Phishing

Phishing: A cyber attack where an attacker impersonates a legitimate entity to deceive the victim into revealing sensitive information, clicking malicious links, or communicating with unverified phone numbers.

Types of phising

Email	Often create urgency, pressuring victims to take action such as providing sensitive information, logging into fake websites, or transferring money/cryptocurrency.
Vishing (via phone)	A phone-based scam where an attacker impersonates a trusted entity to manipulate the victim into compromising personal or organizational assets.
Vishing (via text)	A text-based scam where an attacker impersonates a trusted entity to trick the victim into revealing sensitive information or transferring funds.

Red Flags to look for on phishing attacks

Sender Email Address	Check for slight variations, misspellings, or unfamiliar senders impersonating trusted sources.
Urgent or Fearful Language	Watch for phrases like "urgent," "immediate action required," or "account suspended" meant to pressure you into acting quickly.
Suspicious Links & Attachments	Hover over links before clicking and verify file extensions to avoid malware or fake websites.
Poor Grammar & Spelling	Legitimate organizations proofread emails—errors can signal phishing attempts.

Red Flags to look for on phishing attacks (cont)

Requests for Personal/Financial Info	Be wary of unexpected emails asking for login credentials, banking details, or sensitive data.
Unusual Content	Look out for generic greetings, irrelevant content, or messages that don't match the sender's usual tone.

Elements of Phishing attacks

Impersonation	Appears to come from a trusted source, using official logos, formatting, and language to deceive victims.	*Example*: Fake PayPal email requesting account verification.
Persuasive Language	Uses emotional appeals, threats, or financial incentives to encourage action.	*Example*:You've won $500! Claim now!
Sense of Urgency	Pressures victims to act quickly, often claiming stolen passwords, locked accounts, or security threats.	*Example*:Your bank account is locked! Log in now!
Malicious Links	Directs victims to fake websites or fraudulent contact numbers to steal sensitive information.	*Example*:Reset your Microsoft password here.
Dangerous Attachments	May contain malware disguised as invoices or receipts, creating security vulnerabilities.	*Example*: Fake invoice email with a malicious PDF.

Spam Emails

Purpose:
Spam emails are used to harvest emails, steal sensitive data, or trick users into clicking malicious links or attachments.
Common Forms:
Promotions (fake discounts, giveaways)
Job Scams (fraudulent employment offers)
Lottery Scams (fake winnings, prize claims)
Phishing Attempts (deceptive messages to steal info)
Key Characteristics:
✓ Unsolicited & unwanted (a.k.a. junk email)
✓ Mass-distributed to many recipients
✓ Can be part of phishing campaigns
✓ Often linked to advertising or fraud
✓ Carries potential security risks
Measures of action:
☐ Don’t click links or download attachments
☐ Avoid responding to suspicious emails
☐ Verify senders before taking action
☐ Use spam filters and report phishing attempts