**Ransomware**

**Description 1**

Ransomware is a type of malicious software that infects and restricts access to a computer until a ransom is paid. Although there are other methods of delivery, ransomware is frequently delivered through phishing emails and exploits unpatched vulnerabilities in software. [1]

**Description 2**

There are different types of ransomware. However, all of them will prevent you from using your PC normally, and they will all ask you to do something before you can use your PC. They can target any PC users, whether it’s a home computer, endpoints in an enterprise network, or servers used by a government agency or healthcare provider.

e.g. Ransomware can:

* Prevent you from accessing Windows.
* Encrypt files so you can't use them.
* Stop certain apps from running (like your web browser).

Ransomware will demand that you pay money (a “ransom”) to get access to your PC or files. We have also seen them make you complete surveys. [2]

**Description 3**

Ransomware is a malicious program that locks a computer's files until a ransom is paid. [3]

**Reference**

[1] [**https://www.us-cert.gov/security-publications/Ransomware**](https://www.us-cert.gov/security-publications/Ransomware)

[2] [**https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx**](https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx)

[3] <http://www.bbc.com/news/technology-39896393>