

User Manual

Cybersecurity Awareness Project: USB Drop Attack Simulation

Device: Digispark ATTiny85

Introduction

Thank you for using the USB Drop Attack Simulation Device. This tool is designed for educational and awareness purposes only. It safely demonstrates how attackers can exploit USB Human Interface Device (HID) emulation to gain unauthorized access to a system. This device is a harmless simulation intended to raise awareness about social engineering attacks, specifically the dangers of plugging in unknown USB devices.

What the Device Does

When this USB device is plugged into a Windows computer, it emulates a keyboard and automatically types a warning message into Notepad. The message may read: "You've just experienced a USB drop attack simulation. Do not plug in unknown devices!" This demonstrates how a USB device can act as a keyboard to quickly execute commands even on a locked or monitored system. The device does not store or transmit data, does not install software, and does not make permanent changes to the target system.

Intended Use

This device is intended to be used in the following scenarios:

- Classroom cybersecurity demonstrations
- Awareness campaigns within organizations
- IT security training sessions
- Ethical hacking labs or competitions

How to Use

1. Insert the Digispark USB device into an available USB port on a Windows PC.
2. Wait a few seconds the device will automatically open Notepad and type the scripted message.
3. No further action is required; the demonstration is complete once the message is displayed.

User Manual

Note: Some systems may prompt for driver installation the first time the device is used.

System Requirements

- Operating System: Windows 7, 8, 10, or 11
- Drivers: Digispark drivers (provided in the InstallationGuide/Drivers/ folder)
- USB Port: Type-A (standard USB)

Warnings and Ethical Notice

- This device is strictly for demonstration and educational purposes.
- It must not be used in real-world environments without consent.
- Do not plug this device into public, school-owned, or work-owned computers unless authorized.
- Misuse of this device to deceive or harm others can result in disciplinary or legal action.

Always follow your institution's ethical hacking and responsible disclosure policies.

Support and Troubleshooting

- If the device doesn't respond:
 - Try another USB port
 - Ensure the correct drivers are installed
 - Test on another Windows system
- For reprogramming instructions, refer to the Installation_Guide.pdf located in the InstallationGuide/ folder.

Contact and Licensing

This tool was created as part of an academic cybersecurity awareness project. For questions or further guidance, please refer to the project documentation or contact the project author.