FLIPPER ZERO

BRIDGEFEST

SAT 25.05.24

DISCLAIMER

This workshop is designed for educational and informational purposes only. The demonstrations and examples provided are intended to showcase the device's functionalities and potential applications in a controlled and lawful manner.

Use only your own hardware and networks.

Misusing the Flipper Zero can lead to serious legal consequences.

WHAT IS FLIPPER ZERO?

Flipper Zero is a portable multi-tool for pentesters and geeks in a toy-like body. It loves hacking digital stuff, such as radio protocols, access control systems, hardware, and more. It's fully open-source and customizable, so you can extend it in whatever way you like.

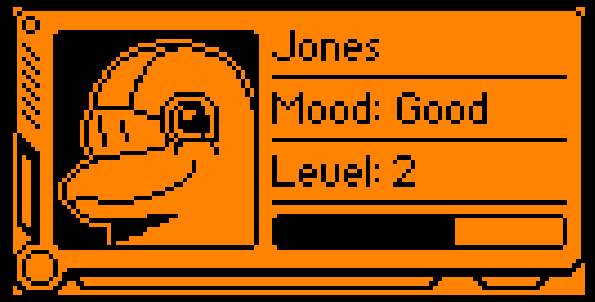
It is compact and pocket-sized, making it highly portable and convenient for on-the-go use. The device is equipped with a wide range of features and modules that allow users to interact with and manipulate various types of electronic devices and systems.

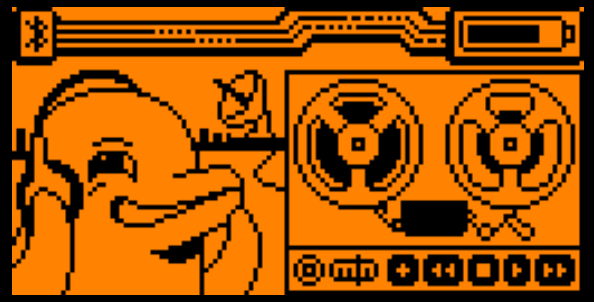
TOY-LIKE? (01/02)

Flipper Zero is a small, portable device that looks like an electronic toy, or Tamagotchi, popular in the late 20th century and early 21st century. With its help, it was possible to take care of a virtual pet – the user was responsible for feeding, washing and cleaning it. Everything was done on a small screen.

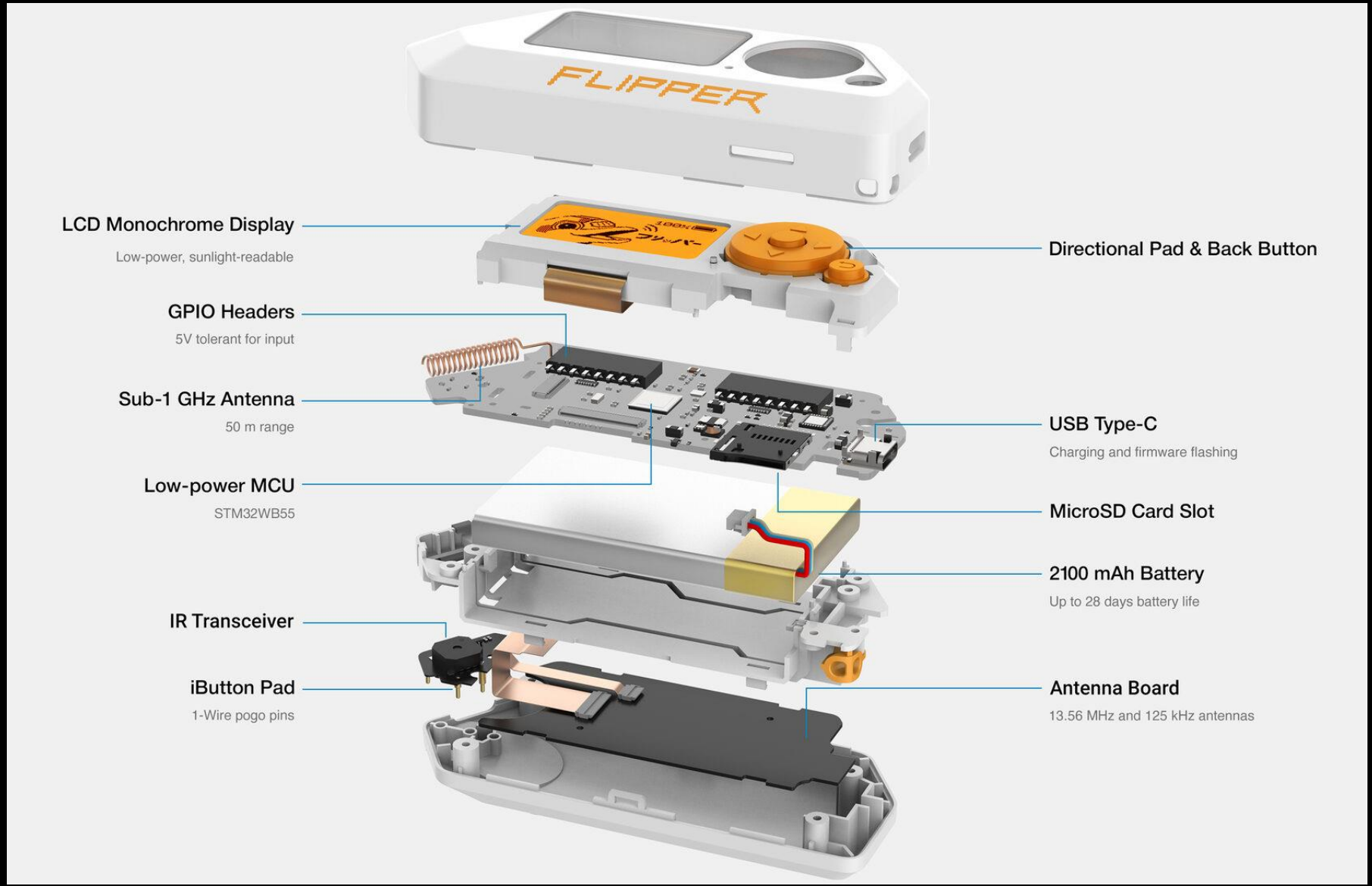
TOY-LIKE? (02/02)

