

K-12 CYBERSECURITY FOUNDATIONS

Protect the school day.
Build safer habits.
Connect learning to cyber careers.

A practical companion to CISA's August 2026 implementation guide, adapted for teachers, school leaders and IT partners.

ACTIONS / LESSONS / WORKSHEETS / REVIEW TOOLS

Independent educational adaptation. No endorsement by CISA, DHS or NIST is claimed. U.S. K-12 context.
Prepared and checked 7 October 2026.

Start with your role

A practical companion, with all eight source objectives retained.

Teachers can make everyday technology use safer and teach sound decisions. School and district leaders own priorities and resources; IT teams implement and verify technical controls. Use local policies and named contacts alongside this guide.

Your role	Begin here	Useful next step
Teacher / librarian / support staff	Daily checklist (3); reporting (8)	Teach the lessons (11-14); explore careers (16).
Principal / district leader	Ownership and planning (9-10)	Run the tabletop (15); review evidence (17).
IT / security / privacy lead	Controls and teacher handoffs (4-8)	Agree priorities, check recovery and approve classroom tools.

The eight objectives, translated into school practice

CISA source objective	Where to find it
1. Protect login credentials	4: accounts and sign-in
2. Safeguard devices and assets	5: approved devices, updates and phishing
3. Perform, verify and test backups	7: recover work and keep teaching
4. Develop and exercise incident response	8 and 15: reporting and a tabletop
5. Train and assess understanding	9 and 11-14: staff and classroom learning
6. Protect sensitive data	6 and 14: sharing and privacy
7. Prioritize near-term effort and investment	9-10 and 17: ownership and action tracking
8. Develop a long-term plan using NIST CSF	9 and 17: review across six functions

Activities, timings, forms and scoring in this edition are suggested teaching tools. They are not CISA requirements, a formal control crosswalk or a compliance certification.

Evidence: [1], source objectives 1-8, pp. 14-49. References: 18-19.

The everyday teacher checklist

Small actions to use before, during and after the school day.

Before using a device or sharing a file

- [] Use your own school account and the approved sign-in method. Keep passwords, recovery codes and authentication codes private.
- [] Use approved devices, apps and storage. Check with IT before installing extensions or introducing a new learning tool.
- [] Save essential work in the approved location. Know who can help recover it.
- [] Check the recipient and access permissions before sending student information.
- [] Lock the screen when stepping away. Sign out when finishing on shared devices.

When a message or prompt feels unusual

- [] Pause before clicking, opening an attachment, scanning a QR code or approving an unexpected sign-in request.
- [] Verify requests for records, account access or money using a contact route you already trust.
- [] Report concerns through the school's agreed channel. If you clicked or entered information, say so promptly.

Prepare this card before an incident

IT / security contact and normal reporting route:

Phone or in-person reporting route if email or the network is unavailable:

Approved storage location / school-approved offline teaching option:

Evidence: [1], objectives 1-6; [2] phishing; [5] classroom app approval.

Protect accounts and sign-in

Teacher habits support controls that IT must configure and maintain.

Teacher actions

- Use a long, unique password or passphrase for each account. Use a school-approved password manager where available. Avoid names, mascots and predictable patterns.
- Use the MFA method provided by the school. Only approve a request you initiated and recognize. Report unexpected prompts or lost authenticators.
- Keep classroom examples fictional. Do not ask students to reveal a real password or type it into an unapproved password-checking website.
- Lock your device when unattended. Use individual accounts rather than sharing a staff login; ask IT about any classroom exception.
- Tell the designated administrator when staff, students or volunteers leave or change roles, so access can be reviewed.

Ask IT and leadership to confirm

Control	Teacher handoff
MFA and account recovery	How do staff sign in safely without a personal smartphone? What accessible recovery process is available?
Passwords and login defenses	Who owns password policy, blocked-password checks and rate limiting?
Access and session controls	Are privileged accounts separate? Who removes obsolete access and sets appropriate timeouts?

Password policy: distinguish guidance from local rules

NIST SP 800-63B-4 specifies at least 15 characters for password-only sign-in, and at least 8 when the password is part of MFA. It rejects routine forced password changes without evidence of compromise and extra character-mixture rules. IT should review local policy against the relevant standard; teachers should follow the approved process. [3]

MFA uses distinct factor types and reduces risk; it does not guarantee account safety. Ask IT about phishing-resistant FIDO/WebAuthn options where appropriate. [1, 4]

Evidence: [1], pp. 14-20; [3], section 3.1.1; [4], CISA MFA fact sheet.

