

Stay Alert: Increased Phishing Attacks Targeting PHL Email Accounts

As Philadelphia serves as a major hub for national and global events, cybercriminals are increasing their phishing efforts against organizations such as PHL/PNE Airport. The Information Security team is observing a significant rise in suspicious emails and hacking attempts targeting employee email accounts and data.

Please remain vigilant and follow these important security practices:

- Use the **phishing alert button** if you are **ever** in doubt about an email, attachment, weblink, meeting request, Teams call, etc.



- Hover before you click on a weblink - Pretend your mouse is a magnifying glass and you are reading the fine print on a postage stamp
- NEVER click on suspicious, unexpected attachments, or URLs
- Be cautious of emails that create urgency, request credentials, or ask for unusual actions.
- Always Be Skeptical and on high alert for every email, all the time.

Think Before You Click

YOU and the **PAB** are the most important defenses against phishing

If you receive a suspicious email, **use the Phish Alert Button immediately** to report it to the Information Security team. Reporting phishing attempts helps us quickly identify threats and protect the organization from potential compromise.