CYBER SECURITY INTERNSHIP

Task 11

PHISHING ATTACK SIMULATION & DETECTION

JASHMI KS

Phishing is a social-engineering attack where an attacker tricks users into revealing sensitive information (like passwords, OTPs, or card details) by pretending to be a trusted entity.

Key characteristics

- Uses fake emails, messages, or websites
- Targets human psychology (fear, urgency, trust)
- Aims to steal credentials, financial data, or access

Common phishing types

- **Email phishing** – Fake emails from banks, companies, or admins
- **Spear phishing** – Targeted attacks on specific individuals
- **Whaling** – Targets high-level executives
- **Smishing & Vishing** – SMS and voice-based phishing

Fake Email

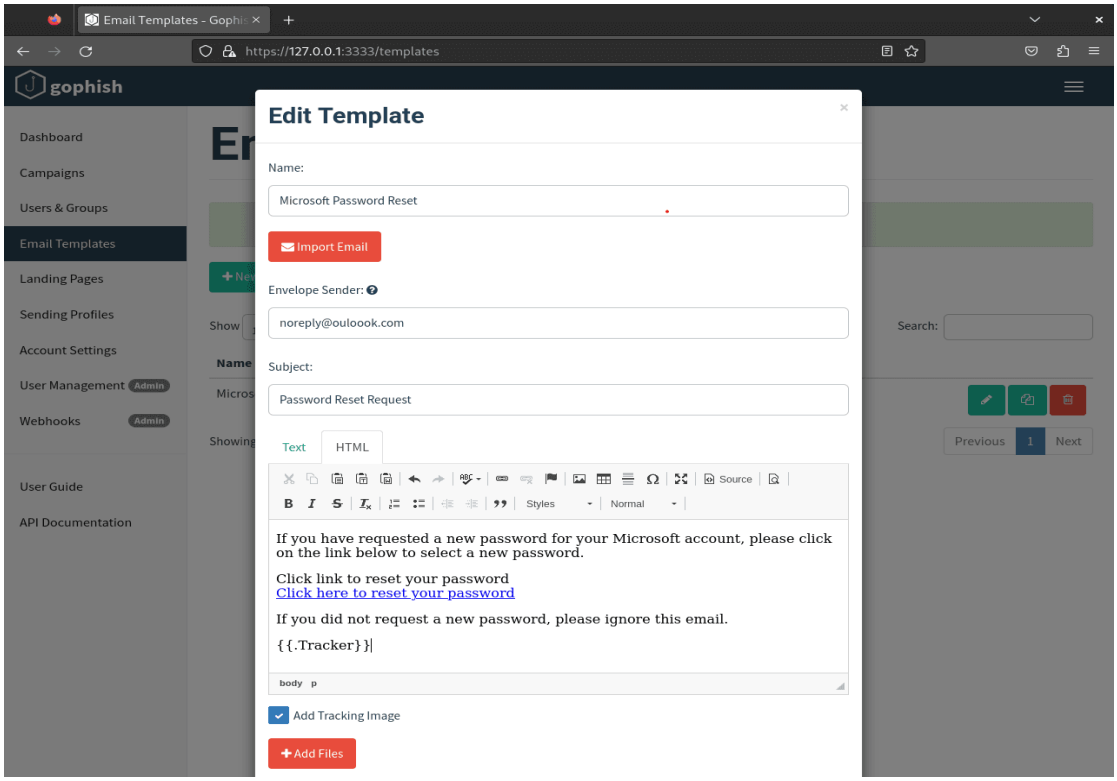
In phishing simulations, **email are studied** to understand how attackers design convincing messages.

Typical elements attackers use

- **Trusted sender identity** (bank, admin, company)
- **Urgent language** (“Account will be suspended”)
- **Call-to-action** (click link, verify account)
- **Spoofed branding** (logos, signatures)

Educational purpose

- Helps learners recognize malicious patterns
- Used in security awareness training
- Demonstrates how easily users can be deceived

