

October is Cybersecurity Awareness Month

Keep our schools secure

Every account, document, and device matters.

Stolen accounts, exposed records, and ransomware can interrupt learning. Small daily actions help protect student privacy and school operations.

-  **Watch for school-related phishing**
Question unexpected shared files, payroll changes, invoices, and urgent messages from a principal or colleague. Verify through a known contact; open familiar services directly.
-  **Protect accounts and MFA**
Use strong, unique passwords and multifactor authentication (MFA) where available. Never share passwords or verification codes. Deny and report sign-in prompts you did not initiate.
-  **Limit access to student information**
Check recipients and file permissions before sharing grades, IEPs, health records, or rosters. Use approved HCPSS storage and tools; avoid public sharing links and personal email.
-  **Secure classroom devices and apps**
Lock your screen when you step away, allow managed updates, and use approved apps and browser extensions. Unexpected downloads can introduce malware or ransomware.

Call to Action

Today, review the sharing permissions on one student-related file, lock your screen whenever you step away, and visit KnowBe4 to review available cybersecurity resources.

Explore the added Artificial Intelligence modules available in the KnowBe4 library.

<https://training.knowbe4.com> | Staff Hub > Services > KnowBe4 Cybersecurity Resources

Videos and Webinars

Staff are invited to explore these videos and webinars. These sessions offer deeper learning for interested staff and technology leaders.

October 21, 2026 | 1:00 - 2:00 PM ET | NIST NICE

Helping to Chart the Course - Unlocking Student Pathways into Cybersecurity Careers (Webinar)

<https://www.nist.gov/news-events/events/2026/10/nice-webinar-helping-chart-course-unlocking-student-pathways>

Online Safety and Privacy Videos

National Cybersecurity Alliance | Video collection

<https://www.staysafeonline.org/resources/online-safety-and-privacy/videos>

Report concerns immediately Do not click links or open attachments in suspicious email. Forward it to abuse@hcpss.org. If you clicked, shared information, approved an unexpected MFA prompt, or notice unusual device activity, contact Technology Support immediately at TechSupport@hcpss.org or 410-313-7004.