Phishing Assessment

Module 1.2: Recognizing Phishing Attacks

Table of Contents

1. Different Types of Phishing

Phishing attacks extend far beyond the basic email scams you might be familiar with. They can appear as text messages, phone calls, and even as targeted attacks on high-profile individuals. Let’s start by breaking down the different types of phishing.

The most common form, where attackers send fraudulent emails.

Email Phishing:

The most widespread and common form of phishing, where fraudulent emails attempt to trick users into clicking malicious links or sharing personal information.

Phishing attacks via SMS or messaging services.

Smishing:

Increasing in popularity with the rise of mobile device usage, attackers use fraudulent text messages to steal personal information or trick users into clicking malicious links.

Voice phishing using phone calls.

Vishing:

Phishing conducted over the phone, where attackers impersonate legitimate organizations like banks, tricking victims into revealing sensitive information.

Attackers impersonate senior executives to defraud companies.

BEC (Business Email Compromise):

Targets companies by impersonating executives or employees via email, often leading to wire fraud or data breaches.

Targeted phishing towards specific individuals or organizations.

Spear Phishing:

Highly targeted phishing aimed at specific individuals or organizations, often using personalized information to increase success rates.

Replicating legitimate emails to exploit trust.

Clone Phishing:

Attackers duplicate a legitimate email, modifying links or attachments to be malicious, then resend it to trick the victim into believing it's a follow-up.

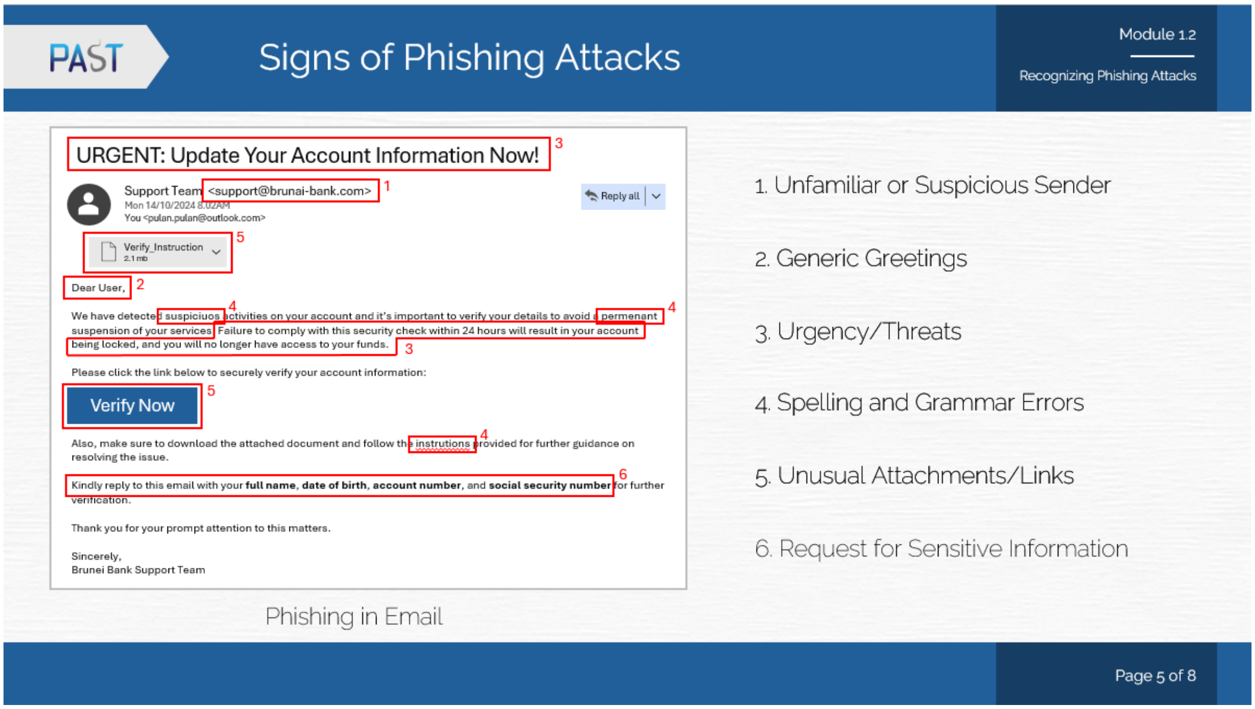
Targeting high-profile individuals like executives

Whaling:

A form of spear phishing that targets high-level executives or important decision-makers in organizations, often seeking financial gain or sensitive corporate data.

