Cybersecurity Coordinator Forum

Todd Pauley, CISSP, CISM

Deputy CISO/Cybersecurity Coordinator

Texas Education Agency

todd.pauley@tea.texas.gov

September 27, 2023

Texas Education Agency

Cybersecurity Coordinator Forum

The TEA **Information Security** team hosts a monthly meeting for **Texas LEA Cybersecurity Coordinators, ESC Cybersecurity personnel**, and other members of the community that support K12 Cybersecurity efforts. It provides content designed to assist LEAs and ESCs towards maturity in an information security program.

Register here with your LEA email address:

https://attendee.gotowebinar.com/register/8234183618339320587

Agenda

- Cybersecurity Announcements
  - TxISAO (Texas Information Sharing & Analysis Organization)
  - State-Local Cybersecurity Grant Program (SLCGP)
  - CyberStart America
  - Cybersecurity Advisory
  - Updated Cybersecurity Incident Reporting

- The White House’s K-12 Cybersecurity Program
  - Detailed Offering from Cloudflare – Sarah Johannes

- Texas K12 Cybersecurity Initiative Update

TxISAO

ACTION: Please sign up for mailing list at the link below.

https://dir.texas.gov/txisao

The Texas Information Sharing & Analysis Organization (TxISAO) is open to all organizations in Texas to include K-12.

State and Local Cybersecurity Grant Program (SLCGP)

CISA Cybersecurity Grant

Texas was allocated approximately $40 million over four years. The allocation requires matching funds that increase through the years. (Note: Matching funds will be paid by grant sub-recipients.)

- The allocation is broken up into 4 years with awards happening individually in each year.
- A minimum of 80% of allocations must be passed through to local governments. In addition, at least 25% of the total funds made available under the grant must be passed through to rural communities.
- Requirements in order to be eligible:
  - Sign and participate in these free CISA services: Web Application Scanning, Vulnerability Scanning, Nationwide Cybersecurity Review (NCSR).
  - Join the TX-ISAO (free).

- Texas submitted our Cybersecurity Plan for grant implementation. Once the plan has been approved, proposals can be submitted and will be reimbursed if approved.

https://dir.texas.gov/information-security/state-and-local-cybersecurity-grant-program-slcgp

TEA
Texas Education Agency

CyberStart America

CyberStart America Early Access

CyberStartTX

CYBERSTART
AMERICA

The National Cyber Scholarship Foundation (NCSF) is listening to teacher feedback and for the first time ever, CyberStart America is offering early access to the game starting THIS WEEK.

Teachers and students now have full access to the game, and students' points from last year will roll over. The official game launch is set for October 16th, 2023, but students will retain the points they earn starting now!

Important! Please use the following links to register:
Educator Registration - **https://register.cyberstartamerica.org/teacher/**
**PRO TIP: Don't forget to make your student groups before signing students up! You will save a lot of time if you have the group code ready to go at the time of registration then having to track them down later on.

(PDF Flyer available in the Handouts Section)

Student Registration -
https://register.cyberstartamerica.org/student/
**PRO TIP: Use the personalized referral link teachers received in their welcome email so your students auto-populate to your school. That will prevent them from accidentally registering for the wrong school due to typos and other issues.

FBI & CISA releases Joint Cybersecurity Advisory for Snatch Ransomware

- First appeared in 2018
- Snatch operates a ransomware-as-a-service (RaaS) model and claimed their first U.S.-based victim in 2019.
- Initial Access:
  - Exploiting weaknesses in Remote Desktop Protocol (RDP).
    - Have been known to purchase credentials from the dark-web marketplaces.
- Gain persistence by elevating privileges and gaining access to administrator accounts.
- Unique in that the ransomware appends a series of hexadecimal characters to each file and folder name it encrypts, resulting in a unique identifier for each infection.

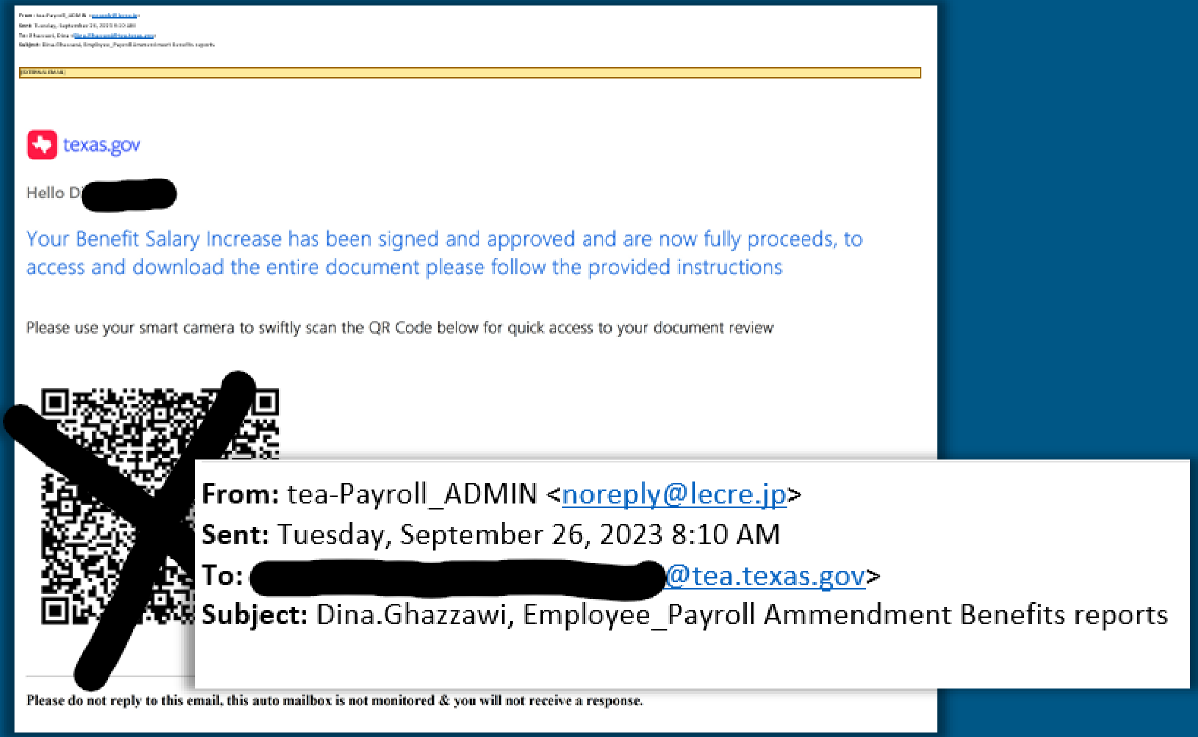
- Mitigations include:
  - Closely monitoring remote access tools.
  - Implement application controls.
  - Strictly limit or disable RDP.
  - Disable command-line scripting.
  - Alert on and review any newly created accounts.
  - Protect domain admin accounts by not caching their password hashes locally.

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-263a

Cybersecurity Advisories

QR Code Phishing Attacks Spread

- Will often spoof Microsoft, Google or other well none systems you may use.
- Be very suspicious of any QR that you aren't 100% confident in the source.
- Examine the link displayed before opening.



[illegible]

[EXTERNAL EMAIL]

texas.gov

Hello D[redacted]

Your Benefit Salary Increase has been signed and approved and are now fully proceeds, to access and download the entire document please follow the provided instructions

Please use your smart camera to swiftly scan the QR Code below for quick access to your document review

From: tea-Payroll_ADMIN <noreply@lecre.jp>
Sent: Tuesday, September 26, 2023 8:10 AM
To: [redacted]@tea.texas.gov>
Subject: Dina.Ghazzawi, Employee_Payroll Ammendment Benefits reports

Please do not reply to this email, this auto mailbox is not monitored & you will not receive a response.

Local Government Incident Reporting (SB 271)

Review

- SB 271 requires state agencies and local governments that experience a security incident to:
  - report to DIR within 48 hours after discovery (or to notify the secretary of state if the incident involves election data),
  - comply with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state, and
  - report to DIR the details of the security incident and an analysis of the cause of the incident within 10 days after incident eradication, closure and recovery.
- Effective September 1, 2023.

