

SPOTTING SOCIAL ENGINEERING/DECEPTION FRAUD



YOU CAN STOP A CRIME BY RECOGNIZING THE 8 SIGNS OF EMAIL FRAUD.



WHEN IN DOUBT, CHECK IT OUT

Criminals can plunder a company's accounts through fraudulent emails.

Recognize the signs, such as:

- Unfamiliar bank account information
- Suspicious requests from unfamiliar vendors
- Misspellings
- Request for complete confidentiality
- Sudden "wire transfer only" policies
- And more

Social engineering fraud, also known as deception fraud, is a serious crime. It's perpetrated by imposters who intentionally mislead or manipulate unsuspecting individuals and businesses into diverting payments or sending them money.

An example: A criminal posing as a company manager or outside vendor sends an email request for a payment by wire transfer. These requests often appear to be legitimate at first glance, but upon closer look, may contain key telltale signs that something is amiss.

KNOWING THE SIGNS OF FRAUD CAN PREVENT MILLIONS IN LOSSES

Social engineering scams can cost businesses millions of dollars annually. But if employees know the signs of potential fraud, they can help prevent these losses. Some social engineering tactics employees and companies need to be aware of include:

1. **Email requests from vendors to wire funds to a new or unfamiliar bank account.** Frequently, these accounts are located overseas. The request may include what seems to be a plausible explanation for using the "new" account. For example, the "vendor" may say that the previous account is frozen due to a tax audit. In some cases, additional emails will be sent to direct funds to yet another account before the transfer is made.

2. Internal email from a manager, purportedly traveling or on vacation, who requests an e-payment to a vendor not approved by the company. The request justification may appear vague, such as payment for “business development” purposes. Or, the requestor may say they’ll provide supporting documentation for the request upon returning to the office.



3. Misspellings, incorrect syntax, or unusual or odd word usage in the transfer request. Social engineering schemes are frequently perpetrated from outside the U.S. by people whose primary language isn’t English.

4. Payment rejection by initial account with a new request to wire funds to a different account. This could indicate that the perpetrators are having difficulty lining up an account for withdrawing the funds.

5. Requests to wire funds on a Friday, urging payment by close of business. This timing gives the perpetrators two non-business days to remove the transferred funds from the receiving account.

6. Requestor instructs the employee to keep the wire transfer a secret from colleagues. They may say it’s for a confidential purpose, like the acquisition of a new subsidiary that hasn’t yet been made public, and assert that disclosing the payment could be a violation of SEC rules.

7. Requests for wire transfers to a foreign bank account by a company that doesn’t engage in overseas business.

8. Vendor email states new “wire transfer only” policy for payments. There may even be a request to stop payment on a payment check already mailed, and to wire-transfer the funds instead.

Also, be aware that tech savvy criminals may be able to monitor, infiltrate and intercept a company’s email accounts and service. This allows them to track and then mirror a vendor or employee communication style to appear legitimate.

BEFORE WIRING FUNDS, BE VIGILANT

The following steps take only minutes, but could save millions.

1. Reach out to the requestor by telephone to verify all facets of the request and confirm the receiving account information.
2. Do some research. If it’s an outside company or vendor, find out if anyone else in the company is familiar with the requestor and the history of wire transfer requests.
3. Remind company employees: “When in doubt, check it out!” It’s important to have a culture where employees feel comfortable asking for verification/clarification that a request is legitimate.

STAY ON THE LOOKOUT FOR EMAIL SCAMS.

Visit [TheHartford.com/crime](https://www.thehartford.com/crime) today to learn more about The Hartford’s strong defense against social engineering attacks.

The Hartford® is The Hartford Financial Services Group, Inc. and its subsidiaries, including Hartford Fire Insurance Company. Its headquarters is in Hartford, CT.



Business Insurance
Employee Benefits
Auto
Home