QUICK REFERENCE

PREVENTING RANSOMWARE ATTACKS

Objective

Provide advice and tools to prevent ransomware attacks.

Cybercriminals know that companies are more likely to pay a ransom since their data is critical to their survival.

Target recipient: Person responsible for IT systems

Last update: 2017-06

Types of ransomware

- **Encryption ransomware**. This encrypts personal files and folders (documents, spreadsheets, pictures and videos).
- **Lock screen ransomware.** This locks the computer's screen and demands payment.
- **Master Boot Record (MBR) ransomware**. This changes the computer's MBR, the part of the computer's hard drive that allows the operating system to boot up, so the normal boot process is interrupted.
- **Ransomware encrypting web servers**. This encrypts files on web servers using the vulnerabilities of the Content Management Systems (CMS).
- **Mobile device ransomware**. This blocks mobile devices through fake apps that masquerade as popular services.

Preventive measures

- **Back-up**. Have a recovery system in place so a ransomware infection can't destroy your personal data forever. It's best to create 2 back-up copies: one to be stored in a cloud and another one on a physical device (hard drive, USB key, extra laptop).
- **Use antivirus software**.
- **Keep the software on your computer and OS up to date**.
- **Be vigilant.** Never open attachments in emails from someone you don't know. Don't click on links in emails if in doubt.
- **Check file extensions before opening.** Be careful with the following file extensions**:** .exe, .vbs, .js, .hta, .docx, .docm, .doc, .chm, .jar, .com, .ocx, .bat, .cmd, .pdf, .cpl and .scr.
- If you discover an unknown process on your machine**, disconnect it immediately from the internet or other network connections** to prevent the infection from spreading.

In case of an attack

It's highly recommended to not pay the ransom, even if it's more expensive to restore backups. By sending money to cybercriminals, you'll only confirm that ransomware works, and there's no guarantee you'll get the decryption key you need in return.

- Use Crypto Sheriff (free) to identify the type of ransomware affecting your system: https://www.nomoreransom.org/crypto-sheriff.php.

- Restore your computer from a backup copy without the malware.

For first generation ransomware, the files can be decrypted with the tools available on the No More Ransomware website: https://www.nomoreransom.org/decryption-tools.html.

Additional information

- Check the No More Ransomware website: https://www.nomoreransom.org/prevention-advice.html