



Scottsdale *Unified*
SCHOOL DISTRICT



IT Vision and Mission

Our vision is to **support a dynamic, technology-rich environment** that empowers all students and staff to become passionate life-long learners and productive participants in our society.

Our mission in integrating technology is to enable staff and students to be **academically successful, technologically aware and fully engaged in the learning process.**



Why K-12 Schools Are High-Value Targets

- **Fact 1:** 82% of K-12 schools have experienced cyber threats recently (CIS/MS-ISAC, 2025)
- **Fact 2:** 80% of K-12 organizations were hit by ransomware in the past year (Sophos)
- **Fact 3:** Ransomware attacks on schools increased 23% in early 2025, with average demands of \$556K (Comparitech)

“Given the resource challenges facing schools, we’ve accumulated a lot of technical debt that is going to make better defending school communities from these threats a challenging endeavor.”

Doug Levin, National Director of the K12 Security Information Exchange, explains why schools are frequent targets.



National Institute of Standards and Technology (NIST) Cybersecurity Framework

- **Govern:** Establish policies, define roles and responsibilities, and promote cybersecurity awareness across the organization.
- **Identify:** Asset management, risk management strategy development, and identifying critical functions that, if disrupted, would impact the organization.
- **Protect:** Implement safeguards like access controls (e.g., multi-factor authentication), data security (encryption, backups), awareness and training, and protective technology (firewalls, antivirus).
- **Detect:** Continually monitor, implement threat detection technologies, and conduct security event analysis to find and investigate unusual activities.
- **Respond:** Incident response planning, containment and mitigation of breaches, communication strategies, and legal considerations.
- **Recover:** Developing and practicing recovery plans, ensuring backup and disaster recovery capabilities, learning from incidents, and communicating recovery progress to stakeholders.



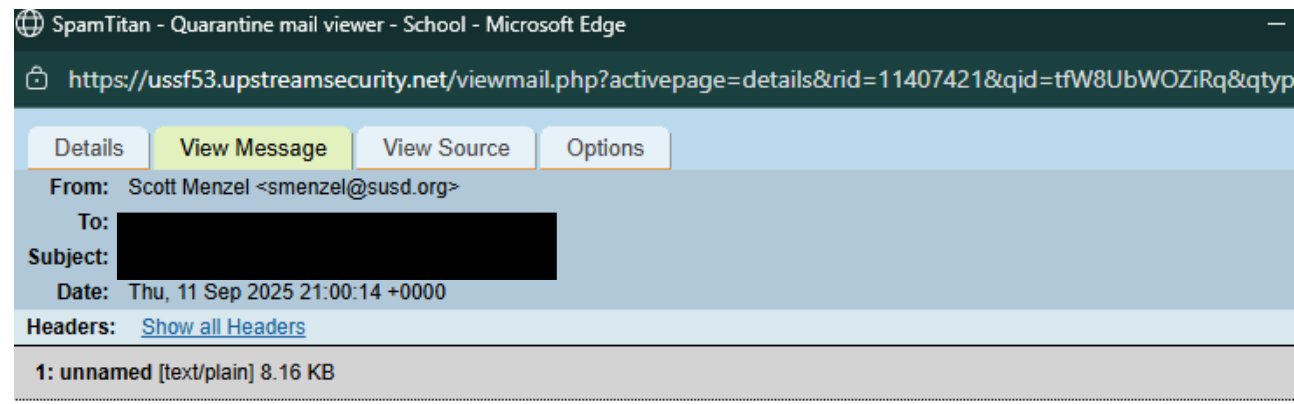
Cybersecurity Insurance Requirements (The Trust)

- Secure Air-Gapped Backups – Barrier between our network and our back-ups
- Phishing Simulations and Training – Raise awareness around the need to be aware
- Multi-Factor Authentication (MFA) – App on our phones and tokens for folks without cell phones
- Vulnerability Scanning – Penetration testing
- Endpoint Detection and Response (EDR) Software -
- Software Patching – Regular Maintenance Schedules
- Managing End-of-Life Software – Windows, Mitel



What is a DPA

- **Data Privacy Agreement (DPA):** A legally binding agreement between the district and a software vendor.
- **Purpose:** Ensures vendor complies with state and federal laws (FERPA, COPPA, etc.) for protecting student and staff data.
- **Key Protections:**
 - Defines how data is collected, used, stored, and shared.
 - Prevents unauthorized use of student information.
 - Establishes clear security expectations.
- **Partners:**
 - 1EdTech [TrustEd Apps](#), Student Data Consortium, CoSN



Can you share what this is regarding? Our IT team has me trained to be careful about opening document like this

[signature_352188152]