2. Signs of Phishing attacks

Phishing in Email



PAST

Signs of Phishing Attacks

Module 1.2

Recognizing Phishing Attacks

URGENT: Update Your Account Information Now!

Support Team <support@brunai-bank.com>
Mon 14/10/2024 8.02AM
You <pulan.pulan@outlook.com>

Verify_Instruction
2.1 mb

Dear User,

We have detected suspiciuos activities on your account and it's important to verify your details to avoid a permenant suspension of your services. Failure to comply with this security check within 24 hours will result in your account being locked, and you will no longer have access to your funds.

Please click the link below to securely verify your account information:

Verify Now

Also, make sure to download the attached document and follow the instrutions provided for further guidance on resolving the issue.

Kindly reply to this email with your **full name**, **date of birth**, **account number**, and **social security number** for further verification.

Thank you for your prompt attention to this matters.

Sincerely,
Brunei Bank Support Team

Phishing in Email

1. Unfamiliar or Suspicious Sender
2. Generic Greetings
3. Urgency/Threats
4. Spelling and Grammar Errors
5. Unusual Attachments/Links
6. Request for Sensitive Information

Page 5 of 8

1. **Unfamiliar or Suspicious Sender**: The email comes from an address you don't recognize or an address that seems similar to a legitimate one but has slight alterations

The email address looks strange, with extra characters or misspellings.

2. **Generic Greetings**: Phishing emails often use general terms like "Dear Customer" or "Dear User" instead of addressing you by name.

"Dear User" instead of addressing the recipient by name.

3. **Urgency or Threats**: Phrases like "Your account has been suspended!" or "Immediate action required!" are used to create a sense of panic and urgency. They try to push you to act without thinking.

The email pressures you to act immediately or face consequences.

4. **Spelling and Grammar Errors**: Legitimate organizations typically proofread their emails. Phishing emails often contain awkward phrasing, spelling mistakes, or grammatical errors.

"Suspiciuos", "permenantly" and "instrutions" have obvious typos.

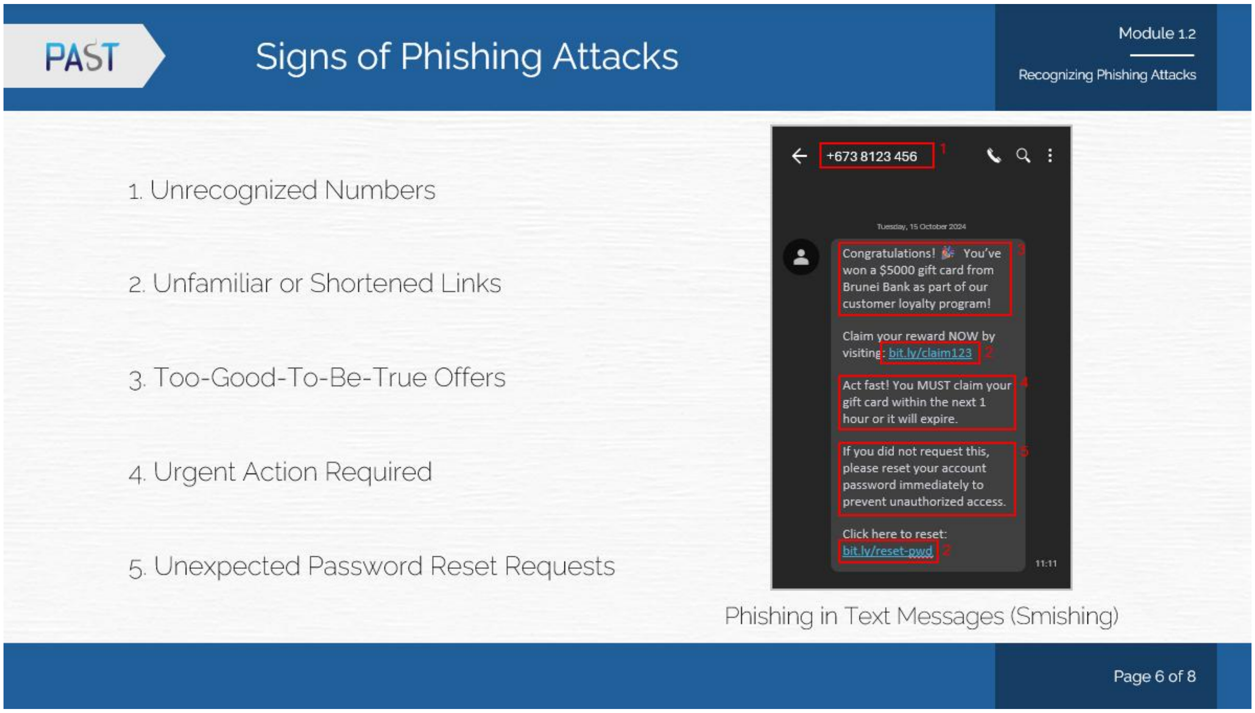
5. **Unusual Attachments or Links**: Unexpected attachments (e.g., ZIP files, EXE files) or links to unfamiliar websites. The link text might look legitimate, but if you hover over it, the URL is unrelated or suspicious.

