How to Identify Email Spoofed Phishing Attacks

It is very easy for email scammers to forge the email address of someone that you would normally trust. It's called email spoofing and it can make the job of spotting scams more difficult. This has happened to the State Officers, and we need everyone to be aware of this and take care not to be fooled by these attempts.

Email spoofing is a form of impersonation where a scammer creates an email message with a forged sender address in hopes of deceiving the recipient into thinking the email originated from someone other than the actual source. Scammers will use email spoofing to help disguise themselves as someone they know or trust, in order to trick users into performing some type of action. Scammers use this method of deception because they know a person is more likely to engage with the content of the email if they are familiar with who sent the message.

There are various types of email spoofing.

Display name spoofing portrays a display name of the person being impersonated while leaving the actual sending email address intact.

Example 1: "John Doe" <jd23950@gmail.com>
Example 2: "John Doe" <johndoe.kofc@scammersite.net>

Scammers can also spoof the entire email address as well or just the domain name, i.e., what follows the @ symbol. In the example that recently happened to our officers, they spoofed the entire email address, using "president.executive1957@gmail.com" instead of the real email address.

There are a few things you can do to help determine if an email is coming from a spoofed email address or is otherwise malicious.

Check the Email Header Information

The email headers contain a significant amount of tracking information showing where the message has traveled across the Internet. Different email programs display these headers in different ways, so be sure to check to make sure that you see the actual email address before taking any action. If necessary, verify that the sender is who they appear to be by calling them, rather than replying by email.

The following tips can help identify a spoofed message in the email headers.

- **Identify that the 'From' email address matches the display name.** The from address may look legitimate at first glance, but a closer look in the email headers may reveal that the email address associated with the display name is actually coming from someone else.
- **Make sure the 'Reply-To' header matches the source.** This is typically hidden from the recipient when receiving the message and is often overlooked when responding to the message. If the reply-to address does not match the sender or the site that they claim to be representing, there is a good chance that it is forged.
- **Find where the 'Return-Path' goes.** This identifies where the message originated from. While it is possible to forge the Return-path in a message header, it is not done with great frequency.

Question the Content of the Message

Sometimes the best defense against phishing is to trust your best instincts. If you receive a message from a supposed known source that appears out of the ordinary, it should raise a red flag. When receiving an unsolicited message, users should always question the content of the message, especially if the message is requesting gift cards, information or directing the user to click on links or open attachments.

Before responding to any questionable message, perform the following tasks to ensure the message is reliable.

- **Ask yourself:**
  - Was I expecting this message?
  - Does this email make sense?
  - Am I being pushed to act quickly?
- **Examine the email and look for:**
  - Sense of urgency
  - Unsolicited request of personal information or money
  - Generic greeting/signature
  - Unfamiliar links or attachments
- **Contact the sender of the message through a trusted channel**
  - If the email appears legitimate, but still seems suspicious, it is best to contact the supposed sender through a trusted phone number or open a new outgoing email message using their real email address found in the current directory. Do not reply to the message in question.

It is important to always remain vigilant when receiving mail whether it is from an unknown sender, someone you are close with, or an organization you are familiar with. Cyber scammers are always looking for new ways to exploit individuals for their own personal gain.