Local Government Incident Reporting (SB 271)

Definitions

Local government: a county, municipality, special district, school district, junior college district, or other **political subdivision of the state.**

Security incident:

a breach or suspected breach of system security as defined by Section 521.053, Business & Commerce Code; and

the introduction of ransomware, as defined by Section 33.023, Penal Code, into a computer, computer network, or computer system.

Texas Education Agency

Local Government Incident Reporting (SB 271)

Process

- Incidents will be submitted using Archer Engage
- After creating an account, users can submit incidents and then the closure/post-mortem form
- This will replace the current School District Incident Report, required by Section 11.175 of the Education Code

https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/sb-271-security-incident

TEA
Texas Education Agency

The White House's Efforts to Strengthen America's K-12 Cybersecurity

White House K-12 Cybersecurity

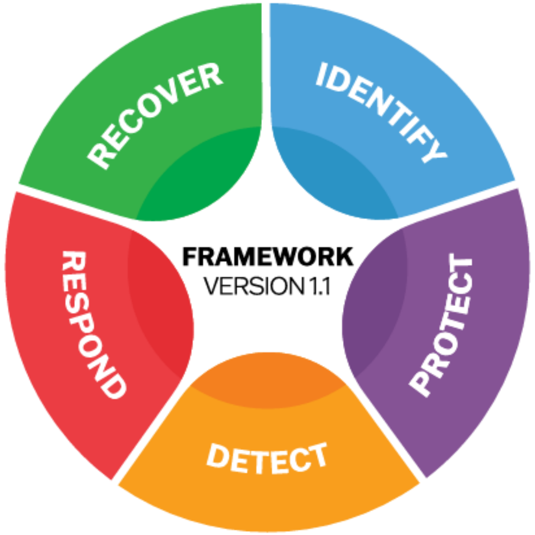
Biden-Harris Administration Launches New Efforts to Strengthen America’s K-12 Schools’ Cybersecurity

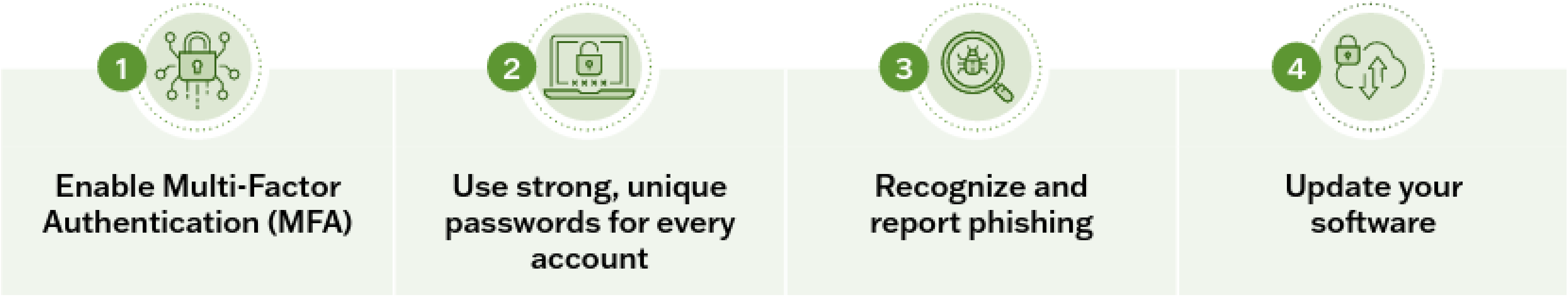
- Loss of learning from a cyberattack ranges from three days to three weeks!
- Monetary losses from an incident cost a district between $50,000 and $1 million.
- Laid out several resources to help the nation’s 13,000+ school districts.

https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/07/biden-harris-administration-launches-new-efforts-to-strengthen-americas-k-12-schools-cybersecurity/

White House K-12 Cybersecurity

The U.S. Dept. of Ed. (DOE) and Cybersecurity and Infrastructure Security Agency (CISA) jointly released a guidance document, “K-12 Digital Infrastructure Brief: Defensible & Resilient.”





1 Enable Multi-Factor Authentication (MFA)

2 Use strong, unique passwords for every account

3 Recognize and report phishing

4 Update your software

High-Impact Recommendations

White House K-12 Cybersecurity

Action and commitments taken to support K-12 Cybersecurity:

- The FCC is establishing a pilot program to provide $200 million over three years.

- U.S. DOE will establish a Government Coordinating Council to coordinate efforts between federal, state, local, tribal and territorial education leaders.

- CISA is continuing support to provide training, exercises and services to the K-12 community.

- Various vendors have announcement programs and opportunities to provide training and funding for K-12.

White House K-12 Cybersecurity

Vendor announcements to support K-12 Cybersecurity:

AWS

- $20 million for K-12 cyber grant program.
- Free security training tailored to K-12 IT staff through AWS Skill Builder.
- No-cost incident response through it's Customer Incident Response Team
- Free security reviews to ed-tech companies

- Start with this link:
  https://pages.awscloud.com/k12-cyber-grant.html?trk=8ff0cd84-6f01-46b7-9498-ab9ddbfb4866&sc_channel=el

- Application is open through December 31, 2023 as funds are available.

- If accepted, credits are issued based on the size of student population, up to $100k for > 100,000 students. Credits issued are good for 1 year.

White House K-12 Cybersecurity

Vendor announcements to support K-12 Cybersecurity:

Cloudflare

- Through its Project Cybersafe Schools, will offer Free Zero Trust cybersecurity solutions to public school districts under 2,500 enrollment.
- Safer internet browsing and email security.
- More information coming from Cloudflare themselves.

White House K-12 Cybersecurity

Vendor announcements to support K-12 Cybersecurity:

PowerSchool

- Free and subsidized “security as a service” courses, training tools and resources to all U.S. districts.

Google

- Released an updated “K-12 Cybersecurity Guidebook.”

D2L

- Providing access to new cybersecurity courses in collaboration with trusted third-parties.
- Extending its information security review for the core D2L integration partners
- Pursuing additional third-party validation of D2L compliance with security standards.

TEA
Texas Education Agency

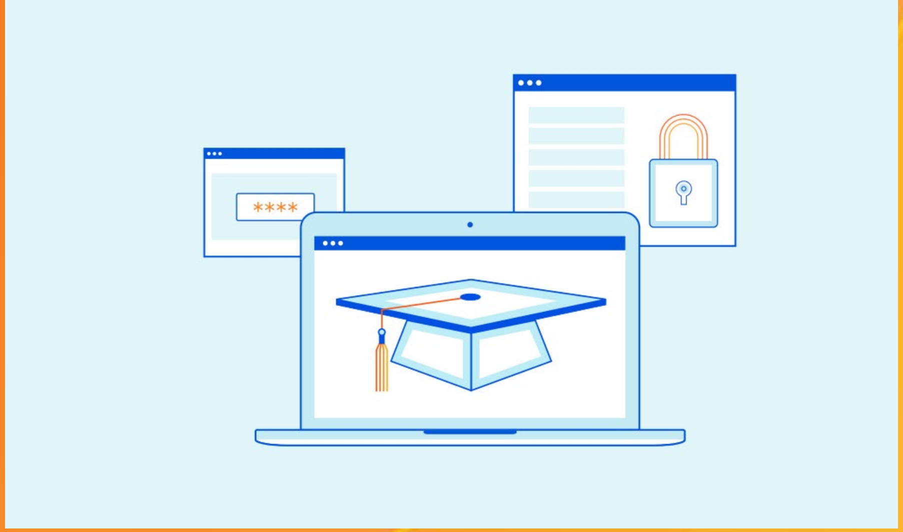
Cloudflare Offering to Support the White House's Efforts