Suspicious links and an attached file that seems unrelated.

6. **Requests for Sensitive Information**: Phishing emails often ask for sensitive details like login credentials, credit card numbers, or Social Security numbers. Legitimate companies rarely ask for this information via email.

Asking for account details, social security number, and other private data via email.

Phishing in Text Messages



PAST

Signs of Phishing Attacks

Module 1.2

Recognizing Phishing Attacks

1. Unrecognized Numbers
2. Unfamiliar or Shortened Links
3. Too-Good-To-Be-True Offers
4. Urgent Action Required
5. Unexpected Password Reset Requests

+673 8123 456

Tuesday, 15 October 2024

Congratulations! 🎉 You've won a $5000 gift card from Brunei Bank as part of our customer loyalty program!

Claim your reward NOW by visiting: bit.ly/claim123

Act fast! You MUST claim your gift card within the next 1 hour or it will expire.

If you did not request this, please reset your account password immediately to prevent unauthorized access.

Click here to reset: bit.ly/reset-pwd

11:11

Phishing in Text Messages (Smishing)

Page 6 of 8

1. **Unrecognized Numbers**: The message comes from an unfamiliar number or a number that looks suspicious (such as an international number you don't recognize).

The message comes from an unknown or suspiciously formatted number.

2. **Unfamiliar or Shortened Links**: Messages often contain short URLs (e.g., bit.ly, t.co) that hide the real destination. Phishers use these to direct you to malicious websites.

Both links use shortened URLs (bit.ly) that hide the actual destination.

3. **Too-Good-To-Be-True Offers**: Messages that claim you've won a prize, are eligible for a free gift, or some other offer that seems unrealistic.

The offer of a $5000 gift card is enticing but suspiciously generous.

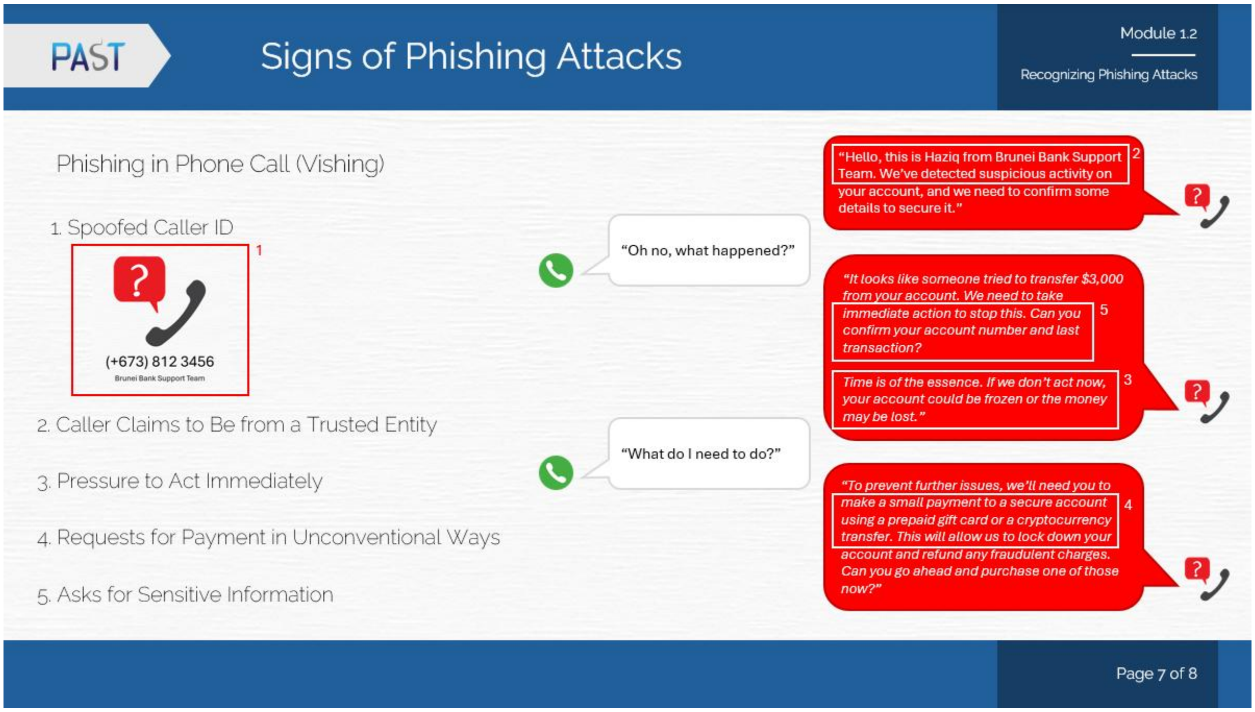
4. **Urgent Action Required**: Messages that say, "You MUST claim your gift card within the next 1 hour or it will expire" or "We need to verify your information immediately" are often used to create panic.

