CyberNut

CyberNut.com

Staying Ahead of the Curve:
Cybersecurity in the Age of AI

- Grasp how AI is transforming cyber threats in education.
- Take away practical strategies and real-world insights.
- Build shared responsibility and stronger security culture.
- Equip leaders, staff, and students to defend effectively.

The bell rings, the inbox fills, testing season looms, and the Wi-Fi is carrying everything from attendance to payroll. Most days, it all just works.

But in 2025, the quiet background hum includes something new: cyber scams and attempted digital break-ins that feel closer, faster, and a lot more human. The twist? Generative AI is the accelerant. Think of it as power tools that criminals now use to write better emails, clone voices, and move faster than our old warning signs can keep up.

Why schools feel this more than most

School districts are prime targets for cyberattacks due to several factors. They hold vast amounts of sensitive student and staff data, valuable on the black market, while often operating with limited IT staff.

A major vulnerability stems from their reliance on numerous third-party solution providers for critical systems like student information, learning management, and payroll. Each solution provider is a potential entry point for attackers, with third-party breaches doubling in the past year from 15% to 30% (Verizon Data Breach Investigation Report, 2025). Additionally, schools face challenges with a dynamic user base, including shared devices, substitute teachers, and volunteers, which makes consistent security enforcement difficult. Persistent threats include system intrusions, human error (like improperly redacting sensitive data), and social engineering (phishing). A multi-faceted approach involving strong defenses, training, and cybersecurity awareness is crucial to address these ongoing risks.

Sensitive data exposure

Student and staff information valuable on the black market

Third-party vulnerabilities

Critical systems like SIS, LMS, and payroll as entry points

Dynamic user base

Shared devices, substitutes, and volunteers

Human error

Accidental leaks or improper handling of sensitive data

Social engineering

Phishing & impersonation targeting staff and student data

How the year tends to unfold
(and where the risks live)

Budget season, busy inbox

Accounts Payable gets a friendly "please rush this bank account change" email. It looks perfect. That's a business email compromise (BEC). This isn't a theory: the School District of Philadelphia, e.g., sent four ACH payments to impostors in 2024—about $700,000—before auditors flagged it.

Nicole,

This is Ok to pay, Please See below and attached. Please set up an ACH for the attach due invoice today.

--------- Forwarded message ---------
From: LinkedIn Receivable Team
<cindy-de-guzman@acctreceivables-linkedin.com>
Date: Mon, Mar 17, 2025 at 12:17 PM
Subject: Reference Numbers: FL306731Fabrizio Lofaro
To: Nita White

Dear Esteemed Customer,

Please find the most recent invoice(s) attached to this email, which have been posted to your account: 105372692

The invoice(s) include payment instructions, We only accept electronic funds through ACH transfer instructions.

Please note: You may notice some improvements to your invoice. As part of our ongoing commitment to delivering a better billing experience, we have introduced several changes. To learn more about your new invoice, check on our website.

Figure 1: Email reported to CyberNut from a school staff member

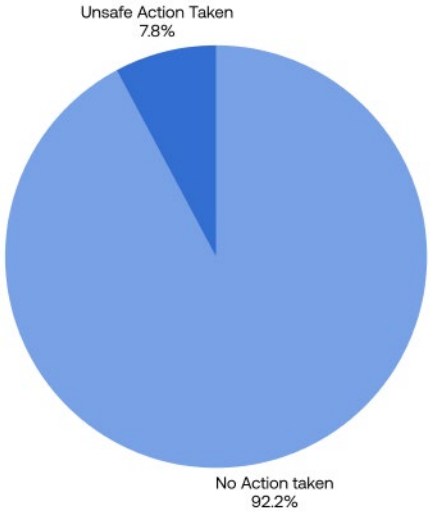


Figure 2: Analyzing User Engagement when a phishing email is reported. CyberNut internal figures, 60,000 emails reported across 1H '25.

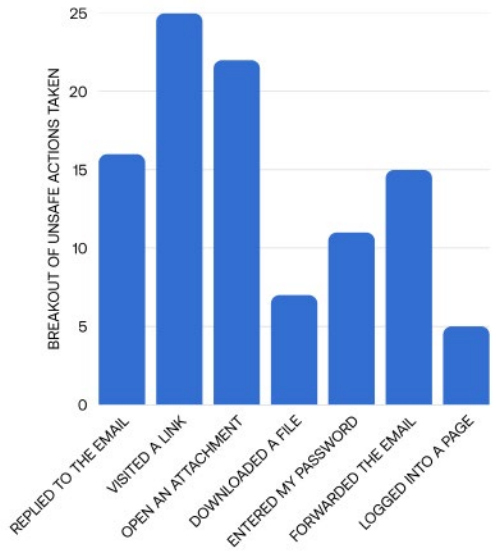


Figure 3: Breaking out User Engagement when a phishing email is reported, and an unsafe action was taken prior. CyberNut internal figures, 60,000 emails reported across 1H '25.

