MUSIC MATTERS
Volume 25 | 1st Quarter 2021

Social Engineering 101: Responding to and Preventing Social Engineering Attacks

Peggy Wilson
Area Vice President Member Services, and
Jackie Turnage-Ferber
Client Training and Technology Coordinator

MUSIC's Commercial Crime Insurance provides coverage for loss of money, securities, or other assets resulting from fraudulent acts such as employee theft, certain types of fraud by third parties, theft of property from your school's premises, and more. Crime coverage areas include the following:

- Employees and Plan Officials
- Premises
- In Transit
- Forgery
- Money Orders and Counterfeit Currency Fraud
- Computer Systems Fraud, and
- Social Engineering Fraud

Cyber criminals have increasingly turned to social engineering schemes because it is a highly effective way to gain employee credentials and access to troves of valuable school data. Social Engineering is one of the most dangerous and high cost crimes facing MUSIC schools.

Social engineering refers to methods employed by hackers to gain the trust of a school employee. Most times, a social engineering attack begins with a phishing email that psychologically manipulates an employee to take action like making an electronic funds transfer. The unsuspecting employee believes the email was sent by a known vendor, client, or school employee.

If you believe that your school district or community college has transferred funds to a criminal posing as a legitimate business associate, your school must have protocols in place to act quickly.

1. Immediately contact the originating bank and **request a recall of the wire transfer.** After this call is made, confirm the recall in writing.

2. Immediately file a **complaint with the FBI** at **www.ic3.gov**. This reporting triggers the FBI's Recovery Asset Team and the FBI's assistance seeking return of the wire transfer.

3. **Preserve records of the incident,** including emails sent and received in their original electronic state.

4. Once the above steps are complete, **contact MUSIC's Property Supervisor, Phillip Spallo** at 314-800-0200 or email him at Phillip_spallo@gbtpa.com.

It is important to realize that regardless of your school's familiarity with a contact, email may be intercepted, altered, and fabricated. You can reduce the changes of social engineering fraud by implementing the following best practices:

1. **Verify Email Requests by Telephone:** Require those responsible for paying invoices or changing bank routing information to verify payment details over the phone as opposed to email or by using documents sent electronically. Making a phone call to a known, preexisting telephone number remains the single best protection against fraud. Do not rely on the phone number provided by email request, this too could be designed to call the " hackers" to confirm what they sent.

2. **Segregate Wire Transfer Responsibilities:** Establish a standing policy that requires at l east three people to review and approve wire transfer requests, pay an invoice, or change your school's bank account information. These types of requests should be entered in by the initiator of the wire transfer and verified by two independent signatories.

3. **Use Multifactor Authentication (MFA):** MFA is available from all major email providers. Using MFA provides a layer of security to accounts beyond a user's account name and password, making it harder for criminals to impersonate your school's employees.

Please Note: When filing a claim, the member will be asked for evidence that the wire transfer was verified by phone, that your school segregates wire transfer responsibilities, and that your school uses multifactor authentication for emails. Failure to implement these simple steps can, and likely will, jeopardize your claim.

MUSIC is creating training specifically for you to help make sure that you are doing everything you can to take the safest steps not to fall victim to these types of claims. They will be available to members in the next few weeks. Until that time, if you have any questions, please feel free to contact the MUSIC staff with any questions.