Use approved, maintained technology

A request for approval is part of lesson preparation.

Keep devices and teaching tools visible to IT

- Use approved hardware, software, websites and browser extensions. Request review early and describe the teaching purpose, access needs and data involved.
- Follow the managed update and restart process. Report failed updates or warnings; do not bypass security settings to get a lesson working.
- Report missing devices promptly with the asset identifier and last known location, through the approved route.
- If a learning site is blocked, ask IT to review it. Prepare a paper or teacher-led alternative while the request is assessed.

Check a suspicious message in three steps

Step	What to do
1. Pause	Treat unusual urgency, requests for secrets or unexpected files as reasons to check. A familiar display name is not proof of identity.
2. Verify independently	Use an existing bookmark, the approved app or a known phone number. Do not use the suspicious message's contact details.
3. Report	Use the school's reporting tool or contact IT. Follow local instructions for retaining or deleting the message.

For IT: prioritize patches by risk

Use CISA's Known Exploited Vulnerabilities catalog as one input to prioritization, alongside exposure, impact and vendor guidance. This edition does not prescribe a blanket 30-day delay before updates. Teachers support the approved schedule and report problems. [1, 8]

Leadership / IT evidence: an updated asset list, software approval decisions, update status and an owner for email security. Staff do not configure mail authentication, scan school networks or change default device credentials as a classroom activity.

Free action for IT / leaders: Request CISA Cyber Hygiene vulnerability scanning. Email vulnerability@cisa.dhs.gov with the subject **Requesting Cyber Hygiene Services**. IT should arrange authorized scope and enrollment. [11]

Evidence: [1], pp. 21-28; [2] phishing; [8] KEV prioritization; [11] Cyber Hygiene.

Protect student and staff information

Know what you need, where it belongs and who may access it.

Before collecting or sharing information

- Ask what information is needed for the task. Use fictional or school-approved de-identified examples for demonstrations and cyber activities.
- Use approved school storage and sharing methods. Check the recipient, access level and audience each time.
- Keep grades, attendance, disability-related records, health details and family contact information out of public slides, screenshots and unrestricted links.
- Do not move school records into personal email, personal cloud storage or unapproved AI and other online tools.
- Follow the school's retention schedule. Ask before deleting records; a record may be subject to retention requirements or a legal hold.

App approval comes before student use

The U.S. Department of Education advises teachers to check with school or district administration that a classroom app is approved, and to consult IT. Under FERPA's school-official exception, specific conditions apply to a provider's use and control of education-record information. Approval cannot be inferred from a tool being free or educational. [5]

Share safely, using the school's process

Use the school-approved transfer method rather than emailing sensitive files. IT should verify encryption and access controls; do not assume a generic "password protected" label establishes appropriate encryption. This edition takes a more restrictive approach than the source's email examples; see the departures note on page 18.

School-approved sharing service / privacy contact:

Leadership / IT evidence: data owners, approved storage and sharing rules, reviewed vendor permissions, retention instructions and a route to report misdirected records.

Evidence: [1], pp. 40-44; [5], Department of Education classroom-app FAQ.

Recover work. Keep teaching.

Backup verification is an IT responsibility; teaching continuity is shared.

Teacher actions

- Know which school-approved locations protect essential teaching files. Ask about recovery of accidentally deleted or changed work.
- List the services your class depends on: learning platform, presentations, attendance access and approved accessibility tools.
- Keep an approved offline lesson option. Coordinate attendance, dismissal and other safety-critical routines with leadership.
- Do not create personal copies of student records or attach backup drives to a device involved in a suspected incident.

Questions for IT and service owners

Question	Useful evidence
What is covered?	Named systems, data owners and vendor recovery responsibilities.
How is it protected?	Separation from live systems and suitable protected, offline or immutable copies where applicable.
Can we restore it?	A dated restore test with results, limitations and follow-up actions.
What should staff expect?	Recovery priorities, agreed acceptable downtime / data loss and a contact for help.

Do not equate sync with proven recovery

Cloud storage, version history and synchronization may offer recovery features, but do not establish that the school's backup needs are met. Confirm coverage and retention with IT and the provider; test restoration. Backups support recovery but do not prevent data theft. [1, 6]

One offline lesson I can teach using approved materials:

Evidence: [1], pp. 29-32; [6], CISA #StopRansomware Guide.

