# What is phishing ?

Phishing is a cyber-attack in which attackers masquerade as a trusted entity via email, SMS, or websites to trick individuals into revealing sensitive data (like passwords or credit card numbers) or installing malware .

**Goals of phishing include:**

Stealing credentials (e.g. login, banking info)

Installing malware, ransomware, spyware

Harvesting personal, financial, or identity data

Evidence: 91% of hacks involve phishing, costing organizations millions

# How to Recognize a Phishing Email

- Sender Address: E.g., “contact@yourbank.com” (note Cyrillic “a”) instead of the real domain
- Greeting: Generic (“Dear Customer”) vs. personalized.
- Urgency & Threats: Pressuring language like “Act now!” or “Your account will be suspended” .
- Grammar & Style: Typos or unusual formatting are red flags .
- Suspicious Links: Hover over links—mismatched URLs or odd domains .
- Unexpected Attachments: Beware of .html, .exe, or macro-enabled docs

# Social Engineering Tactics

**Attackers exploit human psychology:**

- Authority: Pretending to be a boss, bank, or government .
- Fear/Urgency: “Immediate action needed or else...” .
- Greed/Curiosity: Fake rewards like gift cards entice users .
- Social Proof: Referencing colleagues or events to look legitimate

**Types include:**

- Spam phishing (bulk)
- Spear-phishing (targeted)
- Whaling (senior execs)
- Smishing/vishing (SMS or phone)


# Best Practices

- Don’t click unknown links
- Verify sender identity: via separate channel
- Use multi-factor authentication (MFA)
- Report suspicious emails to your IT or email provider

# Key Components of Cybersecurity

- **Fake Apple invoice**: mismatched styling, missing personal data, weird links .
- **Pretend PayPal or Microsoft alerts:** often contain odd formatting and fake phone numbers .
- **Twitter spear-phishing (2020):** attackers created a fake VPN login to hijack high-profile accounts and steal Bitcoin .
- **Ubiquiti (2015):** CFO tricked into sending $47 M via fake invoice email

# Questions

Q1: You get an email that says your account will be closed today if you don’t click a link.

- Is this phishing? (Yes / No)

Q2: You receive this link: : https://paypal.com/login

- Is this a safe link? (Yes / No)

Q3: The email starts with “Dear user” instead of your real name.

- Is that suspicious? (Yes / No)

📝 Think carefully, then go to the next slide to see the answers.

# Answers

Q1: You get an email that says your account will be closed today if you don't click a link.

- Is this phishing? (Yes / No) : ✅ This is phishing. The email uses fear to make you click fast. That's a common trick.

Q2: You receive this link: https://paypaI.com/login

- Is this a safe link? (Yes / No) : ❌ The link has a capital "I" instead of a small "l" in "paypal".This is a fake link made to fool you.

Q3: The email starts with "Dear user" instead of your real name.

- Is that suspicious? (Yes / No) : ✅ Real emails usually use your real name. "Dear user" is a sign that the message might be fake.

# Conclusion

Phishing is a serious and common threat.
By learning how to spot it and follow safe habits,
we can protect ourselves and others online.