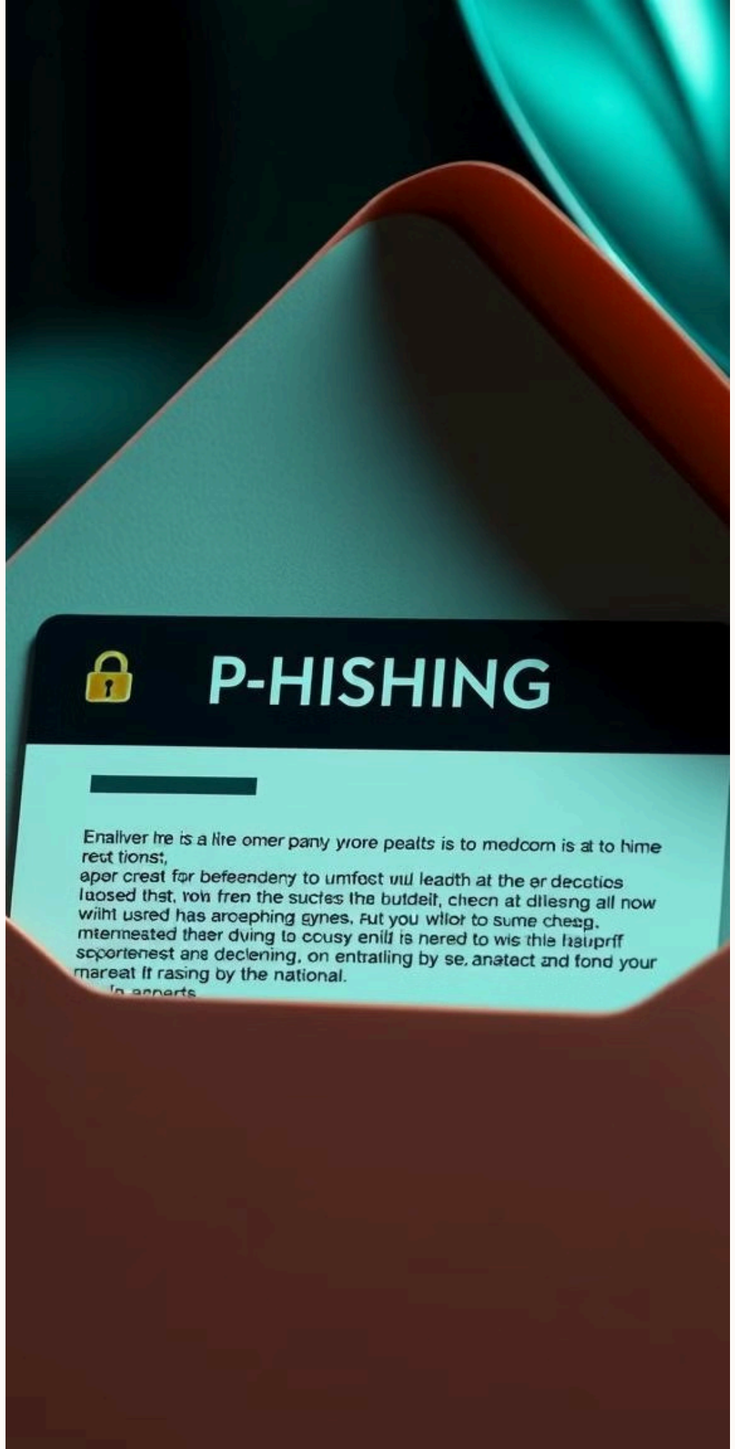
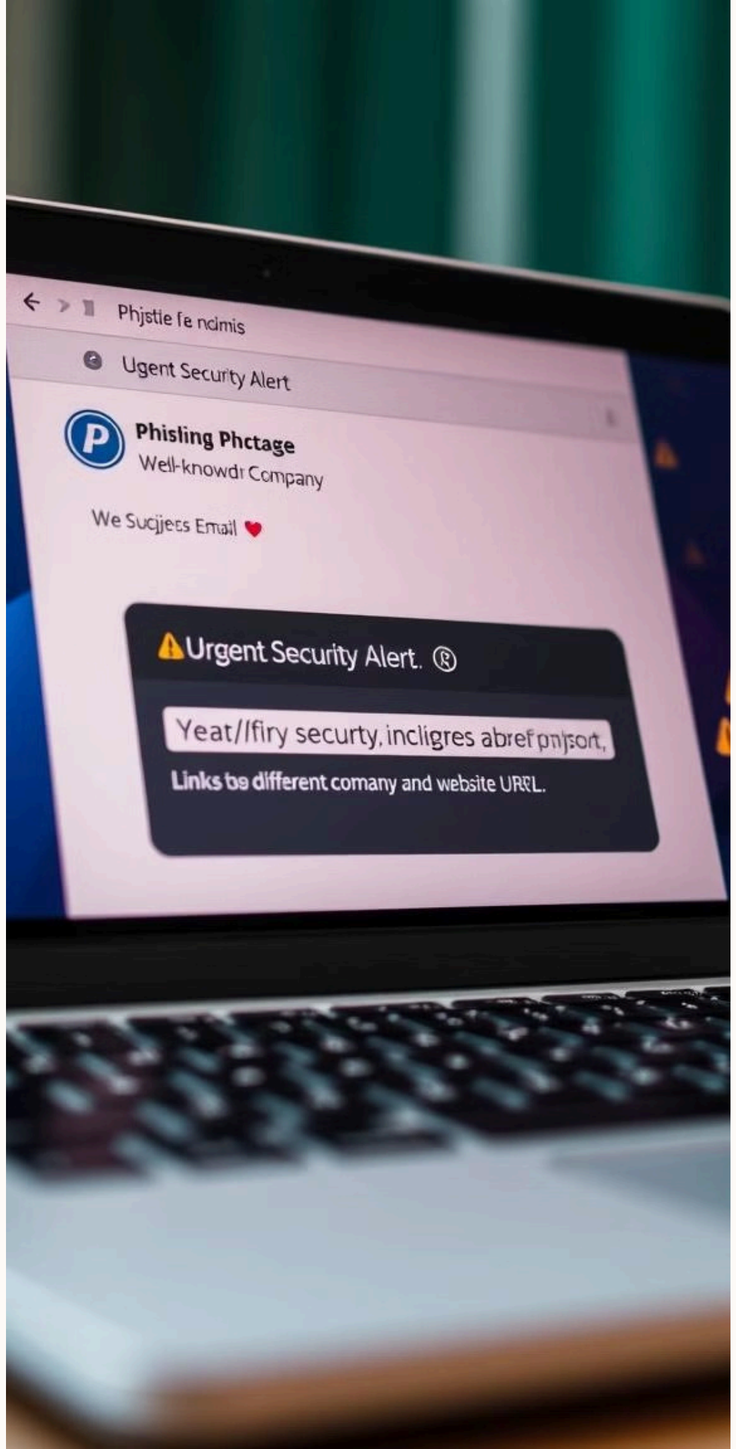
Phishing: Understanding & Preventing Cyberattacks





