Cybersecurity Coordinator Forum (CCF)

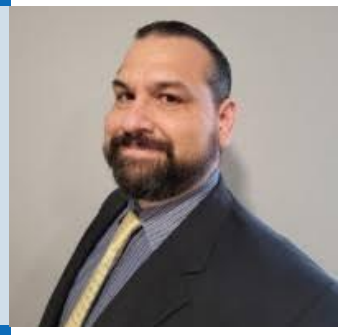
October 2026

Daniel Ramirez

Chief Information Security Officer

Texas Education Agency

cybersecurity@tea.texas.gov



Before we begin

Three quick notes for a smooth session

WATCH

This webinar is being recorded.

Recording and slides will be posted on the TEA Cybersecurity website a few days after the session.

PARTICIPATE

Chat is off – use Q&A for questions.

We will respond during the webinar if we can or follow up after the webinar by email.

JOIN SECURELY

Use unique login per participant.

Duplicate logins and chatbots are not allowed. AI Notetakers will be removed.

Agenda

1. Team and CCF Introductions
2. Legislative Updates
3. Cybersecurity Advisories
4. Emerging Trends
5. K-12 Cybersecurity Initiative Updates
6. Other Helpful Information
7. Upcoming Events
8. Wrap Up

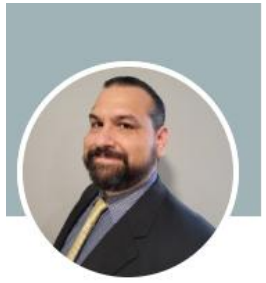


The TEA Team

- Texas Education Agency (TEA) – CISO
  - Daniel Ramirez – Chief Information Security Officer

- TEA K-12 Cybersecurity Initiative Group
  - Julia Schacherl - Executive Director, IT Administration & Compliance
  - Lara Coffer - DCS Contract Manager & K-12 Cybersecurity Project Lead
  - Susan Bain - Sr. Cybersecurity Governance, Risk, & Compliance Analyst
  - Desire Odiwo - Cybersecurity Governance, Risk, & Compliance Analyst

- TEA Security Operations
  - Sam Miller - Cybersecurity Operations Manager
  - Myles Muchineuta - Sr. Cybersecurity Operations Analyst


Daniel Ramirez


Julia Schacherl


Lara Coffer


Susan Bain


Desire Odiwo


Samuel Miller


Myles Muchineuta

Cybersecurity Coordinator Forum (CCF)

- Monthly TEA forum for K-12 cybersecurity leaders and partners
  - Cybersecurity Coordinators
  - Technology Directors
  - Education Service Centers (ESCs)
  - Regional Security Operations Centers (RSOCs)
- Gain insights from the TEA Information Security Office
- Actionable guidance to strengthen your cybersecurity program
- Stay informed on emerging threats, best practices, and statewide initiatives
- Registration Link for CCF Forum (use your school email address)
- Mark your calendar for the **fourth Wednesday** of each month at **11am**.

- No CCF meeting in Nov & Dec. Next CCF will be **January 27, 2027**!

Texas Education Agency

Cybersecurity Advisories

Critical PHP Vulnerabilities (PHP2Shell)

Immediate Review and Remediation Recommended

- Two critical vulnerabilities affecting PHP, commonly referred to as PHP2Shell (CVE-2026-109618 and CVE-2026-109619), have recently been identified.
- These vulnerabilities may allow an unauthenticated attacker to execute code remotely on affected web servers, potentially leading to complete compromise of vulnerable internet-facing systems.
- Because PHP is widely used to support websites, web applications, learning platforms, content management systems, and custom-developed applications, all Texas school systems should immediately review their technology inventories to identify any systems utilizing PHP and assess their exposure.

Why This Matters

- Successful exploitation could allow an attacker to gain control of the web application process, access sensitive information, modify website content, deploy malicious software, establish persistence, or use the compromised system as a foothold for further activity within the environment. Public reporting indicates that exploitation may be possible without authentication and that vulnerability scanning and exploitation activity are expected to increase rapidly following disclosure.

Critical PHP Vulnerabilities (PHP2Shell) - Recommended Actions

1. Identify Potentially Affected Systems

- Conduct an inventory review to determine whether your environment includes systems using PHP.
- Particular attention should be given to internet-accessible systems.