Flipper Zero is a tiny piece of hardware with a curious personality of a cyber-dolphin. It can interact with digital systems in real life and grow while you use it. Explore any kind of access control system, RFID, radio protocols, and debug hardware using GPIO pins.





WHAT'S INSIDE?



Flipper Technology (01/09)

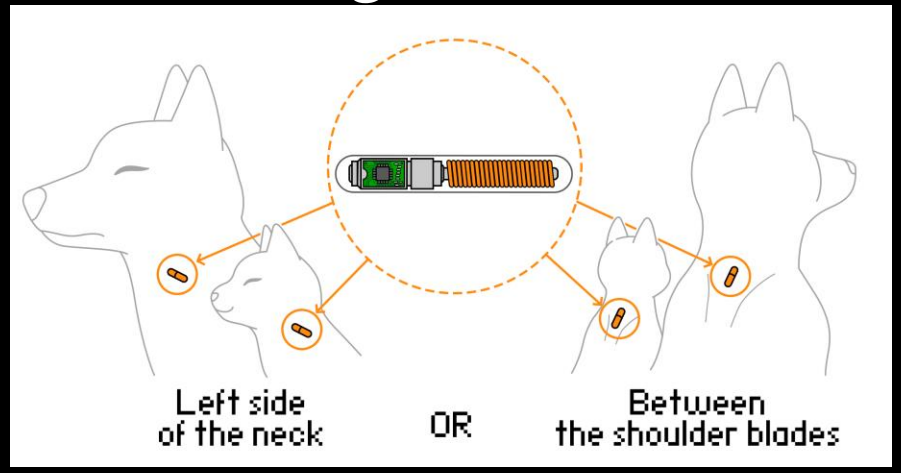
- Sub-Ghz
- 125 kHz RFID (Radio Frequency Identification)
- NFC (Near Field Communication)
- Infrared
- iButton
- BadUSB
- U2F (Universal 2nd Factor)
- GPIO (General Purpose Input/Output) & modules
- Bluetooth
- Microcontroller unit, USB, Buzzer, Vibration motor, Battery, micro-SD

