

Cybersecurity Awareness Doesn't End in October

Use AI safely | Protect student information | Verify unexpected requests



As Cybersecurity Awareness Month concludes, artificial intelligence (AI) is also being used for malicious cyber activities, including convincing phishing, impersonation, and scaled scams. Remain vigilant to protect HCPSS students, staff, and sensitive information.

Why vigilance matters

- According to Microsoft's 2025 Digital Defense Report, AI-automated phishing emails achieved a 54% click-through rate compared with 12% for traditional attempts.
- According to the Center for Internet Security's 2025 K-12 Cybersecurity Report, 82% of reporting K-12 organizations experienced cyber threat impacts.

Use AI safely

Verify convincing messages

AI can produce polished phishing emails. Open familiar HCPSS services directly rather than using an unexpected email link or QR code.

Confirm voices and urgent requests

A familiar voice or video may be AI-generated. Call a known number to verify requests for student records, payments, gift cards, or account changes.

Keep sensitive information out of AI prompts

Do not enter student records, IEPs, health information, staff data, passwords, or confidential documents into unapproved AI tools. Use only HCPSS-approved tools as authorized.

Check AI answers and suggested actions

AI can invent facts, links, and instructions. Verify sources before sharing output. Do not run suggested commands or install software without Technology Support guidance.

Call to Action

Before your next AI task, remove sensitive information. Visit KnowBe4 to review available AI and phishing resources, and explore the videos and webinars below.

Explore the Artificial Intelligence modules in the KnowBe4 library.

training.knowbe4.com | [Staff Hub > Services > KnowBe4 Cybersecurity Resources](#)

Videos and Webinars

Scams in the Age of AI

National Cybersecurity Alliance with Identity Theft Resource Center | On demand

<https://www.staysafeonline.org/events/scams-in-the-age-of-ai>

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 at TechSupport@hcpss.org or 410-313-7004.