Tips to Help Avoid Ransomware Attacks

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 hundred to thousands of dollars — be paid.

According to the FBI, ransomware victims lost more than $18 million between April 2014 and June 2015.

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.

To help combat these malicious threats, the American Bankers Associations is offering these 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.

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.** Backups are essential for lessening the impact of potential malware threats. Store the data on 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.