The escalating nature of cybercrime presents a significant threat to individuals and organizations alike. A broader perspective reveals the alarming scale of this issue: in 2024 alone, the Federal Bureau of Investigation (FBI) recorded a staggering $16.6 billion in reported losses due to cybercrime.

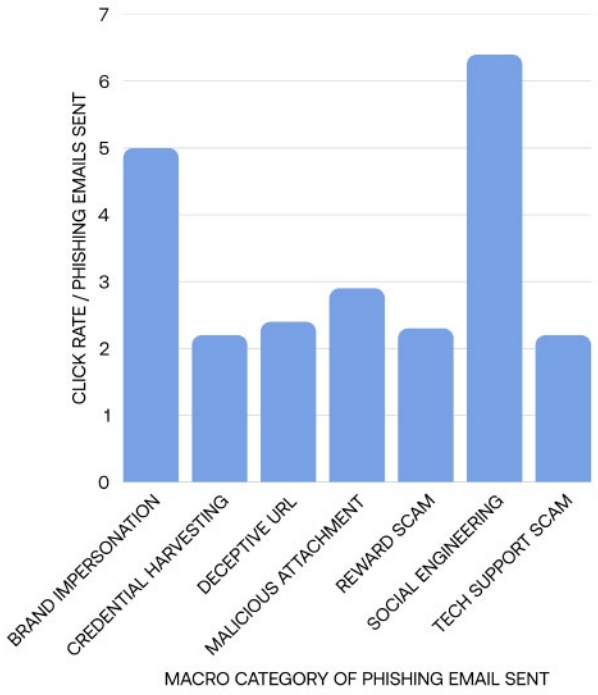


Figure 4: Breakdown of vulnerability to phishing email types. CyberNut internal figures, 1M email sample size across 1H '25.

Macro Category

Brand Impersonation
Pretends to be from trusted brands like Microsoft, Google, Amazon, e-commerce, social media, or streaming platforms.

Credential Harvesting
Uses fake login pages, password resets, account verifications, MFA bypass prompts, or document access requests.

Deceptive URL
Employs shortened links, typo-squatted domains, misleading subdomains, or QR codes to trick recipients.

Malicious Attachment
Delivers fake invoices, weaponized Word/Excel docs, shipping notifications, or disguised multimedia files.

Reward Scam
Promises lottery winnings, free gift cards, survey rewards, or exclusive promotional deals.

Social Engineering
Manipulates via authority exploitation, urgency creation, fear tactics, or curiosity bait.

Tech Support Scam
Claims fake virus infections, urgent software updates, account suspensions, or license expirations.

Berkeley
UNIVERSITY OF CALIFORNIA

AI is accelerating the sophistication of fraudulent schemes. The University of California-Berkeley Center for Long-Term Cybersecurity speaks to this in an article titled **Beyond Phishing: Exploring the Rise of AI-Enabled Cybercrime.**

> *"They are funneling AI-assisted reconnaissance and context generation into meticulously targeted campaigns. Moreover, by tailoring the language used in these communications—whether it be a recipient's regional dialect or their native tongue—cybercriminals gain a powerful force multiplier. This linguistic localization not only broadens the global reach of phishing attacks but also expands the overall attack surface, since victims are more apt to trust communications that appear authentically local or culturally familiar."*

AI-powered tools enable scammers to craft increasingly convincing and personalized messages, making it exceptionally difficult for recipients to discern legitimate communications from malicious ones. These AI-generated emails are often characterized by impeccable grammar, contextually relevant details, and a persuasive tone, mimicking the communication style of trusted contacts or high-ranking leaders.

Scammers are now employing a new tactic that involves a "confirming" phone call to exert pressure on victims, working in conjunction with convincing SMS texts. This tactic serves to amplify the psychological manipulation. After an initial fraudulent email, a follow-up phone call from an accomplice, often impersonating a superior or a solution provider, can create a heightened sense of urgency and legitimacy. This combination of advanced AI and high-pressure tactics drastically boosts scam success rates, leading to significant financial losses.