2. Determine Version and Exposure

- For each identified system:
  - Verify the installed PHP version.
  - Determine whether the system is accessible from the public internet.
  - Confirm whether updates or vendor-provided patches are available.

3. Apply Updates as Quickly as Possible

- Organizations should prioritize patching affected systems as soon as operationally feasible.
- Where systems support critical business, instructional, or operational functions, technology leaders should carefully evaluate maintenance windows, downtime requirements, and service impacts; however, the risk posed by continued exposure should be weighed against the potential disruption associated with emergency maintenance.

Critical PHP Vulnerabilities (PHP2Shell) - Recommended Actions (cont'd)

4. Consider Additional Risk Reduction Measures

- If immediate patching is not possible:
  - Limit public internet exposure where feasible.
  - Implement temporary compensating controls.
  - Increase monitoring of application, web server, and security logs.
  - Review vendor guidance for any available mitigations.

5. Evaluate Whether Temporary Service Interruption Is Warranted

- For highly exposed systems that cannot be patched in a reasonable timeframe, organizations should evaluate whether temporarily removing a system from public internet access presents less risk than continued operation in a vulnerable state.
- This determination should consider:
  - The criticality of the application.
  - Availability of alternative services or processes.
  - Potential impact to instruction and business operations.
  - The likelihood and consequences of compromise.

Frontline Education Breach

- Frontline internally identified the breach on August 14th
- Vulnerability in a Frontline Education application led to attackers accessing internal databases containing administrative and workforce management records
  - Full Names, physical street addresses
  - Direct email addresses associated with district employment
  - Social Security Numbers
- Breach notification emails started in early October and are expected to be fully released at this time (End date of October 16th).
- Recommended Remediation efforts
  - Enable MFA for all accounts
  - Double check your credit reports through annualcreditreport.com

New CVEs: BeyondTrust, Citrix, FortiMail, ProFTPD

- BeyondTrust versions 26.2.3 or earlier: CVE-2026-102764 – 9.3 Remote Execution through File Operations
  - SaaS deployment not affected
- Citrix NetScaler: CVE-2026-88771 – 88779 – 9.5 Remote Code Execution
  - Zero Day discovered on October 2nd affecting versions before 14.1
  - Affects SAML, IdP deployments for Citrix NetScaler Gateway and ADC
- FortiMail versions 8.0.0 or earlier: CVE-2026-104286 – 9.8 Path Traversal and Remote Code execution
  - Allows attackers to write arbitrary files on underlying system through HTTP(S) requests
- ProFTPD version 1.3.5: CVE-2015-3306 – 10.0 Remote Code Execution
  - Mod_Copy module in ProFTPD can allow for attackers to read and write to arbritary files.
- Apply latest patches!

New CVEs: Cisco, Apple, Apache, OnlyOffice

- Cisco Catalyst SD-WAN Manager versions 20.1.12 or earlier: CVE-2026-76504 – 9.8 Unauthorized API access as admin
  - Attackers can send crafted HTTP requests to a specific API endpoint
- iOS and iPadOS versions 26.7.0 or earlier: CVE-2026-86950 – 8.8 Remote Code Execution
  - Fixed in iOS 26.7.1, macOS Sequoia 15.8.1, and Tahoe 26.7.1
- Apache Struts versions 2.3.19 – 2.3.24.1 and 2.3.25 – 2.3.28: CVE-2016-3081 – 8.1 Remote Code Execution
  - Allows remote attackers to execute arbitrary code via method: prefix
- OnlyOffice versions 5.6.3 or earlier: CVE-2021-3199 – 9.8 Remote Code Execution and Directory Traversal
  - ONLYOFFICE Document Server allows for ../ attack and leads to remote execution abilities
- Apply patches!

Texas Education Agency

Emerging Threats

AI (SI) Incident Response

- Artificial Intelligence (AI) may now be referred to as Super Intelligence (SI).
- NIST has published an SI incident readiness document as part of NIST 800-61.
  - Outlines ten key practices for managing rogue SI agents
  - Part of a White House recommendation to provide best practices in securing SI
  - https://www.cisa.gov/topics/cybersecurity-best-practices/super-intelligence

Texas Education Agency

K-12 Cybersecurity Initiative Updates

K-12 Cybersecurity Initiative (K-12CI)

2023

STATEWIDE LAUNCH

TEA responded as ransomware and cyber threats increasingly targeted Texas schools.