Notice. Stop. Report.

Use this response card with the school’s approved incident procedure.

Report promptly, even if you are unsure

Examples: a suspicious message, unexpected authentication prompt, missing device, exposed record, unexplained account activity or unusual system warning. An outage alone does not prove a cyberattack. IT investigates; staff report observations. [1]

Step	Teacher action
1. Stop the risky action	Do not continue using a suspicious link, file or login page. If the device appears compromised, stop using it and contact IT by another approved route.
2. Contact the right person	Use the school’s reporting tool, known phone number or in-person route. Say immediately if you entered a password, approved a prompt or shared information.
3. Record basic facts	Give the time, device / asset ID, what you observed and what you did. Avoid sending passwords or extra copies of student data.
4. Follow the response plan	Follow IT’s instructions for containment and evidence. Do not independently wipe, reset, reinstall, run investigation tools or reconnect a quarantined device.
5. Keep students supported	Use the approved continuity plan. Route external statements, parent communications and breach notices to authorized school leaders.

Active attack on your device and IT cannot be reached

If a ransom message appears or files are visibly being encrypted, follow the school’s isolation instruction below. If none is available, disconnect the affected staff device from Wi-Fi and unplug its network cable. Leave it powered on and keep trying IT by another route. If you cannot disconnect it, CISA advises powering it down to limit spread, although this loses evidence held in memory. Do not reconnect it or alter other systems. [6]

School-approved device isolation instruction (IT to complete before use):

If the normal reporting system is unavailable, use:

Build a school-wide routine

Name owners, train for real decisions and review progress.

Leadership actions

- Name an accountable cybersecurity leader and deputies. Link IT with administration, HR, privacy, safeguarding, communications and service owners.
- Make reporting easy to find and welcome early reports. Include substitutes, contractors and new staff in relevant guidance.
- Train staff on actual school workflows, then assess understanding with short scenarios. Use age-appropriate learning for students.
- Agree a recurring incident exercise and review process. Record lessons and update both digital and printed plans.
- Maintain a risk-based improvement list using applicable CISA goals; use NIST CSF 2.0 to structure the longer-term program.

Six functions for a leadership review [7]

CSF 2.0 function	School review question
Govern	Who owns decisions, policies and resources?
Identify	Which services, data, assets and risks matter most?
Protect	Which safeguards are implemented and maintained?
Detect	How do we notice and assess suspicious activity?
Respond	Who takes action and communicates during an incident?
Recover	How do we restore services and improve after disruption?

These are plain-language review questions, not a formal CSF assessment. The functions work together; they are not six sequential project stages.

External reporting: leadership / incident lead

CISA: cisa.gov/report; report@cisa.gov. Phone: (888) 282-0870 or 1-844-SAY-CISA (1-844-729-2472). **FBI:** report cybercrime at ic3.gov or contact the local FBI field office. [6, 12, 13]

Assign a leader to check applicable state and other notification duties, reporting deadlines and insurer policy conditions with counsel / the privacy lead. Agency reporting does not replace required notices to affected people, regulators or an insurer. Record recipients, deadlines and reports in the response plan.

Evidence: [1], objectives 5, 7-8; [7] CSF 2.0; [6, 12, 13] incident reporting.

A manageable first 30 days

Adjust the pace to local risk, staffing and existing arrangements.

Suggested phase	School / teacher work	Leadership / IT handoff
Days 1-5 Make routes clear	Complete the contact card. Read relevant school policies. Identify key teaching dependencies.	Confirm accountable owner, reporting routes and escalation contacts.
Days 6-10 Check everyday use	Review sharing permissions on your own teaching files. Confirm storage and app approvals.	Address urgent access or exposure risks. Clarify MFA and recovery support.
Days 11-20 Practice decisions	Teach a lesson from this guide. Use a short staff scenario; provide feedback.	Verify critical backup coverage and record restore-test results.
Days 21-30 Exercise and review	Run the outage discussion. Update the offline lesson plan and check understanding again.	Record gaps, owners and target dates. Choose the next priorities based on risk.

Track actions with evidence

Use page 17 to log the gap, owner, due date and what will count as completion. Work already done should have evidence; work planned should have an owner. Do not wait for day 30 to deal with a suspected incident or an urgent vulnerability.