CLOUDFLARE

Texas Education Agency

Project Cybersafe

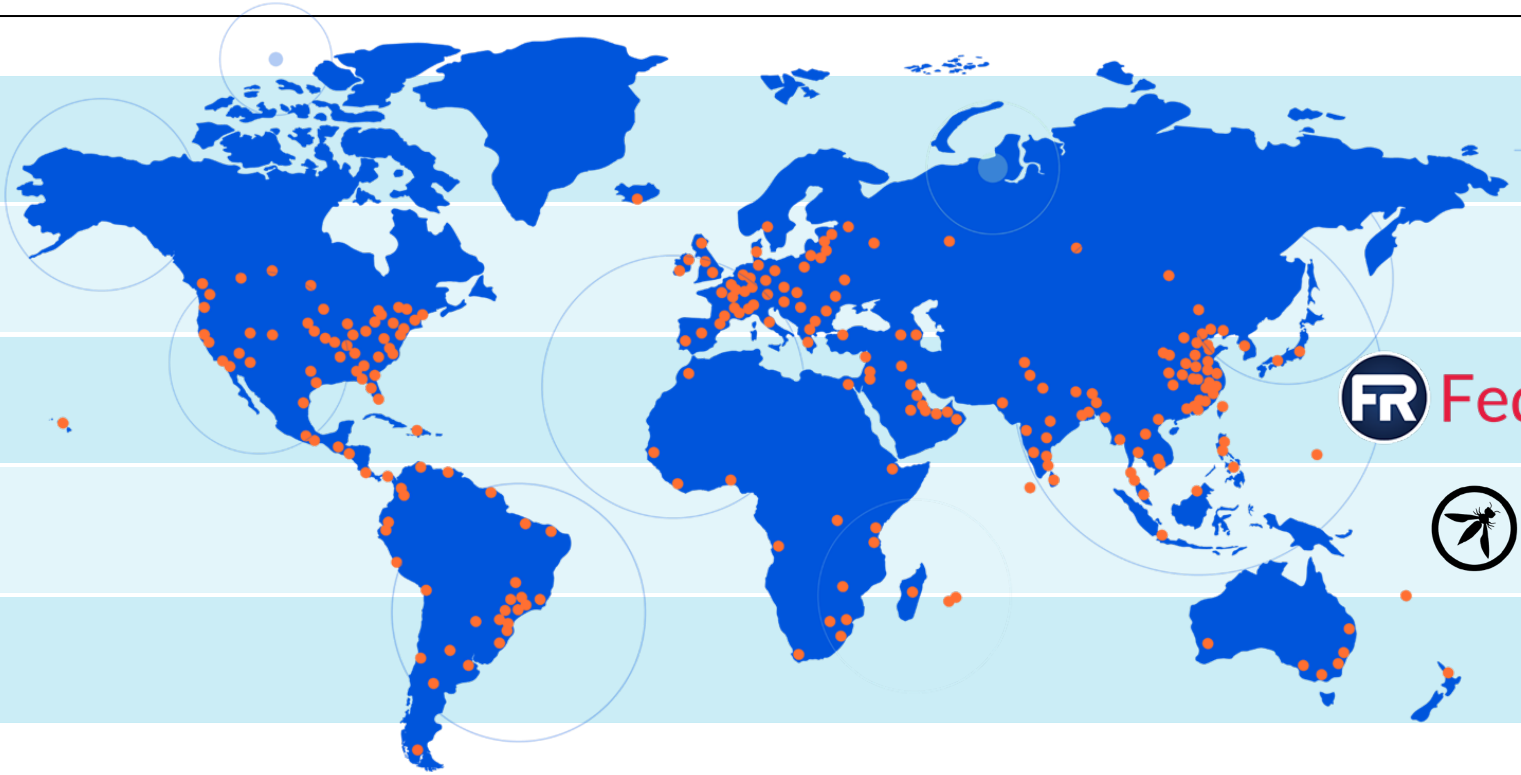
Sarah Johannes
Head of Sales - SLED West
sjohannes@cloudflare.com



Joe Haubner
Account Executive
jhaubner@cloudflare.com

Cloudflare is an Internet-native platform that delivers local capabilities with global scale in the areas of...

CLOUDFLARE



Security

Privacy

Performance

Resilience

Agility

FedRAMP

OWASP®

CRIMINAL JUSTICE INFORMATION SYSTEMS CJIS COMPLIANT

510+
cities in 100+ countries

90
Data centers in the US across **41 cities**

11,000+
networks directly connect to us, including ISPs,
cloud providers & large enterprises

209 Tbps
of network edge capacity and growing

136B
Threats Blocked **Daily**

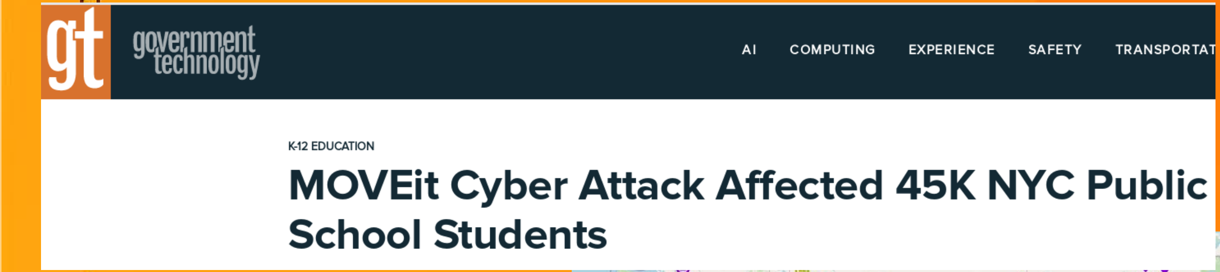
95%
Of the world's Internet users within **50ms**

100%
Uptime **SLA**

20%
of the world's Internet traffic

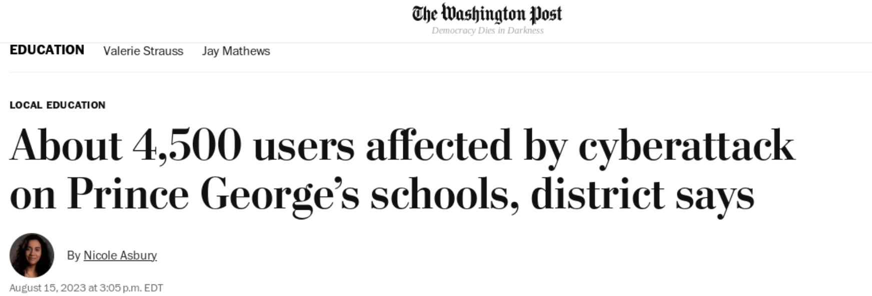
Cyber Threats are a National Issue

CLOUDFLARE



K-12 EDUCATION

MOVEit Cyber Attack Affected 45K NYC Public School Students

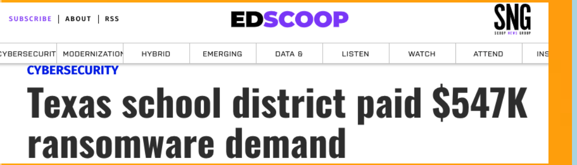


LOCAL EDUCATION

About 4,500 users affected by cyberattack on Prince George's schools, district says

