# Recognizing and Avoiding Phishing Attacks

This presentation will guide you through the identification and prevention of phishing attacks.

# What is Phishing?

## Definition

Phishing is a cybercrime where attackers attempt to steal sensitive information, such as login credentials or financial details, by disguising themselves as a trustworthy entity.

## Motivation

Attackers often use phishing to gain access to your accounts, commit identity theft, or spread malware.


# Types of Phishing Attacks

1 **Email Phishing**

Attackers impersonate legitimate organizations through emails to deceive you into revealing sensitive information.

2 **SMS Phishing (Smishing)**

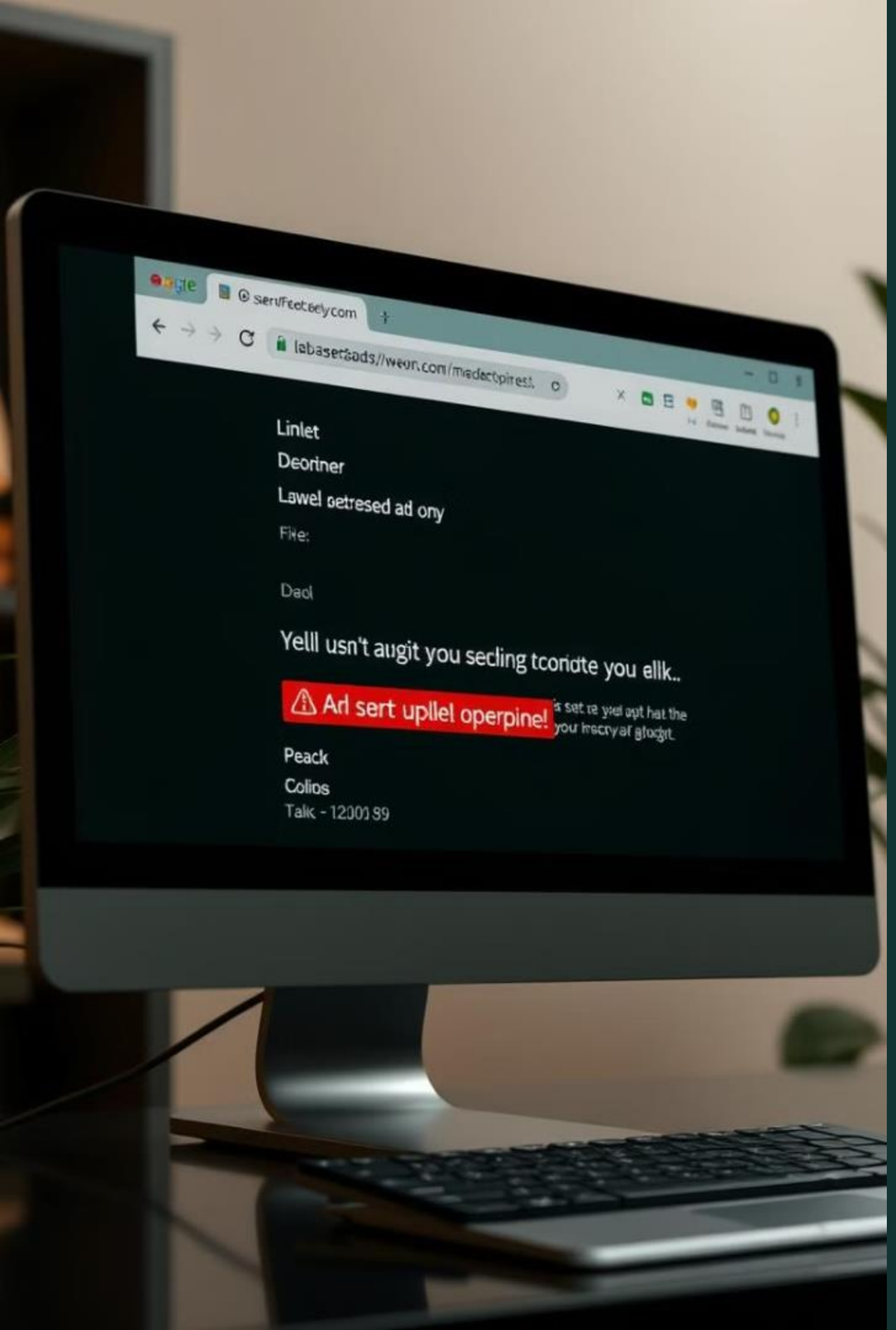
Attackers send fraudulent text messages to trick you into clicking malicious links or providing personal details.

