

3. WHALING / EXECUTIVE TARGETING

Specialized spear-phishing targets high-level roles such as CXOs, directors, and finance leaders.

These attacks aim for maximum impact by going after people with authority and access.

WHAT IS WHALING?

Specialized spear-phishing targeting CXOs, directors, finance leads, etc.



Scenario: “CEO Request” Sent to Arham

Arham in finance receives an email “from the CEO” saying, “Arham, authorize payment of USD 10,000 immediately for a confidential project.”

The attacker even copied the CEO’s email signature perfectly, but the domain was slightly altered and fake.

Lesson: Always verify payment requests through a secondary channel like a phone call or official chat, especially when urgency and confidentiality are emphasized.

SCENARIO: "CEO REQUEST" SENT TO ARHAM



From `ceo@fakedomain.com`

To

`arham@company.com`

Arham, authorize payment of
USD 10,000 immediately for
a confidential project.



Why Executives Are Targeted?

Because executives:

- Approve payments
- Have powerful accounts
- Rarely undergo strict security verification

Signs of a Whaling Attempt

- Secret payments
- Unusual requests
- Time-sensitive orders
- “Do not call me, I’m in a meeting”

Defense Strategy

- Finance must verify big payments via voice/WhatsApp
- Use multi-level approvals
- Train executives regularly