A new door opens: file-sharing and collaboration platform phishing

CyberNut has observed that attackers are increasingly using Google Drive's own sharing system to slip past defenses, e.g., by sending emails from drive-shares-dm-noreply@google.com that look legitimate. In some cases the sender's account is compromised; in others the domain is a near-perfect imitation, but the share still looks routine. Importantly, this is also being done leveraging Sharepoint / OneDrive / Dropbox / iCloud and other cloud platforms.

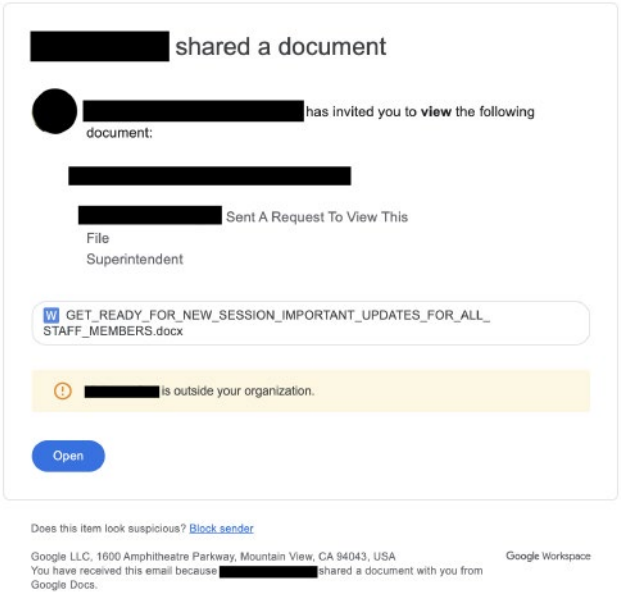


Figure 5: Email from this attack type reported to CyberNut from a school staff member.

The danger hides inside: a file with instructions to take unsafe actions or links that lead somewhere malicious. Because the source is Google itself, both filters and instincts often trust it, making this one of the more convincing phishing tactics now targeting schools and school districts.

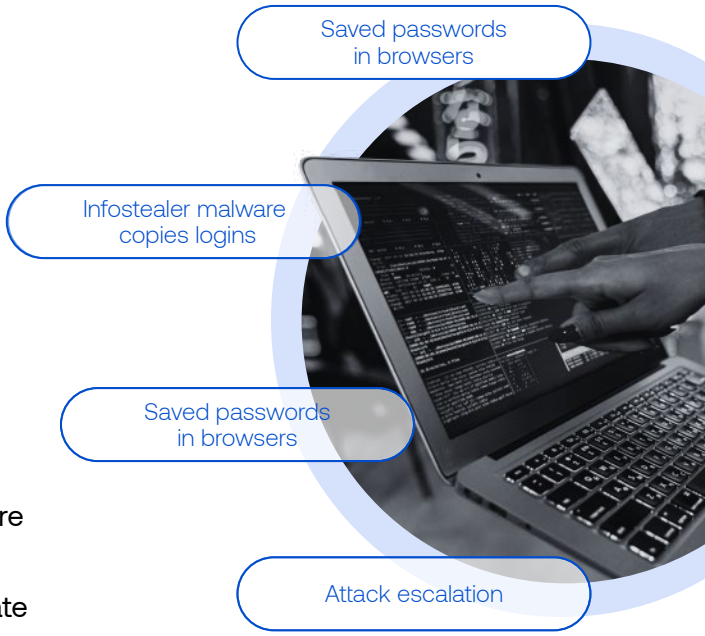
Meanwhile, a door we forgot to lock

Picture your district office: the main door faces the street. In tech, we have "main doors" too—things like our sign-in page, parent/staff portals, or the box that lets people connect from home. They're supposed to get regular "lock changes" (updates). When we're slammed—opening school, testing season—an update may slip. That's all some criminals need. They don't smash windows; they quietly try old keys until one works. If it does, they step inside and wait. You won't see alarms or blinking lights—everything looks normal.

This year's Verizon Data Breach Investigation Report (DBIR) underscores the escalating threat posed by these unpatched vulnerabilities, indicating a 20% increase. The report highlights a median time of 32 days to patch identified vulnerabilities. Even more concerning, only about 54% of these critical issues were fully resolved within a year. To put this simply: our digital doors remained unlocked and exposed to potential threats for far longer than anyone would deem acceptable. This extended exposure significantly amplifies our risk.

