# Case Summary

A suspicious email was received by the accounts department, requesting a change to a vendor’s bank account details for future payments. Upon investigation, multiple red flags were identified: the sender’s email domain did not match the verified vendor’s domain, the new banking information was inconsistent with previously recorded data, and the genuine vendor denied making any such request. These combined factors pointed to a sophisticated impersonation and phishing attempt aimed at diverting funds through unauthorized means. Immediate action was undertaken to mitigate potential loss.

# Actors Involved

* Fraudster: An unknown actor using the email address accounts@xy-z.co, attempting to pose as a representative of the legitimate vendor.
* Targeted Organization: The company’s accounts or finance team, who received and reviewed the fraudulent request.
* Genuine Vendor: XYZ Vendor Ltd., whose identity was impersonated but who confirmed no such request was made.
* Fraud and Cybersecurity Team: Internal team responsible for identifying, reporting, and responding to fraud attempts.

# Visual Timeline of Events

|  |  |  |
| --- | --- | --- |
| Step | Event | Key Detail |
| 1 | Fraudulent Email Received | Email from accounts@xy-z.co requests change in vendor bank details |
| 2 | Domain Review | Sender domain (xy-z.co) flagged as different from verified vendor domain (xyz.com) |
| 3 | Bank Form Analysis | Attached bank form lists a BIC/SWIFT code not matching vendor records |
| 4 | Vendor Verification | Contact with XYZ Vendor Ltd. confirms no change request was made |
| 5 | Fraud Conclusion | Determination of phishing/impersonation attack; payment halted |
| 6 | Incident Escalation | Case reported to fraud and cybersecurity team; staff training reinforced |

# Risk Explanation

This incident demonstrates a targeted phishing attack, where the perpetrator seeks to exploit trust and business processes to divert funds. The attack capitalizes on subtle domain manipulation and falsified documentation. Had the fraudulent request been processed, the organization would likely have suffered significant financial loss, and confidential banking details could have been further compromised. Such incidents highlight the critical importance of multi-factor verification for sensitive vendor changes, vigilant review of sender domains and documentation, and regular staff training to recognize red flags in vendor communications. Continuous awareness and robust protocols are essential to defending against evolving impersonation and fraud schemes.