RANSOMWARE

Ransomware is a type of malicious software (malware) designed to block access to a computer system or mobile device until a sum of money is paid. It can destroy personal and business files, leading to stolen data and large financial losses. Once the PC is infected, files are encrypted and inaccessible.

KNOW

· The severity of ransomware attacks is trending up and are evolving in complexity.

· All devices are vulnerable, but more and more mobile attacks are being reported.

· Attacks are becoming more difficult and costly to recover from. In just the United States, ransomware victims spent an average of $2.09 million on remediation costs.

· Often attacks take place against vulnerable entities such as smaller businesses, in part due to the attacker's assumption that such victims may have fewer resources to invest in cyber protection and will make quick payment to restore services.

IDENTIFY

Ransomware targets a specific individual within a business, or a consumer with a link or attachment that infects your computer system with malware or leads you to an infected website. Three ways ransomware can take shape are:

Spear phishing emails

· The sender appears to be someone you may know or someone relevant to your business.

· The message is often personalized and may include your name or a reference to a recent transaction.

Advertisements or pop-up windows

· Your computer freezes, and a message appears.

· The message may threaten a loss of your files or information or may also tell you that your files have been encrypted.

Downloadable Software

· Ransomware is also present in downloadable games and file-sharing applications.

PREVENT

- ✓ **Always back up your files and save them offline or in the cloud**
- ✓ **Keep your systems up-to-date on patches**
- ✓ **Create a data recovery process**
- ✓ **Don't use the same password across multiple platforms**
- ✓ **Always use antivirus software and a firewall –** Be sure they are set to update automatically
- ✓ **Use Multi-factor authentication (MFA)** whenever possible
- ✓ **Enable popup blockers**
- ✓ **Don't click -** Be cautious when opening emails or attachments you do not recognize – even if the message comes from someone in your contact list
- ✓ **Only download software from sites you know and trust**
- ✓ **Limit the information you share when possible**
- ✓ **Perform vulnerability scans**
- ✓ **Educate Staff and/or family**
- ✓ **Alert your local law enforcement agency as soon as you encounter a potential attack**

3-2-1 BACKUP RULE

X3 — Maintain at least 3 copies of your data

X2 — Keep 2 copies stored at separate locations

X1 — Store at least one copy at an off-site location