Philadelphia International Airport
Northeast Philadelphia Airport

Protecting PHL and PNE from Cyber Threats

Protecting our digital environment is a shared responsibility. As cyber threats grow more sophisticated, staying informed and vigilant is essential. This newsletter highlights current risks and practical steps users can take to help keep PHL and PNE secure.

Cybersecurity remains a critical priority as threats continue to evolve. Attackers are leveraging new technologies and tactics to target organizations, making user awareness and strong security practices more important than ever.

AI-Powered Attacks and Supply Chain Vulnerabilities
Artificial intelligence is rapidly transforming the cybersecurity threat landscape. Threat actors are using AI to create highly convincing phishing emails, messages, and even deepfake audio or video that closely mimic trusted individuals or organizations. These techniques increase the likelihood of successful social engineering and make attacks harder to detect. AI is also being used to automate malware and enable adaptive attacks that change behavior in real time to evade security controls.
At the same time, supply chain vulnerabilities continue to pose significant risk. Cybercriminals increasingly target trusted third-party vendors, service providers, or software dependencies as an indirect way to access larger and more secure environments. Global organizations are reporting increased cyber risk driven by AI-enabled attacks and identity-based compromises, as highlighted by the World Economic Forum.
For PHL, this means heightened vigilance is required. Cybercriminals may attempt to spoof internal communications, bypass identity controls, or exploit weaknesses in third-party systems to gain unauthorized access. Strengthening identity security, verifying communications, and maintaining oversight of vendor relationships are critical to reducing risk.

Threat Awareness: Phishing and Account Compromise
Phishing remains one of the most common attack methods used by cybercriminals. These messages often impersonate trusted sources and create a sense of urgency to trick users into acting quickly.

Common indicators of phishing include:

- Requests for passwords or verification codes
- Urgent, threatening, or unexpected language
- Unusual sender addresses, links, or formatting

If a message appears suspicious, do not engage with it. Report the message using the PAB button or forward it to **PAB@phl.org**.

Key Cybersecurity Practices

Strong password hygiene is essential to protecting systems and data. Use unique passwords for each system or application, never share passwords, and use approved password management tools where available to generate and store strong credentials securely.

Remain cautious when receiving unsolicited or unexpected emails, messages, or requests, especially those that prompt immediate action. Always verify requests for sensitive information, credentials, or approvals through a trusted secondary channel. Avoid clicking unknown links or downloading attachments from unfamiliar sources.

The use of AI tools must also be carefully managed. Employees should only use approved AI platforms for work-related tasks and should never enter sensitive, proprietary, or personal information into public or unvetted AI systems. Clear policies and responsible use help prevent data leakage and compliance issues.

Cybersecurity Reminder

- Legitimate support teams will never ask for your password
- Early reporting helps prevent wider impact
- Security controls are most effective when paired with user awareness

Cybersecurity is an ongoing effort that depends on awareness, accountability, and consistent best practices across PHL. Thank you for your continued cooperation and for doing your part to help keep PHL and PNE secure.