PROTECT YOUR MOBILE DEVICES — PROTECT PHL

DEPARTMENT OF AVIATION INFORMATION SECURITY UPDATE

Your Role in Mobile Security

If your device connects to company email, apps, or networks, you must keep it secure. This means using strong authentication; a passcode, fingerprint, or facial recognition to prevent unauthorized access. Never share your work credentials or save passwords in unprotected notes or apps.

Keeping your device software and apps updated is also critical. Hackers exploit vulnerabilities in outdated systems to steal data or install malware. Enable automatic updates whenever possible to ensure your device is protected.

Be mindful of where and how you connect. Public Wi-Fi is convenient but a prime target for cybercriminals, including evil twin attacks, where hackers create fake networks to steal data. Avoid accessing company resources over unsecured networks. If you must connect, verify the legitimacy of the network and refrain from entering sensitive information.

Think Before You Click

Mobile devices are prime targets for phishing and smishing attacks; fraudulent messages that trick you into revealing information. If you receive an unexpected email or text with a link or attachment, don't click until you verify the source. When in doubt, report suspicious messages to the Information Security team.

Only download trusted apps from official app stores; be cautious of app permissions. A seemingly harmless app could collect your contacts, location, or sensitive data without your knowledge.

Lost or Stolen Device? Act Fast!

A misplaced phone or tablet isn't just an inconvenience; it's a security risk. If your work-issued device is lost or stolen, immediately report it to Information Security. If you use a personal device to access company emails or resources, ensure remote tracking and wiping are enabled to safeguard both personal and company data in case of loss or theft.

For security reasons, modifying or jailbreaking any device used for company work is strictly prohibited. These modifications remove built-in security protections and make devices more vulnerable to cyberattacks.

Protect Your Device, Protect Our Company

Mobile security is everyone's responsibility. By securing your device, staying alert, and following best practices, you help protect PHL's data, systems, and operations from cyber threats.