Payment Fraud
Would you be fooled?

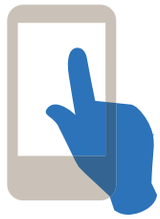
THE SCAM

Phishing

- Employees are lured to click on a link or attachment
- Malware downloaded
- Crook gets access to everything from user credential to emails

Masquerading

- Email sent pretending to be from an executive, issuing instructions on payments
- Crook tells the person to keep it confidential



WHAT TO DO

IT=your first line of defense

- Don't ignore suspicious emails

Email or call: IT HELPDESK

Keeping you safe

- **Be aware**
  Be wary of any urgent or confidential requests. If something looks fishy to you, it probably is. No alert is considered unnecessary.
- **Think before replying**
  Never "reply" to the email containing a suspicious request. That opens the door to the fraudster. Using a slightly altered executive email address is a tactic commonly used by crooks.
- **Authenticate**
  Validate by phone any beneficiary or address changes from vendors. Or ask another person at the company to create a new email to confirm the change.
- **Get two okays**
  No matter the size of the company, dual authorization should, at a minimum, be implemented for certain transactions.
- **Alert your bank**
  It's essential to tell banks, so proper action is taken to stop the wire or prevent more wires from being sent inappropriately.
- **Remove the dirty PC**
  Once a machine is compromised, take it off the company's network until it has been cleaned of malware.

www.bofaml.com

Bank of America
Merrill Lynch