AIG

Claims Intelligence Series

Mitigating Social Engineering Fraud Risk

Social engineering fraud, or losses due to schemes duping an employee into transferring funds, are a significant and growing threat for companies of all sizes. The following guidance aims to raise awareness of attempts by outside third parties trying to steal company funds and provides best practices to help prevent a social engineering incident.

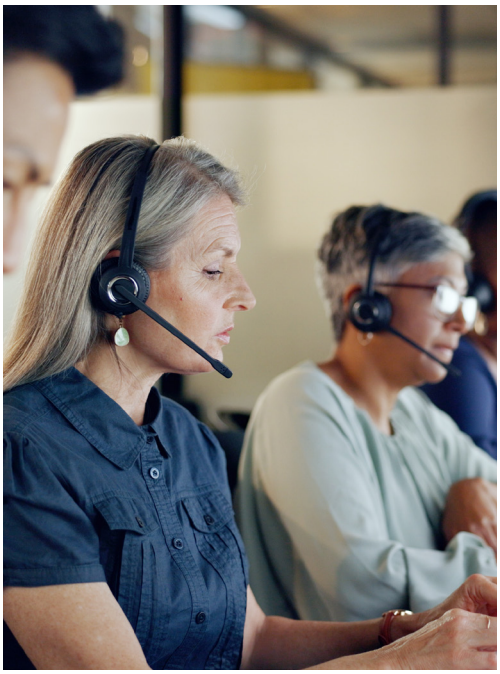
Baseline practices to help prevent a social engineering event:

1. Support the implementation of employee training, education, and awareness.

- **As a matter of priority, alert those that could be targeted across all geographies of your organization and raise their awareness to this type of fraud;** not just at the finance function level but all functions likely to be in contact with third parties, including employees who interface with and manage vendor and client matters. This means that the alert should be general in its distribution, and it should reach all foreign subsidiaries. All levels of management need to support the trickle down of communication throughout the organization and to its stakeholders.

2. Ensure robust processes are in place to mitigate the risk.

- **Consider implementing a secure method for sending important instructions (payment or otherwise) that makes sense for your organization.** All requests for payment or account changes should not be acted upon until verified, ideally with a "call back" to the person purportedly sending the instruction to confirm authenticity. The call back should be to the person's telephone number as taken from internal company records, not that which has been received as part of the account change request, as this could have been fraudulently altered.
- **Be careful and know who you are speaking to on the phone.** Complete a thorough call history by keeping logs of unusual callers and requests so they can be referred to if necessary.
- **Escalate any requests purportedly received from senior management where the tone or style is unusual,** where there is a sense of urgency expressed by the person making the request, or unusual grammatical or typographical errors appear.
- **Ensure employees do not share private/confidential corporate information to third parties** (such as supplier numbers and details).

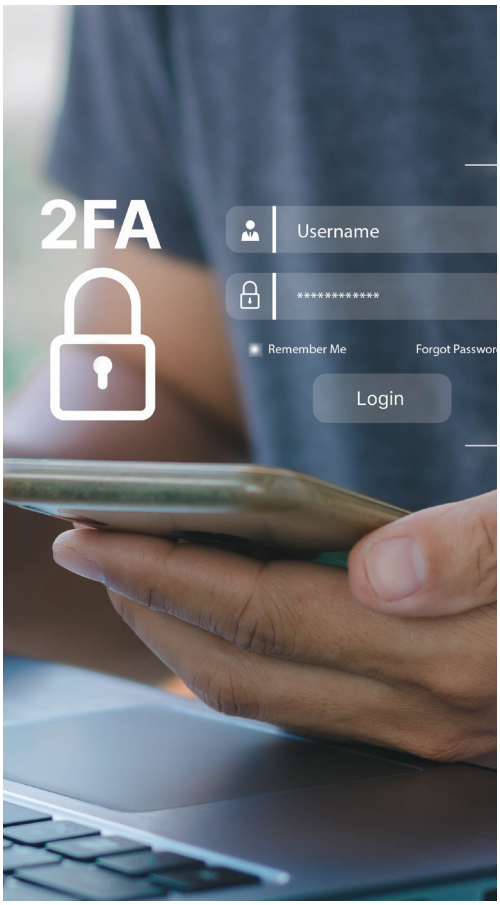


3. Monitor your financial accounts on a regular basis for irregularities.

- **Use dual authorization wherever possible.**
  - Dual authorization approval processes are preferred for any payment, no matter the amount, to ensure that all payments are duly cleared and justified.
  - Make clear to your staff that they should err on the side of caution and should vocalize any suspicions (no matter how small) they have about a payment, financial transaction, or payment change instruction.
- **Streamline your company's bank processes.**
  - The payment authority described above should be confirmed with your banks. Those monitoring your company's finances should be aware of all official financial processes.
  - Bankers must be asked to report, or even stop, any unusual transfer transaction (e.g., amount, beneficiaries, purpose, etc.). This recommendation applies in priority to 'manual' payments.
- **Implement a company-wide, agreed-upon payment methodology for all transactions.**
  - Secure means of payment must be favored. For instance, electronic signatures (with biometric authentication for instance) are now offered by most financial intermediaries and can dissuade a person under influence or duress from being tempted to copy or reproduce a hand-written signature.
  - Non-secure payments (facsimile, paper, telephone, email, checks) if any, should be limited and should always require a prior accounting entry.