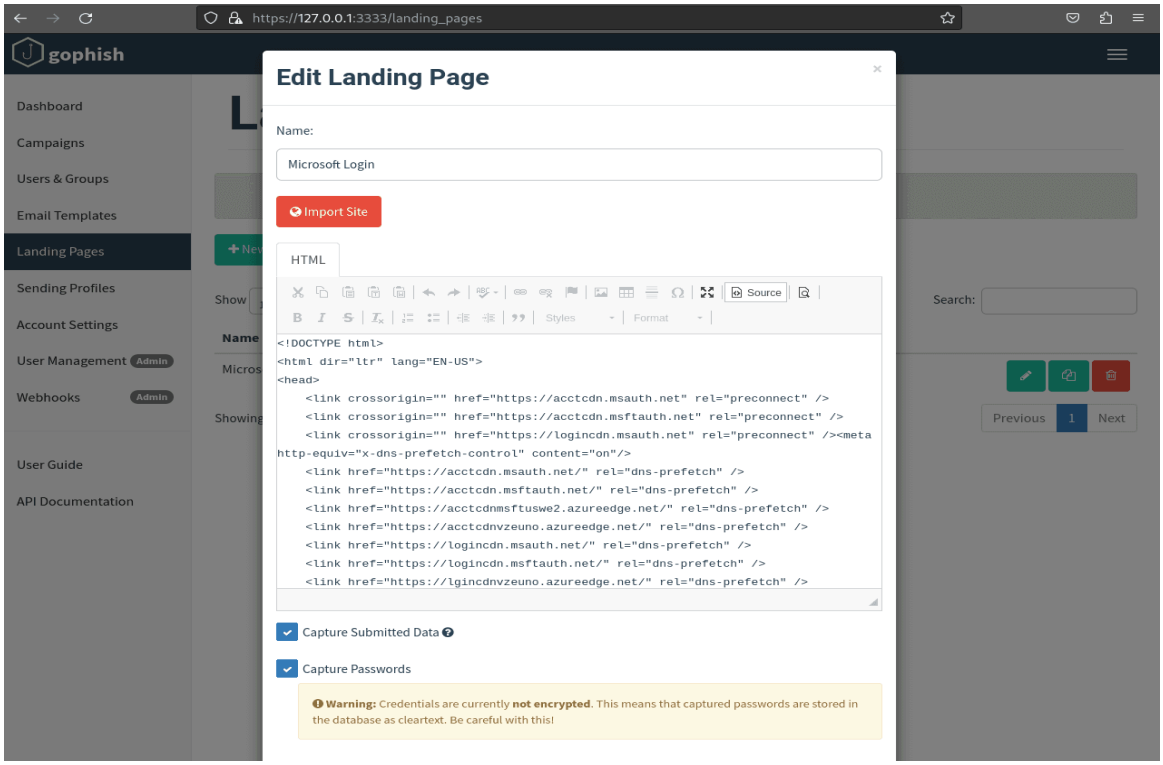


Setup Landing Page

A **landing page** in phishing attacks is a fake webpage that looks like a legitimate login or verification page.

What attackers try to copy

- Login forms
- Brand colors and layout
- URLs similar to real websites



Test Phishing Email

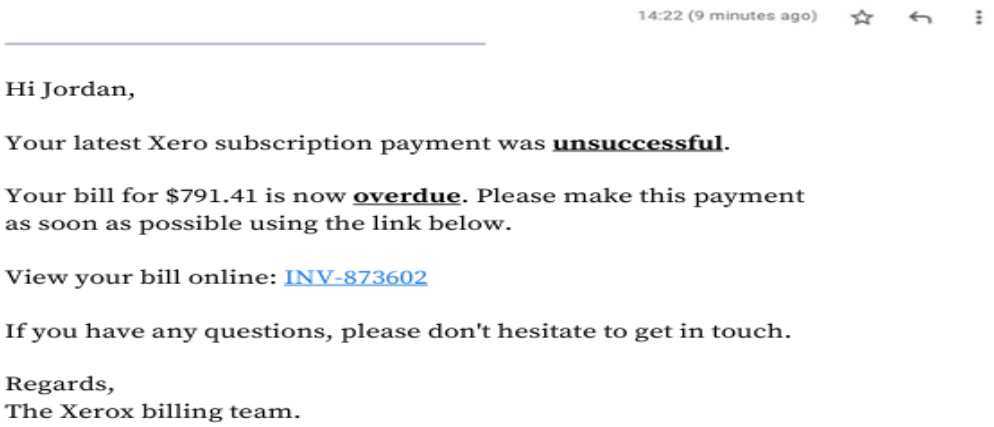
In cybersecurity education, test phishing emails are sent only:

- In controlled environments
- With prior permission
- For employee training or academic labs

Purpose

- Measure user awareness
- Identify risky behavior
- Improve security training programs

Real-world unauthorized phishing is **illegal and unethical**.



