

Awareness & Training

This category asks whether everyone with a district account - staff and students - is trained to spot and report attacks, and whether people in sensitive roles get extra preparation.

Why it matters

- Payment-change scams and business email compromise (BEC) aim at the business office, payroll and HR with convincing requests, and a trained clerk who calls the vendor back at a known number stops the loss before money leaves the district.
- Teachers and students open links and shared documents all day, so a staff habit of reporting suspicious messages quickly gives IT time to pull a phishing email from every inbox before others act on it.
- Completion records and phishing simulation results are what carriers, auditors and the board ask to see, and some social engineering coverage depends on showing that staff were trained to verify payment changes.

One convincing email to a payroll clerk can redirect a large vendor payment, and one clicked link in a teacher's inbox can start a district-wide ransomware event. Insurers and auditors increasingly want completion records and phishing simulation results, not just a policy statement.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>Training happens when someone offers it, nobody tracks who took it, and new hires get credentials before any security orientation.</p> <p>Moving up: Define the program on paper: who must train (all staff and students with accounts), what role-based training exists for security-relevant roles, who documents and monitors training activity, and a records retention policy.</p>	<ul style="list-style-type: none"> • No cybersecurity session on the back-to-school professional development (PD) agenda • Accounts issued on day one with no training step in the onboarding checklist • No named person keeping training records and no retention rule for them
2 · Repeatable	<p>The district has defined who must train, including students with accounts, what role-based training the business office, HR and IT receive, and who keeps the records, but delivery is still uneven.</p> <p>Moving up: Sequence and record: deliver role-based training before people are authorized to access systems, keep your designated record-keeper active in the role, and retain completion records per the retention policy.</p>	<ul style="list-style-type: none"> • Written training plan listing required audiences and role-based modules • Memo naming the training record-keeper • Records retention schedule entry that covers training completion records
3 · Defined	<p>All staff train on a schedule, role-based training is completed before people get access to payroll, the SIS or admin tools, and completion records are kept under the retention schedule.</p> <p>Moving up: Add live-fire elements - regular alerts, campaigns, and simulated phishing - track staff and student progress with data, and put results in front of leadership on a schedule with enforced follow-up for non-completers.</p>	<ul style="list-style-type: none"> • New-hire checklists showing the security module completed before credentials were issued • Completion report by building and role from the learning management system or PD tracking system • Business office records showing payment-verification training completed before access to the finance system
4 · Managed	<p>Training runs year-round with alerts, campaigns and simulated phishing, progress is tracked with data, and leadership reviews results each semester and follows up with non-completers.</p> <p>Moving up: Set numeric performance targets (completion rate, phish click rate, report rate), run a data-based improvement cycle against them, and involve leadership in designing and revising the program, not just receiving reports.</p>	<ul style="list-style-type: none"> • Phishing simulation reports showing click and report rates across several campaigns • Archive of monthly scam-alert emails sent to all staff • Cabinet meeting notes reviewing completion and simulation results, with assigned follow-up
5 · Optimized	<p>Leadership helps design the program, sets measurable targets for completion, reporting and clicks, and adjusts content each cycle based on what the data shows.</p>	<ul style="list-style-type: none"> • Written training targets approved by the superintendent and revisited each year • Trend of report rates and repeat clickers used to choose next year's topics and audiences • Revision log showing content changed in response to real incidents and simulation results

Quick wins

Quick win and how	Cost	Effort	Usual owner
Add a cybersecurity module to this year's back-to-school PD agenda Ask the PD coordinator for a 30-45 minute slot and cover spotting and reporting phishing, what to do with an MFA prompt you did not expect, and safe handling of student data. Take attendance through the PD sign-in so it doubles as a completion record.	Free	Hours	Technology director
Designate a training record-keeper and start a completion tracker Name the record-keeper in a short memo, then set up a tracker in the PD system or a shared sheet with name, role, building, module and completion date. Pull the new-hire list from HR each month so nobody is missed.	Free	Hours	Superintendent
Brief the business office on callback verification for any payment or direct-deposit change Write a one-page rule: any change to vendor banking details or an employee's direct deposit is confirmed by calling a number already on file, never one supplied in the request, and a second person approves it. Walk business office and payroll staff through it and have each person sign it.	Free	Hours	Business and finance officer
Start a monthly two-paragraph scam alert email to all staff Pick one current scam each month, such as a gift-card request from a fake principal, a fake shared-document link or a fake payroll sign-in page, describe what it looks like and how to report it, and send it from a recognized district address. CISA and MS-ISAC advisories supply ready material.	Free	Hours	Technology director
Register IT staff for CISA and MS-ISAC training webinars Sign technicians up for CISA's no-cost training offerings and, if the district or state holds MS-ISAC membership, its webinars. Log each session in the training tracker as role-based training for IT.	Free	Hours	Technology director