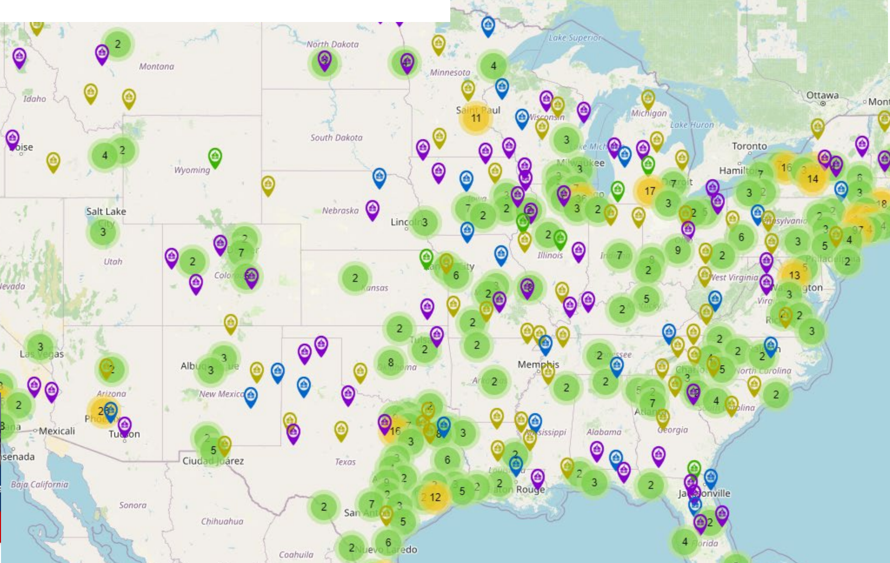
By Nicole Asbury

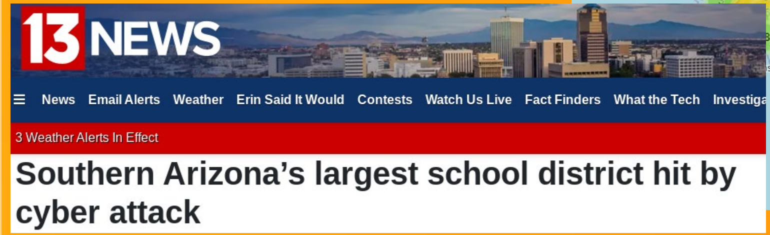
August 15, 2023 at 3:05 p.m. EDT



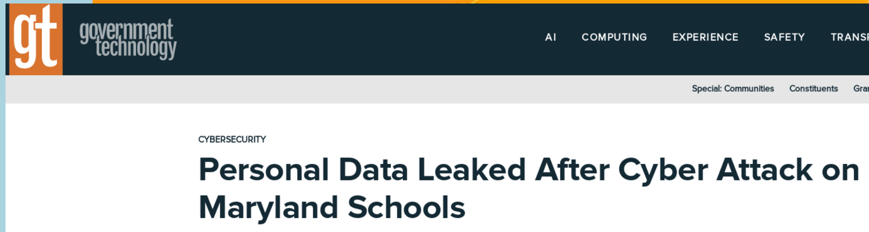
CYBERSECURITY

Texas school district paid $547K ransomware demand



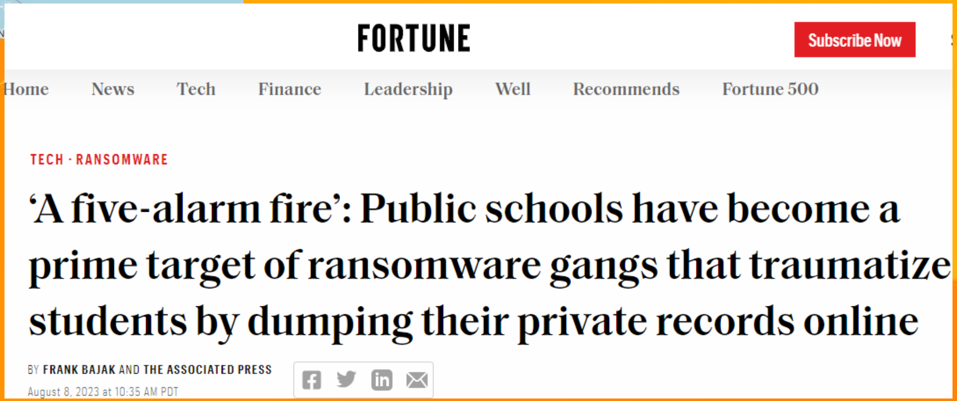


Southern Arizona's largest school district hit by cyber attack



CYBERSECURITY

Personal Data Leaked After Cyber Attack on Maryland Schools

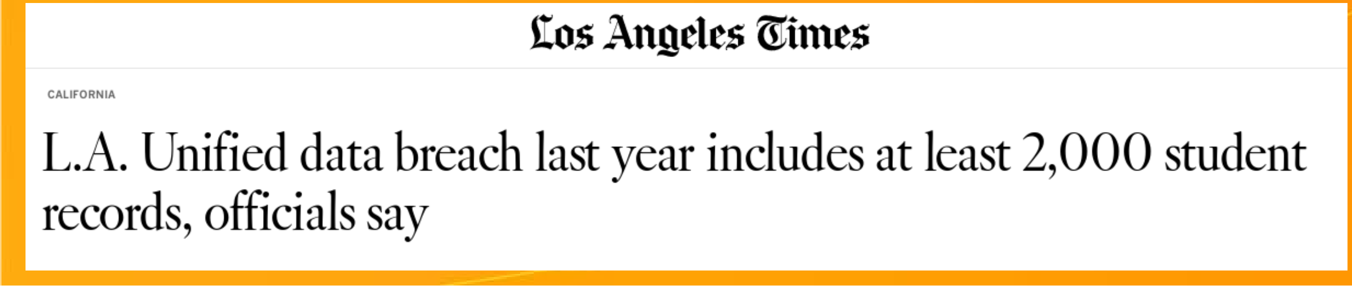


TECH · RANSOMWARE

'A five-alarm fire': Public schools have become a prime target of ransomware gangs that traumatize students by dumping their private records online

BY FRANK BAJAK AND THE ASSOCIATED PRESS

August 8, 2023 at 10:35 AM PDT

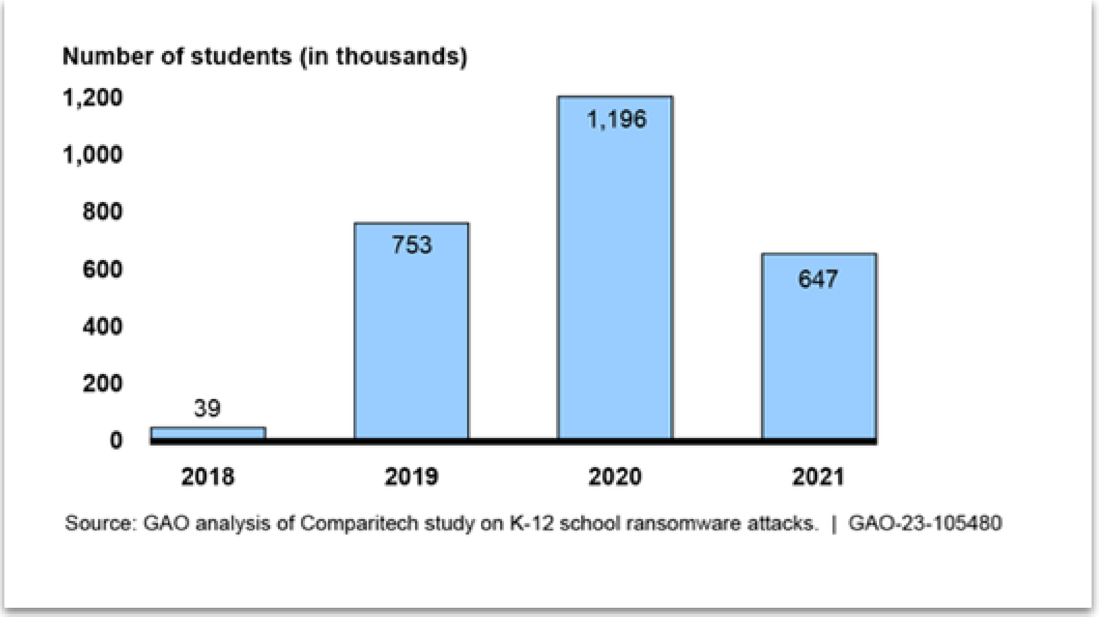


CALIFORNIA

L.A. Unified data breach last year includes at least 2,000 student records, officials say

The Impact of Cyber Attacks on Schools

Number of U.S. Students Affected by Ransomware Attacks on K-12 Schools and School Districts, 2018-2021



