Rubber Ducky is an HID (Human Interface Device), such as a keyboard or mouse that connects human input and computers. More specifically, a Rubber Ducky is a USB flash drive that, when inserted, is seen as a keyboard. It is used as an injection device that cannot be detected by Anti-Virus or a firewall because it is a HID. Once it is connected to a PC, the keystrokes that were programmed into it are executed. The keystrokes are usually commands that are uploaded into the device. The commands being executed on a PC are called payloads.

Uses of a Rubber Ducky consist of targeting vulnerable systems or programming processes and save times. These could be malicious or non-malicious and the device is fast and undetectable by the PC. The Rubber Ducky, being seen as a keyboard, abuses the trust computers have with human inputs, to inject keystrokes. In the industry, it is used for penetration testing to test the resiliency of PC's. However, it can be used for going to a website and downloading malware, pulling up a website with a backdoor, stealing files, and tracking user keystrokes.

A Rubber Ducky consists of 3 main parts, the microSD card, the microSD-to-USB adapter, and the mini "keyboard" adapter. The SD card is used to store the payloads the Rubber Ducky will upload into the victim PC. The microSD-to-USB adapter is a plastic dongle used to mount the SD card. The keyboard adapter is a silicon chip to insert the microSD into which sends the keystrokes to the PC.

Previous versions of the Rubber Ducky were able to make fake windows pop-ups to steal user login credentials or have chrome send all saved passwords to a hackers server. However, the attacks needed to be made for specific operating systems and software versions. New versions of the Rubber Ducky have added logic flows (if this, else that) and the capability to store variables. This, in turn, will allow the Ducky to recognize which operating system the device is plugged into, and execute the corresponding keystrokes.

The major problem with Rubber Duckies is the need for physical access. Once plugged into a PC, the capabilities are endless, but it is obviously seen being plugged into a USB port. This means that most people aren't at high risk of it being plugged in.

https://www.theverge.com/23308394/usb-rubber-ducky-review-hack5-defcon-duckyscript
https://www.geeksforgeeks.org/usb-rubber-ducky-penetrationtesting/
https://sqnbankingsystems.com/blog/what-is-a-rubber-ducky/