Notice: Important Security Alert Regarding Phishing Emails

To: USD 420 Parents, Guardians, and Staff

From: USD 420 Administration

Subject: Security Reminder: Beware of Suspicious/Phishing Emails

Please be advised that the district has recently been targeted by a series of phishing emails. Some of these fraudulent messages may appear to come from known district staff members or official school email accounts.

Phishing emails are designed to deceive recipients into sharing sensitive information, revealing login credentials, or opening malicious attachments.

What You Need to Know & Do:

- **Verify the Sender:** Always double-check the sender's full email address, especially if the message requests sensitive information, money, or immediate action.

- **Do Not Click Links or Open Attachments:** If you receive an unexpected or unusual email—even if it appears to come from a district teacher, administrator, or staff member—**do not click any links or open any attachments.**

- **Look for Warning Signs:** Watch for unusual wording, urgent demands, requests for passwords/personal information, or unexpected requests to purchase gift cards or send payments.

- **Report Suspicious Emails:**

    - **Staff:** Please use the "Report Phishing" button in your email client or forward the message directly to the IT department without clicking any links inside it.

    - **Parents/Guardians:** If you are unsure whether an email from the district or a staff member is authentic, please contact the district office or individual school directly via phone to confirm before responding.

Thank you for your prompt attention to this matter and for helping us keep our district network and community secure.

Respectfully,
Ted Hessong
Superintendent
USD 420 – Osage City Schools