PHISHING AWARENESS

Think before you Click

Identifying and protection from phishing attacks, emails, websites and vishing tactics.

Alvan Kipruto Chumba - Cyber Security Intern

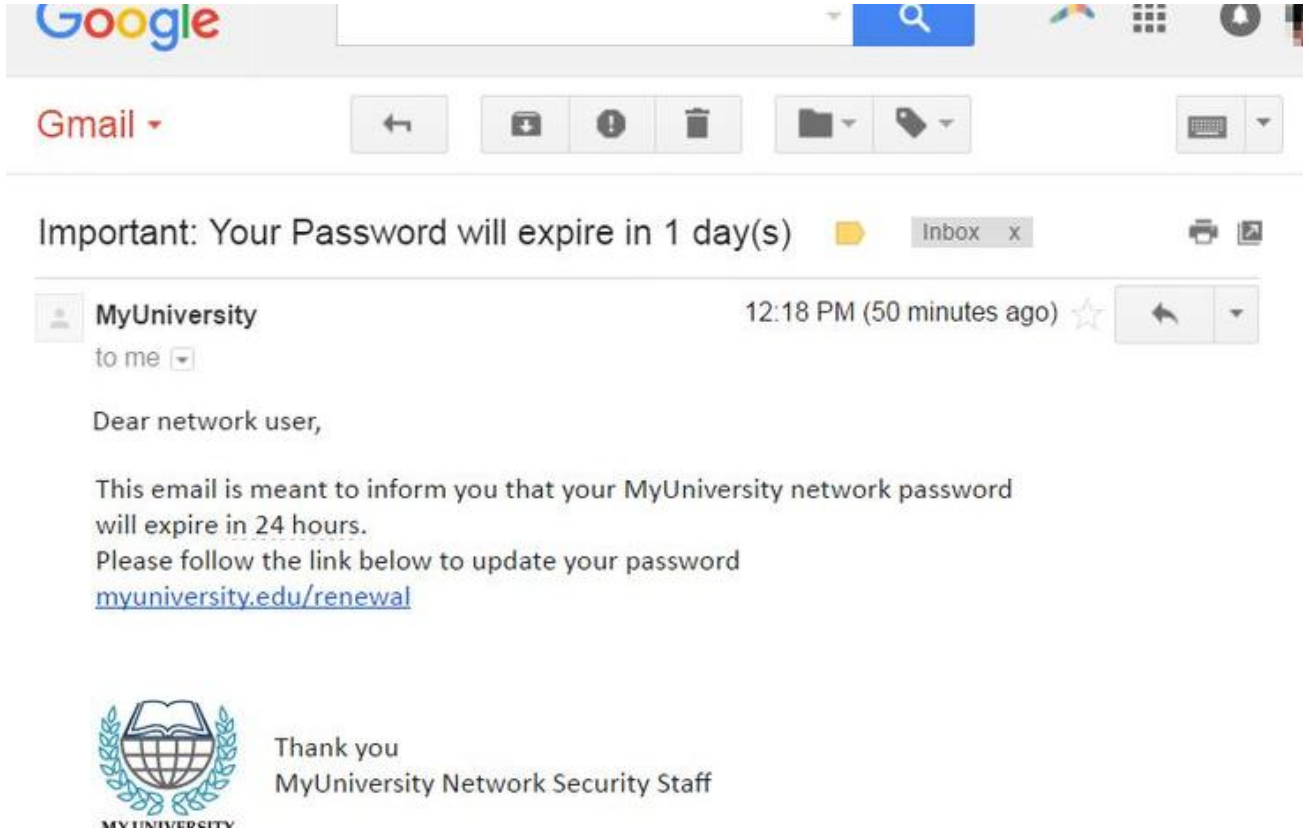
INTRODUCTION

- Phishing is a cyber-attack technique that involves sending fraudulent communications that appear to originate from a reputable source.
- Using fake emails, messages, or fraud websites.

COMMON TYPES OF PHISHING ATTACKS

1. Email Phishing

An attacker impersonates a legitimate entity to trick a user into revealing sensitive information such as login credentials and financial information.