Free means staff time, existing licenses or free government services. Effort: hours, days or weeks.

Common pitfalls

- Making phishing simulations punitive. Naming clickers in public or tying results to evaluations teaches staff to hide mistakes; treat a click as a coaching moment and thank people who report.
- Training teachers but skipping the people with the most access. Business office, payroll, HR, registrars and administrators need role-specific sessions on payment fraud, W-2 requests and records disclosure, not only the general module.
- Holding one annual session and calling it done. Habits fade between August and spring; short monthly alerts and a few simulations a year keep reporting in practice.
- Not giving staff an easy way to report. If reporting means hunting for the help desk address, people delete and move on; turn on the built-in report button in Gmail or Outlook, publish one simple address, and acknowledge every report.
- Forgetting substitutes, coaches and student workers. Anyone who gets a district account needs the basics before first sign-in, so build a short version into substitute and volunteer onboarding.

Evidence that proves it

- Training completion report showing percent of staff finished, by building
- Back-to-school PD agenda listing the cybersecurity session
- New-hire checklist requiring security training before account issuance
- Phishing simulation results showing click and report rates over time
- Role-based training records for business office, HR, and IT staff
- Records retention policy covering training documentation

Who usually owns it

Technology director	Chooses training content, runs alerts and phishing simulations, and reports results to leadership.
HR director	Builds training into onboarding so it is completed before credentials are issued and follows up with staff who have not finished.
Business and finance officer	Makes sure business office and payroll staff complete payment-fraud training and use callback verification for every banking change.

Curriculum and instruction lead

Schedules age-appropriate digital citizenship and online safety lessons for students across grade levels.

Insurance relevance · High

Carriers ask whether every employee completes training each year and whether you run phishing simulations, and social engineering or funds-transfer coverage often turns on documented verification procedures for payment changes.

- Do all employees, including administrators and support staff, complete security awareness training every year?
- Do you run simulated phishing campaigns and assign follow-up training to people who click?
- Do staff confirm any change to vendor or payroll banking details by calling a known number before paying?
- Is training required for account access, or is it optional?

Tip: Keep the latest completion report and simulation summary in the renewal file so the completion figures you give the carrier come straight from the system of record.

Funding and free help**ESSA Title IV, Part A (effective use of technology)**

Annual formula allocation

Flexible formula grant whose 'effective use of technology' and 'safe and healthy students' areas can support staff security training, cyber-safety programs and limited technology purchases. Not an infrastructure-security grant.

State and Local Cybersecurity Grant Program (SLCGP) – Georgia subawards

Georgia FY2024 round closed May 15, 2026 · watch for the FY2025 round

Federal cyber grant passed through the state to local governments, including school districts. Georgia accepted FY2024 subaward applications April 1 – May 15, 2026. Federal authority beyond September 30, 2026 depends on Congress.

CISA K-12 cybersecurity resources and toolkit

Always available

Free federal guidance for K-12: the K-12 cybersecurity report and toolkit, plus access to regional CISA advisors and no-cost services. A resource, not funding.

Programs, eligibility and deadlines change; confirm on the official page before applying.

Learn more

- Phishing Guidance: Stopping the Attack Cycle at Phase One (CISA) <https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one>
- Cybersecurity Awareness Month (CISA) <https://www.cisa.gov/cybersecurity-awareness-month>
- The K12 SIX Essentials Series (K12 SIX) <https://www.k12six.org/essentials-series>
- Internet Crime Complaint Center (IC3) (FBI) <https://www.ic3.gov/>