Published on *University of Colorado* (https://www.cu.edu)

What is Ransomware? [1]

Ransomware is a type of malicious software (sometimes called malware) that locks and encrypts your computer or files, and then demands a ransom to remove the malware and restore access. Ransomware is often delivered via a phishing email with an attachment or link that, when clicked, installs the malicious program.

It appears to be on the rise in higher education with six highly-publicized breaches in 2019 and a loss of untold millions of dollars.

How do you protect yourself from ransomware?

- One of the best ways to protect yourself is to create a good backup of your critical data. These backups should be available offline, for example, on a removable hard drive. For your work files, be sure to follow guidelines from your campus IT department.
- Keep the computer software up-to-date, including antivirus and firewalls.
- Don’t open email attachments you are not expecting, even if it appears to come from someone you know. Their account may have been compromised.
- Be cautious of links provided in an email. Hover your mouse over the link to verify that the URL leads to a site you recognize.

Should you pay the ransom?

No, advises the FBI, because it only encourages the cybercriminals. Even if the ransom is paid, there is no guarantee that you will be able to regain access to your files.

If you experience ransomware…

- At CU, immediately notify your appropriate campus contact
- At home, report it to the FBI Internet Crimes Complaint Center [2]

Groups audience:
Office of Information Security

Source URL:https://www.cu.edu/security/what-ransomware

Links
[1] https://www.cu.edu/security/what-ransomware [2] https://www.ic3.gov/default.aspx