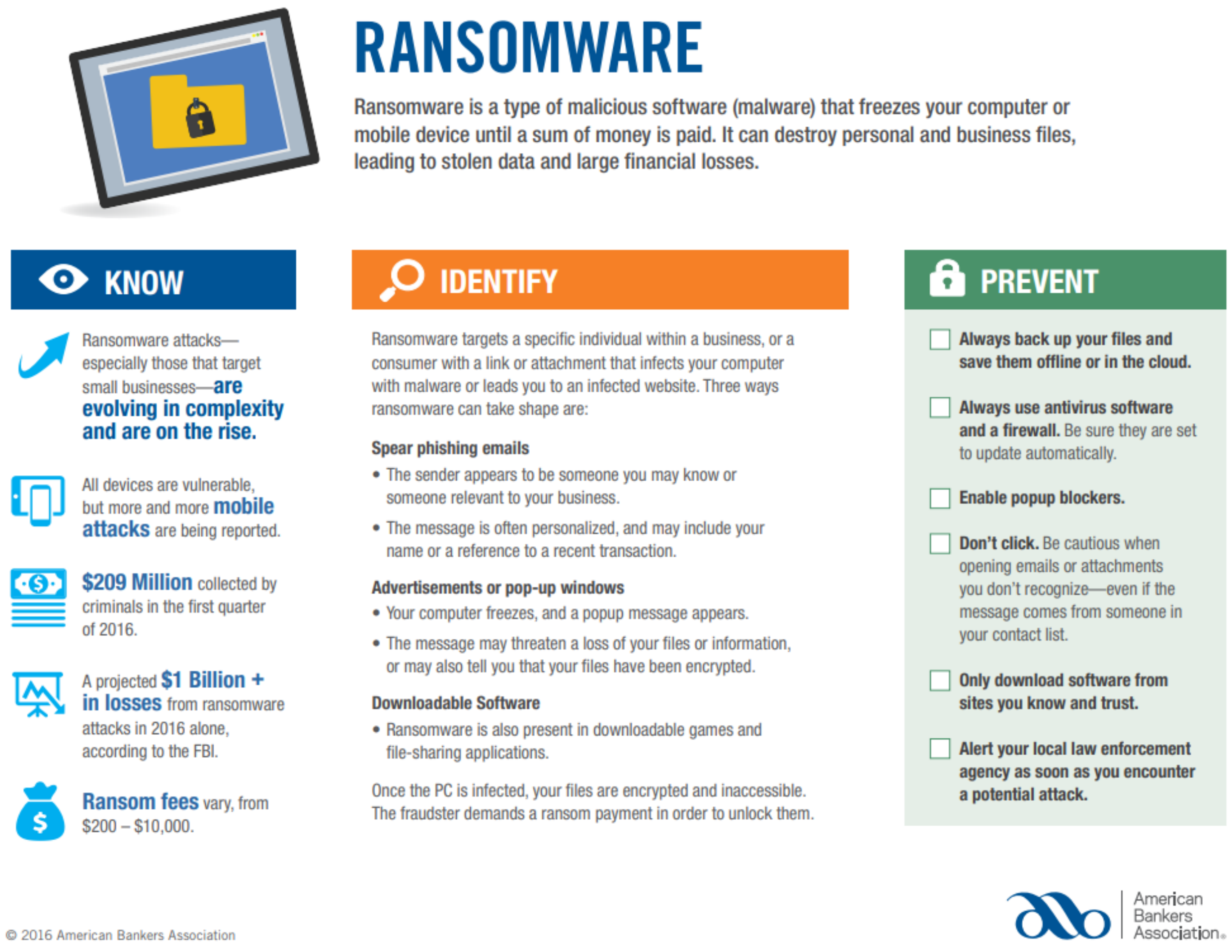
FNB First Neighborhood Bank

Consumer Education

# Ransomware Attacks

Individuals and businesses have become targets to a growing online fraud scheme known as ransomware. **Ransomware** is a form of malware used by cyber criminals to freeze your computer or mobile device, steal your data and demand that a "ransom" — typically anywhere from a couple of hundreds to thousands of dollars — be paid.

Individual computers or laptops, enterprise networks and or servers used by government agencies, financial institutions and healthcare providers are all at risk to malware exposure. Banks and law enforcement officials are bolstering their efforts to neutralize some of the more significant ransomware scams by educating consumers and business individuals on the safe practices they can use to prevent these scams.



## 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.**

American Bankers Association

**Tips for consumers:**

- **Don't click.** Visiting unsafe, suspicious or fake websites can lead to the intrusion of malware. Be cautious when opening e-mails or attachments you don't recognize even if the message comes from someone in your contact list.
- **Always back up your files.** By maintaining offline copies of your personal information, ransomware scams will have a limited impact on you. If targeted, you will be less inclined to take heed to threats posed by cyber criminals.
- **Keep your computers and mobile devices up to date.** Having the latest security software, web browser and operating system are the best defenses against viruses, malware, and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.
- **Enable popup blockers.** To prevent popups, turn on popup blockers to avert unwanted ads, popups or browser malware from constantly appearing on your computer screen.

**Tips for businesses:**

- **Educate your employees.** Employees can serve as a first line of defense to combat online threats and can actively help stop malware from infiltrating the organization's system. A strong security program paired with employee education about the warning signs, safe practices, and responses aid tremendously in preventing these threats.
- **Manage the use of privileged accounts.** Restrict users' ability to install and run software applications on network devices, in an effort to limit your networks exposure to malware.
- **Employ a data backup and recovery plan** for all critical information. Backups are essential for lessening the impact of potential malware threats. Store the data in a separate device or offline in order to access it in the event of a ransomware attack.
- **Make sure all business devices are up to date.** Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans so that your operating systems operate efficiently.
- **Contact your local FBI field office** immediately to report a ransomware event and request assistance. Visit **https://www.fbi.gov/contact-us/field** to locate the office nearest you.

Source: American Bankers Association