Beware of Ransomware. Tips to Protect against Ransomware.

Ransomware is malicious software that digitally locks a victim's computer system or files until they pay a ransom to have them unlocked. Ransomware software types vary, however, all will prevent you from using your PC normally.

They may:

- Prevent you from accessing Windows.
- Encrypt files so you can't use them.
- Stop certain apps from running (like your web browser).

Often the Ransomware will appear as a fraudulent claim that you have done something illegal with your PC, and that you are being fined by a police force or government agency. It will demand that you do something to get access to your PC or files such as: demand you pay money or force you to complete surveys that will gain access to your PC or files.

According to the Federal Bureau of Intelligence (FBI) in an article published in January 2015, the typical victim pays the Ransomware criminal between $200 and $10,000 to regain access to their system with no guarantee that the paid ransom will succeed in unlocking the victim's system.

The FBI's Internet Crime Complaint Center offers these tips to protect against Ransomware:

- Always use antivirus software and a firewall.
- Enable automated patches or updates for your operating system and web browser.
- Use popup blockers. Popups are regularly used by criminals to spread malicious software. To avoid accidental clicks on or within popups, it's best to prevent them from appearing in the first place.
- Only download software, especially free software, from sites you know and trust. Malware can come in downloadable games, file-sharing programs and customized toolbars.
- Don't open attachments in unsolicited emails, even if they come from someone in your contact list.
- Never click on a URL contained in an unsolicited email, even if you think it looks safe. Instead, close out of the email and go to the organization's website directly.
- Always back up the content on your computer. If you back up, verify, and maintain offline copies of your personal and application data, ransomware

scams will have limited impact on you. If you are targeted, instead of worrying about paying a ransom to get your data back, you can simply have your system wiped clean and then reload your files.

- Avoid suspicious websites.
- Use the same precautions on your mobile phone as you would on your computer when using the Internet.

If you have any questions, please feel free to call the CustomerFirst Contact Center at (203)462-4400.