



**Learning
Technology
Center**

vCISO PROGRAM

Monthly Cyber Threat Intelligence

September 2026

Compiled by Technology Learning Center, vCISO Program

Covers August 20, 2026 to September 19, 2026

Table of Contents

Table of Contents	2
Introduction	3
Threat Landscape for September 2026	3
Monthly Areas of Focus	4
PaperCut NG/MF Zero-Day — Education Customer Was First Victim (CVE-2026-81578 / CVE-2026-82078)	4
[Threat / Vulnerability / Incident Name 2]	4
Ubiquiti UniFi — Three Maximum-Severity Flaws Across Network, Camera, and Phone Platforms	5
Google Chrome Zero-Day (CVE-2026-85046) — Sixth Exploited Chrome Flaw of 2026	5
BigBear and Passkey-Themed Phishing — MFA Bypass Against Microsoft 365	6
Mathspace Breach — EdTech Vendor Patch Gap Exposes Over One Million Students and Families	7
[Threat / Vulnerability / Incident Name 2]	7
IDScan and Florida DMV Breaches — More Than 150 Million Identity Documents Exposed	8
AI Crosses the "Critical" Line — Autonomous Exploit Discovery and the Vulnerability Firehose	8
AI Assistants and Browser Agents Become an Attack Surface	9
Avada WordPress Theme — Zero-Click Remote Code Execution (CVE-2026-18431)	10
Microsoft 365 Authentication Outage — Cloud Dependency During the First Week of School	10
Fake Installers and Malicious Browser Extensions — Disabling Defenses From the Inside	11
CISA Retires Free Assessments — Shrinking Federal Support for Districts	11
Recommendations	12
Identity and access	12
Patch and vulnerability management	12
Vendor and third-party risk	12
Network architecture	13
Incident response and continuity planning	13
AI governance and data privacy	13
Awareness and training	13
LTC vCISO Program	13
K-12 Breach Sources (district incidents):	14
References	14
Executive Summary	16

Introduction

The mission of the Learning Technology Center (LTC) in Illinois is to empower K-12 public school districts, schools, and educators through technology services, strategic consulting, and professional learning to improve educational opportunities for all students. In pursuit of that mission, the vCISO Program compiles this monthly intelligence analysis to provide K-12 technology leaders with actionable risk insights.

The September 2026 reporting period is defined by the back-to-school risk we warned about last month becoming reality. Seven school systems disclosed cyber incidents in roughly three weeks, a zero-day in a print management platform used across K-12 hit an education customer first, and phishing kits that defeat standard multi-factor authentication moved into wide circulation. At the same time, AI is shortening the time between a flaw's disclosure and its exploitation, and the federal support districts once relied on continues to shrink.

Threat Landscape for September 2026

In August, we said the back-to-school window would be the difference between a normal opening week and a headline. September proved it. Between late August and mid-September, seven school systems in five states reported incidents. Springfield Public Schools in Massachusetts closed for four instructional days and later learned from the FBI that student and staff data had been stolen. Westfield, NJ ran its first week of school on paper. Slate Valley, VT went almost a week without internet, and Monroe, WI shut down every internet-connected device, phones included. Three of the seven school systems appeared on ransomware leak sites, including INC Ransom, the same group that led July's SonicWall exploitation.

The dominant technical theme continues from August: identity is the perimeter. Last month's Entra ID credential theft campaign has been followed by phishing platforms that defeat SMS, push, and one-time-code MFA in real time. The BigBear service completed MFA bypass at 258 organizations, and a separate campaign impersonates the IT help desk to walk staff through a fake "passkey update." Stolen browser sessions, harvested by infostealers, bypass MFA entirely. When attackers can log in, they do not need to break in.

The platforms districts depend on were just as exposed. PaperCut, a staple of school print environments, was exploited as a zero-day with an education customer reporting the first compromise. Ubiquiti UniFi, common in budget-conscious districts, disclosed three maximum-severity flaws. Chrome shipped its sixth exploited zero-day of the year. On the vendor side, the Mathspace breach showed how a single late patch at an edtech company can expose more than a million students and families, and a ShinyHunters claim tied that breach back to the same crew behind July's Canvas incident.