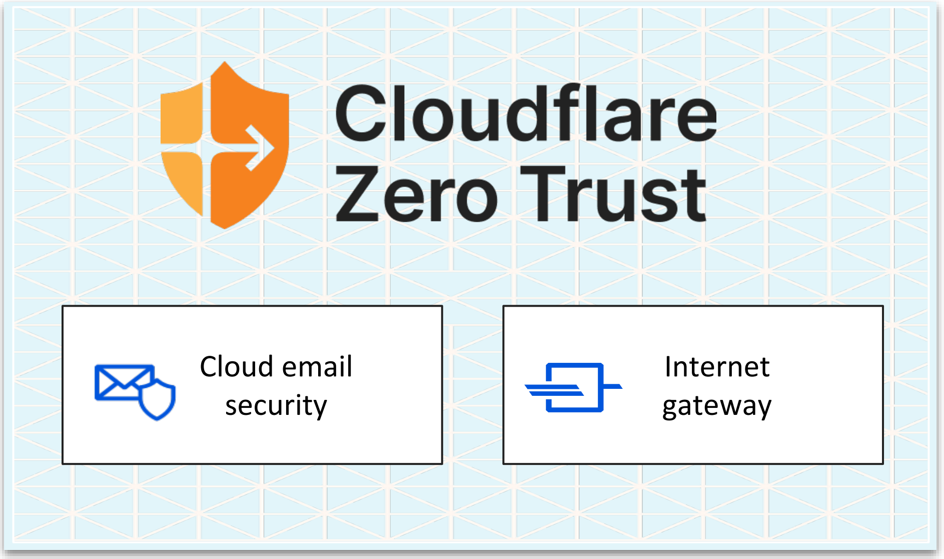
Source: GAO analysis of Comparitech study on K-12 school ransomware attacks. | GAO-23-105480

- Ransom requests varied from $5,000 to $40 million
- The overall cost of these attacks is estimated at around $9.45 billion
- On average, schools lose 11.65 days to downtime and spend more than a month (42 days) recovering from the attack
- Leaks of confidential student data

Cloudflare’s Commitment

Cloudflare’s mission is to ***help build a better Internet***, and we have always believed in helping protect those who might otherwise not have the resources to protect themselves from cyber attack.

Announced as part of the Back to School Safely: K-12 Cybersecurity Summit at the White House on August 8, 2023, **Project Cybersafe Schools** supports eligible K-12 public school districts with a package of Zero Trust cybersecurity solutions — *for free*, and *with no time limit*. These tools will help your school district minimize your exposure to common cyber threats.



A Note on Eligibility

Project Cybersafe Schools participants must be:

- K-12 public school districts
- Located in the United States
- No larger than 2,500 students per district

