Best Practices for Avoiding Malware (Trust No One!)

Install and Maintain good anti-virus software

- Use secondary programs like CCleaner, Malwarebytes and Cybereason RansomFree to catch things your main AV software might miss.
- No AV software is perfect, so don't depend too much on it
- Keep your computer software up-to-date and patched
- Windows, Java, Adobe, Firefox and Chrome all need to be updated regularly
- Use Ninite monthly!

Be Skeptical!

- Assume any unexpected email or popup window is a scam trying to lure you into a trap
- Look for clues like odd spelling and phrasing, vagueness, and dire warnings that reveal the scammers
- ALWAYS mouse over a link BEFORE you click on it
- If you have ANY doubt, check with Pete or Jody BEFORE clicking

How to handle an infection

- For serious infections like ransomware, power down and unplug the network cable from your computer immediately to keep it from spreading on the network.
- Call Pete or Jody!
- Run CCleaner, Ninite, then Malwarebytes
- Infected PUBLIC computers need only be rebooted to clean them up.

Physical Security

- NEVER plug a mysterious USB drive into a staff computer. Use a public computer if you must, preferably after it's been unplugged from the network
- NEVER plug a patron's flash drive into a staff computer. They don't necessarily know if it's been infected or not.
- NEVER let a patron check their email on a staff computer.
- Flash drives are OK to plug into printer/copiers.

Passwords

- Don't use one password for everything
- Be creative! Don't use obvious (names, dates, locations) words in your password
- Check https://haveibeenpwned.com to see if services you have used have been hacked, and your password has been exposed.