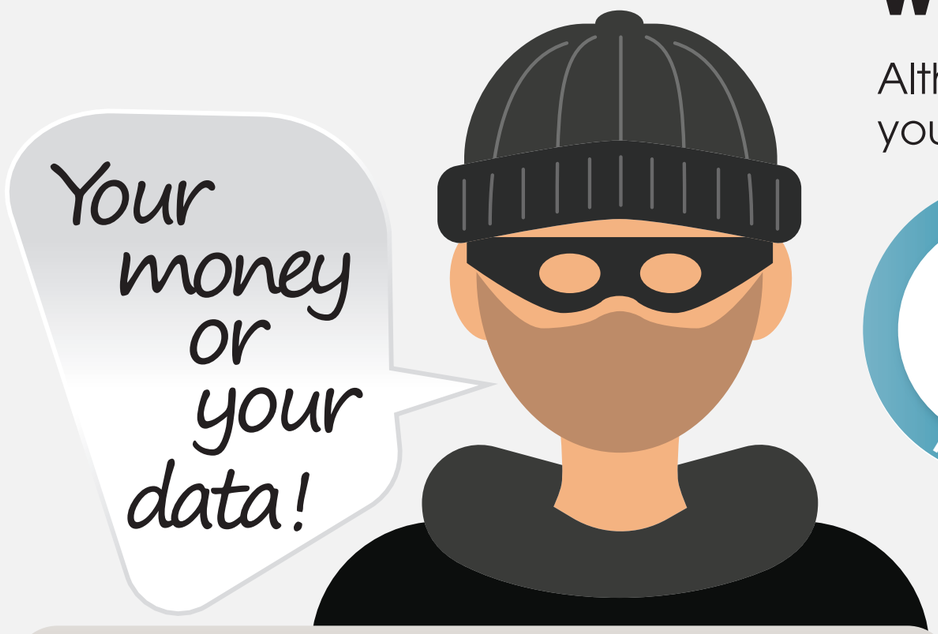


## What is Ransomware

**Malware that blocks access to the victim's data while threatening to publish, delete, or prohibit access unless a ransom is paid.**

**Advanced malware uses crypto viral extortion, which encrypts files and makes them nearly impossible to recover without a decryption key. Attackers demand payment via digital currencies like Bitcoin, making it very difficult to catch or prosecute the perpetrators.**

# What can you do?

Although no defense is completely fool proof against these devious criminals, you can take steps to lessen and possibly prevent some attacks.

### PREVENTION

**Avoiding infection is the best scenario.**

- Back up data as often as possible. Backups are essential for restoring the system after an attack. Store backups in a location that is isolated from the network and routinely verify that the data can be restored.
- Train employees to recognize phishing emails and ransomware, as well as best practices in dealing with unknown threats.
- Malware exploits may be preventable if system patches are applied accordingly. Always keep antivirus and other software updated.
- Discover and maintain a live inventory of network devices. This could help to identify rogue devices that have gained network access.
- Develop, maintain, and enforce a comprehensive cyber security policy.
- Create an incident recovery plan. Identify the personnel, processes, and tools needed for managing interruptions or critical events.

### CONTAINMENT

**Take the necessary critical steps to limit or contain the attack.**

- Identify the threat. For example; monitor your workstations and servers for suspicious activity. Several ransomware infections begin by encrypting a large number of files within a small amount of time.
- Identify the systems that have been compromised. Be aware that ransomware attacks may not encrypt all files. Computers may seem to operate normally yet documents are not accessible.
- Isolate compromised systems to prevent further infection.

### RESPONSE

**Immediately remove compromised computers from the network.**

- Determine the cost-effectiveness of a fresh rebuild or reinstallation of the compromised computer.
- Determine the complexity of threat removal and/or restoration method required. Some threats may be mitigated with antivirus software.
- Identify and correct malware system changes prior to reconnecting previously infected computers to the network.

**Additional Tips:**

- Consider calling an external expert. In many cases, a specialist security firm with experience in cyber incident response will be more adept at dealing with data breaches.
- Be aware that ransomware can potentially affect client data and comply with regulatory and legal requirements.
- Additional best practices for protecting networks from ransomware attacks may be found by browsing resources such as https://www.justice.gov/criminal-ccips/file/872771/download.