

Phishing Assessment

Module 3.2: Spot Smishing

Table of Contents

1. Demonstration

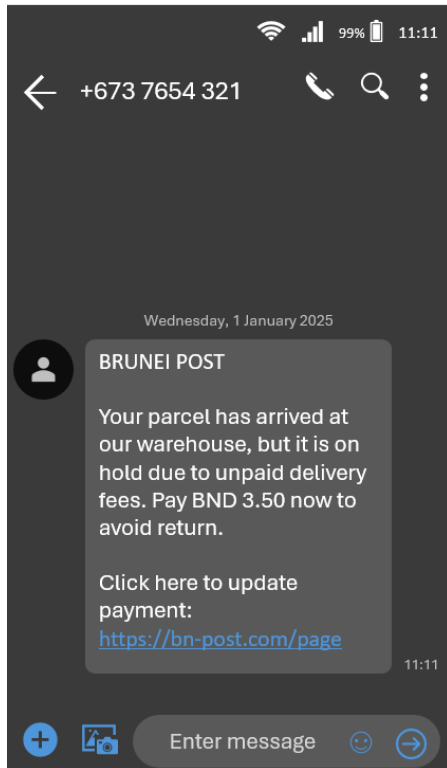
2. Countermeasure

1. Demonstration

Receiving a Suspicious message

Imagine you're checking your phone when you receive a new SMS from an unknown number. The unknown number shows +673 7654 321.

Message contents:



The message claims to be from **Brunei Post** and stated that Your parcel has arrived at their warehouse, but it is on hold due to unpaid delivery fees. You must pay a certain amount of money immediately to avoid being returned and to pay, go to the link.

Key phishing characteristics:

- Unusual Sender

The message comes from a short or random number instead of an official business number. Legitimate organizations usually use verified sender IDs.

- Fake Sense of Urgency

The message pressures you to act immediately to prevent your parcel from being returned. Scammers want you to panic and click the link without thinking.

- Suspicious Link

The link provided is bn-post.com, which is not the official Brunei Post domain. Official government or postal services use verified domains, such as post.gov.bn.

- Request for Payment or Personal Information

Legitimate organizations never ask for card details via SMS.

Clicking on the Phishing Link

The browser opens a page: <https://bn-post.com/page>

Website design:

- Fake Brunei Post branding (logo, colors, and layout).
- Slightly different URL from the real Brunei Post website.
- A fake form asking for login credentials and payment details.

The attackers designed this website to trick users into entering their sensitive information.

Consequences of Entering Credentials

When you enter your credential and financial information to this fake website, here's what will happen:

- The attacker gains your sensitive details such as email, banking, or other.
- Financial loss may occur due to unauthorized transactions.
- The victim's identity may be compromised for further scams.


At this point, your sensitive information is already in the hands of cybercriminals.

2. Countermeasure


PAST

Countermeasure


Module 3.2
Spot Smishing




Disconnect & Secure Your Device



Protect Financial Information



Report the Scam



Watch Out for Further Scams

Page 4 of 5

If you fall for a smishing scam, act quickly to minimize the damage. Here's what you should do:

- **Disconnect & Secure Your Device**

Close the Fake Website and if you entered credentials, assume they are compromised.

- **Protect Your Financial Information**

If you entered credit/debit card details:

- Contact your bank immediately – Report fraudulent activity and request a card replacement.
- Monitor your transactions – Look for any unauthorized payments.

- **Report the Scam**

Inform your bank, police and local cybersecurity agencies, and also to the organization that impersonate them. For this case, report to Brunei Postal Services.

- **Watch Out for Further Scams**

Be wary of follow-up scams – Scammers may contact you pretending to be your bank.

Summary

It is not enough to just implement firewalls and antivirus software. A comprehensive cybersecurity strategy must include a strong focus on the human element. The weakest link is often not the technology, but the user.

By staying alert and recognizing the Phishing signs, you can protect yourself from falling victim to phishing attacks.

- END -