Scam-prevention Guide

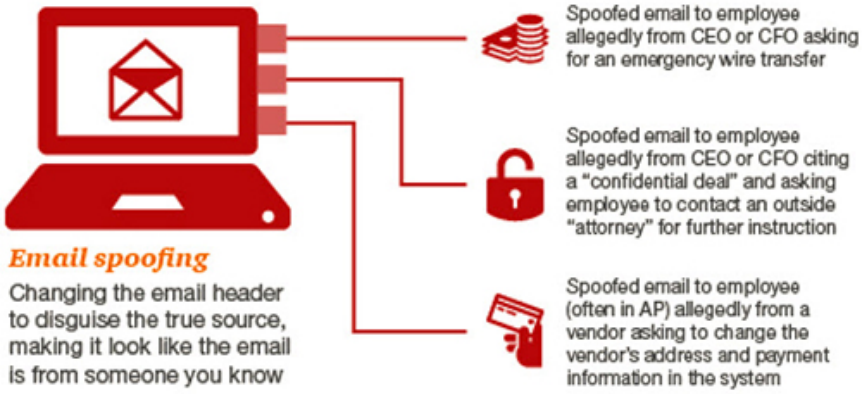
Understanding emails scams and educating key employees is critical!

To avoid wire fraud vulnerabilities within your company, ISRI recommends the following:

1. Train staff on how to shut down social engineering/spear phishing schemes.
2. Use multi-factor authentication to reduce the risk of fraud and increase security.
3. Embark on strong IT, finance, and purchasing controls to protect your company's assets.

Train staff on how to detect and shut down social engineering/spear phishing schemes.

Scammers are successfully targeting companies through that leads to wire transfer fraud. Here are some common methods:



Other versions of this scam may use malware installed in the system via an employee clicking on a compromised website link that is emailed to them (phishing), though this method is less common. Whatever the method, your employees—especially those who have the authority to request, approve, or execute wire transfers—need to be on guard.

Please note that the people perpetrating these scams frequently research employees' responsibilities so they know who to target, and often gather information to try to make the wire transfer request as believable as possible. For example, they may research the executive's schedule using public information or by making inquiries of the executive's assistant with the goal of sending the fraudulent emails when the executive is out of town and cannot be easily reached for verification.

Since many companies have stricter controls (like dual approvals) for amounts over a certain dollar threshold, the scammers often submit requests for lower amounts hoping the looser controls will raise the success rate of their scam. If the scammer is successful in a preliminary request, they may continue to submit additional requests until the scam is detected.

Use multi-factor authentication to reduce the risk of fraud and increase security.

Multi-factor authentication combines knowledge, possession and built-in factors:

a. Knowledge factors include something only the user knows, such as password, PIN, or answers to secret questions.

b. Possession factors leverage something that only the user has, such as, physical token, or a one-time token sent to an employee's smart phone or email account.
c. Built-in factors include such as special login code or iris scans.

For the multi-factor authentication to be successful, it is important to strike a balance between convenience and security. We advise employees to choose which one works best. In the finance department at ISRI, our authentication methods include the following:

a. Hardware tokens: Small hardware devices that we carry to authorize access when dealing with financial products.
b. Soft tokens: These are software-based tokens that generate token code. These are mobile apps installed on smartphone with advantage of notifications for user convenience.
c. SMS/Text message: A security code is sent to a phone via SMS. Once the user receives the text message, the code is entered into the login screen. An alternate phone could also receive a text if one employee is out of the country.
d. Phone call: With this authentication method, a staff member receives a phone call to a registered number and the user provides correct response to the voice prompt for complete authentication.
e. Email: Staff member receives an email with a link to verify the authentication request. Clicking on this link will complete the authentication process.
f. Security Questions: Instead of tokens, users provide answers to security questions which can be predefined or user defined. If our President needs an unusual transaction carried out, a lot of steps will be carried out to authenticate identity. Finally, a code will be requested which will finalize the transaction if correct.

Embark on strong IT, finance, and purchasing controls to protect your company's assets.

It is important that your company's **IT department** puts controls in place to keep the scammer out of your system and stop scams in their tracks.

Your company's **finance department** controls should include:

a. Establishment of a culture that encourages a questioning mindset especially when the request is from executives.
b. Creation of codes for executives to use when out of the country and such transactions need to be affected. Codes are private and only known by human resources, legal, and finance.
c. Requirements that the receiver of a wire transfer request to confirm its validity via phone to a valid phone…not the one in the email.
d. Mandatory dual approvals for amounts over a certain dollar threshold.
e. Mandatory validations for changes in vendor payment information or the setup of new vendors prior to payment approval.
f. Extreme caution when a request is made for your company's financial information to ensure the request is from a valid customer in your database. If a new customer, verify with the department in question.
g. If you suspect that your company has been scammed, contact the local FBI office at (202) 324-3000 or via https://www.ic3.gov/complaint/default.aspx.
h. Contact your company's financial institution and the receiving financial institution to request a halt or unwind the transfer.
i. Seek advice from counsel about any legal obligations or protections that you have relating to this event, such as potential insurance coverage for any loss.
j. Make employees aware about any scam, how it was perpetrated, and encourage them to be vigilant so that they will not be a gateway for the scammer.