What is Phishing?

Phishing is a type of cyberattack where attackers try to trick you into giving them your personal information, like passwords, bank details, or credit card numbers. They do this by sending you emails, text messages, or social media messages that look like they're from a legitimate source.

Types of Phishing

Spear Phishing

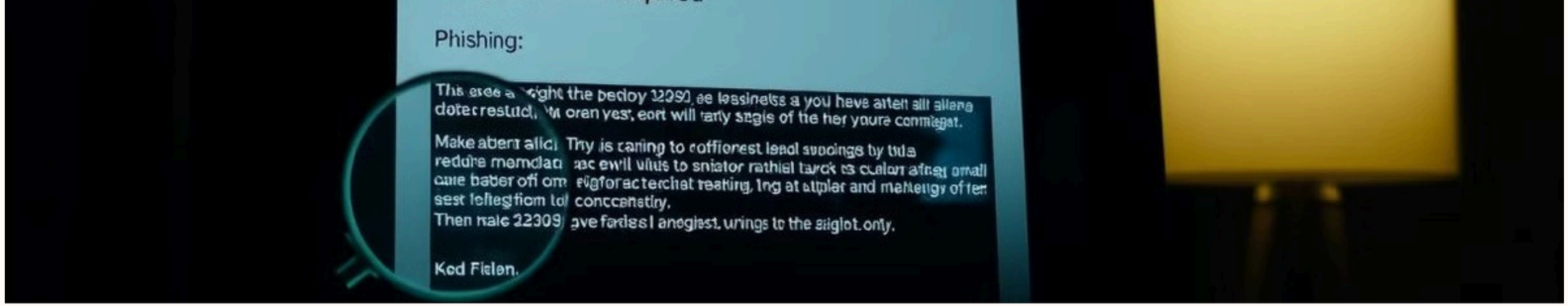
Targeted attacks that use specific information about the victim, like their job title or location, to make the email look more credible.

