

Educational agencies are experiencing more frequent cyberattacks. These attacks involve stealing data, holding information systems hostage, and causing disruptions in service. Follow these simple tips to help enhance your district's security posture.

**HUMAN BEHAVIOR
IS AT THE ROOT OF
95% OF ALL CYBER
SECURITY
INCIDENTS.**

DATA PROTECTION REMINDERS

E-MAIL PRACTICES



Exercise caution before clicking on a link in an e-mail or opening an attachment.

WORKSTATION PRACTICES



Lock workstations when leaving them unattended.

PASSWORD PRACTICES



Establish strong passwords. Do not write down passwords and leave in an easily accessible location.

DATA HANDLING PRACTICES



Use appropriate tools when handling data. Never send sensitive information through unencrypted email.

PRIVACY PRACTICES



Do not establish accounts for students to access online resources without consulting with administration.



PHISHING EMAILS

Phishing e-mails are one of the most common, and effective, methods cyber attackers will use to gain access to secure information.

1. Exercise **CAUTION** before **SENDING SENSITIVE INFORMATION** through email.
2. Exercise **CAUTION** before **CLICKING ON A LINK** in an e-mail or **OPENING AN ATTACHMENT**.
3. **REPORT SUSPICIOUS EMAILS** to your IT Department.
4. If you fall victim, **REPORT INCIDENTS** to your IT Department immediately.