Back to School Cybersecurity: Lessons from Recent School Cyber Incidents
~Matt Komac, Assistant Director of PC Pool Operations

As another school year begins, cybercriminals are becoming more sophisticated, but the methods they use to gain access to school networks remain surprisingly consistent. While artificial intelligence has made phishing emails and impersonation attacks more convincing, many successful breaches still occur because of basic security gaps rather than advanced hacking techniques.

Across the education sector, investigations into school cyber incidents continue to identify the same recurring vulnerabilities. The good news is that many of these risks can be significantly reduced through routine cybersecurity practices.

While every cyber incident is unique, many school breaches begin with one or more of the following:

- A staff member unknowingly entered credentials into a phishing website
- A former employee's account was never disabled after leaving the district
- Multi-factor authentication (MFA) was not enabled on a critical account
- Software or servers had not been updated with available security patches
- A network administrator account had broader access than necessary
- A vendor with access to district systems experienced its own data breach
- Backups had never been tested before they were needed

These aren't failures of technology, but rather failures of routine cyber maintenance. The start of a new school year is an excellent time to verify that these fundamental protections are in place.

Cybersecurity isn't solely the responsibility of your IT department. Every employee who accesses district systems plays a role in protecting student information, financial data, and school operations. By taking time at the beginning of the school year to review accounts, verify security settings, test backups, and discuss your incident response procedures, your district can greatly reduce the likelihood and impact of a cyber incident.

MSGIA encourages district administration to review this checklist with their IT department. If you have questions regarding cybersecurity risk management or your cyber coverage, please don't hesitate to contact our office.

Back-to-School Cybersecurity Checklist

- ☐ **Review Employee Accounts**
  - Disable accounts for retired, resigned, or terminated employees immediately.
  - Review permissions for employees who have changed positions.
  - Confirm users have only the system access necessary to perform their job duties.

- ☐ **Remove Graduated Student Accounts**
  - Remove graduated students' access to district email, cloud storage, and other systems.
  - Review inactive student accounts and disable those no longer needed.

- ☐ **Verify Multi-Factor Authentication (MFA)**
  - Confirm MFA is enabled for the following:
  - Email accounts
  - Student Information Systems
  - Financial and payroll software
  - Remote access (VPN)
  - Network Administrator accounts

    *MFA remains one of the most effective ways to prevent unauthorized access

- ☐ **Review Network Administrator Privileges**
  - Limit network administrative access to employees who require it.
  - Review privileged accounts annually removing unnecessary permissions.

- ☐ **Install Security Updates**
  - Verify security patches have been installed for the following:
    - Servers
    - Staff computers
    - Firewalls
    - Wireless equipment
    - Network infrastructure
    - Student devices (where applicable)
  - Enable automatic updates whenever practical.

- ☐ **Test Your Backups**
  - Perform a test restoration of critical systems.
  - Confirm backup files are complete and recoverable.
  - Ensure recovery procedures meet district expectations.

- **Review Vendor Access**
  - Confirm vendors accessing district systems require MFA
  - Remove unnecessary vendor accounts
  - Verify vendors have a breach notification process

- **Update Your Incident Response Plan** *Template available from the MSGIA
  - Review current contact information
  - Ensure everyone understands their role during a cyber incident

- **Educate Staff**
  - Remind employees to verify unusual requests before responding
  - Never approve financial transactions based solely on an email
  - Report suspicious emails immediately
  - Be cautious when scanning QR codes or opening unexpected links and attachments
  - Ideally a formal annual training/education plan is in place. Recommended Vector Safe Schools Courses within the Information Technology Section:
    - Browser Security Basics
    - Cybersecurity
    - Email and Messaging Safety
    - Password Security Basics
    - Payment Card Industry Data Security (PCI DSS) Standard Overview
    - Protection Against Malware

Name:_____ Name:_____

Date Completed:_____