The scammers often perform a fair amount of research before executing financial scams over email.

The rely heavily on social engineering tactics to trick unsuspecting employees and executives.

Email Financials Scams

These scams target companies and individuals seeking to gain access to funds or to trick someone into performing a financial transaction.

Corporate or publicly available email accounts of executives or high-level employees are either spoofed or compromise to execute these scams.

One example of this is Executive fraud, wherein the scammers spoof or hack into the email of an organization's executive in order to initiate a fund transfer to their own accounts, request payments or the approval of gift cards.

IT Security

Beware of Financial Email Scams

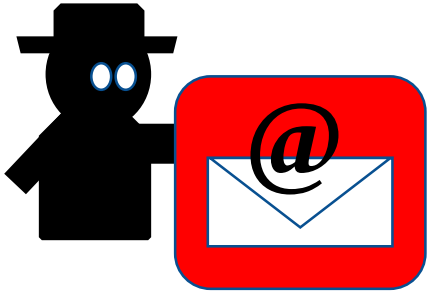
IEEE

The SCAMS

- **The Bogus Invoice**
  - Asks to wire funds for invoice payment to an alternate, fraudulent account via spoofed email or telephone call.
- **Executive Fraud**
  - Impersonate high-level executives or other types representatives requesting the initiation of a wire transfer or invoice payment.
- **Email Account Compromise**
  - An email account of an employee or legal representative is hacked and then used to make requests for invoice payments, wire transfers or gift cards.
- **Attorney Impersonation**
  - Impersonate lawyers or representative of law firms pressuring the contacted party into acting quickly or secretly in handling the transfer of funds.
- **Data Theft**
  - Impersonate role-specific employees to get personal or sensitive information to tailor the scams.

Email Message Red Flags

- **Spoofed sender domain**
  - Scammers usually register a domain similar to its target using slight variations
- **Position or Organizational role of the e-mail sender**
  - Scammer pose as someone influential in an organization
- **Urgent e-mail subject requesting immediate fund transfers, invoice payments or gift cards**
  - Typical subject lines imply urgency regarding these transactions
- **Body of the E-mail**
  - Message is asking for fund or wire transfers to an account that's different from ones normally used for that specific transaction. This may also include requests for purchases of gifts cards.



Always verify!

- ✓ Confirm details with the parties involved, especially when it comes to messages that involve fund transfers, invoice payments and the purchase of gift cards.
- ✓ Do not use any of the information included in the suspicious email to validate the request.
- ✓ Establish secondary verification protocols that include non-email (such as phone or text messaging).