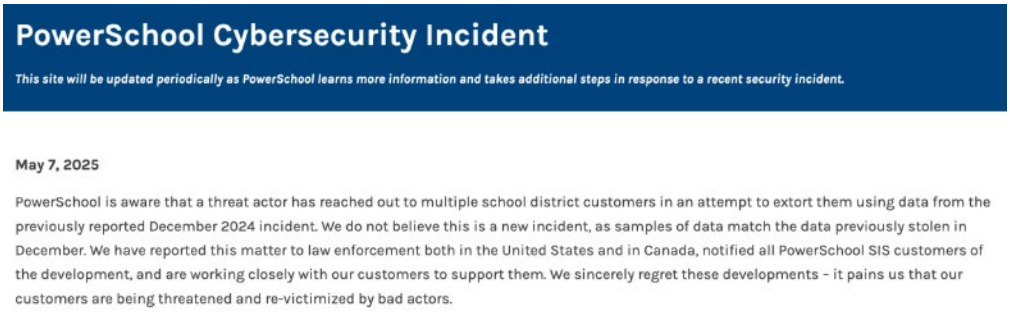
Quiet password trouble

Often people save passwords in their browser and stay signed in—super convenient. The problem: sneaky software on a personal or school device can copy those saved logins without anyone noticing. Weeks later, someone signs in “as you” from somewhere new. Infostealers are directly linked to the rise in ransomware attacks. Verizon's DBIR shows that over half of organizations publicly exposed on ransomware leak sites first appear in infostealer dumps. This suggests stolen credentials from infostealers frequently provide initial access for future ransomware deployments. Stolen login credentials, often from phishing or malware, give attackers network access, allowing them to escalate privileges, move laterally, exfiltrate data, and deploy ransomware. The black market for these credentials worsens the problem.



When a partner has a bad day

Even with a meticulously secured internal network, your organization's sensitive data often resides with various third-party solution providers. These can include critical systems like Student Information Systems (SIS), Learning Management Systems (LMS), online testing platforms, payroll services, and safety tools. Each of these external solution providers represents a potential vulnerability, as their security posture directly impacts the safety of your shared data.



PowerSchool Cybersecurity Incident

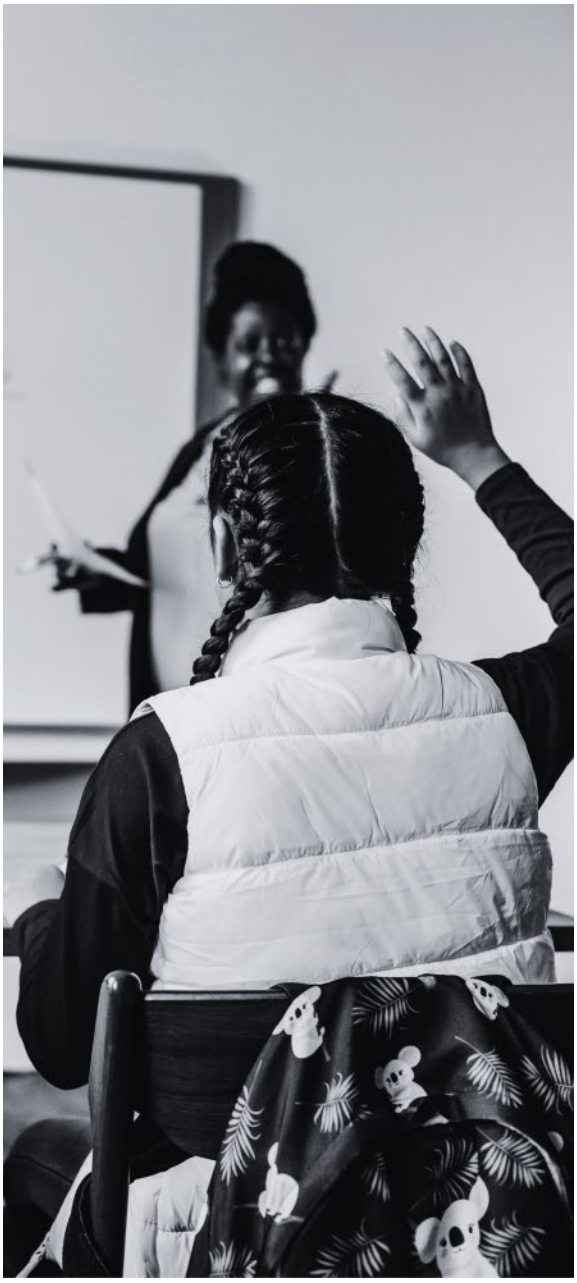
This site will be updated periodically as PowerSchool learns more information and takes additional steps in response to a recent security incident.

