

Phishing Assessment

Module 1.1: Introduction to Phishing

Table of Contents

1. Phishing Overview
2. Phishing Common Tactics and Techniques
3. Why is Phishing Dangerous?

1. Phishing Overview

PAST

Phishing Overview

Module 1.1
Introduction to Phishing

Phishing is a form of cyber attack where attackers impersonate legitimate organizations or individuals to trick users into divulging sensitive information such as usernames, passwords, or credit card details.



Page 3 of 8

Phishing is one of the most common forms of cyber-attack, where attackers impersonate legitimate entities to deceive individuals into revealing sensitive information. These attackers craft emails, text messages, or websites that appear to come from trusted sources, such as banks, e-commerce platforms, or government agencies.

As phishing attacks have evolved, so do its methods. Phishing can happen in many different ways, including email, voice calls, websites, text messages, instant messaging, collaboration apps, and social media.

2. Phishing Common Tactics and Techniques

PAST

Phishing Common Tactics and Techniques

Module 1.1
Introduction to Phishing

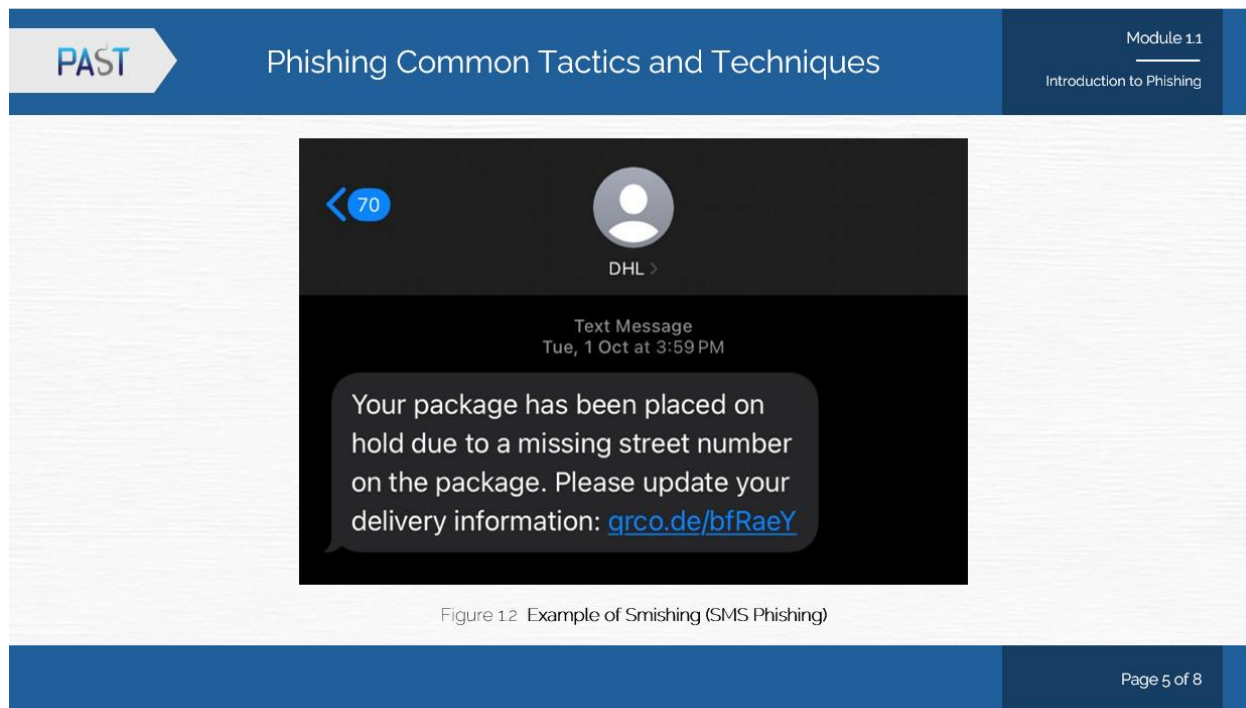
The screenshot shows an email interface. At the top, it says 'Password Expiring Soon'. Below that, the sender is 'IT Department - Mail Helpdesk <cycle2@iilac.plala.or.jp>' and the recipient is 'To: Roger Grimes'. There are four colored squares (red, green, blue, yellow) in a 2x2 grid. Below them, it says 'OFFICE MAINTENANCE'. Then, 'Hello User,'. Followed by 'The current password for your account expires Today.' and 'To keep using current password check below'. There is a blue button that says 'Keep same Password'. At the bottom, a note says 'NOTE: Further messages may be delayed if any of the above actions are not performed.'

Figure 11 Example of Email Phishing

Page 4 of 8

In figure 1.1, is an example of phishing email, the common type of phishing attacks.

The attacker pretends to be an IT department, claiming that your account password is about to expire. They provide a link to 'Keep the same password,' but this link actually leads to a fake website designed to steal your login credentials. The email mimics a legitimate message to create a sense of urgency, prompting the recipient to act without thinking.




In figure 1.2, Example of Smishing (SMS phishing)

The message claims to be from a delivery service, informing the recipient that their package is on hold due to a missing street number. The message includes a link to 'update delivery information,' but just like with email phishing, this link leads to a malicious website. Attackers often use smishing to exploit people's trust in quick, urgent messages on their phones.

PAST

Phishing Common Tactics and Techniques

Module 1.1
Introduction to Phishing

 <p>Personal Information</p> <ul style="list-style-type: none"> • Name • Date of Birth • Home address 	 <p>Financial Information</p> <ul style="list-style-type: none"> • Bank information • Credit/ Debit card details 	 <p>Login Credentials</p> <ul style="list-style-type: none"> • Email address • Username • Password 	 <p>Malware Installation</p> <ul style="list-style-type: none"> • Virus • Spyware • Ransomware
---	---	--	--

Page 6 of 8

What are cybercriminals really after when they launch a phishing attack?

Personal Information: Phishing attacks often aim to steal personal data like names, addresses, birthdates, and Social Security numbers, which can be used for identity theft or sold on the dark web.

Financial Information: Many phishing campaigns focus on tricking individuals into providing bank account numbers, credit card details, or online banking login credentials. This information can be used for fraudulent transactions or draining accounts.

Login Credentials: One of the main goals is to capture usernames and passwords, particularly for email, social media, or business accounts. With these credentials, attackers can gain unauthorized access, take over accounts, or launch further attacks.

Installing Malware: Some phishing messages include malicious attachments or links to websites that download malware to the victim's device. This malware may allow attackers to steal data, spy on users (spyware), or encrypt files (ransomware).

3. Why is Phishing Dangerous?



Phishing is a global issue affecting individuals and organizations across all sectors. Its ease of execution and the potential for high rewards make it a favored tactic for cybercriminals.

Financial Loss: Phishing often leads to significant financial damage. Victims may unknowingly hand over banking details or make unauthorized payments.

Data Breaches: One successful phishing attack can compromise an organization's entire network, leading to data breaches where sensitive customer or company information is stolen.

Identity Theft: Phishing can result in identity theft, where the attacker uses stolen information to impersonate the victim, leading to long-term personal and financial consequences.

Reputational Damage: Organizations that fall victim to phishing can suffer reputational damage, as people lose trust in their ability to secure sensitive information.

Summary

Phishing is a constantly evolving threat that targets our trust to gain access to sensitive information. In the following modules, we will delve deeper into real-world phishing examples, how to spot phishing attempts, and the steps you can take to protect yourself and your organization from falling victim to these attacks. Thank you for watching, and stay safe online.

- END -