The model pairs sustained public investment with practical, local execution.

BACKED	Funded by the 88th Legislature and continued in the 89th to sustain dedicated cybersecurity resources.
BUILT TO	Provide practical solutions that help schools prevent and respond to major cyber incidents.
FOCUSED	Give priority to high-need school systems.
DELIVERED	Use regional ESC cybersecurity practitioners to help schools implement aligned controls.

K-12CI Current Program Participation

- **School systems that have onboarded with DIR**
  - **574** school systems have signed the DIR interlocal agreement form.
- **Endpoint Detection Response (EDR)**
  - **428** school systems have signed up for EDR, installed on **428,500+** endpoints.
  - **105,000+** attacks blocked. **19,000+** ransomware threats neutralized.
- **Texas Cybersecurity Framework (TCF) Assessments**
  - **82** school systems have signed up; **65** completed.
- **Email Security Service**
  - **302** school systems have signed the ILC with UT-RSOC
  - UT-RSOC has successfully onboarded **259** school systems to the Abnormal AI shared cloud tenant.
- **Security Awareness Training**
  - **470** school systems implemented and active, **192** school systems in onboarding process

For more info on how to sign up, visit TEA K-12 Cybersecurity.

Statewide EDR Protection Coverage

TOTAL EDR AGENTS DEPLOYED

428,056

Across all participating school systems

SCHOOL SYSTEMS WITH EDR

428

of 1,213 school systems

35.3% statewide

STATEWIDE PARTICIPATION

35.3%

of Texas school systems

428 of 1,213

DEPLOYMENT GROWTH

+59.3%

Since December 2025

(270,923 → 428,056)

Total EDR Agents Deployed Over Time



Statewide EDR Deployment Overview

SCHOOL SYSTEMS WITH EDR

428 of 1,213

35.3% statewide coverage

APPROVED EDR AGENTS

592,736

Across participating school systems

ACTIVE EDR AGENTS

428,056

30-day active count

OVERALL DEPLOYMENT

72.2%

428,056 active / 592,736 approved

Approved vs. active deployment



165,201 approved agents are not reflected as 30-day active

School-system deployment thresholds

Cumulative counts based on each school system's % deployed

50% or under	>50% to 75%	>75% to 85%	>85% to <90%	90% or higher
137	118	62	30	81
32.0% of EDR systems	27.6% of EDR systems	14.5% of EDR systems	7.0% of EDR systems	18.9% of EDR systems

Deployment ranges are mutually exclusive and together account for all 428 school systems with EDR.

EDR Realignment: Final Deployment Deadline

OCTOBER 31 2026
FINAL DEADLINE

Reminder Deploy EDR to every eligible in-scope system by October 31. The goal is complete security coverage, not consumption of the original allotment.

01

Complete Deployment

Use the remaining time to install EDR on all eligible in-scope devices and confirm agents are actively reporting.

02

Right-Size Allocation

After the deadline, TEA will align each allocation to actual deployed agents plus a 10% operational cushion.

03

Request More if Needed

The Add-On process remains available. TEA may approve justified requests up to the school system's program maximum.

Key takeaway **Protect all in-scope devices now. Realignment preserves a growth cushion, and additional agents remain available through TEA review.**

Abnormal AI Statewide Participation

PARTICIPATING OR IN PIPELINE

379 of 1,213

31.2% statewide participation

ACTIVE SERVICE

259 school systems

21.4% of all school systems

ONBOARDING PIPELINE

120 school systems

Not yet in Active status

Participation stage

Mutually exclusive stages progressing toward active service

Service Requested, ILC Needed	ILC Pending School System	ILC In Progress	Abnormal AI Request Pending	Pending Deployment	Active
22	25	24	13	36	259
1.8% of 1,213	2.1% of 1,213	2.0% of 1,213	1.1% of 1,213	3.0% of 1,213	21.4% of 1,213