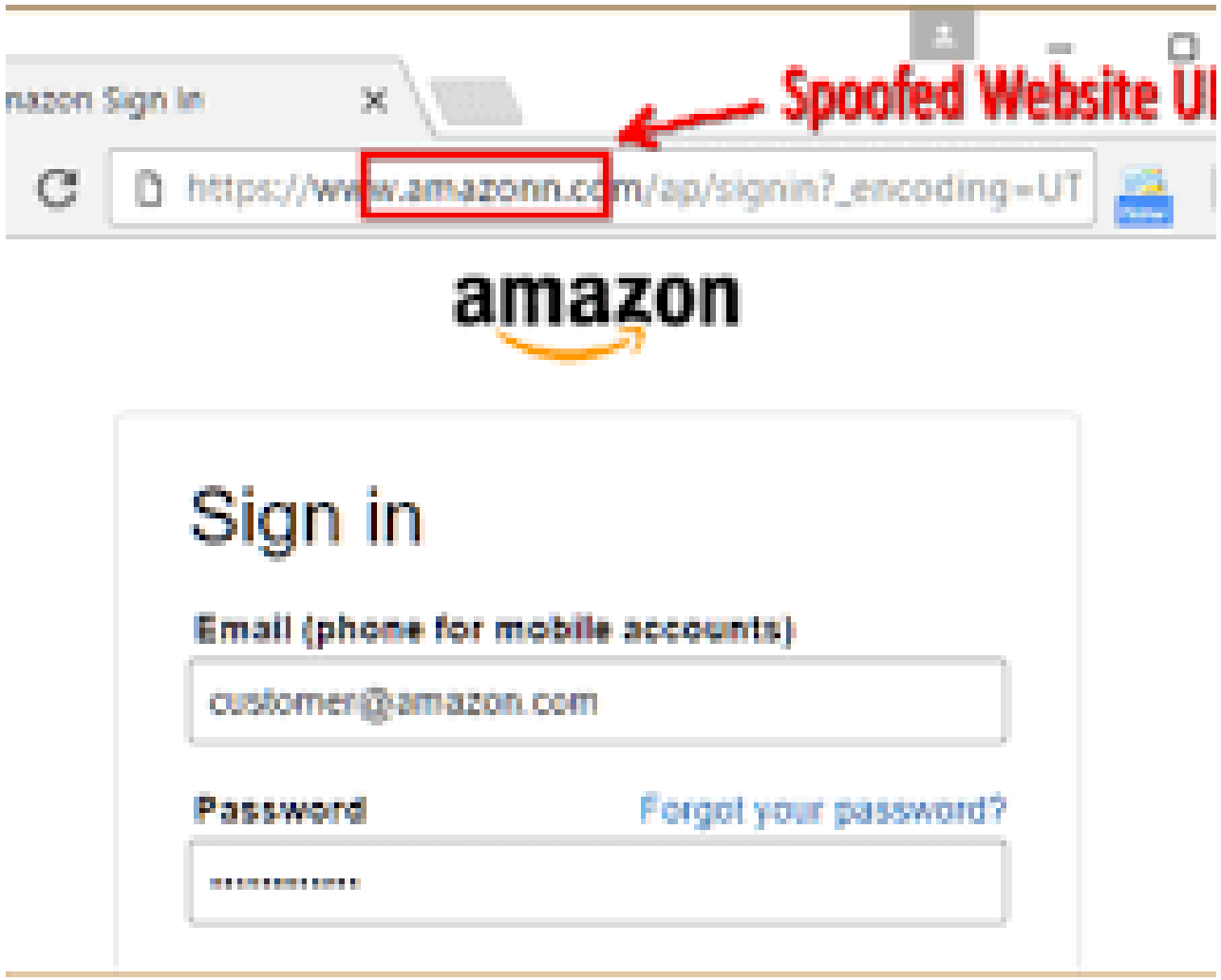


Common Types of Phishing Attacks

2. Website Phishing

The attacker uses techniques such as DNS spoofing, URL manipulation or social engineering to create fake websites that closely resembles a legitimate one in order to trick users into entering sensitive information.

