Understanding and Preventing Phishing Attacks

By
Nirmal S

Introduction to Phishing

- A type of cyber attack where attackers disguise as trustworthy entities to steal sensitive information.
- Commonly conducted through email, websites, and social media.

Types of Phishing Attacks

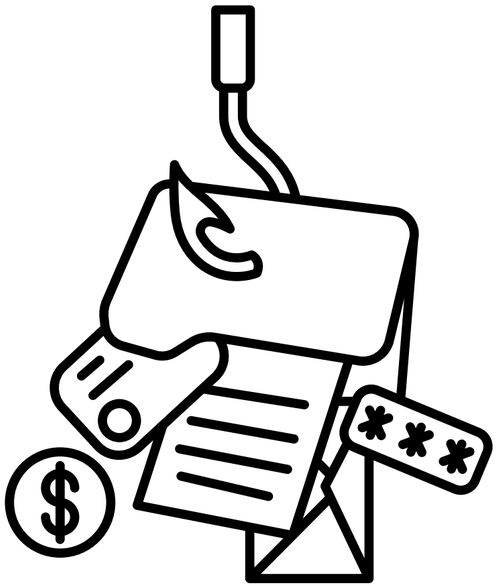
Email Phishing:
Fake emails that appear legitimate.

Spear Phishing:
Targeted attacks on specific individuals.

Whaling:
Attacks targeting high-profile individuals like executives.

Smishing:
Phishing via SMS messages.

Vishing:
Phishing via voice calls.



Common Characteristics of Phishing Emails

Suspicious Sender:

Email addresses that look similar but are slightly altered.

Generic Greetings:

Using generic terms like "Dear Customer".

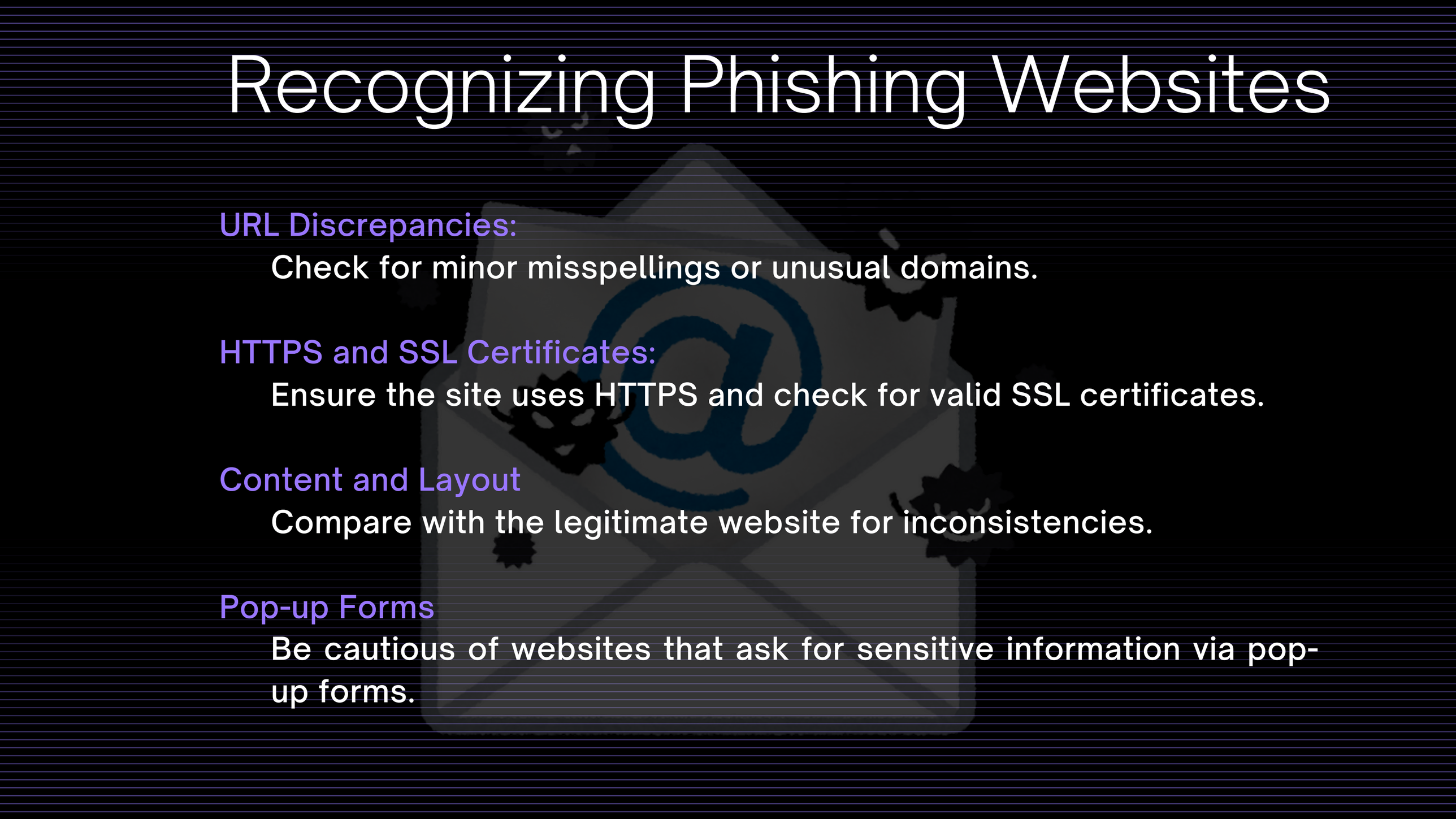
Suspicious Links and Attachments:

