedIn
- Google+
- YouTube
- Instagram
- ABA Press Releases



**American Bankers
Association**
1120 Connecticut Ave
NW
Washington, DC

20036

© 2017 American Bankers Association

Questions?

E-mail the ABA [Webmaster](#) or
[Customer Service](#)
Call 1-800-BANKERS (800-226-
5377)

[Reprint Request](#) | [Privacy Policy](#)

Site Sponsor:

[Corporation for American
Banking LLC](#)