amazon.com = amazonn.com



COMMON TYPES OF PHISHING ATTACKS

3. Smishing(SMS Phishing)

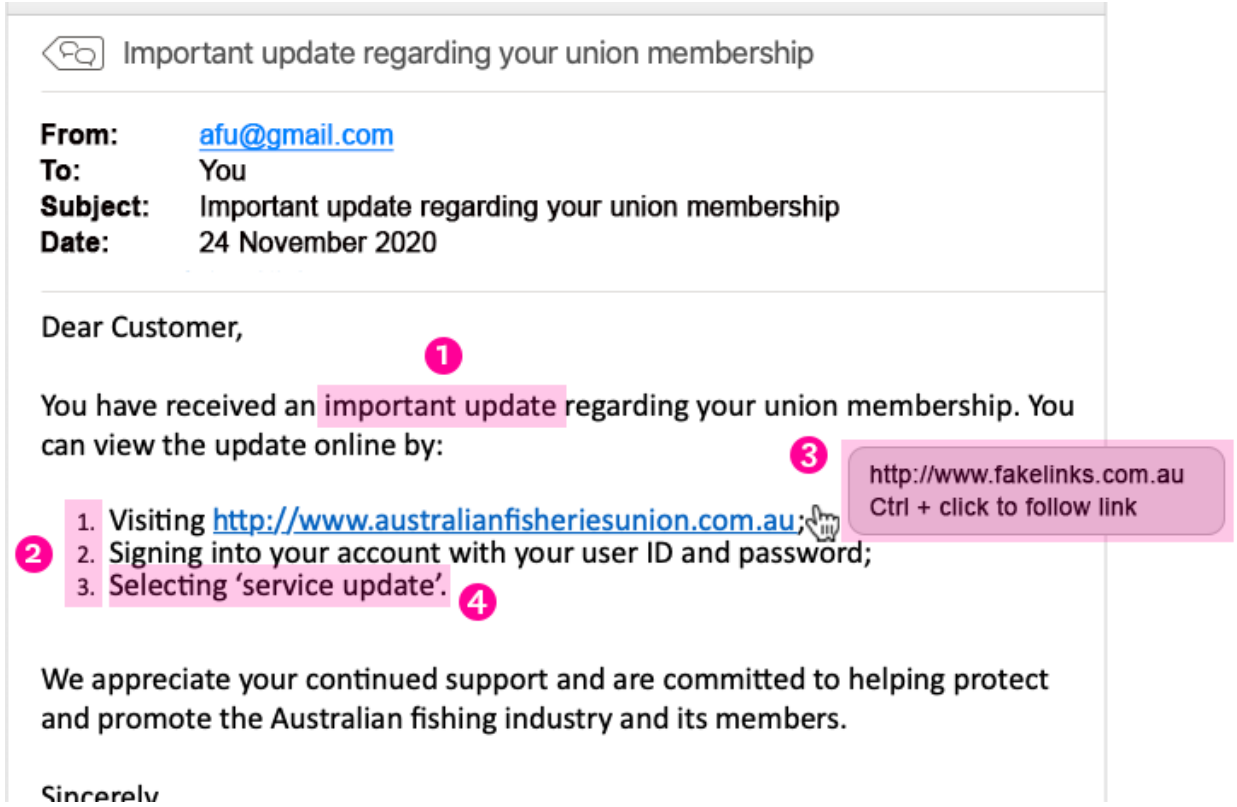
The attack uses fake mobile text messages to trick user to download malware or share personally identifiable information or send money.

COMMON TYPES OF PHISHING ATTACKS

4. Vishing(Voice Phishing)

The attacker spoofs the caller ID, the receiver will view that it originates from a legitimate source such as a bank, government agency or company. As a result the victim will reveal their sensitive information such as personal information, credit card information and bank accounts

DETECTING AN ATTEMPT OF PHISHING EMAIL



- Check the sender's email address
- Examine the links before clicking
- Inspect the email content
- Avoid opening suspicious Attachments

HOW TO PROTECT AGAINST PHISHING ATTACKS

- Creating awareness of the signs and dangers of phishing attacks
- Use spam filters or secure email gateways to monitor incoming emails for unwanted content
- Enable multifactor authentication(MFA), if an employee gives login details to a scammer this measure decreases the ability to gain access
- Do not provide any information to unverified source
- Do not open attachments or links as the may contain malware or executable code that can establish a connection with the attacker.
- Notify the IT department if you receive a phishing email

Thanks!