

Wire Fraud Prevention Checklist



Cyber criminals use phishing scams and other methods to trick organizations into making irreversible wire transfers that cost them thousands of dollars. Protect your business with these simple tips:



Wire transfers are like sending cash. Once sent, they typically cannot be reversed, making them a preferred method for fraud by cyber criminals. The mere mention of a wire transfer should be a red flag.



If you receive a wire transfer request, even from an existing vendor, partner or other trusted source, don't take action before you call the contact. Use contact information, preferably a phone number, that you have in your records and have used to contact the person prior. Do NOT use the phone number, website or email addresses in the email request.



Double check every aspect of the email:

- Does the email domain have any suspicious "mistakes" such as a missing or extra letter? Phishing attacks can be subtle: mycontact@vend**o**r.com vs. mycontact@vend**e**r.com
- Does the request include correct vendor information but not accurate names, amounts or other specifics?
- Does the "reply to" email match the "from" email address?
- Do you know the person requesting you take action? Contact that person or company using a phone number from your records before taking action.



Common warning signs that an email request may be a scam:

- Unexpected ask or change in the amount or process for payments or wire transfers
- "No risk" investment or other request for funds from a foreign country your organization does not currently do business in or with
- Last-minute changes to wire transfer or payment instructions, even if they appear to be from a trusted source
- Alerts about account issues or payment problems that include an urgent or deadline-driven ask for a change to an existing process