Preventing Wire Transfer Fraud at Foundations and Family Offices

It's a daily danger

Your email/firewalls are constantly being pinged. Although your cyber-security filter may stop 90%+ of the attempts, some still get through. Be especially alert around bank holidays. With international clients, the attempts are especially focused when US/European/Asian holidays are not synced. The scammer wants to prevent your ability to "voice verify" the authenticity of a wire request since the requester's office is closed due to holiday.

Check the email source thoroughly

The easiest manner for a scammer is to slightly change the email so it looks close to the authentic email source. E.g. George.Jones@Acmbank.com versus the authentic George.Jones@Acmebank.com. If you're in a hurry, you might miss this.

Beware new wire instructions

Scammers sometimes will spend weeks within your email system. They may learn the proper formatting that you use internally for wire requests. They may mimic personal information or style that your SVP or senior person might use. Moreover, double check the destination account numbers as well as the bank routing numbers to ensure that they are correct and consistent with what you know to be

true. You may want to have a second person review wire instructions above a certain threshold as a standard control mechanism.

Use your privacy settings on social media effectively

Scammers are quite adept at integrating information from Facebook, etc. with Linked-In, with your firm's own website and other information sources. You want to prevent scammers from building a profile that would enable them to better impersonate you or send instructions that would contain sufficient personal information to lull the recipient into thinking that they are dealing with the "authentic" you.

Passwords need to be high quality

People often lapse into using a consistent pattern with their passwords. Using social media, scammers can learn of your connections to schools, delivery services, clubs, who often have minimal or no security. They use these insights to "hack" into your own account.

Beware any sense of urgency

The scammer is reliant on your inattention, complacency, or alternatively placing enough perceived pressure that you shortcut the controls that are in place. They may dangle the threat of material late fees or "deal/offer will be withdrawn" if the wire transfer is not completed immediately.

Summary

Currently, the only failsafe way is to pick up the phone and verbally confirm details with the authorizing person, ideally you call a published company phone and not a Cell Phone. This only works if you know the person and the person's voice. Remember that company logo's and other official looking references and information can be lifted from

Websites and placed within an email. You should be guided by what is in the “four corners” of the email but supplemental validation is critical for new wire instructions, large amounts, urgent requests, or any request that seems different.

Tom Donahoe has served as a Foundation CEO and on 6 Boards. He can be reached at 973 452 3992. This and 30+ related briefings are available at www.manageranalysis.com. Founded in 2003, his firm advises non-profits on governance practices, investment due diligence, outsourcing investment management, and crisis management.

Article published in Exponent Philanthropy, MAY 2020