Phishing Attacks: Recognize, Avoid, and Stay Safe

: BY SUBHANG ARYA

What is Phishing?

Deceptive Tactics

Phishing is a cybercrime where attackers try to trick you into giving up sensitive information like passwords, credit card details, or personal data.

Disguised Intent

They often disguise themselves as legitimate organizations, individuals, or services you trust to gain your confidence and steal your data.

Common Phishing Tactics

Spoofed Emails

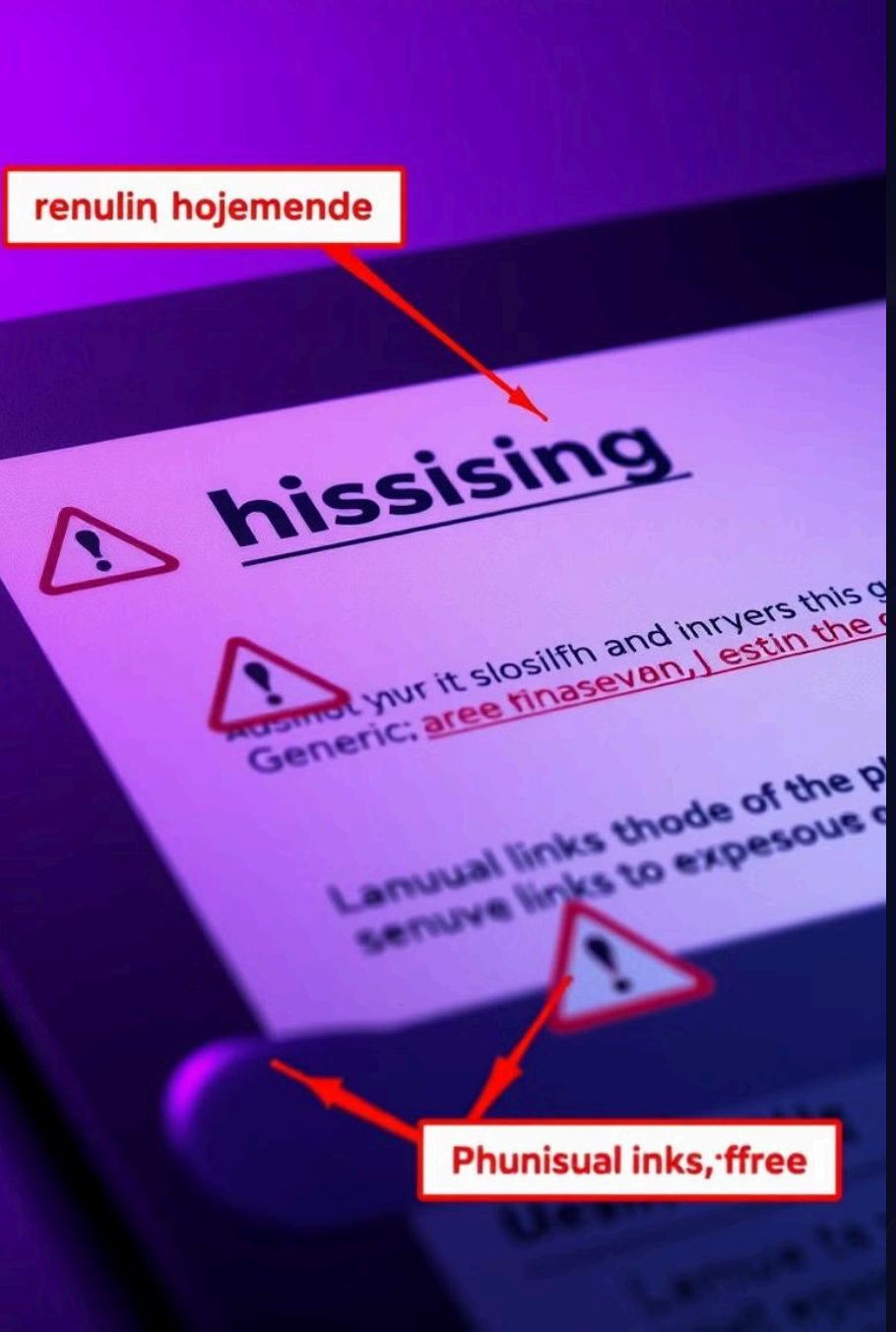
Fake emails that mimic real ones from trusted sources, often with urgent requests or enticing offers.

Fake Websites

Websites designed to look identical to legitimate sites, tricking users into entering their credentials or financial information.

Social Engineering

Manipulating people through social interactions to gain access to sensitive information or systems.



Identifying Phishing Emails

1 **Suspicious Sender**

Check the email address and sender name. Does it match the organization it claims to be from?

2 **Urgent Requests**

Phishing emails often create a sense of urgency, urging you to act quickly without thinking.

3 **Suspicious Links**

Hover over links before clicking to see the actual URL. Does it look legitimate?