Links to unrecognized websites or unsolicited attachments.

Grammatical Errors:

Poor spelling and grammar.

Recognizing Phishing Websites



URL Discrepancies:

Check for minor misspellings or unusual domains.

HTTPS and SSL Certificates:

Ensure the site uses HTTPS and check for valid SSL certificates.

Content and Layout

Compare with the legitimate website for inconsistencies.

Pop-up Forms

Be cautious of websites that ask for sensitive information via pop-up forms.

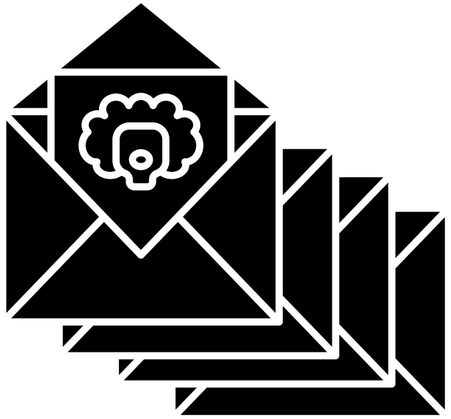
Social Engineering Tactics

Pretexting

Pretending to need information to confirm the identity of the recipient.

Baiting

Offering something enticing to gain access to sensitive information.



Tailgating

Following someone into a restricted area by exploiting their trust.

Examples of **Phishing Scenarios**

Fake Bank Alert

Email appearing from your bank asking you to verify account details.

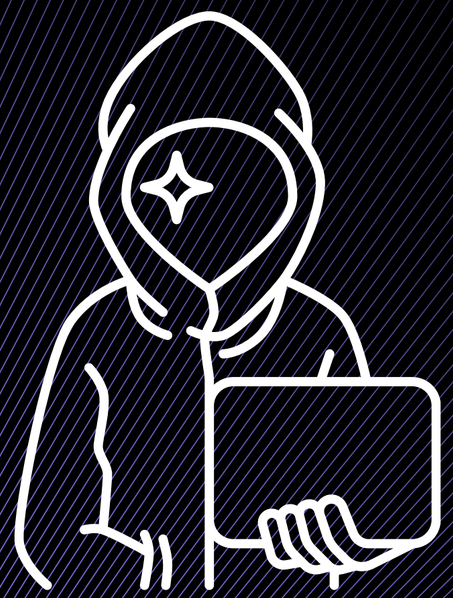
Tech Support Scam

Phone call claiming to be from tech support requesting remote access.

Fake Job Offer

Email offering a job that requires filling out a detailed application form.

How to **Protect Yourself**



Email Precautions:

Verify the sender's email address.

Do not click on suspicious links or download attachments.

Website Safety:

Manually type the URL in the browser instead of clicking links.

Look for security indicators like HTTPS.

General Awareness:

Regularly update passwords and use multi-factor authentication.

Be cautious about sharing personal information online.

Organizational Measures

Employee Training:

Conduct regular training sessions on recognizing phishing.

Phishing Simulations:

Perform mock phishing attacks to test employees' awareness.

Incident Response Plan:

Establish a clear procedure for reporting and handling phishing attempts.

Email Filtering Solutions:

Use email filtering tools to block phishing emails.

Thank You