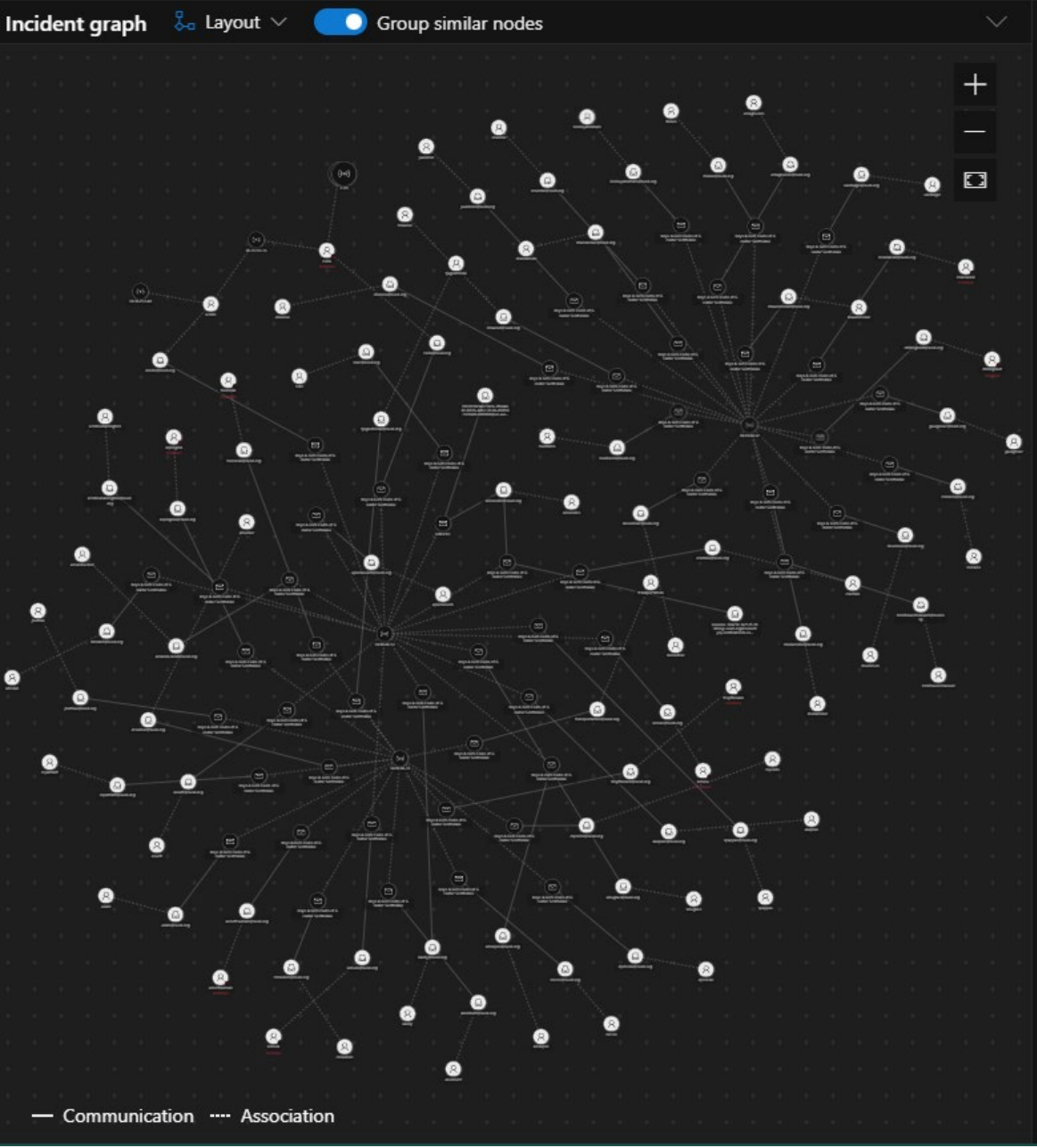
Dr. Scott A. Menzel | Superintendent
Scottsdale Unified School District - MDA
Your Link to Student Success
3500 E. Jackrabbit Road, Scottsdale AZ 85250
TEL (480) 484-6120 Cell (480) 578-8763

Website | SUSD
Magazine

[signature_34714484]
[signature_973782511]
[signature_449108178]
[signature_1640194839]

[signature_1115711494]

[nextdoor]





TECHNOLOGY



LAST CALL FOR WINDOWS 11 UPGRADES!

You **MUST** be updated by Monday, September 15th. If you are unable to do so, please make sure you have filled out an IT work order or reached out to the help-desk for assistance. We do not want anyone to lose access!

BE AWARE OF SCAMMERS! – We have seen an uptick in the number of nefarious emails and phone calls sent to SUSD employees!

Email is one of the most common tools used by scammers. A message may look like it comes from a coworker, the district office, or a company you trust. The display name is easy to fake. What matters is the **email address behind it**.

BEFORE you click or reply:

Check the actual sender address, not just the display name.

- On a computer, hover over the display name to reveal the full address.
- On a phone, expand the details at the top of the message to see the real address.
- Be extra careful with messages that say “urgent,” “immediate,” or “act now,” especially if they ask for **personal information related to a meeting** or anything that feels unusual.
- **Verify using a trusted method:** look up the person in your **address book** and start a new email or call them using a known number. Do not reply directly to the suspicious message.

Report it!

- If you are suspicious of the email, use the [PhishNotify](#) button in the upper right-hand corner of your email message or forward the message to phishing@susd.org

SCAMMERS ALSO MAKE CALLS!

SUSD phone numbers have been spoofed to make calls that look local or official. If a call feels suspicious, hang up and dial the official number yourself.

Bottom line:

Pause, verify, then act. A short check can prevent a costly mistake.



Ongoing Efforts & Measurables

- Tabletop Exercises
- Debriefs after incidents
- Finance Audit
- Trust Audit
- Penetration Audit
- Cyber Security Awareness



Ongoing Projects

NIM – NexGen Identity Management
Active Directory (AD) Clean-Up
Mitel to Ring Central
Jamf
Windows 11
Server upgrades (Pueblo, Hohokam, Cherokee)

Closing- Be a Cybersecurity Superhero

- **DPAs are essential to protect students, staff, and the district.**
- **Update to Windows 11**
- **Do not click, reply, forward suspicious emails**
- *Together, we'll build a safe and secure digital ecosystem for teaching & learning as well as our business enterprise!*

