HOW TO DEFEND AGAINST RANSOMWARE

In September, the FTC hosted a workshop on ransomware, one of the most serious online threats facing people and businesses today — and the most profitable form of malware criminals use. How does ransomware work? Hackers hold your files "hostage"— often encrypting them — then demand payment, typically in bitcoins, for you to get them back.

Georgetown:

- 900 S. Austin Ave
  512-863-2567
- 5321 Williams Dr.
  512-869-8910
- 480 Del Webb Blvd.
  512-864-0379

Round Rock:
500 Round Rock Ave.
512-255-2501

Cedar Park:
1901 Bagdad Road
512-259-2443

Brushy Creek:
7509 O'Connor Drive
512-246-6010

Pflugerville:
1600 W. Pecan
512-251-7889

Liberty Hill:
721 Highway 183
512-778-5757

FirstTexasBank.net

HOW TO DEFEND AGAINST RANSOMWARE

Information provided by the
Federal Trade Commission
Consumer.ftc.gov

FIRST TEXAS BANK
MEMBER FDIC

HOMETOWN COMMUNITY SPIRIT
HOMETOWN COMMUNITY PRIDE™

SHOULD I PAY THE RANSOM?

Law enforcement doesn't recommend paying the ransom, although it's up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back. If you pay the ransom, there's no guarantee you'll get your files back. In fact, agreeing to pay signals to criminals that you haven't backed up your files. Knowing this, they may increase the ransom price — and may delete or deny access to your files anyway. Even if you do get your files back, they may be corrupted. And you might be a target for other scams.

WHAT IF I'M A VICTIM OF RANSOMWARE?

- **Contain the attack.** Disconnect infected devices from your network to keep ransomware from spreading.
- **Restore your computer.** If you've backed up your files, and removed any malware, you may be able to restore your computer. Follow the instructions from your operating system to re-boot your computer, if possible.

Contact law enforcement. Report ransomware attacks to the Internet Crime Complaint Center or an FBI field office. Include any contact information (like the criminals' email address) or payment information (like a Bitcoin wallet number). This may help with investigations.

HOW CAN I DEFEND AGAINST RANSOMWARE

UPDATE YOUR SOFTWARE-

Use anti-virus software and keep it up-to-date. And set your operating system, web browser, and security software to update automatically on your computer. On mobile devices, you may have to do it manually. If your software is out-of-date, it's easier for criminals to sneak bad stuff onto your device

Think twice before clicking on links or downloading attachments and apps-

According to one panelist, 91% of ransomware is downloaded through phishing emails. You also can get ransomware from visiting a compromised site or through malicious online ads.

Back up your important files-

From tax forms to family photos, make it part of your routine to back up files on your computers and mobile devices often. When you're done, log out of the cloud and unplug external hard drives so hackers can't encrypt and lock your back-ups, too.