A realistic finish line

Aim to have usable reporting routes, clear classroom practices, a tested teaching fallback and a prioritized improvement list. This schedule does not imply the whole school is secure after 30 days. Technical verification and the long-term program continue. [1]

Our first priority and accountable owner:

Evidence: [1], objectives 1-8. The timetable is an original suggested implementation aid.

Check before you click

Suggested: grades 6-12 | 35 minutes | paper or approved display

Learning goal: Students identify a request that needs checking, choose an independent verification route and explain how to report a concern. Materials: worksheet on page 12; teacher answers on page 13.

Time	Teaching sequence
0-5 min	Ask: "A message looks as if it came from school. What would you check before acting?" Collect ideas without asking for personal experiences.
5-10 min	Explain that phishing tries to influence actions, including sharing information or opening harmful files. Model an independent check using a known contact route. [2]
10-23 min	Pairs read the three fictional messages on page 12. For each, explain the concern, safe next step and reporting choice.
23-30 min	Discuss the answer guide. Emphasize that appearance or grammar alone cannot establish legitimacy; students should explain their reasoning.
30-35 min	Exit ticket: "What would you do if you already entered your password?" Expected: stop and tell the teacher / approved reporting contact promptly.

Adapt the lesson

- Elementary grades: read one short message aloud and teach "stop and ask a trusted adult." Keep the focus on help-seeking rather than technical analysis.
- Middle grades: compare the request with what the student expected; rehearse asking for help using fictional details.
- High school: discuss impersonation, sign-in prompts and why a convincing message can still require verification.

Safe, accessible delivery

Use printed messages or an approved display. Read aloud where helpful; allow verbal, typed or written answers. Do not send deceptive live emails, collect credentials or ask students to investigate real suspicious messages. All examples are fictional; no account creation is required.

Evidence: [1], objective 5; [2] phishing. Lesson structure and timings are suggested.

Would you act on this message?

Use only these fictional examples. Do not enter any real information.

For each message: **What needs checking? How would you check safely? If you had acted, would you need to report it, and to whom?**

A / Urgent account check

From: School Support

Subject: Your account closes today

"Reply within ten minutes with your password and sign-in code so we can keep your school account working. Do not contact your teacher."

Your concern and safe next step:

B / A school-library reminder

From: School Library

"Your book is due tomorrow. Check your borrowing record in the usual library app or ask at the library desk."

What would you verify? What can you safely do?

C / An unexpected login approval

Your device shows: "Approve sign-in?" You have not tried to sign in. A chat message says: "Just approve it so we can finish fixing your account."

Your concern and safe next step:

Exit ticket: If I have already shared a password or approved a suspicious request, I should:

Reward the reasoning

Assess the safe action, not just a correct label.

A / Urgent account check

Expected response: Do not reply with secrets. Tell a teacher or the school's approved contact and verify any account issue through the usual school route. The request for a password and code, extreme urgency and attempt to prevent verification are important concerns.

B / School-library reminder

Expected response: It may be legitimate, but the text alone does not prove who sent it. Checking the usual library app or speaking to the library desk is a safe independent route. A student should not claim that a familiar display name makes it safe.

C / Unexpected login approval

Expected response: Do not approve the request. Tell the teacher / agreed school contact promptly. The student did not initiate the sign-in; a separate message asking for approval does not make it trustworthy.

If a student says they already acted

Reassure them that telling you quickly is the right action. Follow the school's reporting procedure; do not ask them to disclose the password in class. Report the action taken, relevant time and affected school account through the approved channel. [1]

Suggested assessment: 0-3 points per message

Point	Award when the student...
1	Identifies a meaningful concern or recognizes uncertainty.
1	Chooses a safe action and independent checking route.
1	Explains whether follow-up or reporting is needed after acting, and to whom.

Maximum: 9 points. This suggested classroom rubric is not a validated diagnostic test. Accept equivalent safe answers consistent with local policy. For B, uncertainty earns point 1; point 3 can be earned by explaining that checking the usual app or asking the library desk needs no incident report unless a concern emerges. A and C require prompt reporting if secrets were shared or a sign-in was approved.

Evidence: [1], objectives 4-5; [2] phishing. Examples and rubric are original teaching tools.

Accounts, data and good decisions

Suggested: grades 6-12 | 25 minutes | discussion or paper

Learning goal: Students explain how to protect account secrets, choose an approved sharing route and recognize when permission is needed. Use only fictional examples; no real passwords or records.