Two broader forces sit behind all of this. First, AI is accelerating the attacker's side of the clock: OpenAI rated a model "Critical" for autonomous exploit development, and AI-driven vulnerability

hunting is generating more findings than maintainers can triage. Second, defenders have less outside help. CISA retired six free assessments, including its Ransomware Readiness Assessment, and is operating at roughly a third below prior staffing. For Illinois districts, the takeaway is that the fundamentals are not optional: phishing-resistant MFA, fast patching of actively exploited flaws, real vendor accountability, and continuity plans that work when the network does not.

Monthly Areas of Focus

PaperCut NG/MF Zero-Day – Education Customer Was First Victim (CVE-2026-81578 / CVE-2026-82078)

Severity: Critical

What happened: On August 27, an education-sector customer reported a compromised PaperCut server to the vendor; a second organization reported similar activity that afternoon. Attackers chained an authentication bypass (CVE-2026-81578, CVSS 8.8) with unsafe class loading in the database connector (CVE-2026-82078, CVSS 9.4) to gain unauthenticated remote code execution on PaperCut NG and MF versions 24, 25, and 26. Researchers found bypasses in the first fixes, forcing a series of emergency patches through September 1; systems on an earlier emergency patch remain vulnerable. CISA added both flaws to its Known Exploited Vulnerabilities (KEV) catalog on August 31, and a public Metasploit module now exists. Huntress reports that 47% of the roughly 2,500 PaperCut installations it tracks are still on version 23 or older.

K-12 relevance: PaperCut is one of the most widely deployed print management platforms in K-12, and the first reported victim was an education-sector customer. Print servers are often treated as "set it and forget it" infrastructure, run on-premises with broad network access and service-account privileges, which makes them an ideal foothold for lateral movement toward student information systems and file shares.

Recommended action: Apply the latest emergency build immediately and confirm the version against PaperCut's advisory (Huntress lists 26.0.5, 25.0.13, and 24.1.10). Remove any internet exposure of the PaperCut Application Server. Look for Indicators of Compromise (IoC), including unexpected `.class` files in `server/lib/`, a Derby database named `memory:pwn`, a deleted `server.log`, and `.cmd` or `.out` files in `server/data/content/`. **Districts running version 23 or older should treat an upgrade as an urgent project, not routine maintenance.**

Ubiquiti UniFi – Three Maximum-Severity Flaws Across Network, Camera, and Phone Platforms

Severity: High

What happened: Ubiquiti disclosed three CVSS 10.0 vulnerabilities: an input validation flaw in UniFi Protect allowing unauthenticated remote compromise (CVE-2026-77537), a CRLF injection allowing authentication bypass on UniFi OS (CVE-2026-77550), and a command injection flaw in UniFi Talk VoIP (CVE-2026-77554). In total, 21 of the 22 issues in the bulletin scored 9.0 or higher. Censys counted more than 100,000 UniFi OS instances exposed to the internet and found about 90% still unpatched 16 hours after disclosure. *No exploitation had been confirmed at the time of reporting.*

K-12 relevance: UniFi wireless, switching, Protect cameras, and Talk phones are common in K-12, especially in smaller and budget-constrained districts. A single compromised UniFi controller can expose the network, the building cameras, and the phone system at once, which are the same systems that failed together in this month's district incidents.

Recommended action: Update to UniFi OS Server 5.1.37 or later, Network Application 10.5.67 or later, Protect 7.2.105 or later, and Talk 5.3.2 or later. Remove UniFi management interfaces from the public internet and place them on a restricted management VLAN reachable only by VPN with two-factor authentication, following the same remote-management design recommended for BMCs in August.