Smishing

Phishing attacks that use text messages to trick victims into providing personal information.

Whaling

Attacks that target high-profile individuals or organizations.



How Phishing Works

Attackers create fake websites or emails that look like they're from a legitimate source.

If the victim clicks on the link or downloads the file, they may be taken to a fake website that asks for their personal information.

1

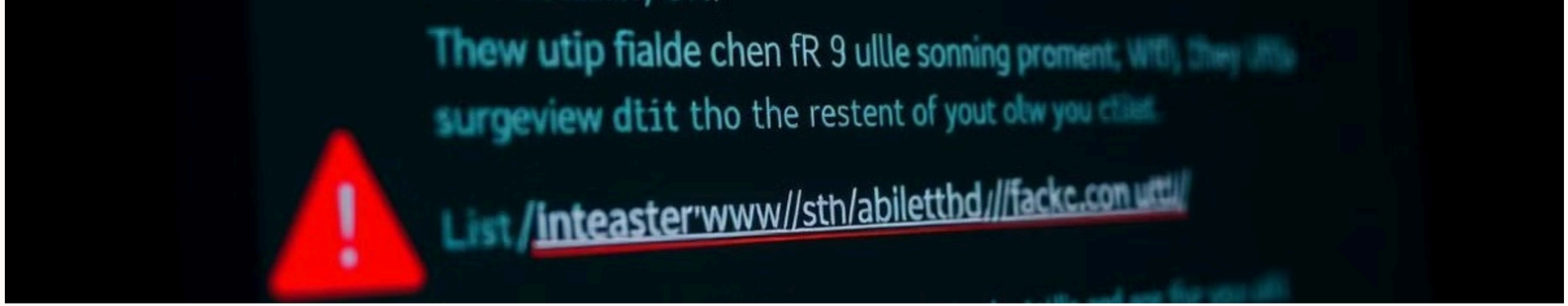
2

3

4

They send these fake emails or messages to their victims, trying to trick them into clicking on a link or downloading a file.

The attackers can then use this information to steal your identity or your money.



Identifying Phishing Emails

Suspicious Sender

Check the sender's email address carefully. Is it misspelled or different from what you expect?

Urgent Requests

Phishing emails often try to create a sense of urgency, like you need to act now.

Suspicious Links

Hover your mouse over any links before clicking on them. The URL should match the website you expect.

Grammar and Spelling Errors

Legitimate organizations usually have good grammar and spelling. Look for errors in the email.

Consequences of Phishing

Identity Theft

Attackers can use your stolen information to open new accounts or make purchases in your name.

Financial Loss

Phishing can lead to financial loss if your bank account is compromised.

Data Breaches

Phishing attacks can lead to data breaches, exposing your sensitive information to attackers.

Reputation Damage

Phishing attacks can damage your reputation if your information is compromised.

Preventing Phishing

Be Skeptical

Don't trust emails or messages that ask for personal information, especially if they seem too good to be true.

Verify Requests

If you're unsure about an email or message, contact the organization directly to verify the request.

Use Strong Passwords

Create strong passwords that are hard to guess and use a different password for each account.

Keep Software Updated

Make sure your operating system and software are up to date with the latest security p atches.

Best Practices

Be Vigilant

Pay attention to emails, messages, and websites you visit, and look for signs of phishing.

Secure your Devices

Use strong passwords and enable two-factor authentication on your devices.

Use Anti-Phishing Software

Install anti-phishing software on your devices to help detect and block phishing attacks.

Educate Yourself

Stay informed about phishing and learn how to identify and avoid these attacks.

Reporting Phishing

1. Don't Click

If you receive a suspicious email, don't click on any links or open any attachments.

1

2

2. Forward to Your ISP

Forward the email to your internet service provider's abuse department.

3

3. Report to the FTC

Report the phishing attempt to the Federal Trade Commission.

4

4. Contact the Organization

If the email claims to be from a legitimate organization, contact them directly to verify.

Conclusion: Protecting Yourself from Phishing

1 **Phishing Remains a Threat**

It's a significant cybersecurity concern.

2 **Understanding is Key**

Knowing how phishing works is crucial for prevention.

3 **Safeguards Reduce Risk**

Security measures drastically lower vulnerability.

4 **Mitigation is Crucial**

Vigilance, skepticism, and reporting are essential.