4. Supply-Chain Phishing Attack

Attackers target a trusted vendor or partner and compromise their systems or email accounts. They then send phishing messages to the vendor’s customers, using the familiar communication channel to appear legitimate. Employees and clients are more likely to trust these messages, which can lead to stolen credentials, malware installation, or unauthorized access.

WHAT IS A SUPPLY-CHAIN PHISHING ATTACK?

VENDOR

Attackers compromise a vendor

EMPLOYEES

Employees trust vendors → attackers exploit it

Scenario: Arham Receives an Email From a Vendor

Arham gets an email from the company’s printer supplier:
“Your service contract is expiring. Please sign the updated agreement.”

The email is sent from the vendor’s real domain, because their account was hacked.

The attached PDF installs malware when opened, giving attackers access to Arham’s system.

This attack exploits the trust between the company and its vendor.

Lesson: Always verify unexpected attachments or links, even from trusted vendors. Contact the sender through a separate, verified channel before opening attachments.

From: info@printer-supplier.com

Subject: Your service contract is expiring. Please sign the updated agreement.

How Supply-Chain Attacks Trick Employees?

- Email comes from a trusted vendor
- Industry-related content looks normal
- Invoices, contracts, tickets appear legitimate
- Uses real communication history

Red Flags Arham Should Notice

- Unusual attachment type
- Vendor tone “feels” different
- Contract updates not scheduled
- Vendor suddenly asking for credentials

Prevention Tips

- Verify unusual vendor requests
- Confirm with vendor via known contact
- Treat all unexpected attachments as suspicious
- Alert security when vendors behave differently