Scam Alert – Defending Against Ransomware

By Putnam County State Bank – To Keep it From Happening to You

(reprinted from consumer.ftc.gov)

Defending yourself

- ✓ **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 If your software is out-of-date, it is easier for criminals to sneak bad stuff onto your device..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 at a Federal Trade Commission workshop, 91% of ransomware is downloaded through phishing emails. Phishing is when internet scammers impersonate a business to trick you into giving out your personal information or trick you into clicking a link. 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 devise often. When you're done, log out of the cloud and unplug external hard drives so hackers can't encrypt your back-ups, too.

What if I am a Victim?

- ✓ **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 (https://www.ic3.gov/default.aspx) or an FBI field office (https://www.fbi.gov/contact-us/field-offices/kansascity). Include any contact information (like the criminals' email address) or payment information (like a Bitcoin wallet number). This may help with investigations.

Paying 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.

Knowledge is Power

Sign up for free scam alerts from the FTC at ftc.gov/scams. Get the latest tips and advice about scams sent right to your inbox.

If you spot a scam, report it at ftc.gov/complaint. Your reports help the FTC and other law enforcement investigate scams and bring crooks to justice.