Repel Ransomware! How to Protect Your Library





DIVISION OF LIBRARY and INFORMATION SERVICES



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.



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 AND PREVENT

Remind employees not to click links from unknown sources.

Create a training and awareness program.

Create an action plan for infection.

Enable strong spam filters & patch software/programs.

Schedule regular antivirus/malware scans.

Test for vulnerability at least once a year.

In Case of Ransomware



This resource is funded under the provisions of the Library Services and Technology Act from the Institute of Museum and Library Services. Florida's LSTA program is administered by the Department of State's Division of Library and Information Services. During FY2020-21, the percentage of total costs for the Community Engagement and Resources Program financed with federal money is 66%; the federal dollar amount to be spent on the program is \$107,855. This program does not receive any non-governmental funding.