Google Chrome Zero-Day (CVE-2026-85046) – Sixth Exploited Chrome Flaw of 2026

Severity: High

What happened: Google's September 1 stable release fixed 26 security issues, including two critical use-after-free flaws. Days later, Google patched CVE-2026-85046, a V8 type confusion flaw (CVSS 8.8) confirmed as exploited in the wild, in Chrome 152.0.7977.82/.83. It is the sixth exploited Chrome zero-day of 2026.

K-12 relevance: Chrome and ChromeOS are the most common student computing platforms in K-12. Districts sometimes pin Chrome versions to protect testing or classroom applications, and those policies can quietly leave thousands of devices behind on a vulnerable build.

Recommended action: Confirm through Google Admin and endpoint management that managed Chrome and ChromeOS devices are on 152.0.7977.82 or later. Review any version-pinning or delayed-update policies and set a clear maximum delay for security releases.

BigBear and Passkey–Themed Phishing – MFA Bypass Against Microsoft 365

Severity: High

What happened: CloudSEK researchers gained access to BigBear 2.0, an adversary-in-the-middle phishing service built on Evilginx2 and leased to at least five affiliates. It targeted 461 organizations and completed MFA bypass at 258, capturing more than 5,000 credential records, over 1,000 plaintext passwords, and more than 4,100 session cookies. The kit even uses custom code to disable FIDO2/WebAuthn on its phishing pages to push victims toward weaker methods. Separately, Microsoft and others tracked a campaign active since May in which attackers call or text staff posing as the IT help desk and urge them to "update" their passkey or MFA. Victims are sent to fake sign-in pages or device-code prompts, after which attackers register their own MFA method and pull mailbox and SharePoint/OneDrive data. A related wave sent more than a million AI-written "CEO" emails asking finance teams to pay fake ServiceNow invoices by ACH. A third platform, ZeroTokens, uses a live human operator to steer each victim through multi-stage phishing in real time.

K-12 relevance: This is the continuation of August's Entra ID credential theft story. Many districts run Microsoft 365, and many are in the middle of rolling out passkeys, which makes a "passkey update" call from the "help desk" sound routine. Business office, payroll, and HR staff are prime targets for ACH and W-2 fraud, and a single compromised staff mailbox can send trusted phishing to the entire district and its families.

Recommended action: MFA as a checkbox is not enough. Prioritize phishing-resistant MFA (FIDO2 keys or device-bound passkeys) for IT administrators, the business office, HR, and the superintendent's office. Enforce Conditional Access that requires managed devices, disable device-code authentication where it is not needed, and alert on new MFA method registrations. When an account is compromised, reset the password and revoke all sessions. Tell staff plainly that IT will never ask them to update a passkey through a link or an unexpected call, and give the help desk a call-back verification script.

Mathspace Breach – EdTech Vendor Patch Gap Exposes Over One Million Students and Families

Severity: High

What happened: Mathspace, an online math platform, disclosed that data on 1,079,819 students, parents, and staff was exposed. Attackers exploited a zero-day SQL injection in the company's self-hosted Metabase analytics server (reported as CVE-2026-72898, CVSS 10.0). Metabase released a fix on August 6, but Mathspace did not apply it until August 29 and did not perform Metabase's recommended post-patch compromise checks. Data was downloaded on August 27, and the breach was confirmed September 3. Affected users were in Australia and New Zealand; ShinyHunters, the group behind July's Canvas breach, claimed the Metabase compromise. Password and SSO data were not exposed. Similar vendor breaches this month

included Veradigm, where stolen vendor credentials were used to access a customer-service API, and CareCloud, where 3.75 million patient records were exfiltrated from a cloud environment.

K–12 relevance: US users were not affected this time, but Mathspace serves US schools, and the pattern applies to every edtech vendor holding student data. A district can do everything right and still have its students exposed by a vendor that patches late. This also shows that patching alone is not enough when a flaw was exploited before the patch arrived; someone has to check whether the attacker is already inside.

