CB **CosmicBytez Labs**
Security Awareness Training

QUICK REFERENCE GUIDE

USB & Removable Media Safety Guide

USB drives and removable media are a proven attack vector. From the infamous Stuxnet worm to modern "USB drop" attacks, attackers exploit our curiosity and convenience. A single infected USB device can compromise an entire network.

Key Points

- ✓ Never insert unknown or found USB drives into any computer
- ✓ USB drop attacks are real — attackers leave infected drives in parking lots and lobbies
- ✓ Disable USB autorun/autoplay on all systems
- ✓ Use only company-approved encrypted USB drives for file transfers
- ✓ Scan all removable media with antivirus before opening any files
- ✓ Consider using cloud-based file sharing instead of physical media
- ✓ Report any suspicious USB devices found on premises to security

Action Items

1. Check your computer's autoplay settings and disable autorun for removable media
2. Replace personal USB drives with company-approved encrypted alternatives
3. If you find an unknown USB drive, hand it to IT security — do not plug it in
4. Review and clean out old USB drives, securely wiping sensitive data

Quick Reference

USB Threat Types: Rubber Ducky (keystroke injection), BadUSB (firmware-level attack), data exfiltration, malware delivery.
Safe USB Policy: Company-issued only, encrypted, scanned before use, registered with IT.
Found a USB drive? Do NOT plug it in. Place it in a sealed bag and deliver to IT Security.