≤ 2,500

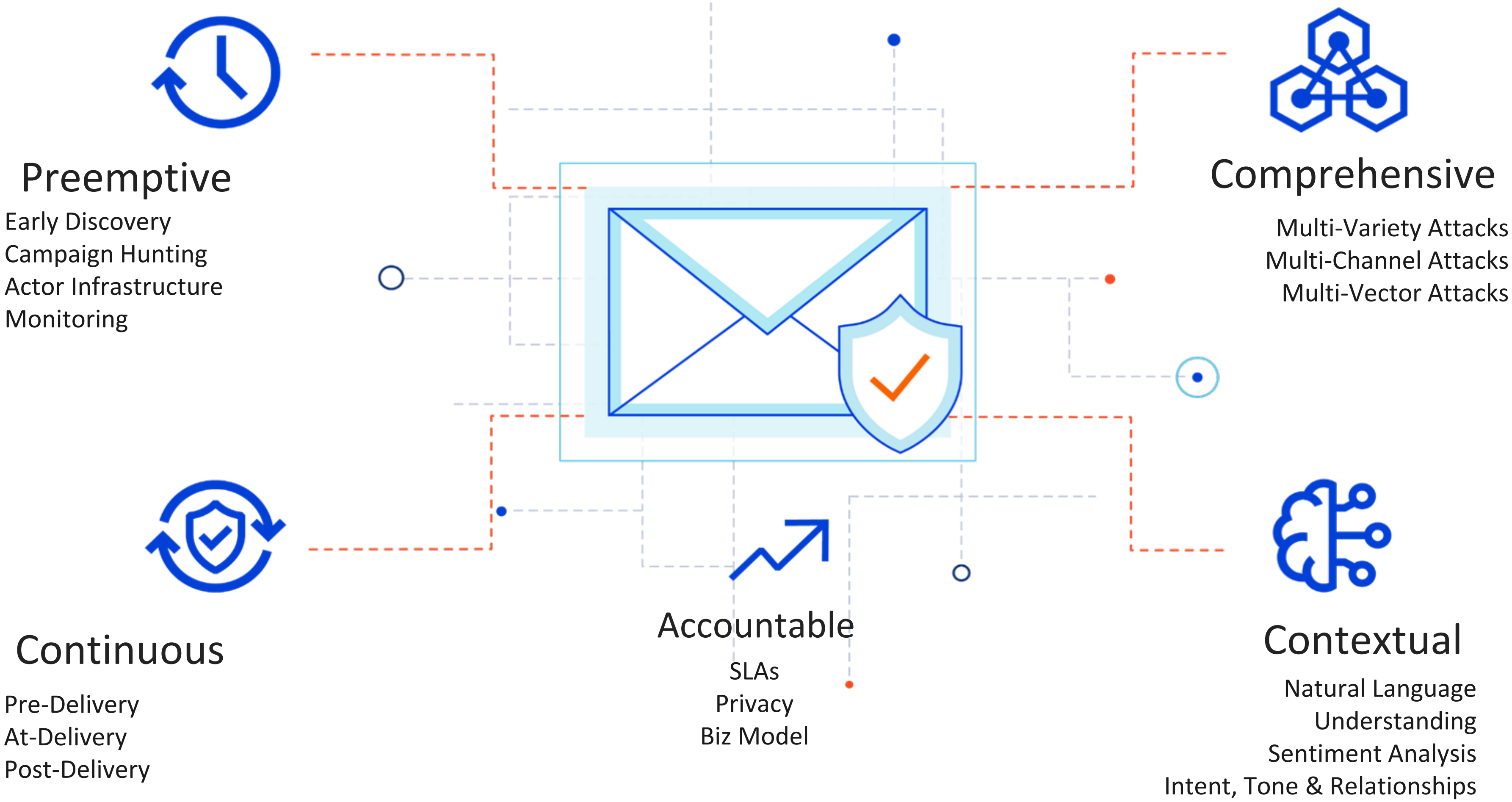
Section

Solution Overview

Section

Cloudflare Email Security

Area 1 Cloud Email Security



Preemptive

Early Discovery
Campaign Hunting
Actor Infrastructure
Monitoring

Comprehensive

Multi-Variety Attacks
Multi-Channel Attacks
Multi-Vector Attacks

Continuous

Pre-Delivery
At-Delivery
Post-Delivery

Accountable

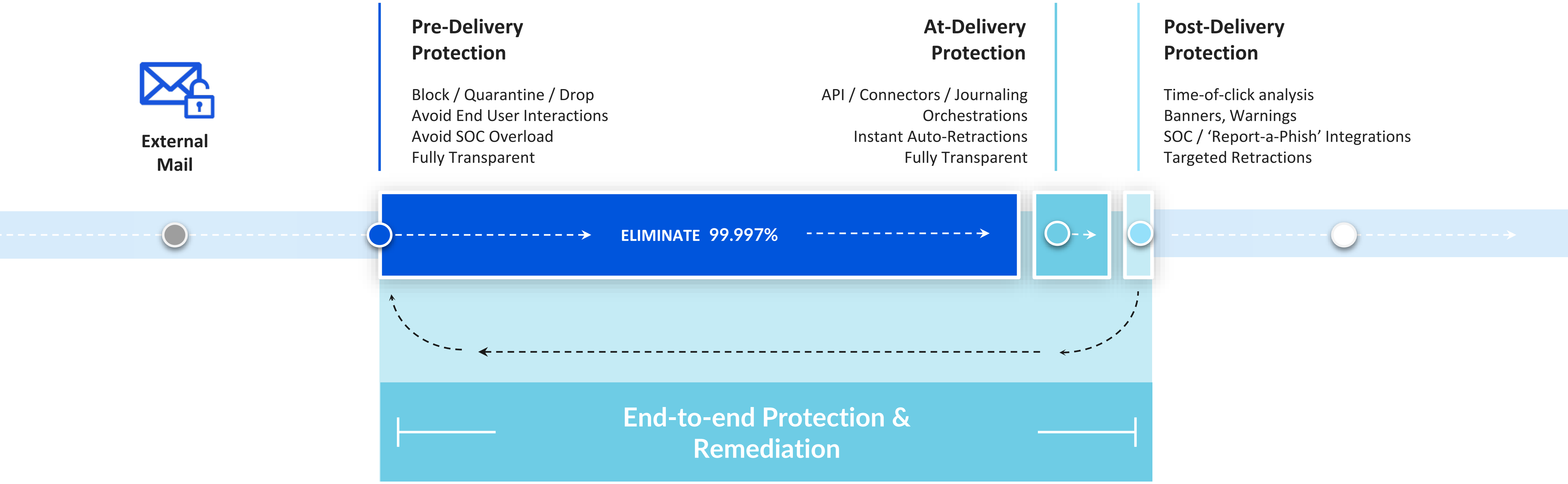
SLAs
Privacy
Biz Model

Contextual

Natural Language
Understanding
Sentiment Analysis
Intent, Tone & Relationships

Area 1 Cloud Email Security

Continuous protection



External Mail

Pre-Delivery Protection

Block / Quarantine / Drop
Avoid End User Interactions
Avoid SOC Overload
Fully Transparent

At-Delivery Protection

API / Connectors / Journaling
Orchestrations
Instant Auto-Retractions
Fully Transparent

Post-Delivery Protection

Time-of-click analysis
Banners, Warnings
SOC / 'Report-a-Phish' Integrations
Targeted Retractions

ELIMINATE 99.997%

End-to-end Protection & Remediation

Preemptive Detection

Massive-Scale Phish Indexing

High speed Web crawlers
3+ Billion Pages, 8+ Petabytes of Data

01 Dynamic Frontier Management

02 Computer Vision / User Impersonation

03 In-the-Wild Content Detonation

SPOT EMERGENT INFRASTRUCTURE BEFORE CAMPAIGNS LAUNCH

Section

DNS Filtering

Gateway DNS Filtering (CIPA Compliant)

CIPA Requirements

CIPA mandates that K-12 schools and libraries adopt Internet safety policies that include measures to block or filter access to specific categories of content. These categories encompass a wide range of topics that could be harmful or inappropriate for minors.

Compliance with these requirements helps ensure that students’ online experiences are safer and more secure.

Cloudflare Configuration

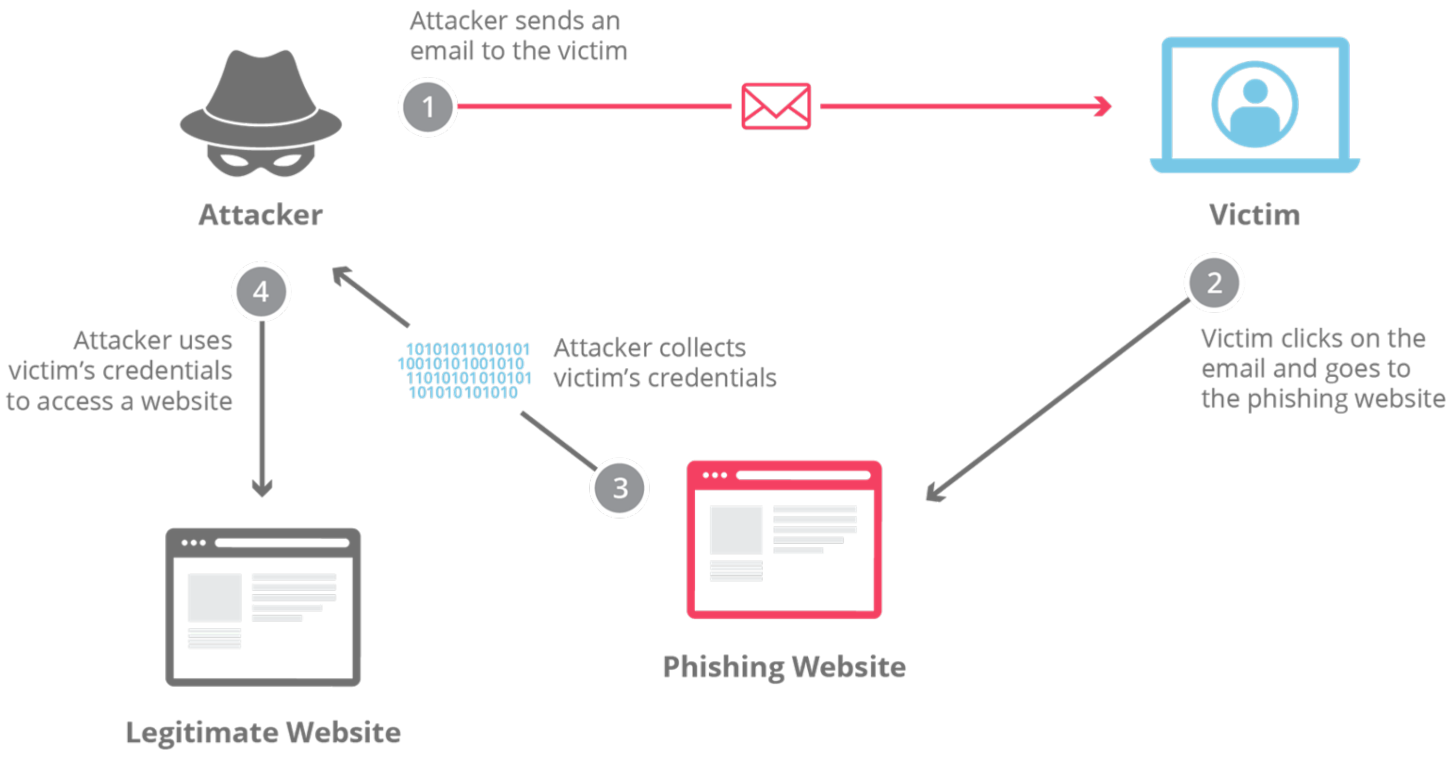
To facilitate compliance with CIPA requirements, administrators can enable a single filtering policy option. This includes applying the required filter categories to block access to unwanted or harmful online content.

It is important to note that while our recommended CIPA compliance rule covers the essential filter categories, CIPA is designed to be flexible, allowing administrators to adjust filtering policies based on local standards and requirements.

Administrators should carefully assess their specific location and userbase to determine if additional categories may need to be added or modified to ensure comprehensive protection.

DNS Filtering

Protects against Internet threats with DNS filtering by preventing users from reaching unwanted or harmful online content like ransomware or phishing sites and can be deployed to comply with the Children’s Internet Protection Act (CIPA).



