Cybersecurity Update 2026

St. Cloud Area School District 742!

Cybersecurity- The Evolving Landscape

- **Cybersecurity**: protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.
- School districts face unprecedented cybersecurity challenges.
- Ransomware attacks on educational institutions have surged 69% in recent years.
- The average cost of a single breach now exceeds $3 million, not counting operational disruption and reputational damage.

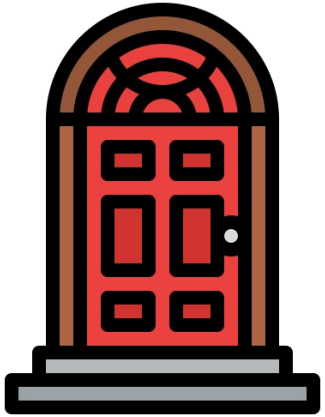
cloud security alliance®

742 Cybersecurity Infrastructure

- Our network is the 'home' for student data and staff records.
- We continue to move from a simple door lock to a com
  security system.

Password Update: Door Locks

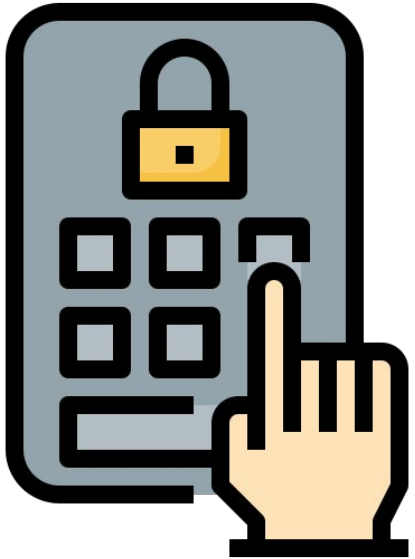
- Summer 2025- Increase password complexity.
- From 9 characters to 12 minimum
  - Must include at least 1:
    - Uppercase letter
    - Lowercase letter
    - Number
    - Symbol
- Passwords cannot be reused



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

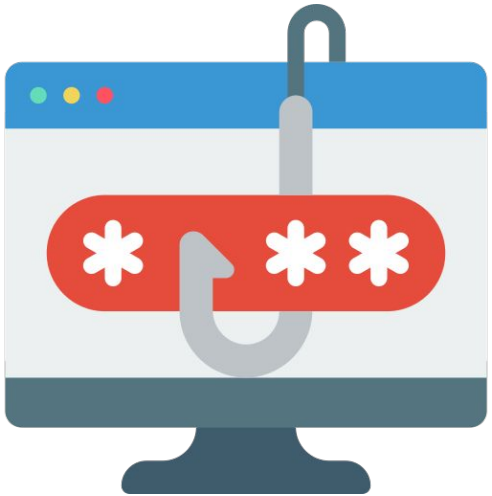
Multi-factor Authentication (MFA): Security System

- MFA: A security process that requires two or more different ways (factors) to prove your identity when logging in, beyond just a password.
  - Fingerprint
  - Code sent to phone
  - Security Question
- Even if a thief steals your key, they can't get past the secondary code.



Phishing Simulation & Training- Neighborhood Watch

- Phishing: a form of social engineering where attackers masquerade as a legitimate and trustworthy entity to deceive individuals into revealing sensitive information or download malicious software.
- Staff receive simulated phishing emails throughout the year to test awareness and response.
- Immediate training provided when users interact with simulated threats, reinforcing learning at the moment.
- Staff are trained to report phishing emails in their district email.
- Staff training provided online monthly and in-person during PD time.
- Transforms staff into active defenders, creating a culture of security awareness throughout the district.



Endpoint Detection & Response- Internal Monitoring (Motion Sensors)

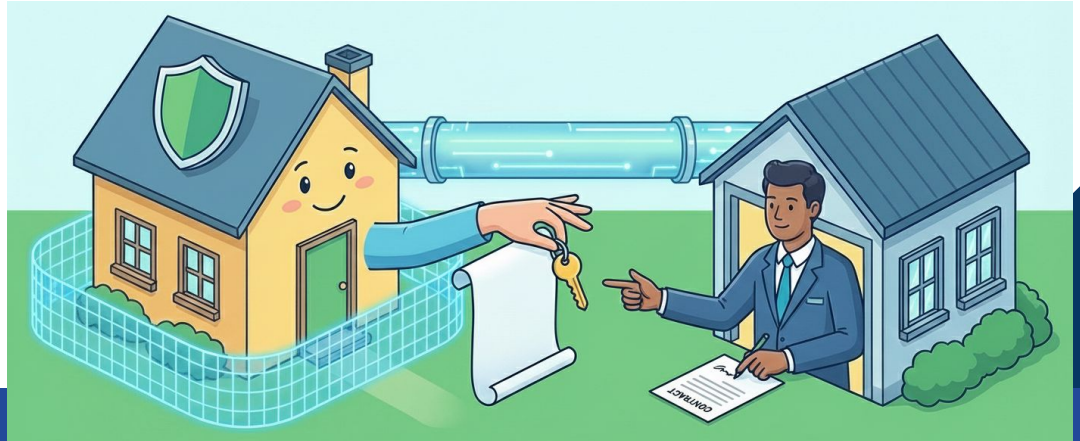
- **Endpoint Detection & Response (EDR)**
- Application is installed on district devices.
- Detects and alerts suspicious behavior in real-time.
    - Malware, unauthorized access, malicious links, etc.

Managed Detection & Response- 24/7 Security Monitoring

- **Managed Detection & Response (MDR)**
  - Round-the-clock monitoring of our entire network by certified security experts who identify and respond to threats in real-time.
- Managed Risk Assessment
  - Continuous scanning identifies vulnerabilities in software, hardware, and configurations before attackers can exploit them.
- Incident Response (IR)
  - Rapidly contain, investigate, and remediate cyberattacks, digital forensics, threat actor negotiation, system recovery, etc.

Data Protection Agreements- Trusted Neighbors

- **Data Protection Agreement (DPA)**
  - A contract between ISD 742 and a third-party service provider that governs the processing, storage, and protection of student data.
- Data is only as secure as our weakest partner
  - Our DPA ensures that any entity handling our students' information is legally obligated to maintain security standards that meet or exceed our own.



What we are working on…

- Continually updating Cybersecurity response plan.
- Assessing our infrastructure for gaps with our MDR partner.
- Creating a three phase AI Deepfake response plan:
  - Prevention and preparedness
  - Incident Response
  - Recovery and review

Building a Culture of Security

Our multi-layered approach combines technology, training, and planning to protect what matters most: student data, operational continuity, and community trust.

Thank you!

Questions?

St. Cloud Area School District 742!