6. INVOICE / PAYMENT DIVERSION SCAMS

Attackers send fake or altered invoices that look legitimate, tricking finance teams into paying the attackers instead of the real vendor.

WHAT IS INVOICE PHISHING?

Attackers send fake or altered invoices to mislead finance teams into paying attackers.

Scenario: Arham Gets a “Vendor Update” Invoice

Arham manages vendor payments.

He receives an email from “ABC Supplies” asking him to send the next payment to a new bank account.

The logo, tone, and signature all look perfect but the real vendor’s email account has been compromised.

Lesson: Always confirm bank account changes directly with the vendor using a verified phone number or official contact method.

ABC Supplies
To

Vendor Update

Dear Arham,

Please note that our bank account for payment has changed. The new bank account details are as follows:

Account number: 123456789
Routing number: 123456789
Bank name: ABC Bank

John Smith

How Attackers Bypass Finance?

- Hijack vendor mailbox
- Reply inside real threads
- Attach modified invoices
- Pressure victims with “late payment” urgency

Red Flags for Accounts Team

- Last-minute bank account changes
- Email tone slightly unusual
- No official vendor change request
- PDF metadata showing a strange creator

Prevention Tips

- Always call the vendor to verify account changes
- Use ticketing systems
- Never trust instruction changes via email alone