Active-service protection impact

TOTAL STUDENTS PROTECTED

1,457,703

2024 enrollment across 259 Active school systems

TOTAL STAFF PROTECTED

203,165

2024 staffing across 259 Active school systems

New Initiatives for FY26-FY27

- All school systems are eligible. These services are provided at no-cost to the school system.
- **Implement Email Security Service (Abnormal Security)**
  - Provided in partnership with the University of Texas Regional Security Operations Center (UT-RSOC)
  - Provide 30-day notice to your existing contract holder.
  - **Available Now - FAQ**
- **DIR Certified Security Awareness Training and Phishing Simulations (InfoSec IQ)**
  - Provided in collaboration with the Technology Alliance for Statewide Initiatives (TASI)
  - **Available Now - FAQ**
- **Microsoft 365 & Google Workspace Hardening Guides**
  - Developed by TASI to support secure configuration practices
  - **Available Now** - Contact your ESC for sign-up and distribution
- **Software Deployment Solution (PDQ Connect Premium)**
  - Provided through TASI to support deployment of EDR agents and other software
  - **Available Now** - Contact your ESC for sign-up and distribution

- More information about these services can be found on TEA Cybersecurity website.

TASI Updates: K-12 Cybersecurity Initiative Support

- **NEW: Software Deployment and Endpoint Management / Patching Solution**
  - PDQ Connect Premium is available at no cost to your school system.
  - PDQ Connect Premium handles software deployment, asset inventory, vulnerability management, patch management, and remote access to assets.
  - You can create automations to establish device baselines and document patch / control compliance. Save headaches by deploying pre-built, vetted software packages.
  - **Contact your ESC to sign up. Second wave of deployments now underway!**

- **Currently Deploying: Phishing Simulation and Cybersecurity Training**
  - Infosec IQ subscription is available at no cost to your school system.
  - Includes current DIR-approved cybersecurity and AI awareness training
  - **Contact your ESC to sign up. Immediately available.**

- **New: Microsoft 365 & Google Workspace Hardening Guides**
  - Developed by TASI to support secure configuration practices
  - Available Now - Contact your ESC for sign-up and distribution

- **Continued Services and Support**
  - Assistance with DMARC compliance, MFA, and limited local administrator access
  - **Contact your ESC for more information.**

Participation Strengthens Protection Across Texas K-12

TX Cyber Command

ANALYZE & CORRELATE

Identifies emerging patterns and develops relevant, actionable threat intelligence and IOCs.

Participating School Systems

CONTRIBUTE TELEMETRY

Endpoint, email, and security-service activity provides visibility into threats affecting Texas K-12.

ONE SCHOOL SYSTEM'S TELEMETRY

may help protect many

DIR MSS + 3 RSOCs

OPERATIONALIZE INTELLIGENCE

Incorporate relevant intelligence into supported managed security services.

Stronger Managed Protection

IMPROVE DETECTION & PREVENTION

Services such as managed EDR and Abnormal AI benefit from a broader statewide threat picture.

VALUE TO THE SCHOOL SYSTEM — **Managed protections informed by a broader view of threats.**

VALUE TO TEXAS K-12 — **Greater collective awareness and a stronger statewide defense.**

TXCC Endpoint Detection and Response

TXCC Endpoint Detection and Response

Endpoint detection and response (EDR) reported 27,106 detections for 474,625 monitored devices.

Metric	Count
Current total count of monitored endpoints	610,797
Current total count of EDR threats	27,106
DIR-Funded Entities	69
DIR-Funded count of monitored endpoints	179,772
TEA-Funded Entities	413
TEA-Funded count of monitored endpoints	423,793
Self-Funded Entities	21
Self-Funded count of monitored endpoints	7,232