4 **Misspelled Words or Grammar**

Phishing emails are often poorly written with grammatical errors or typos.

Spotting Fraudulent Websites

Security Certificate

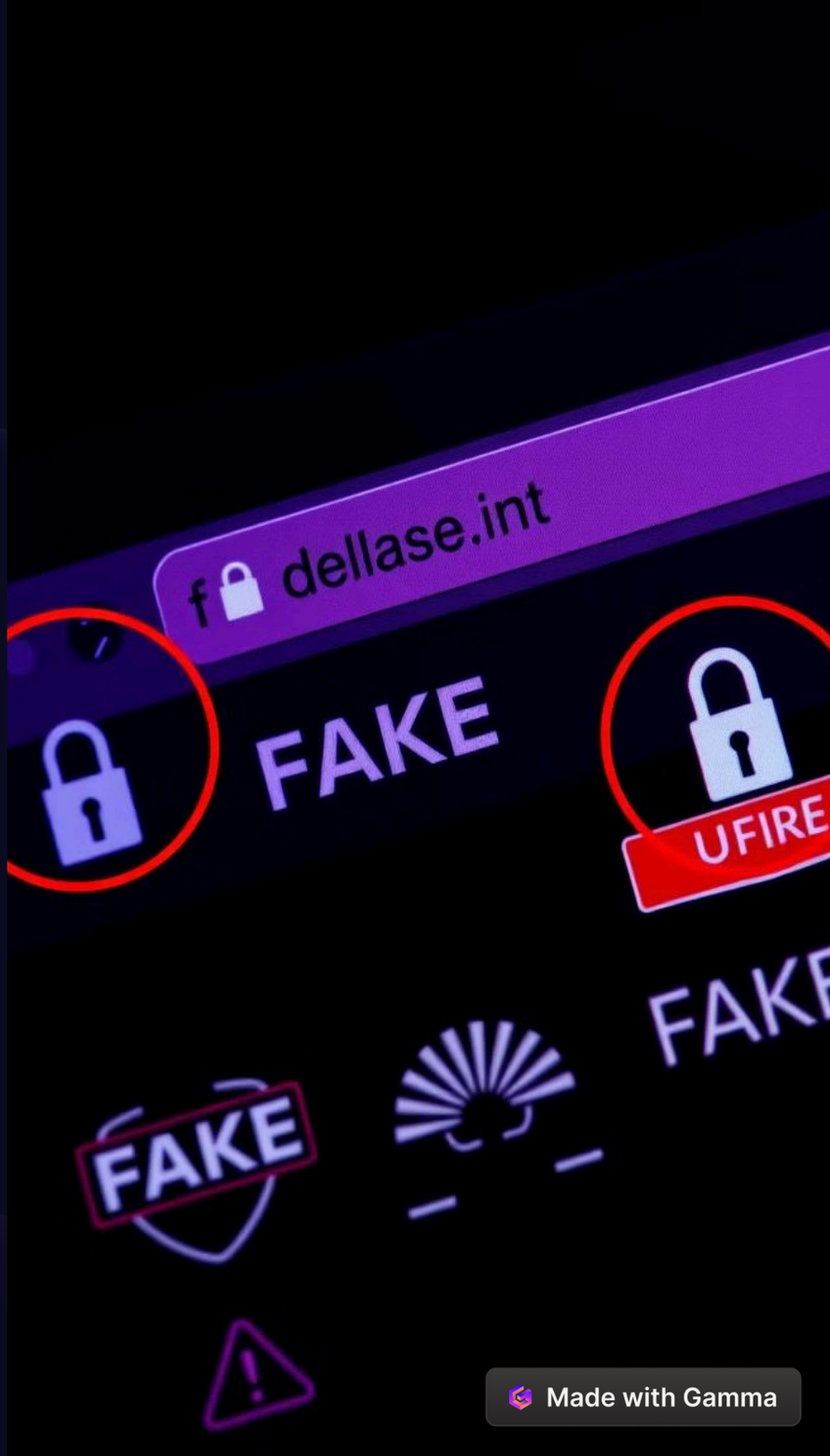
Look for a padlock icon in the address bar and a website address starting with "https".

URL Inspection

Check the website address carefully. Does it look genuine and consistent with the company's name?

Visual Inspection

Pay attention to the design and layout. Does it look professional and consistent with the genuine website?



Social Engineering Techniques

1

Baiting

Offering something enticing to lure victims into clicking on a link or providing personal information.

