



# Introduction to Phishing Attacks

Phishing is a type of cyber attack where criminals use deceptive emails, websites, or messages to trick victims into revealing sensitive information or performing actions that compromise their security. This presentation will explore the tactics used in phishing attacks and provide strategies to recognize and prevent them.



by Adit Vats

# Understanding Phishing Tactics

## 1 Spoofing

Phishers create fake emails or websites that appear to be from legitimate sources, like banks or companies, to lure victims.

## 2 Urgency and Fear

Phishing messages often create a sense of urgency or fear to pressure victims into taking immediate action.

## 3 Social Engineering

Phishers exploit human psychology and rely on tricks to manipulate victims into revealing sensitive information.



### Spear Phishing

Attackers target a specific business or individual and tailor the e-mails to their targets.



### Smishing

Text messages sent to get a user to reveal information via response or link.



# Recognizing Phishing Emails

## Red Flags

Suspicious sender email address, poor grammar, generic greetings, and urgent calls to action.

## Verification Tips

Hover over links to check the URL, and contact the sender through a known, trusted channel.

## Reporting Phishing

Forward suspicious emails to the proper authorities and your organization's security team.

# Identifying Malicious Websites

## Fake Websites

Phishing sites often mimic legitimate websites to steal login credentials or financial information.

## Suspicious URLs

Be wary of URLs with misspellings, strange characters, or that don't match the website's branding.

## Unsecured Connections

Phishing sites may use HTTP instead of the secure HTTPS protocol, putting your data at risk.

## Unusual Requests

Legitimate sites won't ask you to enter sensitive information without a clear reason.

## Engineering Tactics to W

ed flags can help you avoid beco



You  
a.  
Your emotions  
are heightened.



You're receiving help  
you didn't ask for.

# Protecting Against Social Engineering

1

## Impersonation

Phishers may pretend to be a trusted authority figure to manipulate victims.

2

## Baiting

Leaving behind USB drives or other devices containing malware as bait.

3

## Tailgating

Phishers may follow an employee into a restricted area by piggybacking on their access.

# Best Practices for Avoiding Phishing



## **User Education**

Train employees to recognize and report phishing attempts.



## **Multi-Factor Authentication**

Require additional verification steps beyond just a username and password.



## **Email Filtering**

Use spam filters and other email security measures to block phishing messages.



## **Website Monitoring**

Continuously scan for and block any lookalike or malicious websites.





# Reporting and Responding to Phishing

1

## Identify

Recognize a phishing attempt and gather relevant information.

2

## Report

Notify your organization's security team and the appropriate authorities.

3

## Respond

Implement incident response procedures to mitigate the impact and secure systems.

# Phishing Attack

**1** **2**

**W: Please Update Payment Card Information Immediately**

From: John Doe <john.doe@microsoft.com> **3**

Hi Jane,

Please see below conversation with your CEO, Mike Smith.

As stated in the original email, you need to update your payment card information by EoP today or else all your Microsoft accounts will be deactivated.

Follow link below or open the attachment to do so:

<https://bit.ly/jskdfu&xhC37> **4**

---

From: Mike Smith <mike@company.com> **5**

To: John Doe <john.doe@microsoft.com>

**Subject: Please Update Payment Card Information Immediately**

Hi John,

Sorry that we have not updated the payment card information, we need to do this ASAP! **6**

Jim about to go into a meeting, but if you email our Receptionist, Jane, she will be able to update the payment information.

**7** **Attachment:** Microsoft\_Invoice72638.pdf

**2** Falsified Forwarding of Email

**3** Urgent Call to Action

**4** Fake URL or URL Hijacking

**6** Different

**7** Strange

**7** Malicious

**4** Short URL to Hide Malicious Link

## Conclusion and Key Takeaways

In conclusion, phishing attacks are a persistent and evolving threat that require ongoing vigilance and a multilayered security approach. By understanding the tactics used, recognizing the warning signs, and implementing best practices, organizations and individuals can better protect themselves against the devastating consequences of phishing.