REFERENCE SHEET

PROTECTING AGAINST RANSOMWARE

Purpose of the document

The purpose of this document is to provide advice and tools to protect against ransomware.

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

Types of ransomware

- **Encryption ransomware** encrypts personal files and folders.
- **Lock screen ransomware** locks the computer's screen and demands payment.
- **Master Boot Record (MBR) ransomware** changes the computer's MBR (the part of the computer's hard drive that boots the operating system) and interrupts the normal booting process.
- **Ransomware that targets web servers** encrypts files on web servers by exploiting vulnerabilities in the Content Management System (CMS).
- **Mobile ransomware** blocks mobile devices through fake apps that masquerade as popular apps.

Preventive measures

1. **Save**. Have a restoration system in place to prevent ransomware from destroying your personal data. It is recommended that you make two backup copies: one on a cloud service, and one on a physical support medium (e.g. hard drive, USB key, secondary computer)
2. **Use an antivirus program.**
3. **Keep your computer's software and OS up to date.**
4. **Be vigilant.** Never open an email attachment from someone you don't know. Don't click on hyperlinks in emails if you have doubts.
5. **Check the file extension before opening it.** Be careful with the following file extensions: .exe, .vbs, .js, .hta, .docx, .docm, .doc, .chm, .jar, .com, .ocx, .bat, .cmd, .pdf, .cpl, .scr.
6. If you discover an unknown process on your computer, **disconnect from the Internet or any other network connection** to prevent the infection from spreading.

In case of an attack

It is highly recommended that you not pay ransom, even if it's more costly to restore the backups than to pay the ransom. By sending money to criminals, you'll only confirm that the ransomware works. Plus, there's no guarantee you'll get the decryption key you need in exchange.

1. Identify the type of ransomware that's affecting your system with Crtypto Sheriff (freeware) - https://www.nomoreransom.org/fr/crypto-sheriff.php

2. Restore your computer with a backup copy that hasn't been infected.

Files infected by first generation ransomware can be decrypted with tools available on the No More Ransomware site: https://www.nomoreransom.org/en/decryption-tools.html

Additional information

No More Ransomware: https://www.nomoreransom.org/en/prevention-advice.html