Recommended action: Districts should not hesitate to engage vendors about their security processes. Add language to contracts and data privacy agreements requiring vendors to disclose patch timelines for critical flaws, perform compromise assessments after emergency patches, notify the district within a defined window, and provide logs on request. Inventory which vendors hold student PII and health data, and use tools such as Educause's HECVAT to structure vendor security reviews. Questioning EdTech providers' need for specific data should become a standard part of the implementation process.

IDScan and Florida DMV Breaches – More Than 150 Million Identity Documents Exposed

Severity: Medium

What happened: A service called "Nexus," advertised on a Russian cybercrime forum, offered scans of more than 153 million US and Canadian driver's licenses, front and back with infrared and UV images, plus more than 10 million ID cards, 3 million travel documents, and 579,000 medical cards. The data came from IDScan.net, an ID verification vendor that confirmed a long-running breach of its cloud systems. The FBI is investigating. Separately, ShinyHunters claimed more than 200,000 records from Florida's DAVID law-enforcement DMV database. Florida says a police employee's credential stored on a personal device was used, and the group leaked hundreds of thousands of files after the state refused to pay.

K–12 relevance: Staff, parents, and many older students are likely in these datasets. High-quality ID images make it easier for attackers to impersonate staff during help desk password resets, payroll direct-deposit changes, and even remote hiring. Many districts also use visitor management systems that scan driver's licenses, which is the same kind of vendor that was breached here. This data will also be added to the already vast data used by phishing campaigns.

Recommended action: The days of asynchronous single-item authentication are over. Staff will need to be trained to not accept a photo of an ID as sufficient proof for account recovery or payroll changes; require call-back verification to a number already on file. Ask visitor-management and HR vendors what they retain from ID scans, for how long, and how it is protected. Verify identity in person or through trusted ID proofing before issuing credentials to new remote staff or contractors.

AI Crosses the "Critical" Line – Autonomous Exploit Discovery and the Vulnerability Firehose

Severity: Medium

What happened: OpenAI rated its GPT-6 Astra model "Critical" for cybersecurity under its Preparedness Framework, the first model to reach that level. In testing, it found and chained two zero-days, escaped a browser sandbox, and gained root on a hardened system without step-by-step human guidance. OpenAI is restricting those capabilities to vetted testers. At the same time, Anthropic's Claude Mythos program has generated more than 26,000 vulnerability findings since April, but only 202 have been patched, and maintainers rated far fewer of them critical or high than the AI did. OpenAI leadership also warned that AI-driven attacks will become "ongoing, persistent" rather than one-off campaigns.

K-12 relevance: In July, we reported on JadePuffer and the shrinking time from intrusion to attack. This month's developments extend that trend to the front of the attack chain: the time between a flaw's disclosure and the emergence of a working exploit is collapsing. PaperCut and GitLab were both exploited within days of patches this month. Districts should also expect more CVEs, many with inflated severity scores, landing in the software their vendors use.

Recommended action: Patch priority should follow what is actually being exploited. Use CISA's KEV catalog and EPSS scores alongside CVSS to decide what gets patched this week versus this quarter. Shorten the patch window for internet-facing systems and for KEV-listed flaws, and ensure layered detection (EDR, MDBR, and log monitoring) is in place to catch what patching misses.

AI Assistants and Browser Agents Become an Attack Surface

Severity: Medium

What happened: Several new techniques target AI tools directly. "BragJack" showed that a malicious browser extension can hijack the built-in AI agent in Chrome (Gemini), Edge (Copilot), and other AI browsers; Google and Microsoft have patched their flaws (CVE-2026-0628 and CVE-2026-55945). Researchers hid encrypted instructions on a web page that Grok decrypted and obeyed, leaking the user's name, location, and chat prompts. Nvidia's NemoClaw tool exposed a local AI model server that any website could take over and poison (CVE-2026-65105; no Windows fix yet). Infostealer malware is stealing logged-in Claude sessions to spend victims' paid usage.

K-12 relevance: Students and staff are adopting AI assistants and AI-enabled browsers faster than districts can write policy. These tools can leak data without a click, and teachers pasting student information into unapproved AI tools creates FERPA and SOPPA exposure. On a positive note, the AFT and Microsoft reached a legally enforceable agreement that Microsoft will not train AI on student or teacher data or track students, with protections available to districts starting November 1.

