Cybersecurity Awareness Month

October is recognized nationally as Cybersecurity Awareness Month since 2004. The goal is a collaborative effort between government, industry, and other organizations - public and private- to recognize the importance of cybersecurity.

In addition, Oklahoma Gov. J. Kevin Stitt, in collaboration with OMES Oklahoma Cyber Command and the Oklahoma Information Sharing and Analysis Center (OK-ISAC), has declared October 2024 as Cybersecurity Awareness Month in the State of Oklahoma.

The State Department of Education, with a commitment to stakeholders, provides this list of best practices to significantly reduce online risks at the personal, school site or district level.

- **Use Strong Passwords or Passphrases** – Strong passwords are the first line of defense against unauthorized users. Passwords should be complex and avoid guessable information like birthdays or common words. Utilize a password manager tool and change passwords regularly.
- **Keep Software Updated** – Maintain all devices and applications up to date to protect against newly discovered vulnerabilities. Cybercriminals often exploit outdated software to gain access to systems.
- **Employ Multi-Factor Authentication (MFA)** – It adds an additional layer of security by requiring users to provide two or more verification factors to access systems. It makes it harder for unauthorized users to gain access, even if they obtain a password. Use MFA with both personal and work-related accounts.
- **Be Cautious, Identify and Report Phishing Attempts** – Phishing attacks often trick users into clicking malicious links that can compromise security. Help your team recognize suspicious email and links, especially those from unfamiliar sources or unexpected messages from known contacts. Verify the sender's authenticity before opening attachments, clicking links, or sharing information.
- **Develop a Cybersecurity Culture** – Create a culture where staff is proactive about cybersecurity to protect the organization. It involves ongoing education and training to foster an environment where everyone is aware of the potential risks.

- **Implement Access Controls, Firewalls, and Antivirus Software** – Limit access to sensitive information and systems only those who need it – Least Privilege Principle. Firewalls can act as barriers between internal network and external threats, while antivirus software can scan for and eliminate malware.

- **Conduct Risk Assessments** – Regular risk assessments can help identify potential threats and vulnerabilities in IT infrastructure. Assessing the risks can then lead to prioritizing actions to mitigate threats, such as improving security protocols or staff training on emerging risks.

- **Monitor Systems for Unusual Activity** – Monitoring of networks and systems can help detect suspicious activities early, such as unauthorized access attempts or unusual data transfers.

Implementing these practices can help individuals and districts to reduce cybersecurity risks and protect sensitive data and systems from malicious attacks.