7 WAYS TO SPOT PHISHING EMAIL:

However, phishing emails often have common characteristics; they are frequently constructed to trigger emotions such as curiosity, sympathy, fear and greed. If a workforce is advised of these characteristics – and told what action to take when a threat is suspected – the time invested in training a workforce in how to spot a phishing email can thwart attacks and network infiltration by the attacker.

1. Emails Demanding Urgent Action

Emails threatening a negative consequence, or a loss of opportunity unless urgent action is taken, are often phishing emails. Attackers often use this approach to rush recipients into action before they have had the opportunity to study the email for potential flaws or inconsistencies.

2. Emails with Bad Grammar and Spelling Mistakes

Another way to spot phishing is bad grammar and spelling mistakes. Many companies apply spell-checking tools to outgoing emails by default to ensure their emails are grammatically correct. Those who use browser-based email clients apply autocorrect or highlight features on web browsers.

3. Emails with an Unfamiliar Greeting or Salutation

Emails exchanged between work colleagues usually have an informal salutation. Those that start "Dear," or contain phrases not normally used in informal conversation, are from sources unfamiliar with the style of office interaction used in your business and should arouse suspicion.

7 WAYS TO SPOT PHISHING EMAIL:

4. **Inconsistencies in Email Addresses, Links & Domain Names**

Another way how to spot phishing is by finding inconsistencies in email addresses, links and domain names. Does the email originate from an organization that is corresponded with often? If so, check the sender's address against previous emails from the same organization. Look to see if a link is legitimate by hovering the mouse pointer over the link to see what pops up. If an email allegedly originates from (say) Google, but the domain name reads something else, report the email as a phishing attack.

5. **Suspicious Attachments**

Most work-related file sharing now takes place via collaboration tools such as SharePoint, OneDrive or Dropbox. Therefore internal emails with attachments should always be treated suspiciously – especially if they have an unfamiliar extension or one commonly associated with malware (.zip, .exe, .scr, etc.).

- 6. **Emails Requesting Login Credentials, Payment Information or Sensitive Data**

Emails originating from an unexpected or unfamiliar sender that requests login credentials, payment information or other sensitive data should always be treated with caution. Spear phishers can forge login pages to look similar to the real thing and send an email containing a link that directs the recipient to the fake page. Whenever a recipient is redirected to a login page or told a payment is due, they should refrain from inputting information unless they are 100% certain the email is legitimate

- **7. Too Good to Be True Emails**

Too good to be true emails are those which incentivize the recipient to click on a link or open an attachment by claiming there will be a reward of some nature. If the sender of the email is unfamiliar or the recipient did not initiate the contact, the likelihood is this is a phishing email.