

## CYBER-SECURITY

Students will:

- A. Recognize security risks, make informed decisions, and protect themselves while using technology.
  - Understand and discuss security risks and the potential harm of intrusive applications related to technology, technology systems digital media and information technology including the Internet (e.g. email viruses, digital propaganda, spyware, adware, identity theft, phishing/pharming/spoofing scams, spam, social engineering).
  - Practice effective security practices and analyze new options, beyond the basic level, related to technology, technology systems, digital media and information technology, including the Internet, and critically evaluate digital resources.
  - Recognize and understand the purpose of security protection measures for technology, technology systems, digital media, and information technology.
- B. Understand appropriate protection methods and secure practices.
  - Adhere to security guidelines, policies, and procedures.
  - Describe and practice strategies for managing everyday hardware and software problems.
  - Describe and practice strategies for securing wireless connections (e.g., connect only to legitimate wi-fi hot spots or turn off w-fi, turn off file share mode, encryption of sensitive data/information, use and update of anti-virus software, use of a firewall, and update of operating system).
- C. Demonstrate commitment to stay current on security issues, software, and effective security issues, software, and effective security practices.
  - Demonstrate commitment to stay current on security issues and effective security practices.
  - Model secure practices within a variety of digital communities
- D. Advocate for secure practices and behaviors among peers and community.