Phishing Attacks: Understanding the Threat

Welcome! This presentation aims to equip you with the knowledge and skills to recognize and avoid phishing attacks, a common cyber threat that targets individuals and organizations.

S by Sunidhi Mahato

What is Phishing?

Deceptive Tactics

Phishing is a type of social engineering attack that uses deceptive tactics to trick individuals into revealing sensitive information such as login credentials, credit card details, or personal data.

Impersonation

Attackers often impersonate legitimate organizations or individuals to create a sense of urgency or trust, enticing victims to click on malicious links or open attachments.

Types of Phishing Attacks

1 Email Phishing

The most common type, where attackers send emails disguised as legitimate communications from known sources, prompting victims to click on malicious links or download infected attachments.

2 SMS Phishing (Smishing)

Attackers send text messages that mimic legitimate communications from banks, retailers, or service providers, attempting to trick victims into revealing personal information or clicking on malicious links.

3 Website Phishing

Attackers create fake websites that closely resemble legitimate websites, tricking victims into entering their credentials or personal information on the fake site.

Recognizing Phishing Attacks

Suspicious Sender

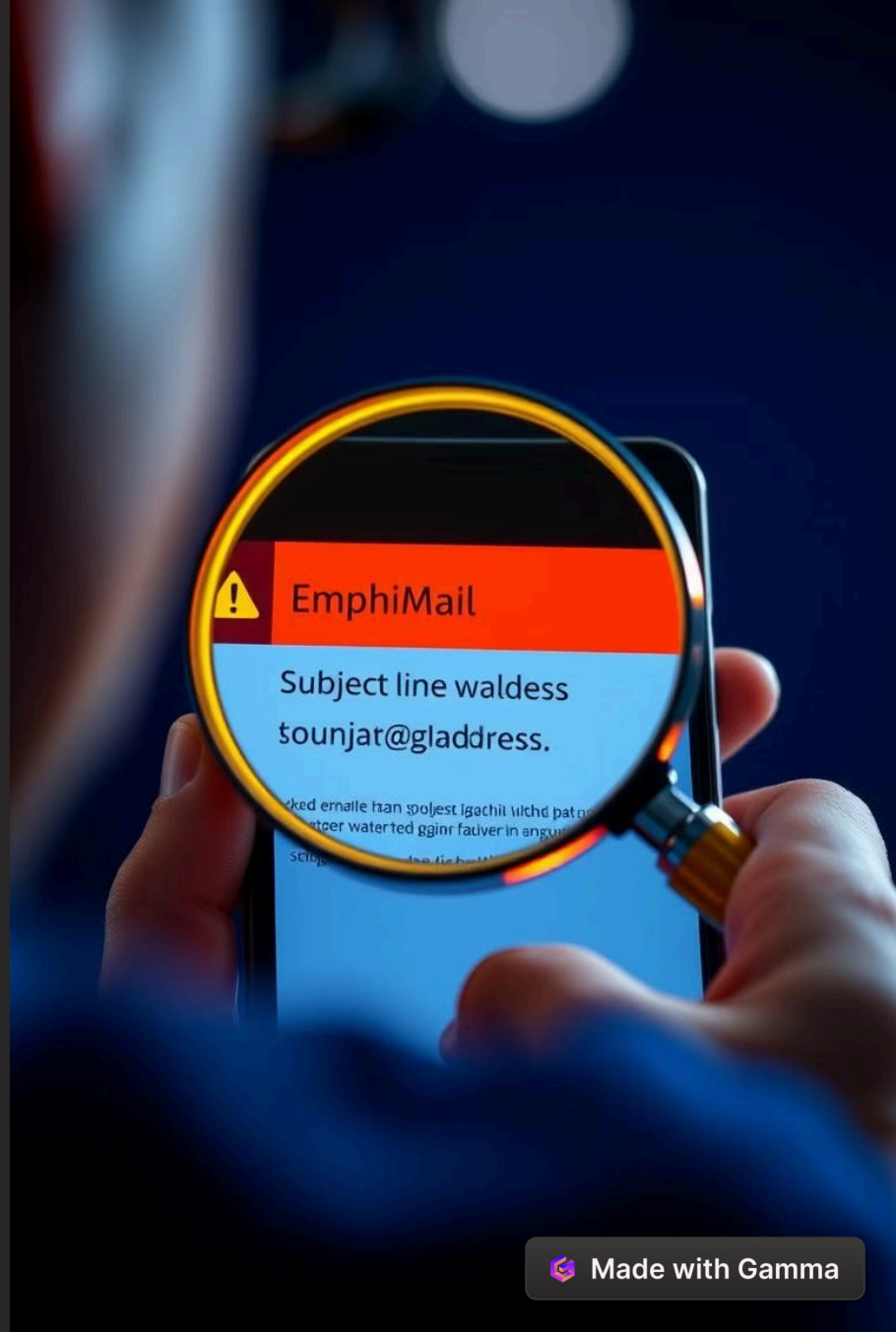
Check the sender's email address or phone number for any misspellings or inconsistencies. Legitimate organizations have consistent branding and communication practices.

Urgent Requests

Be wary of emails or messages that create a sense of urgency, pressuring you to take immediate action. Legitimate organizations rarely use threats or ultimatums.

Suspicious Links

Hover over any links in emails or messages to see the actual URL. If it doesn't match the expected domain name, don't click on it. Legitimate links should match the organization or individual's official website.



Social Engineering Tactics

Impersonation

Attackers may impersonate colleagues, supervisors, or trusted individuals to gain access to information or systems.

Urgency

They create a sense of urgency or fear to pressure victims into making hasty decisions or revealing sensitive information.

Trust

Attackers often exploit trust and relationships to manipulate victims into complying with their requests.

Protecting Yourself from Phishing

1

Be Vigilant

Always be aware of your surroundings and the information you're sharing online. Treat any suspicious emails or messages with caution.

2

Verify Information

If you receive an unexpected email or message requesting personal information, always verify it with the organization or individual in question through a known and trusted channel.

3

Use Strong Passwords

Create strong and unique passwords for all your online accounts. Avoid using the same password for multiple accounts. Use a password manager to store your passwords securely.

Reporting Phishing Attempts

1

Forward Suspicious Emails

Forward any suspicious emails to your IT security team or the appropriate authority for investigation and action.

2

Report Phishing Websites

If you encounter a website that appears suspicious, report it to the website's administrators or the relevant authorities.

3

Stay Informed

Stay informed about the latest phishing scams and tactics by reading security updates, articles, and participating in security awareness training.

Key Takeaways

By remaining vigilant, verifying information, and following these simple steps, you can protect yourself and your organization from phishing attacks. Stay aware, report suspicious activity, and contribute to creating a safer online environment.