# Keeper Security Issues Cybersecurity Guidance for Education IT Teams Ahead of New Academic Year

*AI-powered phishing attacks, deepfake impersonations and a surge of unmanaged machine identities are turning the back-to-school rush into a security blind spot*

LONDON, UNITED KINGDOM, August 13, 2026 /EINPresswire.com/ -- Every fall, schools, colleges and universities across the country race to onboard thousands of new students, faculty and staff, provisioning accounts, issuing credentials and connecting a wave of new devices to institutional networks. It is a moment of organised chaos, and cybercriminals know it. Now, with artificial intelligence supercharging phishing campaigns and a hidden layer of unmanaged machine identities quietly expanding the attack surface, Keeper Security, the leading provider of zero-trust and zero-knowledge identity security and Privileged Access Management (PAM), is providing guidance to education IT teams this back-to-school season. Keeper is sharing the top threats facing primary and secondary schools and higher education institutions this fall and the steps IT teams can take to protect their students and faculty before the semester begins.

> Back-to-school is the right moment for education IT teams to take stock of every identity on their network, human and non-human alike."
>
> *Darren Guccione, CEO and Co-founder of Keeper Security*

The Threat Window Is Growing

The education sector is one of the highest targeted industries for ransomware, credential theft and data breaches. Schools and universities present an appealing combination of high-value data, including student records, financial information and research, alongside chronically underfunded IT departments and an enormous, ever-rotating user base.

Back-to-school season intensifies every one of these vulnerabilities. Bulk account creation, mass device enrollment and a surge of third-party application onboarding all happen simultaneously, creating a window of misconfiguration and exposure that attackers are primed to exploit. However, Keeper research finds only 14% of schools mandate security awareness training, and that lack of education shows, with nearly one in five students and parents reporting they reuse the same passwords across both personal and school accounts.

AI has made cybersecurity threats significantly more dangerous. Phishing emails can now precisely mimic communications from student funding offices, IT helpdesks or university leadership, with none of the red flags that once made them easy to spot. Deepfake voice and video attacks are putting convincing faces and voices behind those messages, making it harder for staff to trust what they see and hear. Keeper research found 52% of education leaders identify deepfake impersonation as a top concern, yet only 26% feel confident in their ability to recognise AI-enabled threats. And the barrier to entry for attackers has dropped dramatically: tools that once required real sophistication are now widely available, meaning credential attacks that previously targeted only the largest institutions can now be aimed at any school or campus. Forty-one percent of institutions report that they have been targeted by AI-generated phishing attempts or misinformation campaigns.

The Hidden Attack Surface: Non-Human Identities in EdTech

While IT teams focus on securing human accounts, a far larger and largely invisible population of digital identities is growing unchecked across education environments: Non-Human Identities (NHIs). In a modern school or university, NHIs are widespread and almost entirely unmanaged:

- Service accounts synchronise student rosters and course enrollments between Student Information Systems like SIMS, Arbor or Banner, and Learning Management Systems like Canvas, Blackboard or Google Classroom. Their credentials are rarely rotated, often shared and almost never audited.
- API keys and integration tokens connect third-party learning applications, digital textbooks, library databases and payment gateways to central institutional databases. Orphaned tokens from prior-year integrations frequently remain active.
- Machine identities and digital certificates authenticate campus-wide Wi-Fi connections, interactive smart boards, lab equipment, 3D printers and security cameras. Expired or misconfigured certificates create silent gaps in network security.
- Cloud-managed identities and workloads on platforms like Azure, AWS and Google Cloud manage automated data backups, research data pipelines and administrative reporting, often with far broader permissions than their tasks require.
- AI agents and automated bots powering admissions chatbots, helpdesk scripts and grading assistants each carry their own identity and access rights, and are among the fastest-growing and least-governed NHIs in education today.

In most institutions, NHIs outnumber human users by a wide margin, yet few schools maintain an inventory of them. This causes the attack surface to explode, as each NHI represents a potential entry point for attackers.

"The conversation about education cybersecurity has historically focused on human accounts: students, teachers and administrators," said Darren Guccione, CEO and Co-founder of Keeper Security. "But the real blind spot is the vast ecosystem of machine identities that power modern

EdTech. Back-to-school is the right moment for education IT teams to take stock of every identity on their network, human and non-human alike."

How Education IT Teams Can Reduce Their Risk

For most institutions, the fundamentals are manageable: enforcing MFA, auditing privileged access and removing stale credentials before new users arrive. The harder challenge is building visibility and governance over the NHIs that power modern EdTech: service accounts, API tokens, machine certificates and AI agents that multiply with every new integration. Keeper recommends education IT teams take the following steps before the semester begins:

-Enforce MFA across all faculty, staff and student accounts before new users are onboarded. It remains the single most effective control against credential-based attacks.
-Deploy an enterprise password manager institution-wide to eliminate weak, reused and shared passwords. Ensure all privileged accounts are covered.
-Audit privileged access, both human and non-human, before the semester starts. Remove access for departed employees, expired service accounts and applications no longer in use.
-Build a non-human identity inventory. Catalogue every service account, API key, machine certificate, cloud identity and AI agent in your environment. You cannot secure what you cannot see.
-Establish credential rotation policies for machine identities, with particular attention to AI agents and third-party EdTech integrations added for the new school year. Automate rotation wherever possible.
-Update phishing awareness training to reflect the reality that AI-generated messages may now be indistinguishable from legitimate institutional communications.

Keeper's zero-trust, zero-knowledge platform is purpose-built for these challenges, enabling institutions to discover, govern and automatically rotate credentials tied to human users and NHIs, including the AI agents and automated bots proliferating across EdTech environments. KeeperPAM also delivers the privileged access controls, session recording and audit trails institutions need to meet UK GDPR, the Data Protection Act 2018 and the Department for Education's safeguarding and filtering requirements, and to ensure every identity on the network, human or non-human, is accounted for.

For more information on how Keeper protects education institutions, visit keepersecurity.com.

###

About Keeper Security
Keeper Security is the leading zero-trust and zero-knowledge identity security solution, trusted by millions of people and thousands of organisations globally. KeeperPAM® is Keeper's privileged access management platform that unifies password and passkey management, secrets management, privileged session management and endpoint privilege management in a single

cloud-native platform, protected with quantum-resistant encryption. KeeperAI delivers real-time, AI-native threat detection across every privileged session. As AI agents proliferate and identity becomes the defining attack surface, Keeper governs access for humans, machines, non-human identities and AI agents, serving as the unified control plane for access, compliance and visibility across the enterprise. For more information, visit keepersecurity.com.

Charley Nash
Eskenzi PR
email us here