
# Ransomware Cheatsheet

Ransomware is computer malware (a program) that installs itself covertly on a victim's computer. It performs a cryptovirology attack (encrypting all or key files on your computer) and then demands some form of ransom in order to unlock or decrypt.

Not all ransomware is created equal. Some versions are crude and easily corrected, others are very complex and not easily corrected if corrected at all.

**What does ransomware do?**

- Prevent you from accessing your computer.
- Encrypt files so you can't use them.
- Disable certain applications (like your web browser).

**How did ransomware get on my computer?**

In most instances, ransomware is installed on your machine when you visited a malicious or hacked website. There may be no indication that it was installed.

**Should I pay the ransom?**

Hard to say. There is NO guarantee that that paying will gain you access to your computer or files. Further, by paying you may make yourself a larger target for MORE malware.

**If you DID pay the ransom,** you should contact your bank and local authorities immediately. If you paid with a credit card, your bank may be able to block the transaction. Further, you can seek guidance from the following government website. (https://www.consumer.ftc.gov/)

**How do I get my files back?**

If you've performed a previous backup of your system, you may be able to roll back to that. (Assuming the backup hasn't been compromised)

**How do I protect myself from ransomware?**

- Install and use up-to-date antivirus.
- Make sure your software is up to date.
- Avoid clicking on links or opening attachments from people you don't know.
- Use a pop-up blocker.
- Segmentation. Business/Corporate grant users only limited access to shared drives.
- REGULARLY BACKUP YOUR IMPORTANT FILES. (Legal documents, Pictures, etc)

Joe Blanchard
STL OWASP Lead
joe.blanchard@owasp.org

Cliff Smith
STL OWASP Lead
cliff.smith@owasp.org