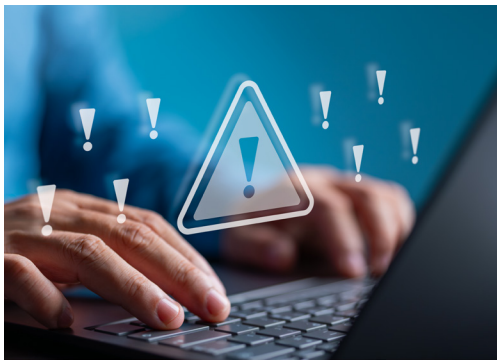
4. Consider implementing IT controls throughout the year.

- **Enable multi-factor authentication for all company email accounts.**
- **Prohibit legacy email protocols,** such as POP, IMAP, and SMTP1 that can be used to circumvent multi-factor authentication.
- **Disable legacy account authentication.**
- **Prohibit automatic forwarding of email to external addresses.**
- **Add an email banner to messages coming from outside your organization.**
- **Configure Sender Policy Framework, DomainKeys Identified Mail, and Domain-based Message Authentication Reporting and Conformance to prevent spoofing and validate email.**
- **Ensure changes to mailbox login and settings are logged and retained for at least 90 days.**
- **Enable alerts for suspicious activity,** such as foreign log-ins.
- **Enable security features that block malicious email,** such as anti-phishing and anti-spoofing policies.
- **Confirm the use of outside virtual meeting platforms not normally utilized in your internal office setting.**
- **Use secondary channels or two-factor authentication to verify requests for changes in account information.**
- **Be alert to hyperlinks that may contain misspellings of the actual domain name.**



4. Consider implementing IT controls throughout the year. (continued)

- **Refrain from supplying login credentials or personally identifiable information (PII) of any sort via email.** Be aware that many emails requesting personal information may appear to be legitimate.
- **Verify the email address used to send emails,** especially when using a mobile or handheld device, by ensuring the sender's address appears to match who it is coming from.
- **Ensure the settings in employees' computers are enabled to allow full email extensions to be viewed.**



If you think or know you've been a victim of social engineering fraud:

1. Immediately alert your bank/financial institution, request that your bank cancel any pending transfers that appear suspicious, and attempt to recover any already-transferred funds from the recipient bank(s).
2. Contact the authorities. Event notifications can be filed online through the Internet Crime Complaint Center (IC3), at bec.ic3.gov.
3. Review other recent transfers to identify any possibly affiliated transfers and determine scope of loss/event.
4. Save all documents and files related to the event.
5. Work with your broker to submit notice to your insurance carrier.

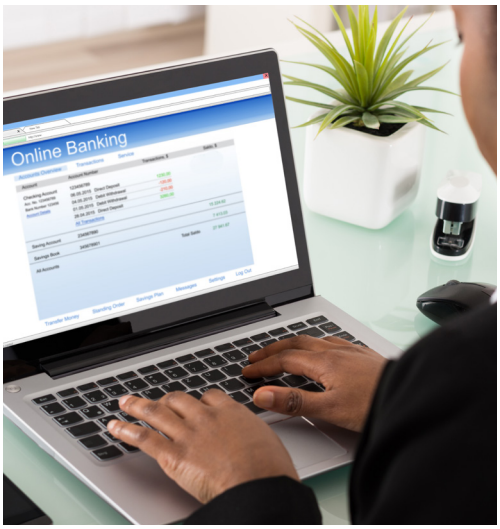
After a social engineering event has occurred:

1. Assess what went wrong. Was it human error caused by failure to follow established SEF prevention procedures?
2. Evaluate your company's existing internal controls — could processes be improved to prevent a similar future loss?
3. Conduct employee training and reinforce the necessity of company-wide adherence to policies and procedures.
4. Promptly implement any identified improvements in internal controls or IT Security.

Case Studies

An employee of an insured's subsidiary company was contacted via mobile messenger app by a perpetrator alleging to be the parent company's CEO. In the message, an AI-generated voice impersonation of the CEO directed the employee to answer an email from the insured's (purported) legal counsel. In doing so, the employee provided proprietary documents, bank account numbers, and account balances. After additional communications, the purported attorney emailed the employee instructions to wire $1.8 million to a bank account. The employee wired the funds. Upon confirming receipt of the funds, the purported attorney then requested an additional wire transfer of $3 million to the same beneficiary bank account. The employee became suspicious and notified the parent company, which detected the fraud and notified federal authorities. While the insured determined that there was no intrusion into their computer/information systems, they do not know exactly where and how the perpetrator(s) gathered the detailed information about the insured that allowed them to perpetrate the fraud.

An insured's employee issued wire transfer payments totaling $1.4 million intended to pay a construction supply vendor. Instead of reaching the vendor's account however, the payments were sent to the account of an unknown wrongdoer impersonating the vendor. The wrongdoer, while purporting to be an employee of the vendor, had sent instructions to change the vendor's payment information. Shortly after payment was wired, the insured discovered that the payment instructions were fraudulent and informed the bank and federal authorities. It was discovered that the vendor's system had been hacked, which led to the issuance of the fraudulent payment instructions. The insured and the real vendor entered into a settlement agreement, whereby the insured issued partial payment to the vendor and the vendor issued a marketing rebate credit to the insured. The insurance carrier issued payment to the insured based on the net loss, subject to the sublimit for impersonation fraud coverage.



For more information on AIG's Crime Insurance and Fidelity Bond products, contact your local Financial Lines underwriter or Distribution partner.

07/24