What are phishing schemes?
These deceptive messages can take the form of emails, phone calls or websites, and are designed to steal funds from an organization by tricking an employee into divulging confidential personal or business information such as a user name, password, bank account number, Social Security number or Employer Identification Number (EIN).

Phishing attacks most often appear as emails, but can also be conducted via instant messages or over the phone. While most organizations’ email services and firewalls are equipped with spam filters, cyber criminals can craft messages that appear trustworthy or impart a sense of urgency, and can sometimes penetrate security filters.

To give a sense of how innocuous phishing emails can appear, we’ve included an example chain here. Characteristics of a typical phishing email include:

► Slight variations on an email address of the sender;
► Misspellings and grammar mistakes; and/or
► An urgent request to complete the task, i.e., “I need you to do this ASAP.”

Cyber criminals are persistent when devising new ways to capture sensitive information from unsuspecting individuals, and spam filters and firewalls are only the first line of protection against phishing schemes. To proactively mitigate these risks, organizations can take the following steps to protect themselves:

Educate employees - Provide training on the risks associated with phishing schemes and caution employees away from offering confidential information, such as user names and passwords, over email or executing banking transactions based on instructions received via email. Employees should be advised to follow internal company policies and procedures when executing transactions or sharing confidential information.

Institute two-party authentication controls - Electronic security and authentication controls are now offered within online banking.
systems, making it so that an individual initiating a wire transfer cannot also authorize the transfer. If these systems are in place, a wire transfer initiated by an unknowing victim of a phishing scheme cannot be executed until a second individual authorizes the transaction, thereby increasing the chance an error will be discovered.

**Require verbal confirmation** - Organizations can protect themselves by instructing employees to obtain verbal authorization, no matter how urgent the request might seem, from the sender of an email prior to processing a transaction such as a wire transfer.

**Use a code word** - If an organization regularly communicates requests to process transactions via email, a “secret word” can be established internally to include in all email transaction requests in order to differentiate a valid email from a phishing email. This should be a unique word or phrase agreed upon by the financial executive department and known only internally.

Additionally, it’s important to note that information technology (IT) staff should be notified if employees receive phishing emails, so that spam filters and firewall settings can be adjusted to mitigate the risk of future messages bypassing these defenses. If an organization does fall victim to a phishing scheme, it’s important to quickly investigate the source of the email. Given the ever-changing cyber landscape and the speed at which digital attack tactics evolve, utilizing approaches to mitigate risk from both an IT and a personnel perspective is an organization’s best line of defense. For more on investigative practices for a nonprofit once it learns it’s fallen victim to fraud, see article "Wire Transfer Fraud: It Could Happen To You."

*Article reprinted from the BDO Nonprofit Standard Blog.*

For more information, contact Kelli D’Amore, principal, at kdamore@nathanwechsler.com