HOW TO PUT THE FREEZE ON PHISHING EMAILS

With the increase in ransomware infections in K-12 institutions that are often initiated through phishing emails, it is important to be proactive to help protect you and your school.
Here is a quick list of ways to spot a phishing email.

1 Beware of urgency

The emails may try to confuse you with an extreme sense of immediacy.
"You must click here or you will lose 5 sick days!"

2 Look but don't click

Hover over any links without clicking on them. If the link looks strange or from an unexpected domain-- don't click on it!

3 Consider the salutation

Is the address general or vague? Beware greetings like "valued customer" or "dear".

4 Check the signature

Most legitimate senders include a full signature at the end of the email.

5 Who is it from?

Just because the display name says it's from a person you know doesn't mean it is. Spend time to look at the email address of the sender.

6 Attachments

If you are receiving an unexpected email that has attachments- be wary.

7 Spelling errors

Attackers often have misspellings and/or grammatical errors in their emails.

8 Personal information

Legitimate companies are very unlikely to request personal information via email.

EduTech
Data Governance