2

Pretexting

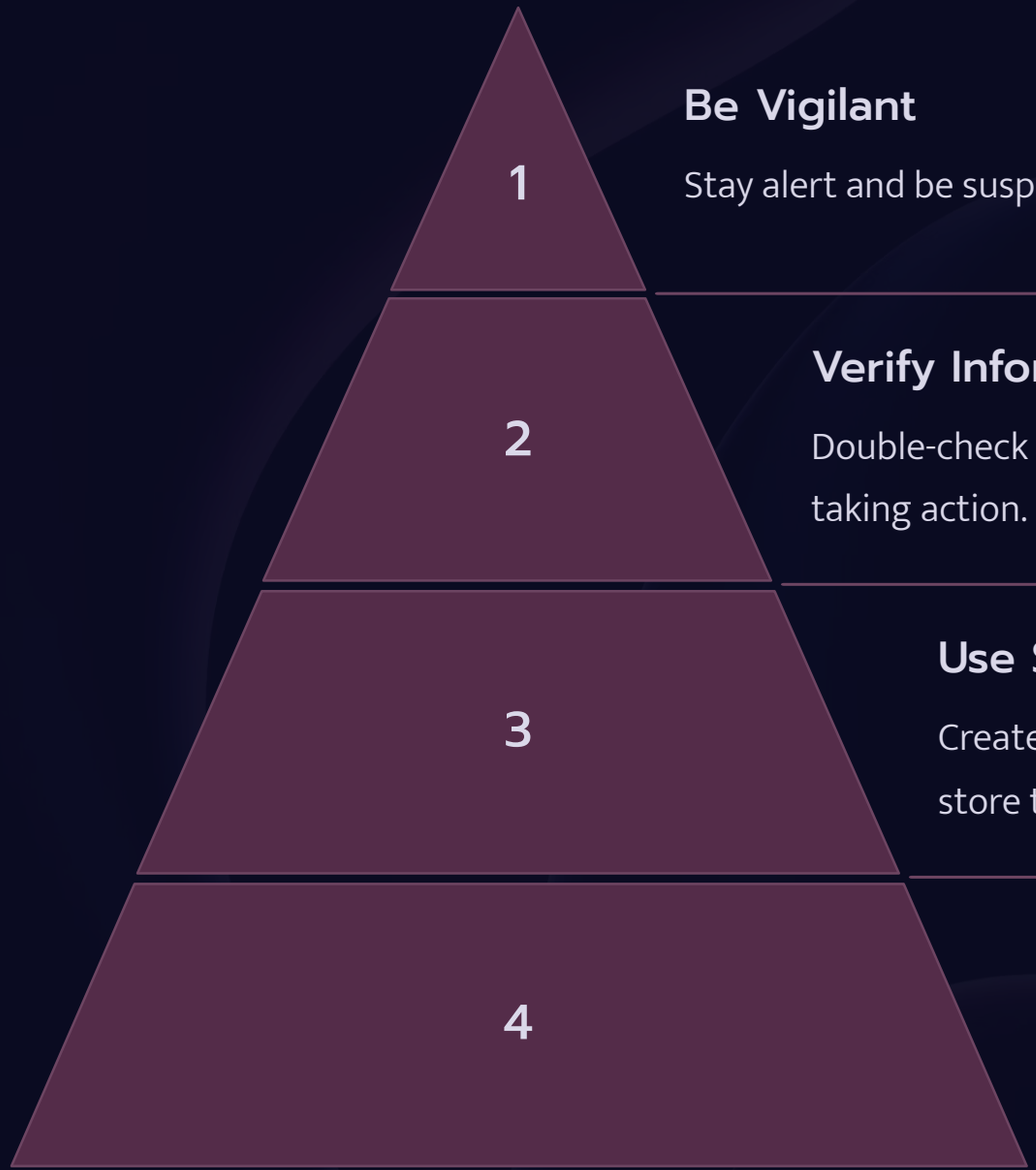
Using a fabricated story or scenario to gain trust and access information, such as pretending to be from a tech support department.

3

Scare Tactics

Threatening users with negative consequences if they don't comply with a request, often involving security threats or account suspensions.

Protecting Yourself from Phishing



Be Vigilant

Stay alert and be suspicious of emails and websites that seem too good to be true.

Verify Information

Double-check any suspicious requests with the actual organization before taking action.

Use Strong Passwords

Create unique, strong passwords and use a password manager to store them securely.

Install Security Software

Use a reputable antivirus program and keep your software updated to protect against malware and phishing attacks.

Password Security Best Practices

1

Length

Use at least 12 characters for your passwords, the longer the better.

2

Complexity

Include a mix of uppercase and lowercase letters, numbers, and symbols.

3

Uniqueness

Don't reuse the same password for multiple accounts.

4

Password Manager

Consider using a password manager to store and generate strong passwords securely.

Reporting Phishing Attempts

1

Don't Click

If you receive a suspicious email, avoid clicking any links or opening any attachments.

2

Report

Report the email to the organization it claims to be from or to the appropriate authorities.

3

Delete

Delete the email immediately to prevent further attempts at phishing.

Phishing Response and Recovery

Change Passwords

Immediately change your passwords for any accounts that may have been compromised.

Contact Bank

If you suspect your financial information was stolen, contact your bank or credit card company.

Scan Devices

Run a scan on your devices with antivirus software to detect and remove any malware that may have been downloaded.