Utica National Insurance Group®

EDUCATIONAL INSTITUTIONS

RISK MANAGEMENT ALERT

HEAD of the CLASS

False Impersonation: An Emerging and Evolving Risk

False impersonation, also called social engineering or spear phishing, involves a fraudster impersonating someone else for financial gain by using a fraudulent email, telephone call, text message, or fax telling a victim what to do. We've all seen things like this with the IRS and FBI in the news. Banks and law enforcement agencies report that these incidents are increasing because they are easy to do successfully.

Example: An imposter pretends to be the superintendent or head of the school system. By email, this person provides enough meaningful information to convince an employee in the business office that a request to transfer money out of regular channels is legitimate. The employee makes the transfer willingly, without an outsider hacking into the system or learning bank passwords to steal the money.

Help Protect Your School

Schools may fall victim to this type of fraud if the appropriate controls are not in place.

- **Train all employees about fraudsters' tactics and school policies.** This should include acceptable and safe use of email and the internet, especially for those within the school business functions.
- **Educate employees on how to review email addresses.** In many common email formats, the sender's name is shown in the address line. Hovering the cursor over the sender's name shows the sender's email address, which might not match the school's domain name and could include slight variances to the actual address.
- **Never deviate from the school's money transfer procedures, no matter who makes the request.** School policies should:
  - include a written policy addressing wire transfers,
  - limit manual fund transfers to less than $25,000,
  - limit the authority to execute transfers to designated persons and document this in writing, and
  - include the validation of transfers by two people. For example, have a no-exception policy on approving money transactions with "out-of-band authentication," such as verbal confirmation as a second step or confirmation of a password that only a select few know. This verification should be by means other than how the request was initiated (i.e., phone verification of an email request or vice versa).
- **Never send passwords or code words electronically.** Change them frequently.
- **Use comprehensive and up-to-date security software.**
- **Use this process, or one similar, to respond to a problem:**
  - Contact the bank to stop payment.
  - Review pending transactions and transfers for legitimacy.
  - Change bank account passwords.
  - Report the event to police.
  - Establish and understand how the situation happened.
  - Determine if there is an open threat of it happening again.
  - Implement preventive measures.

Talk to Your Insurance Agent and Your Financial Institution

Ask your agent about your coverage. Some insurance policies do not cover losses a school suffers if funds are transferred voluntarily under false pretenses. In addition, check with the financial institutions you do business with to learn what their policies and abilities are for recovering funds the school voluntarily transfers under false pretenses.