TLP:Amber

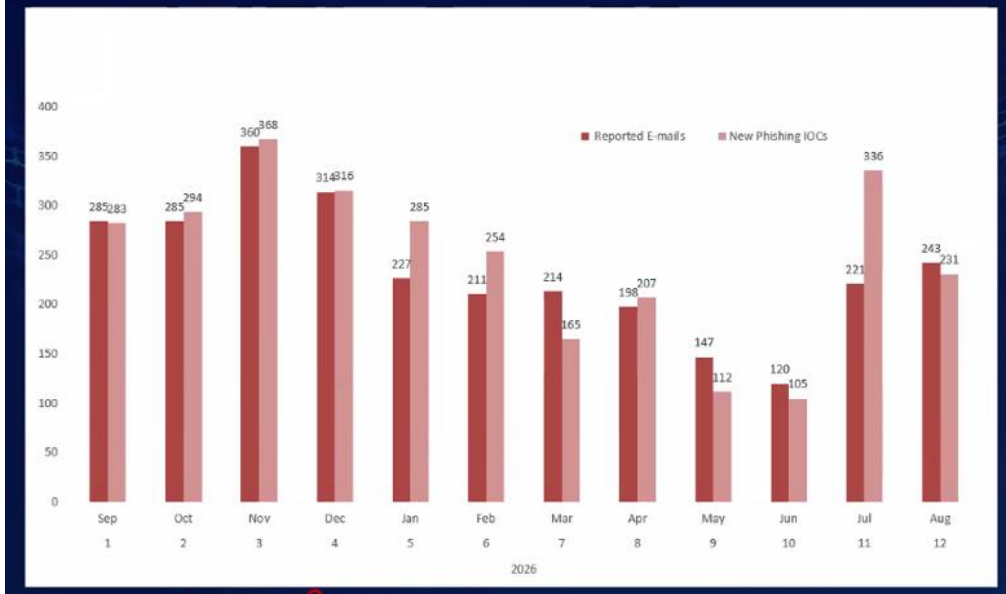
TXCC TEXAS CYBER COMMAND

TXCC Phishing Email Analysis

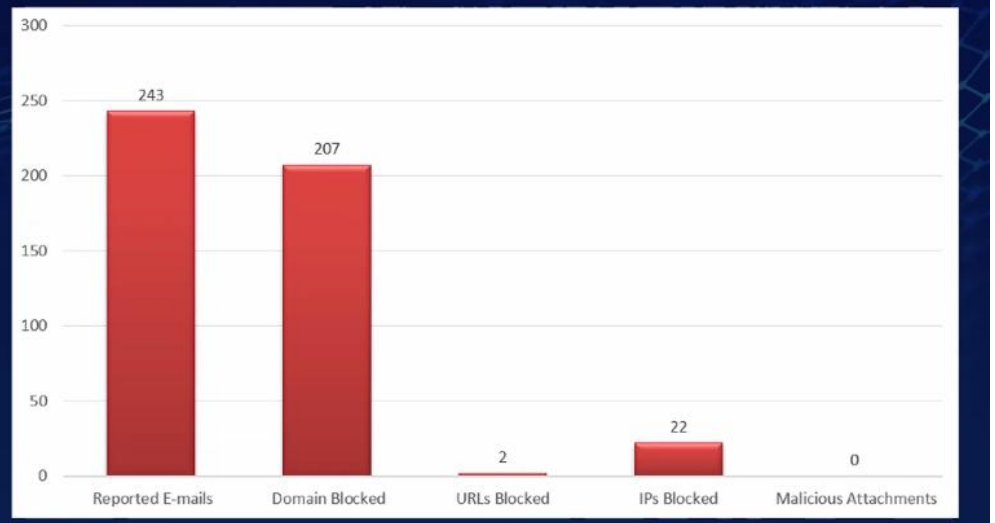
TXCC Phishing Email Analysis

CyberOps received 243 forwarded phishing emails. Of the emails reported, 94 percent were confirmed to be malicious, resulting in the blocking of 207 new domains, 2 new URLs, and 22 new IP addresses. There were 0 malicious attachments identified this month.

Reporting vs IOCs Discovered



Emails Reported and Subsequent Actions



TXCC TEXAS CYBER COMMAND

TLP:Amber

Starting With The Service You Need

The K-12 Cybersecurity Initiative connects school systems to the appropriate authorized provider.

AUTHORIZED PROVIDERS

DIR MSS • 3 RSOCs • 20 ESCs

Endpoint Protection

- Managed Endpoint Detection and Response (EDR)
- PDQ Connect software deployment and patch management

Identity & Access

- Staff email MFA configuration assistance
- Assistance restricting local administrator access

Email Security

- Abnormal AI email security
- DMARC compliance configuration assistance

Cloud Hardening

- Microsoft 365
- Google Workspace

Awareness & Testing

- SecurityIQ State-certified cybersecurity awareness training
- Phishing simulations

Assessment

- Texas Cybersecurity Framework (TCF) assessment

IDENTIFY NEED → SELECT SERVICE → CONNECT TO AUTHORIZED PROVIDER

Not every provider offers every service. Focus on the capability needed; the initiative will help identify the appropriate delivery resource.

