STATE OF SOUTH CAROLINA
DEPARTMENT OF EDUCATION

MEMORANDUM

TO: District Business Officials

FROM: Kendra M. Hunt, CPM, CGFO
Chief Financial Officer

DATE: February 27, 2024

RE: Phishing Scam

The South Carolina Department of Education (SCDE) would like to take the opportunity to advise district leadership of a security threat that affected a local district. The threat actors initiated a phishing scam in an attempt to wire funds to a fraudulent account. Below are some general tips to help prevent falling victim to such scams:

1. Verify Requests: Always verify any unusual or unexpected financial requests through a secondary means of communication, especially if it involves a large sum of money or unusual requests for wires, or wires to other countries.
2. Beware of Urgency: Scammers may create a sense of urgency or pressure to rush you into sending funds. They may send fake invoices or requests that appear legitimate.
3. Check Email Addresses: Pay close attention to email addresses and domains used in the requesting email. Scammers may spoof email addresses to appear to be from your company or someone you know or trust.
4. Implement Internal Controls: Establish internal controls and approval processes for financial transactions.
5. Report Suspicious Activity: Prompt reporting of any suspicious activity to your IT or security team can help mitigate fraud and allow for timely responses.

If you believe you are a victim of a potential scam, **contact your local law enforcement office first**. The local law enforcement office will determine if a police report should be completed and will contact the SC Law Enforcement Division (SLED) Computer Crimes Unit.

ELLEN E. WEAVER · STATE SUPERINTENDENT OF EDUCATION
RUTLEDGE BUILDING · 1429 SENATE STREET · COLUMBIA, SC 29201
PHONE: 803-734-8500 · FAX: 803-734-3389 · ED.SC.GOV