Time	Activity
0-5 min	Explain: a password is a secret; MFA adds a distinct authentication factor; access should match the task. [1]
5-17 min	Discuss the four prompts below in pairs. Ask for both the action and the reason.
17-22 min	Compare answers. Clarify that school approval and permissions matter alongside technical protection.
22-25 min	Exit ticket: one habit to keep an account safe, and one habit to protect someone else's information.

Prompts and expected answers

Fictional situation	Expected safe response
1. A friend asks to borrow your school login.	Do not share it. Ask a teacher to help the friend access the approved resource through their own account.
2. A demo uses the same short password for two accounts.	Explain that each password should be long and unique. Use approved account support; never submit a real password to the class.
3. A slide includes a fictional class list with grades and home addresses.	Identify unnecessary sensitive details; replace them with an appropriate fictional example before wider sharing.
4. A free new app asks for the class roster.	Ask the teacher to check school approval before use or upload. Free access does not establish privacy suitability.

Assessment: Award one point for a safe action and one for a relevant reason per prompt (maximum 8). Provide feedback; this suggested rubric is not a security certification.

Adaptation: For younger learners, use pictures and a trusted-adult response. Offer oral answers, paired discussion and a teacher-led demonstration. Never use a learner's actual data.

Evidence: [1], objectives 1, 5 and 6; [5] app approval. Original suggested lesson.

What if the systems go offline?

Suggested: 20 minutes | teacher, school leader and IT representatives

Fictional scenario

At the start of the day, the learning platform and school email are unavailable. A staff member reports an unexpected sign-in prompt. The cause of the outage is unknown. Students are arriving and several lessons depend on online materials.

Time	Facilitator prompt	Decision to record
0-5 min	How do staff report when email is unavailable? What observations does IT need?	Named alternate channel, escalation contact and initial facts.
5-10 min	Which routines must continue safely? How do classes use the approved teaching fallback?	Owners for attendance, safeguarding, dismissal and lesson continuity.
10-15 min	Who verifies the situation and communicates with staff or families?	Investigation lead, authorized spokesperson and approved contact route.
15-20 min	What must be checked before normal use resumes? What gaps did the discussion expose?	IT restoration decision; action owners, due dates and a review date.

Run this as a discussion. Do not disable live systems, generate deceptive sign-ins or circulate real student records. Avoid speculating that a confirmed breach has occurred; record what is known and unknown.

One gap, its owner and target date:

Who will update the written plan and replace old contact cards?

Evidence: [1], pp. 33-36. This is an original exercise, not an official CISA tabletop package.

Connect the habit to the work

Show students the people and skills behind a safer school.

Use getintocyberjobs.com for career exploration after school review. Its profiles explain different cybersecurity pathways. NIST NICE provides a shared language for cybersecurity work and capabilities; a Work Role is not the same as an employer's job title. [9, 10]

Classroom practice	Career to explore	Evidence students can produce
Explain an alert and escalate a concern	SOC Analyst / Incident Responder	A fictional incident note: observation, risk and escalation.
Consider who should access a file	Identity & Access Management Engineer / Privacy Analyst	An access decision with reasons and limits.
Plan device care and recovery	Systems Administrator	A fictional maintenance and recovery checklist.
Teach peers how to verify a message	Security Awareness Specialist	A short explanation using a safe example.

These are suggested career connections, not formal mappings to NICE Tasks, Knowledge or Skills. Students can explore investigation, operations, development, privacy and leadership without assuming every cyber career is the same.

Suggested 15-minute extension

- Choose one career profile. Identify a task or responsibility and one skill the student wants to develop.
- Connect it to an activity from this guide. Explain what the activity demonstrates and what further learning would be needed.
- Write a next step: a supervised school club, approved learning activity or conversation with a careers adviser.

Games can support a lesson when reviewed first

Optional: browse [GamingForLearning.com](https://gamingforlearning.com). Preview the selected activity on a school device, check access and privacy requirements, provide an accessible alternative and debrief the decisions. Participation or game time alone does not demonstrate learning. No individual game is required for this guide.

Evidence: [9] NIST NICE; [10] Get Into Cyber Jobs. Connections and timing are suggested.

Turn gaps into owned actions

Review date: _____ School / team: _____

Check evidence, then choose the next priority. Use “not verified” where you have not checked a control. Do not mark a technical control complete from a teacher’s assumption.