Texas Education Agency

Other Helpful Information

AskTED Updates

- Most TEA Cybersecurity emails will be sent to the Cybersecurity Coordinator and/or Technology Coordinator.
- TEA pulls this information from the TEA official contact information portal called AskTED.
- This is located at this link: AskTED. You do not need a logon ID to access this public information.
- Changes to the AskTED portal can only be made by your school's TED Administrator. You can look up your TED Administrator in the AskTED portal.
- Update your AskTED contact information at least once a year and anytime there is a staff change in key positions (Cybersecurity Coordinator or Technology Coordinator).

Texas Education Agency

Cybersecurity Awareness Month

Cybersecurity Awareness Month: Beyond the Basics

Cybersecurity and Infrastructure Security Agency (CISA) identifies four foundational practices everyone can take to help reduce cybersecurity risk. Governance, Risk and Compliance (GRC).



Avoid and Report Phishing



Use Strong Passwords



Use MFA and a Password Manager



Update Software

But what do these practices look like at the organizational level?

CISA tells us **WHAT** to do. GRC helps us understand **WHY** we're doing it, **WHO** is responsible, whether it's **WORKING**, and how we can **DEMONSTRATE** it.

Looking Through a GRC Lens

GOVERNANCE → RISK → CONTROLS → EVIDENCE → CONTINUOUS IMPROVEMENT

Phishing Through a GRC Lens

SCENARIO: An organization provides cybersecurity awareness training that includes phishing and a way to report suspicious emails. Is that enough to conclude phishing risk is being effectively managed?

GOVERNANCE

Are responsibilities, requirements, and accountability clearly defined?

- Reporting process
- Assigned ownership
- Escalation path

RISK

What threat scenarios and impacts are we trying to reduce?

- Credential theft
- Unauthorized access
- Data exposure
- Operational disruption

CONTROLS

Do preventive, detective, and responsive controls address the risk?

- Awareness training
- Email safeguards
- Reporting process
- Incident response

EVIDENCE

What demonstrates that controls are operating as intended?

- Training records
- Reporting data
- Control assessment results
- Incident information

IMPROVEMENT

Are results driving changes to controls or risk treatment?

- Recurring patterns
- Identified gaps
- Control adjustments
- Targeted awareness

GRC TAKEAWAY: Completing an activity demonstrates implementation. It does not, by itself, establish that the control is effective or that the remaining risk is acceptable.

Applying the GRC Lens

STRONG PASSWORDS

GOVERNANCE
Are requirements defined?

RISK
Where could weak credentials expose us?

CONTROLS
Are requirements enforced?

EVIDENCE
What shows requirements are enforced?

IMPROVEMENT
Where do gaps or exceptions remain?

MFA

GOVERNANCE
Where is MFA required?

RISK
What's the exposure if credentials are compromised?

CONTROLS
Is MFA implemented across scope?

EVIDENCE
What shows MFA coverage?

IMPROVEMENT
How are exceptions addressed?

SOFTWARE UPDATES

GOVERNANCE
Are responsibilities and requirements defined?

RISK
Which vulnerabilities create the greatest exposure?

CONTROLS
Are updates addressed?

EVIDENCE
What shows systems are up to date?

IMPROVEMENT
What treatment is used when systems cannot be updated?

The GRC Lens: The technology may change, but the questions remain consistent: What is the risk? Who owns it? What controls address it? What evidence do we have? What needs to improve?

Beyond Awareness: Managing Cybersecurity Risk

Good cybersecurity practices are the starting point. GRC helps determine whether they are managing risk.

IMPLEMENTED

Did we do it?

- Training completed
- Reporting available
- Safeguards in place

→

EFFECTIVE

Is it working?

- Employees recognize suspicious emails
- Suspected phishing is reported
- Results inform control improvements

→

RESIDUAL RISK

What risk remains?

- Credential compromise
- Control gaps
- Exceptions
- Additional risk treatment needed?