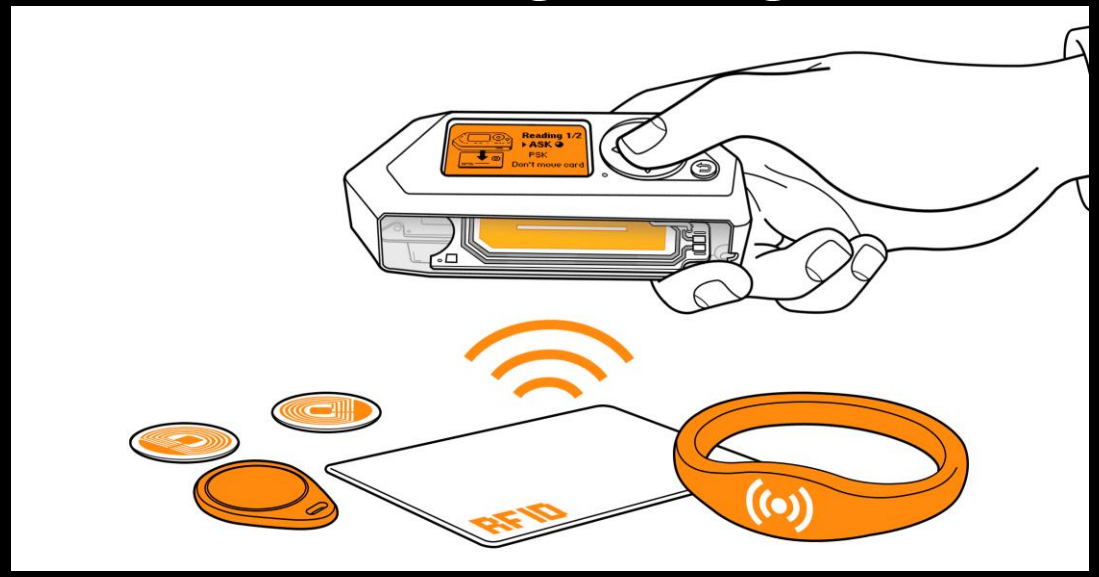
Flipper Technology(02/09) - Sub-Ghz

Flipper Zero can receive and transmit radio frequencies in the range of 300-928 MHz with its built-in module, which can read, save, and emulate remote controls. These controls are used for interaction with gates, barriers, radio locks, remote control switches, wireless doorbells, smart lights, and more.

Flipper Technology(03/09) - 125 kHz-RFID

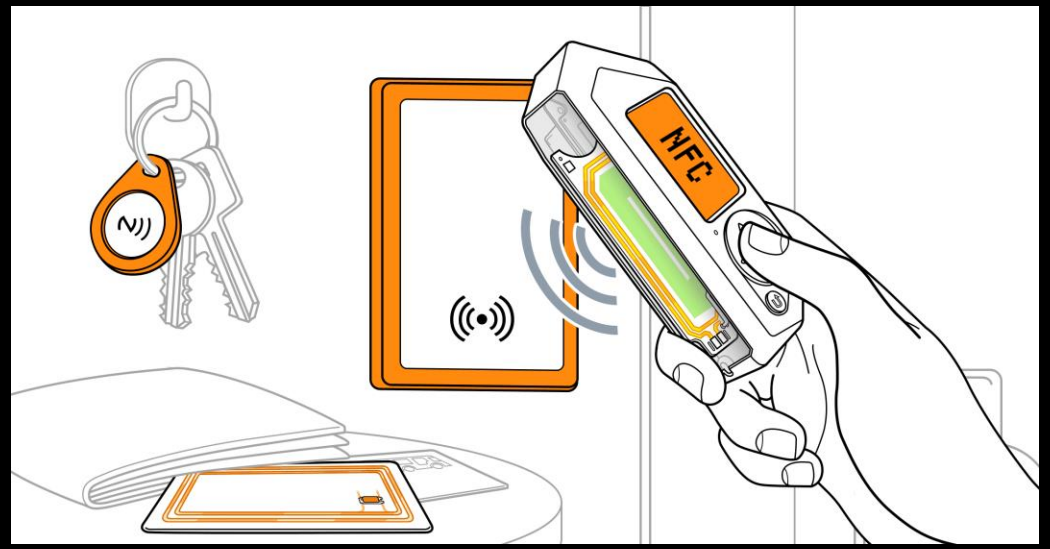
Flipper Zero supports low-frequency (LF) radio frequency identification (RFID) technology that is implemented in access control systems, animal chips, and supply chain tracking systems. Unlike NFC cards, LF RFID cards usually do not provide high levels of security. This technology comes in many form-factors, such as plastic cards, key fobs, tags, wristbands, and animal microchips. Flipper Zero has a low-frequency RFID module capable of reading, saving, emulating, and writing LF RFID cards.





