Top 6 Cyber Security Tips for Starting the School Year Safely

1. Update software and operating systems to current versions and automate regular application of patches
    - Resources https://www.cisecurity.org; https://www.cisa.gov/cyber-hygiene-services

2. Practice good password hygiene
    - Use strong passwords: at least 8 characters in length, with a mix of uppercase characters, lowercase characters, numbers, and special characters.
    - Don't include personal information or use the same password for multiple systems.
    - Enforce strong passwords via system policy.
    - Train users in setting up passwords.
    - Encourage the use of password vaults. One free encrypted vault option is Keepass.

3. Encrypt all computers and devices
    - Start with new computers and apply encryption to older computers as they are worked on.

4. Perform regular phishing training and testing
    - Free phishing campaign assessment: https://www.cisa.gov/cyber-hygiene-services
    - Free employee cyber training through Beazley: www.beazleybreachsolutions.com
      Beazley provides free cyber security, assessment, breach response and training resources to NBSIA Property/Liability Program Members. If not already registered, contact Maria Cantera at mariac@nbsia.org for activation code.
    - KnowBe4: Phishing testing, assessment, and training. Discount offered to NBSIA Property/Liability Program members via Beazley. Contact NBSIA for more information.

5. Update outdated internet browsers and remove unsupported browsers
    - Microsoft will no longer support Internet Explorer after 6/15/2022.

6. Remind staff about safeguarding devices and hardware in transit:
    - Make sure device is off or locked.
    - Prior to departure, store device in trunk, or hidden location, if you will not be heading directly to office or home.
    - Keep other personal or valuable items in car out of site to prevent break-ins.
    - Do not store confidential data on CDs in transit.
    - Encrypt and password-protect confidential data on USB or hard drives.
    - Do not store password or login information with or near device.
    - Report lost or stolen devices or data storage immediately.

References for expert recommendations: The Center for Internet Security, CIS Critical Security Controls for Effective Cyber Defense, Version 8, https://www.cisecurity.org/