CYBERSECURITY

FIRST SERVICE BANK

It is recommended that these practices be implemented to the greatest extent possible based on the availability of organizational resources.
(Visit cisa.gov/stopransomware for an extensive list of suggestions.)

- It is critical to maintain offline, encrypted backups of data and to regularly test backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.

- Create, maintain and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.

- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those an internet-facing devices, to limit the attack surface. CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments (https://www.cisa.gov/cyber-resource-hub).

- Regularly patch and update software and OSs to the latest available versions.

- Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity or incidents. Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails. (Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message or text message.)

- Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions. CISA recommends using a centrally managed antivirus solution. This enables detection of both “precursor” malware and ransomware.

- If you are using passwords, use strong passwords (https://us-cert.cisa.gov/ncas/tips/ST04-002) and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts. Password managers can help you develop and manage secure passwords.

- **Ransomware:** What It Is and What to Do About It (CISA): General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: *https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One -Pager_and_Technical_Document-FINAL.pdf*

- **Ransomware (CISA):** Introduction to ransomware, notable links to CISA products on protecting networks, specific ransomware threats and other resources: *https://www.us-cert.cisa.gov/ransomware*

- **Security Primer – Ransomware (MS-ISAC):** Outlines opportunistic and strategic ransomware campaigns, common infection vectors and best practice recommendations: *https://www.cisecurity.org/white-papers/security-primer-ransomware/*

- **Ransomware: Facts, Threats and Countermeasures (MSISAC)** - Facts about ransomware, infection vectors, ransomware capabilities, and how to mitigate the risk of ransomware infection: *https://www.cisecurity.org/blog/ransomwarefacts-threats-and-countermeasures/*
Source: *cisa.gov/stopransomware*