Mitigating Email Threats

Phishing emails continue to be one of the most common initial attack vectors employed by for malware delivery and credential harvesting. Attacking the human element—considered the weakest component in every network—continues to be extremely effective. To infect a system, the attacker simply has to persuade a user to click on a link or open an attachment. The good news is that there are many indicators that you can use to quickly identify a phishing email. The best defense against these attacks is to become an educated and cautious user and familiarize yourself with the most common elements of a phishing attack. Below are some common indicators of a phishing email.

- **<u>Suspicious Sender's Address</u> -** Pay attention to the sender's email address. It may imitate a legitimate business. With only few characters altered or omitted, cybercriminals will often use an email address that closely resembles one from a reputable company.

- **<u>Generic Greetings and Signature</u>** - Both a generic greeting - such as "Dear Valued Customer" or "Sir/Ma'am"- and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.

- **<u>Spoofed hyperlinks</u>** - Hover your cursor over any links in the body of the email. The links not matching the text that appears when hovering over them should raise a red flag. Additionally, the use of a URL shortening service to hide the true destination of the link should also raise a red flag.

- **<u>Spelling and Layout</u>** - Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.

- **<u>Suspicious Attachments</u>** - An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.