Attacker

1 Attacker sends an email to the victim

Victim

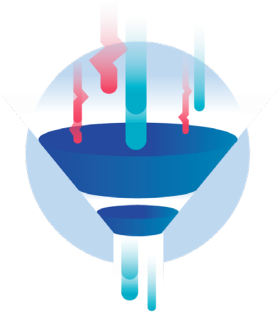
2 Victim clicks on the email and goes to the phishing website

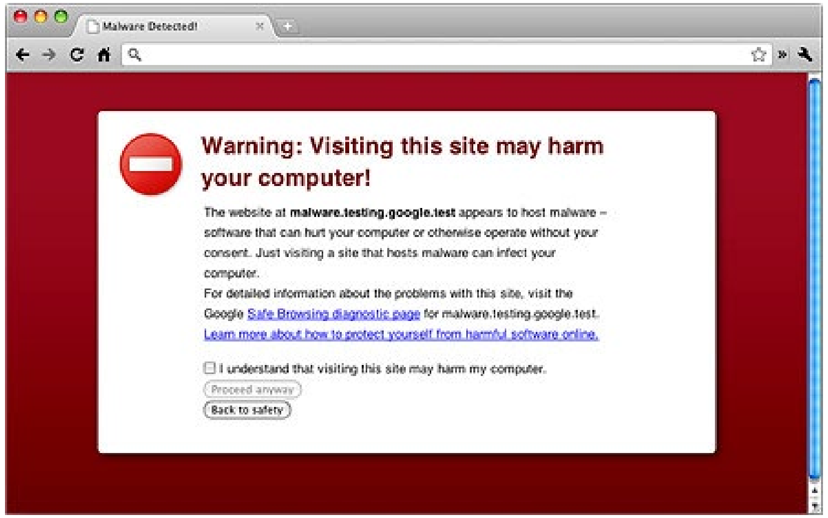
Phishing Website

3 Attacker collects victim’s credentials

4 Attacker uses victim’s credentials to access a website

Legitimate Website





Warning: Visiting this site may harm your computer!

The website at **malware.testing.google.test** appears to host malware – software that can hurt your computer or otherwise operate without your consent. Just visiting a site that hosts malware can infect your computer.

For detailed information about the problems with this site, visit the Google Safe Browsing diagnostic page for malware.testing.google.test.

Learn more about how to protect yourself from harmful software online.

□ I understand that visiting this site may harm my computer.

Proceed anyway

Back to safety

Section

CLOUDFLARE

Quick Start Guide

Schools student size 2,500 or less

How to get started

1. Create your Cloudflare account, Area 1 account, and Zero Trust organization

   Note: You will receive an email following this webinar requesting some inputs we require in order to provision some of these services. Please complete the intake form and we will let you know when you can begin onboarding.

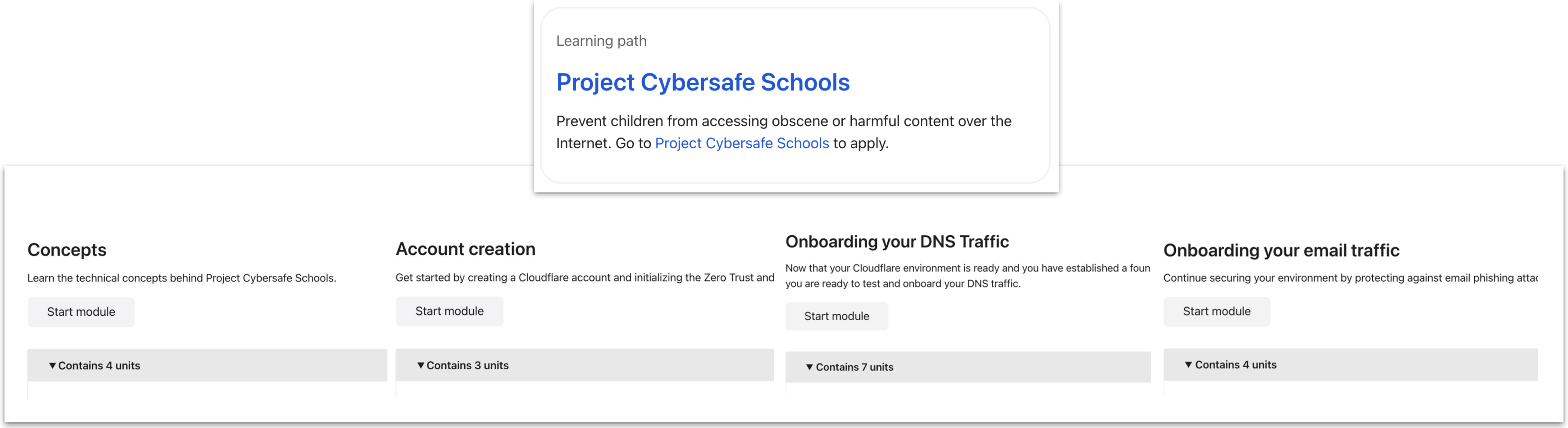
1. Onboard your email traffic
   a. Decide between Inline or API setup options
   b. Proceed with simple onboarding steps based on setup decision and email provider

2. Onboard your DNS traffic
   a. Add a DNS location to Gateway
   b. Change your DNS resolvers to send test traffic to your environment
   c. Verify local connectivity
   d. Test a simple firewall policy
   e. Create CIPA policy
   f. Enable (and customize) your block page

Please refer to the Project Cybersafe Schools learning path (linked here) for comprehensive instructions.

Learning Path - Project Cybersafe Schools

You can find a step-by-step onboarding guide specific to Project Cybersafe Schools on Cloudflare Docs, which should contain all the information you need to onboard.



Learning path

Project Cybersafe Schools

Prevent children from accessing obscene or harmful content over the Internet. Go to Project Cybersafe Schools to apply.

Concepts

Learn the technical concepts behind Project Cybersafe Schools.

Start module

▼Contains 4 units

Account creation

Get started by creating a Cloudflare account and initializing the Zero Trust and

Start module

▼Contains 3 units

Onboarding your DNS Traffic

Now that your Cloudflare environment is ready and you have established a foun you are ready to test and onboard your DNS traffic.

Start module

▼ Contains 7 units

Onboarding your email traffic

Continue securing your environment by protecting against email phishing attac

Start module

▼ Contains 4 units

Support Resources

Self-serve documentation

Click here to access to Project Cybersafe Schools Learning Path, your best resource for onboarding assistance. You can also access the comprehensive guides below for more information:

- Area 1 Cloud Email Security
- Cloudflare Gateway

Office Hours

This initial group of school districts will be invited to attend an **Office Hours session in September**, for live assistance with any remaining onboarding steps.

Note: This will not be held regularly, so please plan to attend if you need live guidance.

Technical questions & troubleshooting

For general troubleshooting assistance and general technical questions not answered in the above documentation, submit a ticket via the 24/7 Support Portal in the Cloudflare dashboard. A Technical Support Engineer will respond to your inquiry.

Support Tips & Best Practices

Cloudflare Support only assists individuals whose email addresses are validated against the list of registered account users.

Please review and update all contacts accordingly in your Cloudflare Dashboard.

Security Verification Options:

