The City University of New York

Information Security Advisory

Information Security, Computing and Information Services

security.cuny.edu

Ransomware

What is ransomware?

Ransomware is malicious software (malware) that seeks to elicit a ransom payment from a victim. When ransomware infects a system it commonly encrypts all of the document files on the hard drive as well as accessible network folders. Documents so encrypted are unusable unless decrypted with a unique decryption key held by the attackers.

After a ransomware infection takes hold, instructions on how to pay the ransom are presented, typically demanding payment in the virtual currency known as Bitcoin to obtain the decryption key. Paying the ransom doesn’t guarantee successful recovery.

What can I do to help prevent infection by ransomware?

- Be wary and skeptical of unsolicited email that demands immediate action even from well-known and reputable companies or government agencies, including well-designed but counterfeit invoices and failed courier delivery notices or claims of illegal activity
- Don’t click on links or attachments in email from unfamiliar sources or that seem suspicious—call the source to confirm authenticity
- Maintain up-to-date security (anti-virus) software
- Practice safe online behavior

What can I do to protect documents against ransomware?

All important documents and files must be backed up on a regular, ongoing basis. Should ransomware render documents unusable in an unfortunate circumstance, the documents can then be recovered from a pre-infection backup copy.

If your system is supported by a CUNY campus/central IT department, you should ascertain to what extent your system’s documents are backed up for you. If your system is self-supported, you need to perform backups yourself.

It is additionally important to abide by the following backup practices:

- Backup media must be kept offline—a ransomware-encrypted backup copy on an always-connected portable drive is useless
- the backup process must be monitored to ensure backups complete successfully
- periodically verify that files can be successfully restored from the backup
- keep multiple backup sets

How can a system become infected with ransomware?

Ransomware infections typically occur by opening malicious attachments and links in spam/phishing emails and by browsing to a website that's been compromised to infect visitors. Systems infected with other forms of malware can also be commanded by attackers to retrieve and install ransomware.

Can ransomware spread from one computer to another?

Yes. Ransomware is becoming contagious. A recent ransomware version additionally attempts to infect other computers and transform affected document files into infectious ransomware programs. An uninfected system can become infected when such a document is opened. In this way, ransomware infections can spread across systems that access a common shared folder, for example.

Does security (anti-virus) software protect against ransomware?

Anti-virus software detects and prevents infection from known ransomware variants, but there can be a period between the release of a new ransomware variant and effective anti-virus protection. Running up-to-date anti-virus software (as required by CUNY policy) is important but protection is not absolute. Security software that includes an intrusion prevention feature can also help to prevent ransomware from spreading between systems.

Can ransomware-encrypted files be recovered without paying ransom?

Document recovery has been achieved in limited circumstances with earlier ransomware versions. Unfortunately, more recent ransomware can't be circumvented as "flaws" in the underlying encryption techniques have been eliminated.

I think my system's infected with ransomware and my files are unusable. What should I do?

Turn off your computer and contact your CUNY campus/central IT department help desk immediately for assistance.

Where can I find the CUNY IT Security policies and advisories?

Please visit http://security.cuny.edu/