# TOP 10 CYBERSECURITY TIPS FOR TEACHERS

From the U.S. Department of Education's Student Privacy Policy Office (SPPO) and its Privacy Technical Assistance Center (PTAC)

## 1 Be Aware of Social Engineering Techniques

- Be skeptical. Question unexpected or atypical emails or requests for information, especially if they create a sense of urgency or pressure you into immediate action.
- Verify the identity of the person or organization by contacting them independently through official channels.

## 2 Use Strong Authentication Practices

- Use strong passwords.
- Enable multi-factor authentication.

## 3 Keep Devices Updated with the Latest Software & Security Patches

- Enable automatic updates.
- Regularly check for updates to your software and apps.

## 4 Use Anti-Virus Software & Scan Devices Often

- Install and use reputable antivirus software that checks in real-time to spot threats early.
- Ensure the software runs regular system scans.

## 5 Avoid Public Wi-Fi

- Use your mobile data or personal hotspot instead.
- Avoid accessing or sending sensitive information while connected to public wi-fi.

## 6 Encrypt Sensitive Information

- Enable full-disk encryption.
- Apply a password to sensitive files & folders.

## 7 Use Safe Browsing Strategies

- Be cautious when clicking on links or downloading files.
- Regularly clear your web browser cache and cookies.

## 8 Use Only Approved Software

- Use only school-approved software.
- Always scan downloaded software and data files.

## 9 Back Up Your Data

- Diversify your backup methods.
- Regularly test your backups.

## 10 Never Leave Devices Unlocked or Unattended

- Never leave a phone, laptop, or storage media unlocked or unattended.
- Do not attempt to plug in or attach any untrusted media.

**Questions or requests for additional information should be directed to SPPO and PTAC at PrivacyTA@ed.gov, or call 1-855-249-3072.**