- Generate a single use token
- Authenticator app + QR code

Section

Appendix

Section

Onboarding Demo

Section

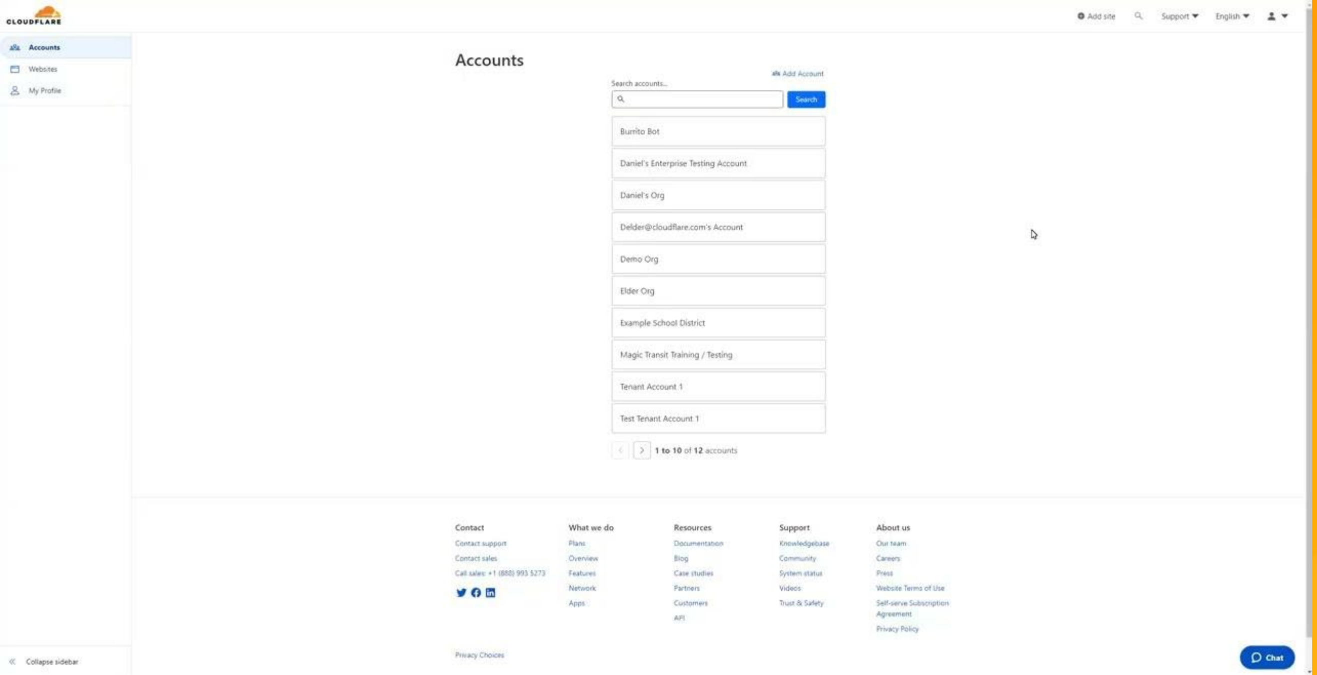
Area 1 Cloud Email Security

Nick Perry
Technical Support Engineer

Section

Gateway DNS Filtering

Daniel Elder
Customer Solutions Engineer



Accounts

- Burrito Bot
- Daniel's Enterprise Testing Account
- Daniel's Org
- Delder@cloudflare.com's Account
- Demo Org
- Elder Org
- Example School District
- Magic Transit Training / Testing
- Tenant Account 1
- Test Tenant Account 1

1 to 10 of 12 accounts

Texas K12 Cybersecurity Initiative

September 2023

Texas K12 Cybersecurity Program Outreach

- **TAA published on June 15th.**
  - Request LEAs to take action to sign Inter-Local agreement with DIR prior to September 1, 2023.
  - Eligibility for fully funded Endpoint Detection and Response (EDR) includes LEAs with student enrollment of 15,000 or less. Initial distribution will only be available for servers and staff, with a maximum limit of licenses equal to ~~10%~~ of student enrollment.
  - Other cybersecurity services are on a first come first serve basis and will include Cybersecurity Assessments and Network Detection and Response (NDR).
  - TEA has created a webpage with up-to-date information as the program matures.

Texas K12 Cybersecurity Program Outreach

- **TAA released on September 21st.**
  - Eligibility for fully funded Endpoint Detection and Response (EDR) includes LEAs with student enrollment of 15,000 or less. Initial distribution will only be available for servers and staff, with a maximum limit of licenses equal to 20% of student enrollment.
  - Cybersecurity Assessments – TEA and DIR are finalizing criteria and will communicate in the fall of 2023 with details for requesting this service.

Texas K12 Cybersecurity Program Outreach

- **TAA released on September 21st.**
  - Eligibility for fully funded Endpoint Detection and Response (EDR) includes LEAs with student enrollment of 15,000 or less. Initial distribution will only be available for servers and staff, with a maximum limit of licenses equal to 20% of student enrollment.
  - Cybersecurity Assessments – TEA and DIR are finalizing criteria and will communicate in the fall of 2023 with details for requesting this service.

Grant for Cybersecurity Practitioners

Current recommendation based on feedback:

- Single grant awarded to one Region to centrally manage and coordinate best fit solutions for all regions.
- Grantee will distribute funds and help identify staffing solution for each region according to business need.
  - Direct hire, contract, interns, virtual, on-site, clustered team etc.
- Grantee will help facilitate uniform training, documentation, and team building opportunities for cybersecurity practitioners.
- Grantee will help facilitate resource sharing according to statewide needs and priorities.

Resources, Questions or Assistance?

Contact cybersecurity@tea.texas.gov

OR

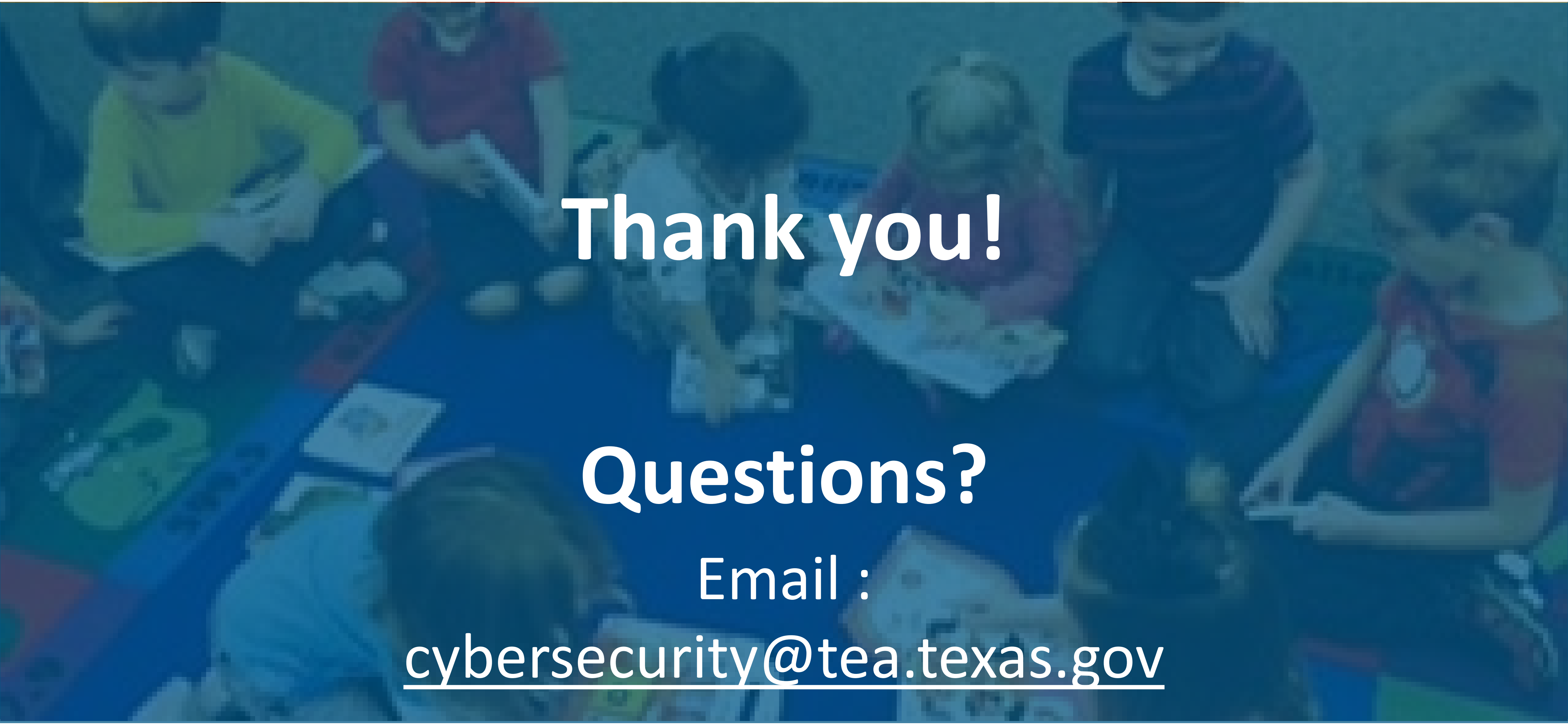
Contact the Texas Department of Information Resources CISO Office at DIRSecurity@dir.texas.gov

Cybersecurity Coordinator Forum

Register here with your LEA email address:
https://attendee.gotowebinar.com/register/8234183618339320587

TEA K-12 Cybersecurity Initiative Webpage

https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative



Thank you!

Questions?

Email : cybersecurity@tea.texas.gov