May 7, 2025

PowerSchool is aware that a threat actor has reached out to multiple school district customers in an attempt to extort them using data from the previously reported December 2024 incident. We do not believe this is a new incident, as samples of data match the data previously stolen in December. We have reported this matter to law enforcement both in the United States and in Canada, notified all PowerSchool SIS customers of the development, and are working closely with our customers to support them. We sincerely regret these developments - it pains us that our customers are being threatened and re-victimized by bad actors.

Figure 6: PowerSchool Cybersecurity Incident Page

A stark reminder of our interdependent security landscape was the PowerSchool incident, initially discovered on December 28, 2024. This breach, impacting a widely used education technology provider, led to months of widespread data exposure and necessitated numerous district-level notifications to families across the country. This ripple effect highlights the crucial need for vetting and continuous monitoring of all third-party solution providers. Organizations must ensure that their contracts with these providers include robust data protection clauses and that regular security audits are conducted to mitigate the risks of sharing sensitive information outside their direct control.



Back-to-school & testing windows... then the network crawls

One of the most disruptive cyber threats facing educational institutions today is the Distributed Denial of Service (DDoS) attack. These attacks overwhelm systems with a flood of illegitimate traffic, effectively knocking critical services like phones, online portals, and standardized testing platforms offline precisely when they are most needed. The impact of such an attack during a crucial period, like testing week, can be catastrophic, leading to significant delays, compromised data, and widespread frustration.

The escalating prevalence of DDoS attacks in the education sector is a cause for serious concern. Data from NetScout, as reported by EdTech Magazine, reveals a disturbing trend: K-12 DDoS attacks nearly doubled at the start of the school year. This surge coincides with a period when schools are often onboarding new students, deploying new technologies, and conducting initial assessments, making them particularly vulnerable.

To counter increasing DDoS attacks, especially during critical academic periods, educational institutions need proactive planning and strong collaboration with their Internet Service Provider (ISP) and other network solution providers. This includes strategic sessions, capacity planning, and clear communication protocols.

Helpful staff, accidental leaks (plus “shadow AI”)

The most prevalent form of data breach often doesn't involve malicious hackers orchestrating elaborate cyberattacks.

Instead, a significant number of incidents stem from unintentional human error, such as mistakenly sharing sensitive information or sending emails to unintended recipients.

A striking example of this occurred in St. Louis Park, Minnesota, where the transportation details of thousands of students were accidentally emailed to other families. This incident highlights that a lack of criminal intent doesn't diminish the potential for substantial data exposure.

Figure 7: CBSNews September 4, 2023

ST. LOUIS PARK, Minn. -- School officials in St. Louis Park say thousands of students' personal information was accidentally shared with other families in the district via email.

According to St. Louis Park Public Schools, the student IDs, names, addresses, parent/caregiver phone numbers, email addresses and bus pick up/drop off times for 3,753 students was accidentally included as an attachment on a district email about transportation routes.

"The matter was brought to our attention by a few parents within one hour of the message being sent," the district said in a letter to families. "We immediately contacted the technical support team for the communications platform, however, unfortunately, it was not possible to recall the email or disable the attachment. Please respect the privacy of our school community and kindly delete the email from your inbox and trash as soon as possible."

Furthermore, the increasing reliance on personal AI accounts by staff members introduces a new layer of risk. When educators use these digital tools, they can inadvertently transfer sensitive student information into systems that are outside the district's control and visibility.

This loss of governance means the district cannot monitor or secure the data effectively, creating a significant compliance and privacy vulnerability. To mitigate these risks, it is crucial to establish clear, simple, and user-friendly guidelines.

People generally want to adhere to proper procedures, and straightforward policies can significantly reduce the likelihood of accidental breaches, fostering a culture of data security within the organization.

The Friday surprise: ransomware & data extortion

In the evolving landscape of digital threats, ransomware has emerged as a particularly insidious form of cyberattack, transforming what might begin as a seemingly minor security lapse—an unlocked network door or a stolen login credential—into a catastrophic event. This type of breach can culminate in the encryption of critical data and the appearance of a chilling "pay us or we post it" ultimatum, effectively holding an organization's most valuable assets hostage.

Headlines frequently chronicle the struggles of school districts nationwide grappling with ransomware incidents. While many ultimately manage to recover their data and systems, the recovery process is far from trivial. It often entails countless long nights of dedicated work by IT professionals and necessitates difficult conversations about financial allocations, operational disruptions, and the potential impact on student learning.

