Philadelphia International Airport
Northeast Philadelphia Airport

New Year, New Scam: The latest Scam and How to Protect Yourself

Goodbye 2025, and hello 2026! As we welcome a new year, we carry forward the achievements earned from the past while embracing the future with gratitude. To all of those who have continued to do their part in helping us protect PHL and PNE, thank you!

With a new year comes new challenges and an increased need for awareness. Cybercriminals and scammers are continually evolving, always seeking new methods to steal your information, take your money, or cause harm to you and those around you. One of those methods they use is deepfake.

Deepfake is a form of artificial intelligence (AI) that creates hyper-realistic images, videos, and audio. This technology has been around since 2017 and has continuously improved and spread, thanks in part to social media. Many of us, with untrained eyes, might encounter a seemingly harmless video of a celebrity doing or saying something bizarre and mistakenly believe it's real. Now, imagine that scenario, but instead of a celebrity, it's someone you know, calling or even Face Timing you, asking you to wire money or provide personal information. As the technology behind deepfakes becomes more accessible, the potential for misuse grows, making it crucial for everyone to stay informed about these threats. Below are tips and way you can protect yourself and those around you from deepfake scams:

- Avoid answering phone calls or FaceTime requests from unknown numbers or those you do not recognize. If the call is important, the caller will often leave a voicemail. If you receive a voicemail from someone you know, question why they are calling from an unfamiliar number. If you have their contact number, call them back using the number you have saved and verified.
- If you do answer an unknown call, be skeptical of everything the caller says. Do not provide any personal information. Instead, ask them specific questions that only the real person would know, such as details about a shared experience, an inside joke, or a recent event you both attended. Consider questions that a scammer would not easily find online or through social media. You can also establish a safe phrase to

use with family members, friends, and colleagues for added security.

- **Do not click on or download anything that a suspected scammer sends**, whether it's via text or email.
- Always seek a second opinion and use a secondary form of verification to confirm the caller's identity. Ask caller to meet in person or to switch to a different communication method that is harder to fake such as a call or message from their actual social media account or from a verified number.
- Scammers will often time create scenario and present a sense of urgency to manipulate victim, do not fall for that and **never wire large sum of money over**.

As we continue to build on our existing knowledge and refine our cyber hygiene practices, cybercriminals are simultaneously devising new and sophisticated scams. The most effective way to protect yourself and your loved ones is through knowledge and increased awareness. With that, thank you, and may you continue to do your part in keeping PHL and PNE cybersecure.

Here's a recap of 2025's email security efforts:

- **Total Emails Reported via PAB**: 1,784
  - **Threats/Phishing**: 691 emails
  - **Spam**: 542 emails
  - **Clean**: 551 emails