PHISHING EXAMPLE

100% of employees completed phishing awareness training	Are employees recognizing and reporting suspected phishing?	Where does phishing risk remain?

GRC TAKEAWAY

Cybersecurity awareness starts with individual action. GRC helps turn those actions into defined, measurable, and continually improving organizational practices.

Additional Resources

- Texas DIR and Cyber Command have lots of unique webinars and courses.
  - https://www.txcc.texas.gov/cybersecurity-awareness-month
  - https://dir.texas.gov/information-security/cybersecurity-awareness-month
- Organizations and vendors are running cybersecurity games, simulations, and exercises.
  - Get involved in creating your own!

Texas Education Agency

Upcoming Events

Upcoming Events

- **ESC 1**

  Event: **Cybersecurity Summit 2026**

  Date: October 29, 2026

  Info: https://www.esc1.net/cyber-security-summit

- **ESC 11**

  Event: **Annual Technology Vendor Fair**

  Date: November 6, 2026

  Info: https://www.esc11.net/what-we-do/departments/technology/tvf26

- **ESC 16**

  Event: **Panhandle EdTech Conference**

  Date: November 11, 2026

  Info: https://www.esc16.net/apps/news/category/19252

- **ESC 2**

  Event: **Cybersecurity Summit 2026**

  Date: January 29, 2027

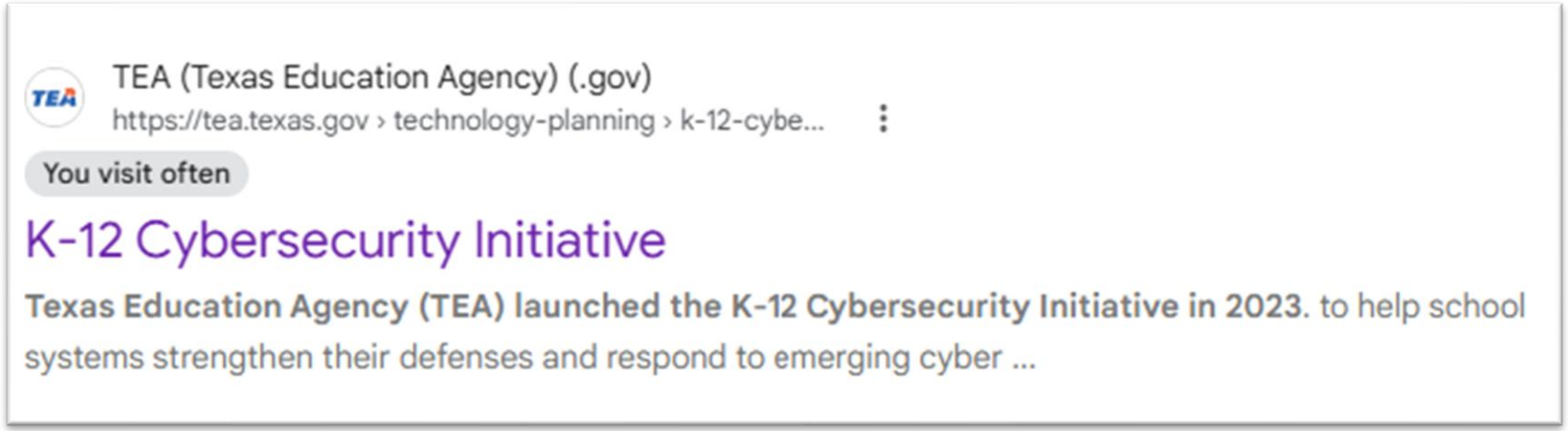
  Info: https://apps.esc1.net/ProfessionalDevelopment/esc2/Registration/Workshop/438875

Texas Education Agency

Wrap Up

K-12 Cybersecurity Initiative Website

- Easy to find → Type **TEA** & **Cybersecurity** into search



- Website: https://tea.texas.gov/k12cyber
  - Steps for onboarding school systems to K-12 Cybersecurity Initiatives
  - New program updates
  - Frequently asked questions
  - Previous K-12 Cybersecurity Initiative Webinars posted on this page
- Program email: k12cyber@tea.texas.gov

Stay Safe & Secure

Thank you!

Questions?

Email:
k12cyber@tea.texas.gov