



**Howard
County**
Public School System



HCPSS

Cybersecurity Best Practices

— 2026–2027 School Year —



1. THINK BEFORE YOU CLICK

- Be cautious of unexpected emails, links, or attachments.
- Verify requests involving sensitive information or financial transactions.
- When in doubt, don't click—ask first.



4. REPORT SUSPICIOUS EMAILS IMMEDIATELY

- If you receive a suspicious or phishing email, do not interact with it.
- Instead, forward the email immediately to:

abuse@hcpss.org

- Prompt reporting helps protect everyone across HCPSS.



2. PROTECT YOUR CREDENTIALS

- Never share your password.
- Use strong, unique passwords.
- Enable Multi-Factor Authentication (MFA) whenever available.



3. PRACTICE GOOD DIGITAL HYGIENE

- Lock your computer whenever you step away.
- Keep devices updated.
- Handle student records and other confidential information carefully.
- Store files only in approved HCPSS locations.



5. COMPLETE YOUR ANNUAL CYBERSECURITY AWARENESS TRAINING

- All HCPSS staff are required to complete the Cybersecurity Awareness Training available in Vector.
- Complete your training by visiting:

<https://howard-md.safeschools.com/login>

- This annual training will help you:
 - ✓ Recognize phishing and other cyber threats.
 - ✓ Protect sensitive student and staff information.
 - ✓ Follow cybersecurity best practices.
 - ✓ Understand your role in safeguarding HCPSS systems and data.

SCAN TO COMPLETE
YOUR REQUIRED
ANNUAL CYBERSECURITY
AWARENESS TRAINING



THANK YOU FOR DOING YOUR PART TO KEEP HCPSS SECURE.

If you have any questions or concerns regarding cybersecurity, believe you may have encountered a phishing email, or need assistance with a security-related issue, contact Technology Support at TechSupport@hcpss.org or 410-313-7004. Our team appreciates your partnership in keeping our school community safe.



TECHNOLOGY SUPPORT

TechSupport@hcpss.org
410-313-7004



WE WISH EVERYONE A SAFE, SUCCESSFUL, AND CYBER-SECURE 2026–2027 SCHOOL YEAR!