Recommended action: Publish an approved-AI-tools list and clear staff guidance on what data may not be entered into AI tools. On managed Chrome and Edge, allowlist extensions and consider disabling built-in AI agent features for students. Inventory local AI tools in computer science and CTE labs. Add AI training-data and tracking prohibitions to data privacy agreements, using the AFT-Microsoft terms as a benchmark.

Avada WordPress Theme – Zero-Click Remote Code Execution (CVE-2026-18431)

Severity: Medium

What happened: Wordfence disclosed a critical flaw (CVSS 9.8) in the Avada theme (versions up to 7.16) and its Fusion Builder plugin (up to 3.16) that lets an unauthenticated attacker run arbitrary code on a WordPress site. Avada has more than one million sales. Fixes were released August 25 in Avada 7.16.1 and Fusion Builder 3.16.1. A proof of concept exists, but no exploitation had been reported at publication.

K-12 relevance: This follows directly on August's wp2shell WordPress core flaw. Avada is one of the most popular premium WordPress themes, and district, school, PTO, booster club, and alumni sites often run it on shared hosting with no clear owner for updates.

Recommended action: As we said in August, open-source software is not free; it transfers responsibility to the people who run it. Inventory every WordPress site associated with the district, identify an owner for each, and update Avada and Fusion Builder to the fixed versions. Sites without an owner should be retired or moved to a managed platform.

Microsoft 365 Authentication Outage – Cloud Dependency During the First Week of School

Severity: Medium

What happened: Beginning August 31, a core authentication configuration problem disrupted Microsoft 365 for days. Exchange Online, Teams, OneDrive, SharePoint, Universal Print, Copilot,

and even the Defender XDR security console were affected. Outlook was degraded for about 12 hours on the first day, and Microsoft declared full resolution on September 3. A separate issue left some users unable to open the Teams desktop app on September 3–4. In parallel, NIST released draft IR 8613, which identifies 23 security challenges unique to multi-cloud environments, including inconsistent identity controls and limited incident data from providers. Public comments are due October 5, 2026.

K–12 relevance: For many districts, this landed in the first week of school. One provider misconfiguration took email, files, printing, and the security console offline simultaneously. Many districts run Microsoft 365 and Google Workspace side by side plus hundreds of SaaS apps, which is exactly the multi-cloud environment NIST describes.

Recommended action: Maintain a way to reach staff and families that does not depend on Microsoft 365 or Google sign-in, and document "provider down" procedures for attendance, communication, and printing. Use NIST IR 8613's vocabulary when asking vendors for logs and incident notification commitments, and consider submitting comments by October 5.

Fake Installers and Malicious Browser Extensions – Disabling Defenses From the Inside

Severity: Medium

What happened: Microsoft tracked a campaign using counterfeit software download sites to deliver remote access trojans that disable Windows Update services, add Microsoft Defender exclusions, and delete shadow copies. Microsoft lists education among the victim sectors, though targets were mostly China-based. Researchers also profiled "PEEP," a backdoor disguised as a "Smart Bookmarks" extension for Chrome and Edge that steals cookies and browsing history, hijacks sessions, and runs commands on the host. An allied advisory described Iranian-linked malware using the same Defender-exclusion technique.

K–12 relevance: Staff downloading "free" tools from search results and installing unvetted browser extensions remain common entry points in districts. Malware that disables updates and adds antivirus exclusions can sit quietly on a machine long after the initial infection, and stolen browser cookies can bypass MFA.

Recommended action: Turn on Defender Tamper Protection and alert on new exclusions or disabled Windows Update services. Move from allowing all browser extensions to an allowlist of browser extensions in Google Admin and Intune and disable developer mode. Restrict software installation to a managed catalog, so staff has an approved way to get the tools they need.