The critical differentiator between a manageable crisis and a devastating setback often lies in two key areas: robust, restorable backups and thoroughly practiced incident response playbooks. Simply having backups is not enough; their integrity and restorability must be regularly verified. This proactive approach ensures that, in the event of an attack, an organization can effectively roll back to a point before the compromise, mitigating data loss and minimizing downtime.

Equally important are meticulously developed and regularly rehearsed playbooks. These detailed guides outline the steps to take when a security incident occurs, from initial detection and containment to eradication, recovery, and post-incident analysis. A well-rehearsed playbook empowers teams to react swiftly and efficiently, transforming what could be a lost semester of educational activity into an unfortunate, but recoverable, bad weekend.

Training students

A new front line in this story isn't just staff; it's also students. In North Dakota, every student now takes cybersecurity as part of their coursework, and states like California, Florida, Indiana, and Ohio are beginning to weave cybersecurity into lesson plans. The focus is simple but high stakes: email.

Training software that lets students practice spotting bad subject lines, suspicious senders, and too-good-to-be-true attachments builds instincts the same way fire drills build muscle memory. In the end, it's about turning awareness into routine so that identifying a phishing email is as automatic as locking a locker at the end of the day.

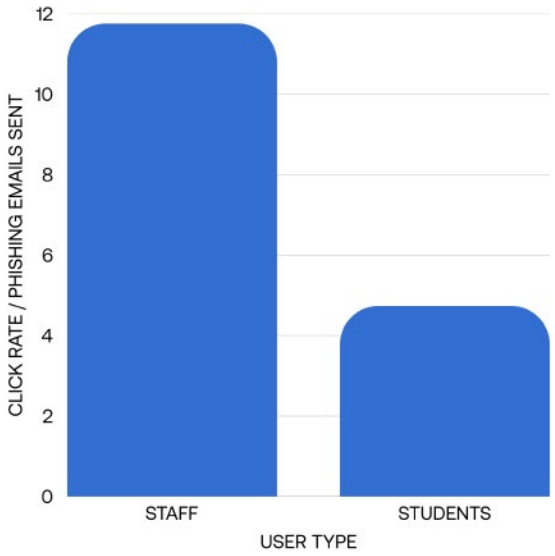


Figure 8: Breakdown of vulnerability to phishing emails by user type. CyberNut internal figures are based on two-week baseline phishing email campaigns when both user groups are active and emails are sent during the same time period.

How AI is changing the game

Cybercriminals are rapidly evolving their tactics, leveraging advancements in artificial intelligence (AI) to create increasingly sophisticated and convincing attacks. The traditional indicators of a scam, such as blatant typos or awkward phrasing, are becoming less common as AI tools generate more coherent and natural-sounding text.

One report from a DBIR partner revealed a striking doubling of synthetic text in malicious emails within just two years, indicating a significant escalation in the quality and volume of AI-generated phishing attempts.

Beyond text, the threat extends to voice. Voice cloning technology has become remarkably affordable and highly convincing, making it increasingly difficult to discern genuine callers from AI-generated imposters. Imagine receiving a phone call from someone perfectly mimicking the voice of your superintendent; this scenario is now a tangible threat. A notable real-world example involved a deepfaked CFO on a video call who successfully orchestrated the transfer of $25 million, highlighting the immense financial risks associated with these advanced deception techniques.

AI also empowers attackers with sophisticated targeting capabilities. By analyzing publicly available information, AI can tailor malicious messages to specific roles within an organization—whether it's someone in transportation, athletics, or an accounts payable clerk.

This personalized approach significantly increases the likelihood of a recipient falling for the scam, as the message appears to be directly relevant to their responsibilities and interests.

New vulnerabilities are emerging in digital spaces. AI-powered "email summaries," chat assistants, and various plug-ins, if not adequately secured, can be manipulated by attackers. These tools, designed for efficiency, can inadvertently become entry points for malicious actors if their underlying security protocols are not robust.

Finally, the proliferation of "Shadow AI" presents a significant challenge to organizational security. The DBIR notes that 15% of employees are accessing generative AI tools from their work devices, often using non-work accounts.

This practice creates a substantial risk of sensitive data migrating off the district's secure network and onto platforms beyond the organization's visibility and control. This unmonitored data movement can lead to breaches, compliance violations, and a general erosion of data security.

What to do this school year
Slow down the money moves.

Make a two-person rule for bank account changes and wires. Call a known number (not the one in the email). Add a 24-hour hold for big transfers. If someone yells “urgent,” that’s your cue to pause—not speed up.