The message pressures the recipient to act within an hour, heightening the urgency.

5. **Unexpected Password Reset Requests**: Phishers may send a text message that appears to be a password reset request. They prompt you to click a link to reset your password.

The mention of a password reset is unexpected and out of context.

Phishing in Phone Call


PAST

Signs of Phishing Attacks

Module 1.2

Recognizing Phishing Attacks

Phishing in Phone Call (Vishing)

1. Spoofed Caller ID

2. Caller Claims to Be from a Trusted Entity

3. Pressure to Act Immediately

4. Requests for Payment in Unconventional Ways

5. Asks for Sensitive Information

"Hello, this is Haziq from Brunei Bank Support Team. We've detected suspicious activity on your account, and we need to confirm some details to secure it." 2

"Oh no, what happened?"

"It looks like someone tried to transfer $3,000 from your account. We need to take immediate action to stop this. Can you confirm your account number and last transaction? 5

Time is of the essence. If we don't act now, your account could be frozen or the money may be lost." 3

"What do I need to do?"

"To prevent further issues, we'll need you to make a small payment to a secure account using a prepaid gift card or a cryptocurrency transfer. This will allow us to lock down your account and refund any fraudulent charges. Can you go ahead and purchase one of those now?" 4

Page 7 of 8

1. Spoofed Caller ID: Attackers can manipulate caller ID to make it look like the call is coming from a legitimate number (like your bank or government agency).

The caller ID displays a number that looks like it's from your bank, making the call appear legitimate.

2. Caller Claims to Be from a Trusted Entity: The caller may claim to be from your bank, a government agency, or tech support, asking for your personal or financial information. They might reference an urgent problem, such as suspicious activity in your account or a tax issue.

The attacker impersonates a representative from your bank's support team.

3. Pressure to Act Immediately: The caller insists you need to act quickly to resolve an issue, whether it's a tax bill, account breach, or unpaid fines. This urgency is meant to rush your decision-making process.

The urgency to act immediately makes you feel rushed and stressed, impairing critical judgment.

4. **Requests for Payment in Unconventional Ways**: The caller may ask you to pay fines or fees via prepaid gift cards, cryptocurrency, or wire transfer methods that are difficult to trace.

Asking for payment through gift cards or cryptocurrency is highly suspicious, as legitimate companies never request these forms of payment.

5. **Asks for Sensitive Information**: They may ask for your account details, Social Security number, or even your password or PIN. This is highly suspicious, especially if the call was unsolicited.

They ask for sensitive details, such as your account number and recent transactions, to “secure” your account.

Summary

Phishing can take many forms, from email phishing to smishing, vishing, BEC, Spear phishing, Clone phishing, Whaling and more. Common signs to look out for include unfamiliar senders, generic greetings, urgency, spelling errors, suspicious links or attachments, and requests for sensitive information. By being aware of these signs, you can better protect yourself from falling victim to phishing attacks.

- END -