CISA Retires Free Assessments – Shrinking Federal Support for Districts

Severity: **Medium**

What happened: CISA is retiring six free assessments: Cyber Resilience Reviews, Cyber Resilience Essentials, Ransomware Readiness Assessments, Incident Management Reviews, External Dependencies Management Assessments, and Cyber Infrastructure Surveys. Organizations are being directed to the Cross-Sector Cybersecurity Performance Goals (CPGs) and the self-run CSET tool instead. CISA's acting director said the agency's technical debt is "overwhelming"; CISA has lost about a third of its staff, with roughly 250 hires awaiting clearance. On the positive side, CISA released a K-12 Cybersecurity Foundations Resource Package in August and new guidance on using cyber decoys, such as honeytokens, to catch attackers using stolen credentials. MS-ISAC, now a paid membership since federal funding ended, has lost about 70% of its members.

K-12 relevance: Districts that relied on CISA regional advisors for free ransomware readiness or resilience reviews no longer have that option, and federal help will stay thin until hiring catches up. The burden shifts to self-assessment, state programs, consortia, cyber insurance, and partners.

Recommended action: Use CISA's K-12 Foundations package and the CPG self-assessment to replace retired reviews. Consider subscribing to the MS-ISAC membership. Small IT teams should consider honeytokens, such as a decoy admin account or canary files in shared drives, as a low-cost way to detect intruders. The LTC vCISO Program can help districts fill the gap left by the retirement of federal assessments.

Recommendations

Identity and access

Require phishing-resistant MFA (FIDO2 keys or device-bound passkeys) for IT administrators, the business office, HR, and the superintendent's office first, then expand to all staff. Enforce Conditional Access requiring managed devices, disable device-code authentication and legacy authentication where not required, and alert on new MFA method registrations. When an account is compromised, reset the password and revoke all sessions. Verify identity before issuing credentials to new staff and contractors, and apply least privilege for their first 30 days.

Patch and vulnerability management

Patch PaperCut NG/MF, Ubiquiti UniFi, and Chrome/ChromeOS immediately, and update any WordPress sites running Avada. Where used, patch GitLab (CVE-2026-85706, exploited), ServiceNow, and Fortinet FortiMonitorOnSight and FortiPAM. Prioritize with CISA KEV and EPSS, not CVSS alone, and set a short, documented patch window for internet-facing systems and actively exploited flaws. Keep optional preview updates in a test ring; this month's Windows preview update KB5120998 reset desktop settings until it was fixed in September's Patch Tuesday.

Vendor and third-party risk

Inventory vendors that hold student PII and health data. Add contract and data privacy agreement language requiring critical-patch timelines, post-patch compromise assessments, defined breach notification windows, and log access. Use HECVAT and NIST IR 8613's vocabulary to structure vendor conversations. Ask visitor-management and HR vendors what they retain from ID scans.

Network architecture

Segment VoIP phones, cameras, building automation, and safety systems from general IT, and place management interfaces for UniFi, PaperCut, and BMCs on restricted VLANs reachable only by VPN with two-factor authentication. Where the district shares a network with a municipality, define the separation and each party's incident response role. Confirm DDoS protection with your upstream provider ahead of state testing windows; the NightmareStresser service seized this month explicitly listed educational institutions among its targets.

Incident response and continuity planning

Test that offline, immutable backups restore, including the SIS and student health records. Document paper-based procedures for attendance, meals, transportation, and health services. Verify that emergency phones and public-safety links work without the district network. Maintain a family and staff notification method that does not depend on district sign-in. Prepare communication templates that avoid early speculation about cause. Know your cyber insurance incident response contacts and law enforcement points of contact before you need them.

AI governance and data privacy

Publish an approved-AI-tools list and staff guidance on student data in AI tools consistent with FERPA and SOPPA. Add AI training-data and student-tracking prohibitions to data privacy agreements, using the AFT-Microsoft terms (available November 1) as a benchmark. On managed browsers, allowlist extensions and consider disabling built-in AI agent features for students.

