GONE PHISHING: 8 SIGNS THAT AN EMAIL COULD SPELL DISASTER FOR YOUR SCHOOL DISTRICT

Just as cyber security has evolved over time, so have hackers' tactics. In-the-know school districts have implemented many security measures, but confidential data may still be at risk for scams, fraud, and phishing campaigns.

Hackers continue to up the ante, changing their strategy in order to confuse unsuspecting internet users in your schools and prompt them to click on a link or open an attachment that gives hackers access to data tied to students and staff.

In order to keep your school safe from cyber threats, it's important to stay on top of current trends in cyber security and educate your students and staff to recognize when they may be a target of a scam. Phishing is one trend that your staff and your students need to actively identify and combat.

WHAT IS PHISHING?

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment that puts your data at risk. These communications may:

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- ask to confirm personal information
- include a fake invoice or a document you didn't request

SIGNS THAT YOU MIGHT HAVE A PHISHING EMAIL

1. An Unfamiliar Tone or Greeting
2. Grammar and Spelling Errors
3. Inconsistencies in Email Addresses, Links & Domain Names
4. Threats or a Sense of Urgency
5. Suspicious Attachments
6. Unusual Request
7. Short and Sweet
8. Request for Credentials, Payment Information or Other Personal Details

Cyber security continues to be in flux as new technology allows hackers to get creative with their scam attempts. If you're unsure if your school has the right security policies in place to mitigate your risk, reach out to your insurance partner find out more details on phishing schemes and cyber security. Safer data = safer schools and safer communities – that's what motivates us to do what we do.