Evidence to review	Owner / status / next action
1. Account protection and access removal	_____ _____
2. Approved devices, apps and update process	_____ _____
3. Backup coverage and dated restore test	_____ _____
4. Reporting card and incident exercise	_____ _____
5. Staff / student learning and assessment	_____ _____
6. Data sharing, storage and retention rules	_____ _____
7. Named leadership and near-term priorities	_____ _____
8. Longer-term review across CSF functions	_____ _____

Priority action / owner / due date / evidence of completion:

Learning evidence: Record the lesson, learner count, rubric used and common misconceptions; reteach, then reassess. Use approved storage and minimum necessary information. A small classroom assessment does not establish improved school security or career outcomes.

Evidence: [1], objectives 1-8; [7] CSF 2.0. Review sheet is an original implementation aid.

Sources and departures

Sources checked 7 October 2026. Numbered references appear throughout the guide.

Primary source [1]: Cybersecurity and Infrastructure Security Agency (CISA). K-12 Cybersecurity Foundations: Implementation Guide. 2026. Department of Homeland Security. August 2026 edition, 57 pages.

The CISA guide is in the public domain; permission is not needed to copy or adapt its text. Its notice requests the citation format used above when quoting, paraphrasing or referring to the report. Reproduction or other use of the CISA logo requires advance written permission. No CISA logo is used here.

[Official CISA publication page](#)

Departures and clarifications in this edition

Topic	Editorial treatment in this edition
Password guidance	The source’s 12-character suggestion (p. 16) is not presented as the current NIST threshold. Page 4 distinguishes NIST’s password-only and MFA rules. [3]
Patch timing	The source says patch within 30 days on p. 23, but suggests a minimum 30-day wait on p. 28. A blanket delay is not adopted; IT prioritizes risk and known exploitation. [8]
MFA	No guarantee is claimed and no email-to-laptop code is presented as inherently a separate factor. Distinct factors and phishing-resistant options are described. [3, 4]
Backups	Restore testing is retained; cloud sync alone does not establish adequate backup coverage. [1, 6]
File transfer / encryption	Departure: the source gives a separate-email password example (p. 43) and describes native document password protection as reliable in transit (p. 43). Page 6 instead recommends school-approved transfer rather than emailed sensitive files, and IT verification of encryption. This is this edition’s more restrictive recommendation, not a CISA requirement.
Roles and privacy	Teachers escalate; IT verifies controls; authorized leaders manage notices. Classroom app approval follows Department of Education advice. [1, 5]
Benefits and claims	No attack-rate, salary, job-demand or learning-impact statistics are reproduced. Suggested schedules, lessons and rubrics are clearly identified as teaching tools.

School requirements vary. This educational companion does not establish compliance; local IT, privacy and leadership owners should approve its operational use and fill in reporting details.

Primary references and resources

Use current official guidance alongside the school's own policies.

[2] [NIST: Phishing](#)

Message verification, suspicious requests and reporting.

[3] [NIST SP 800-63B-4: Digital Identity Guidelines](#)

Section 3.1.1: password length and policy; authentication factors.

[4] [CISA: Implementing Phishing-Resistant MFA](#)

FIDO/WebAuthn and stronger authentication planning.

[5] [U.S. Department of Education: Classroom-app approval FAQ](#)

Check school approval; consult IT about student privacy.

[6] [CISA and partners: #StopRansomware Guide](#)

Backup, containment and response; [official FBI-hosted PDF](#).

[7] [NIST: The Cybersecurity Framework \(CSF\) 2.0](#)

Six functions and organization-specific risk management.

[8] [CISA: Known Exploited Vulnerabilities Catalog](#)

Monitor known exploitation and prioritize remediation.

[9] [NIST: Getting Started with the NICE Framework](#)

Work Roles, learner capabilities and career exploration.

[10] [Get Into Cyber Jobs](#)

Independent career resource; visual theme and career examples.

[11] [CISA: Cyber Hygiene Services](#)

Free vulnerability scanning and enrollment contact.

[12] [FBI / CISA: June 2026 phishing-campaign guidance](#)

Current CISA email and 1-844-Say-CISA contact details.

[13] [FBI IC3: Ransomware](#)

Report ransomware incidents through [ic3.gov](#).

Sources checked 7 October 2026.

School use

Lessons, worksheets and forms in this edition may be copied for school use. No government endorsement is implied.