Awareness and training

Brief business office, payroll, and HR staff on AI-written superintendent and CEO payment requests, W-2 requests, and "passkey update" help desk scams. Give the help desk a call-back verification script and tell all staff that IT will never ask them to update a passkey through a link. Continue ClickFix awareness from July and August, and remind staff to download software only from the district's approved catalog. After a breach announcement, warn staff and families about follow-on phishing impersonating the district or credit-monitoring providers.

LTC vCISO Program

The vCISO Program provides K-12 school districts with affordable, shared, senior-level cybersecurity leadership, risk guidance, and strategic decision support without the high cost of hiring a full-time Chief Information Security Officer.

This monthly report is compiled by the vCISO program from research and observations. It is used in the service of the vCISO program's direct work with partner districts, but is also shared with the broader community. If you are interested in engaging the vCISO program to apply this data directly to your district's needs, please contact the LTC.

K-12 Breach Sources (district incidents):

- Springfield Public Schools, Springfield, MA
- Westfield Public Schools, Westfield, NJ
- Slate Valley Unified Union School District, VT
- School District of Monroe, Monroe, WI
- Sutton Public Schools and Town of Sutton, MA
- Lovejoy ISD, Lucas, TX
- Missouri Military Academy, Mexico, MO

References

- <https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/>
- <https://www.papercut.com/blog/news/behind-the-scenes-august-security-incident/>
- <https://www.rapid7.com/blog/post/etr-papercut-ng-mf-critical-zero-day-exploited-in-the-wild/>
- <https://www.huntress.com/blog/papercut-actively-exploited>
- <https://www.securityweek.com/more-details-emerge-on-exploited-papercut-vulnerabilities/>
- <https://www.bleepingcomputer.com/news/security/ubiquiti-patches-three-max-severity-security-vulnerabilities/>
- <https://censys.com/advisory/cve-2026-77550-cve-2026-77549-cve-2026-77550/>
- <https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html>
- <https://www.helpnetsecurity.com/2026/09/04/google-chrome-zero-day-cve-2026-85046/>
- <https://www.bleepingcomputer.com/news/security/bigbear-microsoft-365-phishing-service-bypassed-mfa-at-258-organizations/>

- <https://www.cloudsek.com/blog/tracking-bigbear-2-0-evilginx2-phishing-campaign>
- <https://thehackernews.com/2026/09/attackers-use-passkey-phishing-to.html>
- <https://www.bleepingcomputer.com/news/security/passkey-themed-phishing-attacks-lead-to-microsoft-365-data-theft/>
- <https://www.infosecurity-magazine.com/news/zerotokens-phishing-real-time/>
- <https://www.theregister.com/security/2026/09/04/ascii-smuggling-isnt-just-an-ai-security-risk/5294595>
- <https://www.microsoft.com/en-us/security/blog/2026/09/03/ascii-smuggling-crosses-over-from-ai-prompt-injection-to-phishing-evasion/>
- <https://www.theeducatoronline.com/k12/news/mathspace-breach-exposes-23day-patch-gap-in-school-systems/289186>
- <https://www.securityweek.com/mathspace-data-breach-exposes-over-1-million-people/>
- <https://www.metabase.com/blog/security-update-6-aug-2026>
- <https://www.bleepingcomputer.com/news/security/veradigm-discloses-patient-data-breach-after-gentlemen-gang-claims-attack/>
- <https://techcrunch.com/2026/08/19/carecloud-confirms-3-7m-patients-had-their-medical-records-stolen-in-data-breach/>
- Identity-document breaches and hiring fraud
- <https://krebsonsecurity.com/2026/09/fbi-probes-service-selling-153m-drivers-licenses/>
- <https://techcrunch.com/2026/09/10/id-verification-giant-idscan-confirms-data-breach-with-more-than-150-million-drivers-licenses-stolen/>
- <https://www.bleepingcomputer.com/news/security/shinyhunters-hackers-claim-breach-of-florida-david-dmv-database/>
- <https://www.bleepingcomputer.com/news/security/florida-confirms-dmv-database-breach-via-stolen-police-account/>
- <https://www.infosecurity-magazine.com/news/fraudulent-hires-credentials/>
- <https://www.wired.com/story/openai-astra-first-ai-model-with-critical-cyber-abilities/>
- <https://www.securityweek.com/openai-astra-becomes-first-model-to-cross-critical-cybersecurity-threshold/>
- <https://www.darkreading.com/application-security/mythos-vulnerability-firehose-hits-human-bottleneck>
- <https://www.harishapc.com/blog/persistent-ai-cyber-attacks-the-new-chapter-in-offensive-threat-vectors>
- <https://cisoserries.com/openai-safety-rules-iranian-hackers-defender-crashes/>
- <https://www.darkreading.com/endpoint-security/bragjack-browser-agentic-ai>

