

Repel Ransomware!

How to Protect Your Library



What is Ransomware?

"A form of malware targeting both human and technical weaknesses in an effort to make critical data and/or systems inaccessible."*

Users are locked out of their system until they pay a ransom.



2,047

**Victims
in 2019****

Education & government sectors sustain the highest rates of attacks.

*: www.ic3.gov/Home/Ransomware

**: pdf.ic3.gov/2019_IC3Report.pdf

How Ransomware Works

Malware received through an email link or website.

Malware then infects the computer, locking it down.

A ransom note demands money to release the device.

Paying a ransom does not guarantee access will be restored.



Shield Your Library



EDUCATE

Remind employees not to click links from unknown sources.

Create a training and awareness program.

Create an action plan for infection.

AND

PREVENT

Enable strong spam filters & patch software/programs.

Schedule regular anti-virus/malware scans.

Test for vulnerability at least once a year.

In Case of Ransomware

Isolate infected device.

Verify safety of backup data.

Contact law enforcement.