## Small Device, Big Impact: The USB Security Risk

"One of aviation's most overlooked threats isn't mechanical or weather-related—it's **removable USB media**. This category encompasses everything from standard flash drives to external hard drives and portable optical drives (CD/DVD). Across all departments, a single infected device can migrate from office systems to critical operational networks, potentially grounding flights as effectively as a mechanical failure."

Malware doesn't just target systems—it targets people. A "dropped" USB in a parking lot, a "free" giveaway at a conference, or even a personal USB used for alternative projects can all introduce hidden threats. Once plugged into a workstation, malware can:

- Spread through the network, moving from a single device to critical operational systems
- Launch ransomware attacks that lock maintenance or billing systems and disrupt operations
- Steal login credentials, allowing deeper access to sensitive company data

## Best Practices and Recommendations


1. **The "Company-Only" Rule.** Never plug personal USB devices (including cameras, phones, or old thumb drives) into any company-owned computer. Similarly, never use company-issued drives on your home computer. Maintaining a "digital air gap" between your work and personal life is your strongest defense.


2. **Be Cautious with Promotional USB "Swag".** Attending a conference or seminar? Those free USB sticks branded with a vendor's logo are high-risk. They are often mass-produced in facilities with low security and can possibly contain pre-installed malware. If you need the data on them, send it to IT for a professional scan first.

**3. Use Designated Charging Stations.** If possible, avoid charging your phone via your computer's USB port. This creates a data bridge between your mobile device and the corporate network. Use a standard wall outlet if a USB port is your only power source.


**4. Secure Your Workspace.** If you work in a building with public access or frequent visitors, never leave your workstation unlocked or your USB drives lying on your desk. Physical access is the easiest way for an intruder to plant a malicious device.


**5. Report "Lost and Found" Media.** If you find USB media in a hallway, breakroom, or parking lot, **do not plug it in** to see what's on it. Contact the helpdesk or Infosec team immediately. A "lost" drive is often a deliberate test of our security awareness.

## Vigilance is Everyone's Job

Our safety culture doesn't stop at the door. By treating every USB port with the same caution we treat a restricted area, we ensure that our data—and the systems we rely on— remain safe and operational.

**Remember: If you didn't request it, and IT didn't clear it, don't plug it in. If you find a lost USB drive, do not plug it in. Turn it over to IT immediately. They have the tools to inspect it safely without risking the network.**

For any questions or further guidance on USB security, feel free to reach out to the Infosec Team at Infosec@phl.org . Thank you for your continued commitment to the security of PHL and PNE.