Mount Juliet Christian Academy ~Direct Deposit

K karf.fza@gmail.com
to me

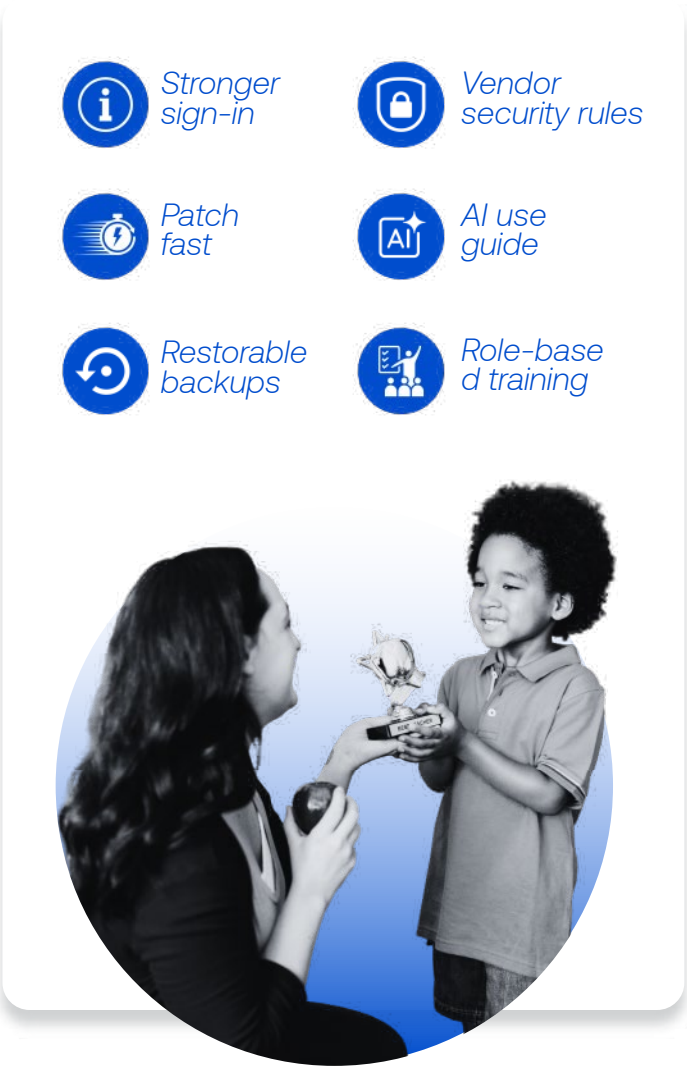
Hi Colleen,

I would like to update my new banking information on file before the next payroll is completed. What details will you need?

Thanks!

[redacted]
Teacher
Mount Juliet Christian Academy.

Figure 9: Email reported to CyberNut by finance staff member



Turn on stronger sign-in where it matters most

Start with finance, HR, IT admins, and anyone with SIS access. Use phishing-resistant MFA (passkeys/security keys). If you're not there yet, require number-matching in the authenticator app (no more blind "Approve" taps).

Patch the front door first

Keep a short, living list of internet-facing systems (sign-in, portals, VPN, and firewall). Patch those within days, not weeks. Track it like a KPI and show progress to leadership—quick wins build trust.

Set third-party solution provider minimums

For SIS/LMS/testing/payroll and anything with PII: require MFA, logging, quick breach notice, and clear off-boarding steps. Treat third-party solution providers like part of your team. Ensure that they are following security policies as stringent as, if not more so, than you are.

Backups you can actually restore

Have an offline/immutable copy. Run one restore test this semester and tell your board the results.

Develop a guide for AI use

Use district-approved tools and accounts. Ask when in doubt. Don't paste student PII into personal or district AI tools without understanding the FERPA requirements and how the model is being trained.

Prioritize role-based training over hourly requirements

Two minutes to spot a scam beats two hours of slides. Prioritize AP/payroll, school secretaries, principals, and coaches/club advisors. Give them checklists and practice, not just policies. Products like CyberNut allow for just-in-time training and practice rather than compliance videos at the beginning of each year.

