mimecast® | Awareness Training *for Cyber Resilience*

Ransomware

What you should know about ransomware.

Ransomware is a form of malicious software (or malware) that, once it's taken over your computer, threatens you with harm, usually by denying you access to your data.

The attacker demands a ransom from the victim, promising — not always truthfully — to restore access to the data upon payment.

How do I protect my computer against ransomware?

As with all threats, prevention is key. This is especially true for threats as damaging as ransomware.

You should:

- Backup your important files regularly.
- Consider using the 3-2-1 rule for your home use data: Make three backup copies, store in at least two locations, with at least one offline copy. (Data protection for colleges is already done in accordance with all best practices.)
- Use a vetted cloud storage service to store an archive of your files. You can try to restore your files from backup in the event of a ransomware infection.
- Install and use an up-to-date antivirus solution.
- Don't click links or open attachments on emails from people you don't know or companies you don't do business with.
- Make sure your software is up-to-date to avoidexploits.
- When browsing the Internet, use a vetted browser which stops exploit