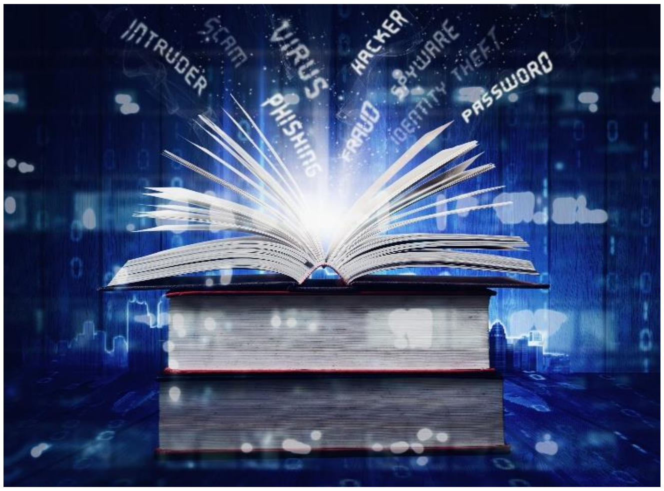
ALLIANCE OF SCHOOLS FOR COOPERATIVE INSURANCE PROGRAMS

ASCIP

SAFETY SPOTLIGHT

CYBER SECURITY IN SCHOOLS

As schools and colleges increasingly integrate digital technologies into their educational frameworks, the need for robust cybersecurity measures has become more critical than ever. From student records to financial transactions, educational institutions store vast amounts of sensitive data, making them prime targets for cyber threats.



Here are some best practices individual employees can implement to help prevent data breaches or cyber security attacks within their organization:

Strong Password Management: Use strong, unique passwords for each account and avoid sharing passwords across multiple accounts.

Be Wary of Phishing Attempts: Exercise caution when opening emails, especially those from unfamiliar senders or containing suspicious links or attachments. Verify the legitimacy of unexpected emails by contacting the sender directly through a trusted means of communication.

Keep Software Updated: Regularly update operating systems, applications, and security software to ensure they are equipped with the latest patches and security updates, reducing the risk of exploitation by cyber attackers.

Secure Devices and Workstations: Secure physical devices and workstations by locking screens when unattended, encrypting data stored on devices, and utilizing strong passwords or biometric authentication methods to prevent unauthorized access.

Report Incidents Promptly: Immediately report any suspicious activity, security incidents, or potential data breaches to the organization's IT or security team for investigation and remediation.

Avoid Social Engineering Attacks: Be cautious of unsolicited requests for sensitive information or urgent financial transactions, especially via email, phone calls, or messages. Always verify the identity and legitimacy of the requester through a direct phone call or face to face confirmation before sharing any personal or confidential details.

Vendor Verification Procedures: A vendor requesting urgent payment is a red flag. Before processing payments or sharing financial information with vendors, verify their legitimacy by confirming their identity, checking references, and ensuring compliance with established procurement policies and procedures.

Stay Informed and Vigilant: Stay informed about common cyber threats and security best practices through ongoing training and awareness programs provided by the organization. Remain vigilant and proactive in identifying and addressing potential security risks or vulnerabilities.

By implementing these best practices, employees can play a crucial role in helping to protect their organization's data and infrastructure from cyber threats and contribute to maintaining a secure work environment.

Please contact your ASCIP Risk Services Consultant or our Risk Services team at RM_Info@ascip.org for questions or to discuss further.