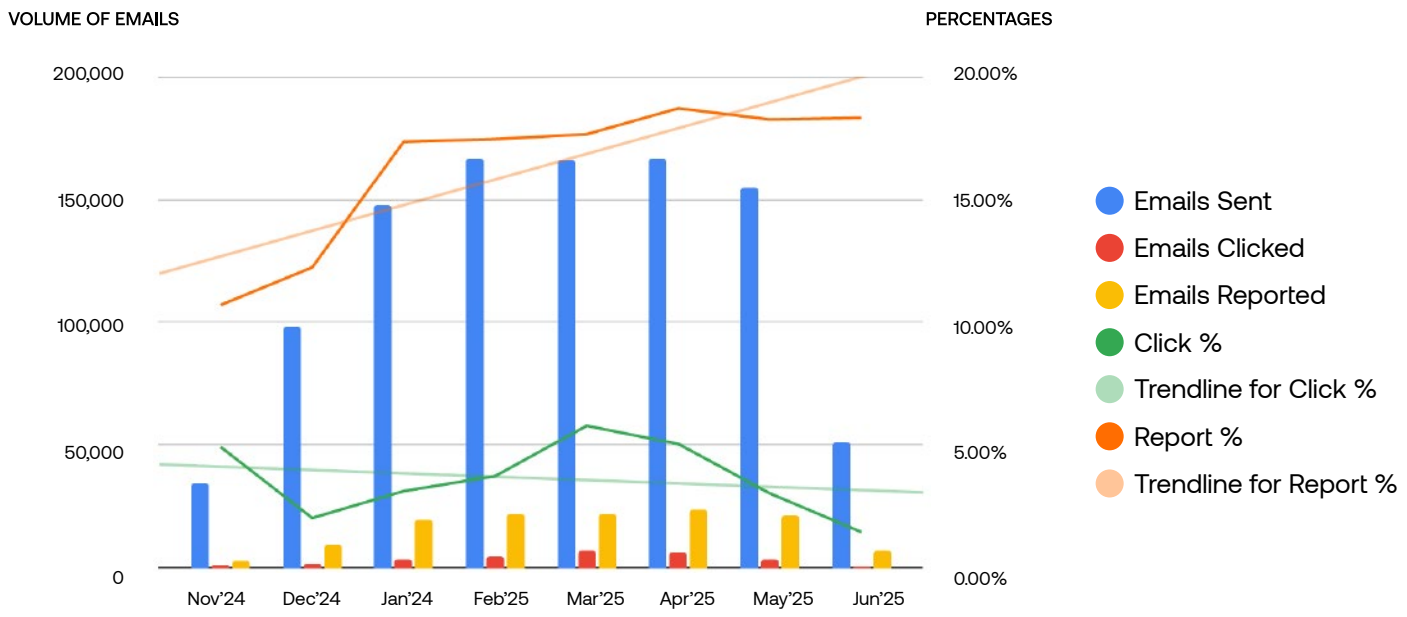


Figure 10: Change over time with training drives to an increase in report rate % and a decrease in click rate %. CyberNut internal

Cybersecurity in schools

Cybersecurity in schools is no longer just an IT issue; it's a shared responsibility that demands constant vigilance and proactive measures from every member of the educational community. By implementing these strategies and fostering a culture of security awareness, school districts can significantly enhance their resilience against evolving cyber threats, ensuring a safe and productive learning environment for all.

References

"1 2024 IC3 Annual Report." Internet Crime Report, Federal Bureau of Investigation, www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

2025 Data Breach Investigations Report, Verizon Business, www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf.

Erickson, Lief. "City Controller Refers Philadelphia School District Cyber Fraud to PA Attorney General." Christy Brady, CPA, 22 May 2025, controller.phila.gov/city-controller-refers-philadelphia-school-district-cyber-fraud-to-pa-attorney-general.

Manky, D., & Baram, G. Beyond phishing: Exploring the rise of ai-enabled Cybercrime - CLTC UC berkeley center for long-term cybersecurity. CLTC. 16 January 2025, https://cltc.berkeley.edu/2025/01/16/beyond-phishing-exploring-the-rise-of-ai-enabled-cybercrime/

"Report: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats: CISA." Cybersecurity and Infrastructure Security Agency CISA, CISA, 19 Jan. 2023, www.cisa.gov/resources-tools/resources/report-partnering-safeguard-k-12-organizations-cybersecurity-threats.

"SIS Incident." PowerSchool Cybersecurity Incident, 1 Aug. 2025, www.powerschool.com/security/sis-incident/.

"St. Louis Park Public Schools Accidentally Shares Thousands of Students' Personal Information." CBS News, CBS Interactive, 4 Sept. 2023, www.cbsnews.com/minnesota/news/st-louis-park-public-schools-accidentally-shares-thousands-of-students-personal-information/.

Torchia, Rebecca. "DDoS Attacks Double as the School Year Starts." Technology Solutions That Drive Education, CDW EdTech Focus on K-12, 22 Apr. 2025, edtechmagazine.com/k12/article/2025/08/ddos-attacks-double-school-year-starts.