8 Warning Signs of Financial Fraud

Financial fraud is one of the most common cybercrimes. At-Bay data shows that nearly 75% of financial fraud occurs in transactions with known vendors and 89% during an expected transaction[1]. Because financial fraud almost always happens when things seem normal, it can be challenging to identify and prevent.

The following questions will help equip your team to spot and react to the eight most common warning signs of financial fraud.

How to use this document

1. Share this document with everyone on your team to make sure they're aware of the warning signs of financial fraud.
2. Review the questions below with all team members. Make sure they are familiar with this document as well as the company's protocols for authenticating financial transactions.
3. For any team members who process invoices/payments, print this document and ask them to reference it during every transaction.

At-Bay Cyber and Tech E&O policyholders have access to At-Bay Stance™ Advisory Services*. This team of cybersecurity experts can help assess financial fraud risk, advise on employee training, and make recommendations to improve company protocols for verifying and authenticating financial transactions.

Schedule a call with At-Bay's Advisory Services team for your assessment for information on how to prevent financial fraud.

QUESTION	WHAT TO LOOK FOR
Did your vendor or customer change payment instructions mid-transaction?	Any message containing **new payment instructions** (e.g., bank account wiring instructions, mailing addresses for checks, etc.) should be treated as highly suspicious. Follow your organization's specific protocols to verify all payment instructions before proceeding.
Did you receive an email where the name in the signature doesn't match the sender's email address?	Many financial fraud attempts involve a legitimate-looking but fake email address signed with the name of a trusted person. Always check that the sender of messages actually matches the email and name you expect to receive invoices and/or payment details from, as established in your agreement with each vendor and customer.

QUESTION	WHAT TO LOOK FOR
Did you receive an email discussing a transaction or payment from a lookalike domain?	Cybercriminals can easily register a fake domain that looks like the real one by altering the extension (e.g., changing ".com" to ".co" or ".net") or editing a letter/number in the URL to one that looks similar. Scrutinize return email addresses and URLs against those you have saved in your address book or vendor agreements. If in doubt, call your contact at the business with the phone number you have on file.
Did you receive a message with an unexpected attachment?	If a vendor who has never sent an invoice with a file attachment suddenly does so, this is a red flag. Call your contact at the business with the phone number you have on file for them to confirm the attachment is authentic before opening it.
Did you receive an email with an unexpected QR code?	QR codes are a tricky way for cybercriminals to transmit malicious phishing links. If a customer or vendor sends you a QR code but you haven't previously known them to use QR codes, don't scan it, and definitely don't click it. Call the sender at the phone number you have on file for them to verify that it's legitimate first.
Did you receive an email, SMS message, or phone call from a company leader that you don't normally interact with?	Cybercriminals often impersonate CEOs and other executives to manipulate employees. If you receive communication from an executive who doesn't typically reach out to you in this manner, and especially if the message comes from a phone number or email address you don't recognize, then be sure to verify the sender's identity through a known channel before taking any action.
Did you receive an email, SMS message, or phone call from a company leader who urgently needs help?	If an executive reaches out with an urgent, time-sensitive task that asks you to share private information (like a password) or wire money to a "business partner," this is a red flag — especially if this person doesn't regularly communicate with you in this way. Verify the sender's identity through a known channel before proceeding.
Did you receive unsolicited communication from someone claiming they need your help resolving a technical problem?	Cybercriminals may contact you claiming to be from your company's IT department or an IT contractor working on an issue (maybe for the CEO). They may say they need sensitive information, like your password or PIN, to solve the problem. If this isn't an ask you normally receive from this person, verify their identity using a known, trusted contact in IT or with your contractor before proceeding.

About Financial Fraud

Financial fraud refers to cybercriminals using technology to steal money from individuals or organizations by manipulating victims into sending funds to seemingly legitimate but actually fraudulent recipients. Attack tactics range from identity theft to phishing scams to sophisticated technical breaches.

At-Bay's 2024 InsurSec Rankings: Email Security and Financial Fraud Report found that financial fraud accounted for 72% of all email-related claims in At-Bay's portfolio in the first half of 2024. These attacks can also devastate a growing company. In 2023, cybercriminals stole an average of $219K in financial fraud incidents — and in the most extreme cases, over $5M.

Businesses must address this growing risk through a combination of email security, identity management and control, company protocols, and employee training.

About At-Bay

At-Bay is the InsurSec provider for the digital age. By combining world-class technology with industry-leading insurance, At-Bay was designed from the ground up to empower businesses of every size to meet cyber risk head-on. At-Bay Insurance Services, LLC provides insurance protection and security prevention solutions to close to 40,000 businesses in the US, safeguarding up to $800B in collective business revenue, and offers coverage by admitted and non-admitted insurers for Cyber, Technology Errors & Omissions (Tech E&O), and Miscellaneous Professional Liability (MPL). The At-Bay Group also includes an active full-stack insurance company and a cybersecurity company. At-Bay Security offers proprietary cybersecurity solutions including At-Bay Stance Managed Detection & Response (MDR).

The information contained herein is for general guidance on matters of interest only and is not intended to be construed as the rendering of professional services of any kind. If professional advice is required, the services of a professional should be sought.

1 At-Bay's 2024 InsurSec Rankings: Email and Financial Fraud Report

* At-Bay Cyber insurance not available for escrow agent services, title abstractors, or title agents.
Access to At-Bay Stance Advisory Services is available to policyholders via the "Embedded Security" fee and the corresponding endorsement. Your Embedded Security Endorsement refers to "At-Bay Stance Advisory Services" as "At-Bay Stance Managed Security." Please contact your authorized insurance representative for information concerning your Policy.