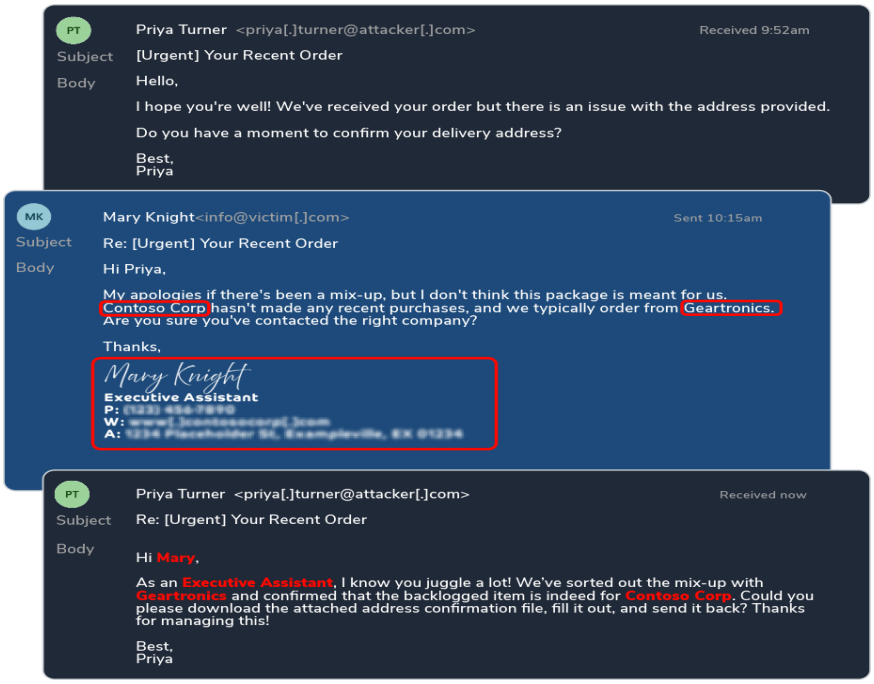
Track Responses (Analysis Perspective)

Tracking responses helps understand **how users interact with phishing attempts**.

Common metrics (theoretical)

- Email opened or ignored
- Link clicked
- Credentials attempted

- Reported as suspicious



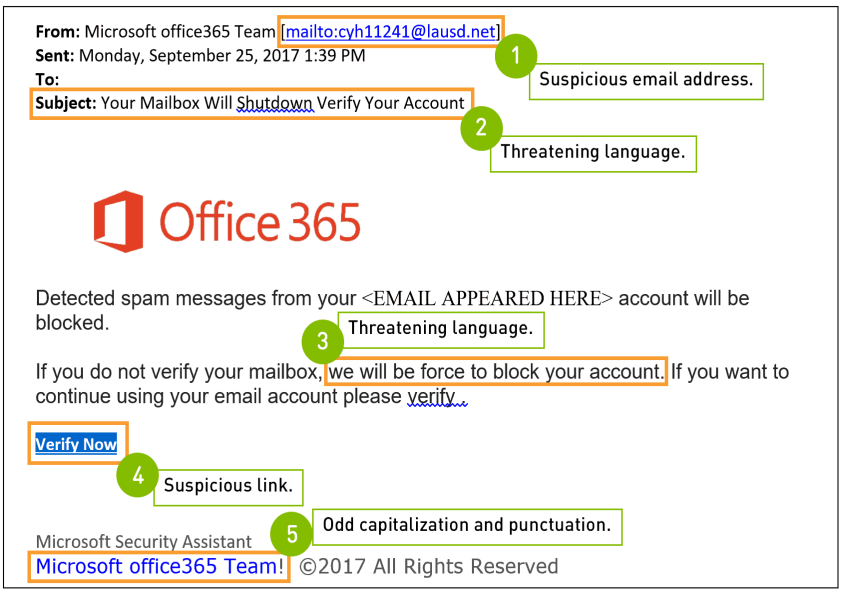
Identify Red Flags

Red flags are **warning signs** that indicate phishing.

Common phishing indicators

- Unknown or misspelled sender address
- Suspicious links or shortened URLs
- Grammar or spelling mistakes
- Urgent or threatening messages
- Requests for sensitive information

Recognizing these signs is the first line of defense.



Prevention

Phishing prevention focuses on **user awareness + technical controls**.

User-level prevention

- Verify sender identity
- Hover over links before clicking
- Never share OTPs or passwords

- Report suspicious emails

Technical prevention

- Email filtering
- Spam detection
- Multi-factor authentication
- Secure DNS and HTTPS checks

Phishing attack simulation is an ethical cybersecurity exercise used to understand attacker techniques, identify user vulnerabilities, and improve awareness and preventive security measures.