Philadelphia International Airport
Northeast Philadelphia Airport

How to Spot a Phish 

Phishing attacks remain one of the most common cybersecurity threats today. According to the Federal Bureau of Investigation's Internet Crime Complaint Center, phishing is consistently the **most reported cybercrime**, with hundreds of thousands of incidents reported each year. These attacks are increasing in frequency as attackers use automation and new technologies to scale their campaigns.

The rise of tools powered by Large Language Models (LLMs) has also made phishing easier to create. In the past, phishing emails were often easy to identify due to poor grammar or awkward wording. Today, attackers can use AI tools to generate **highly convincing messages** that mimic legitimate companies, making them harder to detect.

Here are a few common signs of phishing:

- **Urgent language** – Messages claiming your account will be locked or requiring immediate action.
- **Suspicious sender addresses** – Slight misspellings or unusual domains.
- **Unexpected links or attachments** – Especially if you were not expecting the message.
- **Requests for sensitive information** – Legitimate organizations rarely ask for passwords or personal data via email.

If you suspect a phishing email, **do not click links or open attachments**. Report it to the information security team using the PAB button.

For any questions or further guidance on email security, feel free to reach out to the **Infosec Team** at Infosec@phl.org. Thank you for keeping PHL and PNE secure!