BUREAU OF CUSTOMS
MAKABAGONG ADUANA, MATATAG NA EKONOMIYA

PROFESSIONALISM INTEGRITY ACCOUNTABILITY

MISTG Memo No. 12 -2023

MEMORANDUM

TO : **ALL BOC OFFICIALS AND EMPLOYEES**
ALL OTHERS CONCERNED

BOC-07-02094

FROM : **ATTY. KRIDEN F. BALGOMERA**
OIC - Deputy Commissioner
Management Information System and Technology Group

SUBJECT : **CYBERSECURITY AWARENESS**

DATE : 23 October 2023

This is in reference to the Customs Memorandum Order (CMO) 01-2022 with the subject " Bureau of Customs Information Security Policy" and Proclamation No. 353, (s. 2023) Amending Proclamation No. 2054 (s.2010) by Transferring the Observance of the "Cybersecurity Awareness Month" from September to October of Every Year.

The rise of spoofing and phishing attacks poses a huge risk to the Bureau and its sensitive information. To safeguard our data, privacy, and overall security, all officials and employees must be aware of these threats and take proactive measures to prevent them.

I. Understanding Spoofing and Phishing Attacks

a. **Phishing Attacks**: Phishing is a form of social engineering where attackers attempt to trick individuals into revealing sensitive information or taking harmful actions. Common phishing techniques include email phishing, where the attacker poses as a trusted entity, and spear-phishing, which targets specific individuals.

b. **Spoofing Attacks**: Spoofing occurs when an attacker disguises their identity to appear as someone or something trustworthy. This can include email spoofing, where the sender's address is manipulated to mimic a legitimate source.

i. **Spoofing via display name** - Display name spoofing is a type of email spoofing, in which only the email sender's display name is forged.

Example:
From: **Juan dela Cruz** (malicious@domain.com)
Sent: October 10, 2023
To: pedro.reyes@customs.gov.ph

ii. **Spoofing via look-alike domains** - attackers create domain names that closely resemble legitimate domain names in order to deceive and trick users into believing they are interacting with a trusted entity.

Example:
landbank.com vs. lɑndbɑnk.com
amazon.com vs. amaz0n.com

iii. **Legitimate domain spoofing** - is a much more believable email spoofing example. In this case, the display name and the sender's address are fake. Cybercriminals can do this by taking advantage of Simple Mail Transfer Protocol (SMTP), which is an email protocol used for sending messages.

Example:
From: **Juan dela Cruz** (juan.delacruz@customs.gov.ph)
Sent: October 10, 2023
To: pedro.reyes@customs.gov.ph

II. Recognizing Red Flags

The following are some red flags that may signal a spoofing or phishing attempt:

a. **Unsolicited Emails** - Be cautious of emails, messages, or pop-up windows from unknown or unexpected sources.

b. **Generic Greetings** - Be suspicious of emails or messages that start with generic greetings like "*Dear User*" or "*Hello Customer.*" Legitimate organizations usually address you by your name.

MASTER COPY

c. **Urgent Language** - Attackers often use urgency to pressure victims into making hasty decisions. Watch for phrases like "*immediate action required*" or "*your account will be suspended*."

d. **Suspicious Links** - Hover over hyperlinks without clicking to see the actual destination URL. Look for misspelled domains or unusual website addresses. The most commonly used character is "**ɑ**" to replace the letter "**a**", the number "**0**" to replace the capital letter "**O**", and the uppercase i "**I**" to replace the lowercase L "**l**".

e. **Attachment Caution** - Do not open attachments from unverified sources. Malicious attachments can contain malware.

f. **Requests for Personal Information** - Legitimate organizations will never ask for sensitive information like passwords, Social Security numbers, or credit card details via email.

III. Protecting Yourself and the Bureau of Customs

a. **Report Suspicious Activity** - If you receive an email or message that seems suspicious, report it to the Management Information System and Technology Group (MISTG) immediately.

b. **Verify** - When in doubt, contact the supposed sender through official channels (not using contact information from the suspicious message) to verify the request's authenticity.

c. **Educate Yourself** - Stay informed about evolving cyber threats and best practices for online security.

d. **Security Software** - Ensure your computer has updated antivirus and anti-malware software.

e. **Two-Factor Authentication (2FA)** - Enable 2FA wherever possible to add an extra layer of security to your accounts.

Protecting our organization against spoofing and phishing attacks is a collective responsibility. By increasing our awareness and vigilance, we can significantly reduce the risks associated with these threats. Remember that every official and employee plays a crucial role in maintaining our digital security.

For any urgent concerns, you may coordinate with our MISTG Site Managers on your respective ports or through our MISTG Helpdesk through email address mistg-helpdesk@customs.gov.ph or landline (02) 8705-6034.

For information and strict compliance.