PHISHING AWARENESS TRAINING

Welcome

In today's digital age, phishing attacks have become an increasingly common threat to individuals and organizations alike. These attacks can lead to sensitive information being compromised, financial loss, and damage to your reputation.

OBJECTIVE

This phishing awareness training is designed to educate you on the dangers of phishing, how to identify phishing attempts, and provide you with the knowledge and skills necessary to protect yourself and your organization from these types of attacks.

IMPORTANCE OF PHISHING AWARENESS:

Phishing awareness is crucial in preventing attacks and protecting sensitive information. By being aware of the tactics used by phishers, you can significantly reduce the risk of falling victim to an attack.

WHAT TO EXPECT

In this training, we will cover the following topics:

1. What is phishing and how does it work?
2. Types of phishing attacks
3. How to identify phishing attempts
4. Prevention strategies and best practices
5. Real-life examples of phishing attacks

By the end of this training, you will be equipped with the knowledge and skills necessary to identify and prevent phishing attacks.

WHAT IS PHISHING AND HOW DOES IT WORK?:

WHAT IS PHISHING?

Phishing is a type of cyber attack where attackers use fake emails, messages, or websites to trick victims into revealing sensitive information such as passwords, credit card numbers, or personal data.

HOW DOES PHISHING WORK?
Phishing attacks typically involve the following steps:

1. RESEARCH: Attackers research their targets to gather information about their interests, habits, and contacts.
2. BAIT: Attackers create a convincing message or email that appears to come from a legitimate source, such as a bank or a popular online service.
3. HOOK: The message or email contains a link, attachment, or prompt that encourages the victim to take action, such as clicking on a link, downloading a file, or providing login credentials.
4. EXPLOIT: If the victim takes the bait, the attacker can gain access to their sensitive information, install malware, or take control of their device.

TYPES OF PHISHING ATTACKS:
There are several types of phishing attacks, including:

SPEAR PHISHING: Targeted attacks against specific individuals or organizations.
WHALING: Targeted attacks against high-level executives or decision-makers.
SMISHING: Phishing attacks via SMS or text messages.
VISHING: Phishing attacks via voice calls.

WHY IS PHISHING EFFECTIVE?
Phishing attacks are often successful because they:

1. Exploit Human Psychology: Attackers use social engineering tactics to create a sense of urgency or fear.
2. Use Convincing Messages: Attackers create messages that appear legitimate and convincing.
3. Take Advantage of Lack of Awareness: Victims may not be aware of phishing tactics or how to identify them.

HOW TO IDENTIFY PHISHING ATTEMPTS:

Phishing attempts can be identified by looking out for certain red flags. Here are some common characteristics of phishing attempts:

1. **URGENT OR THREATENING LANGUAGE**
Be cautious of messages that create a sense of urgency or fear. Phishing attempts often

I. Threaten to cancel your account or subscription
II. Claim that a promotion or offer will expire unless you take immediate action
III. Imply that your sensitive information has been compromised or is at risk

Use intimidating language to prompt you into taking action
Legitimate organizations rarely use threatening language or create artificial urgency. If you're unsure, it's best to verify the message through other channels.

2. **SUSPICIOUS SENDER INFORMATION**

I. Verify the sender's email address to ensure it is legitimate.
II. Look out for misspelled domain names or unusual email addresses.

3**. GENERIC GREETINGS**

Phishing attempts often use generic greetings such as "Dear customer" instead of addressing you by name.

4. **POOR SPELLING AND GRAMMAR**

Legitimate organizations typically have professional communications that are free of errors. Be wary of messages with:

I. Multiple spelling mistakes
II. Grammatical errors
III. Inconsistent formatting
IV. Unprofessional tone

If a message contains numerous errors, it is actually a phishing attempt.

PREVENTION STRATEGIES AND BEST PRACTICES:

To protect yourself from phishing attacks, follow these prevention strategies and best practices:

VERIFICATION

1. Verify sender information: Check the sender's email address to ensure it's legitimate.
2. Verify website authenticity: Check the website's URL and ensure it's secure (https).

PASSWORD MANAGEMENT

1. Use strong passwords: Use unique, complex passwords for all accounts.
2. Use password managers: Consider using a password manager to securely store passwords.
3. Enable two-factor authentication (2FA): Add an extra layer of security to your accounts.

EMAIL PRECAUTIONS

1. Be cautious with links: Avoid clicking on suspicious links or downloading attachments from unfamiliar emails.
2. Use spam filters: Enable spam filters to help block phishing emails.
3. Report suspicious emails: Report suspicious emails to the relevant authorities.

SOFTWARE UPDATES

1. Keep software up-to-date: Regularly update your operating system, browser, and other software to ensure you have the latest security patches.

2. Use antivirus software: Install and regularly update antivirus software to protect against malware.

EDUCATION AND AWARENESS

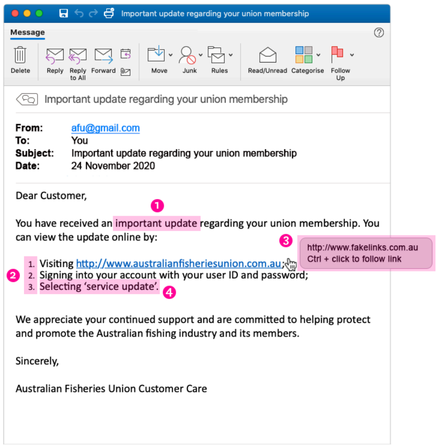
1. Stay informed: Stay up-to-date with the latest phishing tactics and security best practices.
2. Educate others: Share your knowledge with friends, family, and colleagues to help prevent phishing attacks.

ADDITIONAL TIPS

1. Use a secure browser: Use a reputable web browser that has built-in security features.
2. Monitor your accounts: Regularly monitor your bank and credit card statements for suspicious activity.
3. Use a VPN: Consider using a virtual private network (VPN) to encrypt your internet traffic.

By following these prevention strategies and best practices, you can significantly reduce the risk of falling victim to phishing attacks.

REAL-LIFE EXAMPLE OF A PHISHING ATTACK:



Important update regarding your union membership

From: afu@gmail.com
To: You
Subject: Important update regarding your union membership
Date: 24 November 2020

Dear Customer,

You have received an important update regarding your union membership. You can view the update online by:

1. Visiting http://www.australianfisheriesunion.com.au;
2. Signing into your account with your user ID and password;
3. Selecting 'service update'.

http://www.fakelinks.com.au
Ctrl + click to follow link

We appreciate your continued support and are committed to helping protect and promote the Australian fishing industry and its members.

Sincerely,

Australian Fisheries Union Customer Care