- <https://thenewstack.io/encrypted-prompt-injection-grok/>
- <https://www.darkreading.com/cyber-risk/nemo-claw-networking-llm-poisoning-openclaw>
- <https://www.bleepingcomputer.com/news/artificial-intelligence/anthropic-warns-infostealer-malware-is-hijacking-claude-sessions-to-drain-usage/>
- <https://www.infosecurity-magazine.com/news/ncsc-warns-shadow-ai-security-risks/>
- <https://www.politico.com/news/2026/09/09/aft-union-microsoft-ai-deal-01068544>
- <https://www.engadget.com/2254167/microsoft-strikes-deal-with-national-teachers-union-to-not-use-school-data-to-train-ai/>
- <https://www.bleepingcomputer.com/news/security/critical-avada-wordpress-theme-flaw-enables-zero-click-rce/>
- <https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-online-outage-causes-email-failures-auth-issues/>
- <https://techcrunch.com/2026/08/31/microsoft-tests-fix-for-latest-hours-long-outlook-outage/>
- <https://www.bleepingcomputer.com/news/microsoft/microsoft-says-some-users-cant-open-the-teams-desktop-client/>
- <https://www.bleepingcomputer.com/news/microsoft/microsoft-says-kb5120998-windows-update-resets-desktop-settings/>
- <https://www.nist.gov/news-events/news/2026/08/multi-cloud-architecture-challenges-draft-ir-8613-available-public-comment>
- <https://www.infosecurity-magazine.com/news/nist-risks-multi-cloud/>
- <https://securityboulevard.com/2026/08/district-administration-k12s-biggest-cybersecurity-risk-isnt-devices-its-everything-beyond/>
- <https://thehackernews.com/2026/09/fake-software-installers-disable.html>
- <https://thehackernews.com/2026/09/peep-turns-chrome-and-edge-into-post.html>
- <https://www.cybersecuritydive.com/news/cisa-cybersecurity-assessments-ending/829371/>
- <https://therecord.media/cisa-hiring-nick-andersen-warning>
- <https://www.securityweek.com/cisa-releases-guidance-on-deploying-cyber-decoys/>
- <https://www.k12dive.com/news/cisa-issues-k-12-cybersecurity-guidance-as-schools-risks-persist/827841/>
- <https://www.cybersecuritydive.com/news/ms-isac-membership-loss-states-federal-funding-cut/821984/>

Executive Summary

This month, the back-to-school risk we warned about in August became real. Seven schools in five states reported cyberattacks or data breaches in about three weeks. Springfield, Massachusetts closed schools for four days, and the FBI confirmed that student and staff information was stolen. Other districts ran on paper for a week or lost phones and internet.

Attackers mostly got in by stealing logins and by using weaknesses in everyday school systems. New phishing tools can get past the text-message and app codes many districts rely on. Print, network, and browser software used in most schools needed urgent fixes, and the first known victim of the print software flaw was in education. A math learning company exposed data on over a million students and families because it installed a security fix late. Artificial intelligence is helping attackers work faster, while federal help for schools is shrinking.

The lesson for leadership: districts should require stronger sign-in protection for staff, install critical updates quickly, hold vendors accountable for security, and practice running school without the network. These steps are the best way to keep a cyber incident from closing school.