3 **Website Phishing**

Attackers create fake websites that resemble legitimate ones to steal login credentials or credit card information.

4 **Social Media Phishing**

Attackers use social media platforms to spread fake links or messages to obtain personal information from unsuspecting users.




# Identifying Phishing Emails

## Suspicious Sender

Check the sender's email address for misspellings, unusual domains, or unfamiliar names.

## Fake Links

Hover over links before clicking to reveal the actual destination URL. Be wary of shortened links or links that don't match the expected website.

## Urgency and Scarcity

Phishing emails often create a sense of urgency by claiming immediate action is needed to avoid consequences, such as account suspension.

## Poor Grammar and Spelling

Look for grammatical errors, typos, or inconsistencies in language that might indicate a fake email.


# Spotting Malicious Websites

## Look for the Lock

Verify that the website uses a secure HTTPS connection, indicated by a padlock icon in the address bar and "https" at the beginning of the URL.

## Check for Trust Seals

Legitimate websites often display trust seals from organizations like VeriSign or McAfee.

## Examine Website Design

Be suspicious of websites with poor grammar, outdated design, or excessive pop-ups.

## Trust your Instincts

If a website seems too good to be true or you have any doubts, it's best to err on the side of caution and avoid it.

# Social Engineering Tactics

## Impersonation

Attackers may pretend to be someone you know or trust, such as a colleague, friend, or family member.

1

## Pretexting

Attackers create a believable story to trick you into revealing personal information.

2

## Baiting

Attackers offer enticing rewards, such as free gifts or discounts, to entice you into clicking on malicious links or providing personal details.

3

## Scare Tactics

Attackers use threats or scare tactics, such as claiming your account is compromised, to pressure you into taking action.

4

# Best Practices for Phishing Prevention

1

## Be Cautious with Emails and Links

Be wary of emails from unknown senders or those with suspicious subject lines, and double-check URLs before clicking.

2

## Enable Two-Factor Authentication

This adds an extra layer of security by requiring you to enter a code sent to your phone or email in addition to your password.

3

## Keep Software Updated

Software updates often include security patches that protect against known vulnerabilities.

4

## Use Strong Passwords

Create strong, unique passwords for each of your accounts and avoid reusing passwords across multiple services.

5

## Beware of Social Engineering

Think twice before clicking on links or providing personal information in unsolicited messages or requests.

# Reporting Suspected Phishing Attempts


### Report to Your Organization

Forward the email to your IT department or security team.

### Report to the Phishing Authority

Report suspicious websites or emails to the appropriate authorities, such as the Federal Trade Commission (FTC).

### Report to Social Media Platforms

Report suspicious accounts or posts to the relevant social media platform.

# Implementing Security Awareness Training

1

## Regular Training

Provide employees with ongoing security awareness training to educate them about phishing threats and best practices.

2

## Simulation Exercises

Conduct simulated phishing attacks to test employees' awareness and ability to identify phishing attempts.

3

## Feedback and Improvement

Provide feedback to employees on their performance in simulations and identify areas for improvement.

# Staying Vigilant and Adaptable

1

## Stay Informed

Keep up-to-date on the latest phishing scams and tactics.

2

## Be Critical

Question everything, especially unsolicited requests for personal information.

3

## Trust Your Instincts

If something feels off, it probably is.