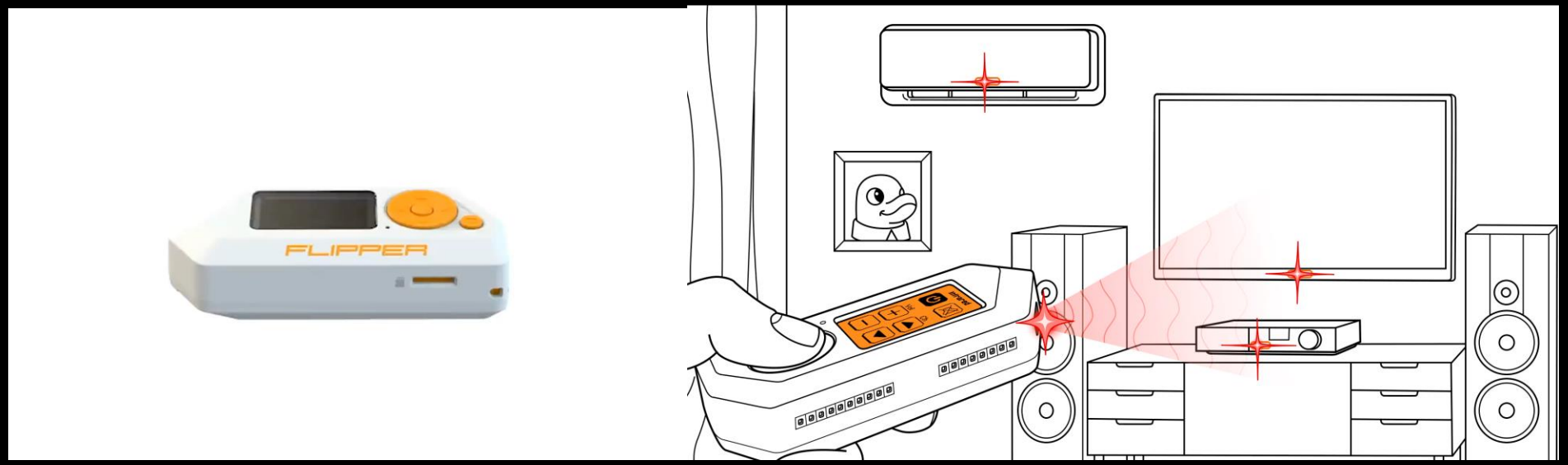
Flipper Technology(04/09) - NFC

Flipper Zero supports NFC technology, which is implemented in public transport smart cards, access cards or tags, and digital business cards. These cards have complex protocols and support encryption, authentication, and full-fledged two-way data transfer. Flipper Zero has a built-in 13.56 MHz NFC module capable of reading, saving, and emulating NFC cards.



Flipper Technology(05/09) - Infrared

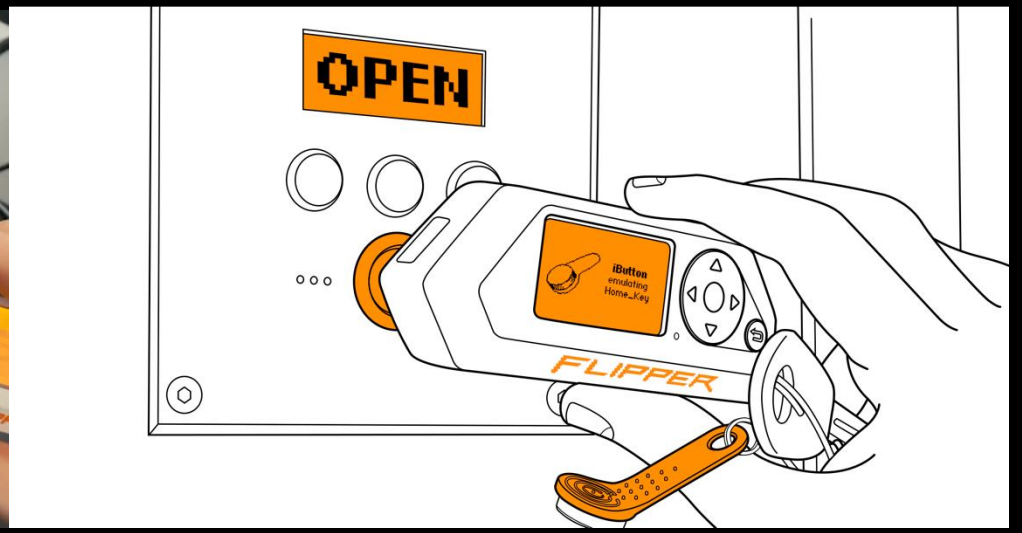
Flipper Zero can interact with devices that use infrared (IR) light to send commands, such as TVs, air conditioners, multimedia systems, etc. With its built-in infrared module, Flipper Zero can learn and save infrared remotes and use its own universal remotes to control other devices.



Flipper Technology(06/09) - iButton

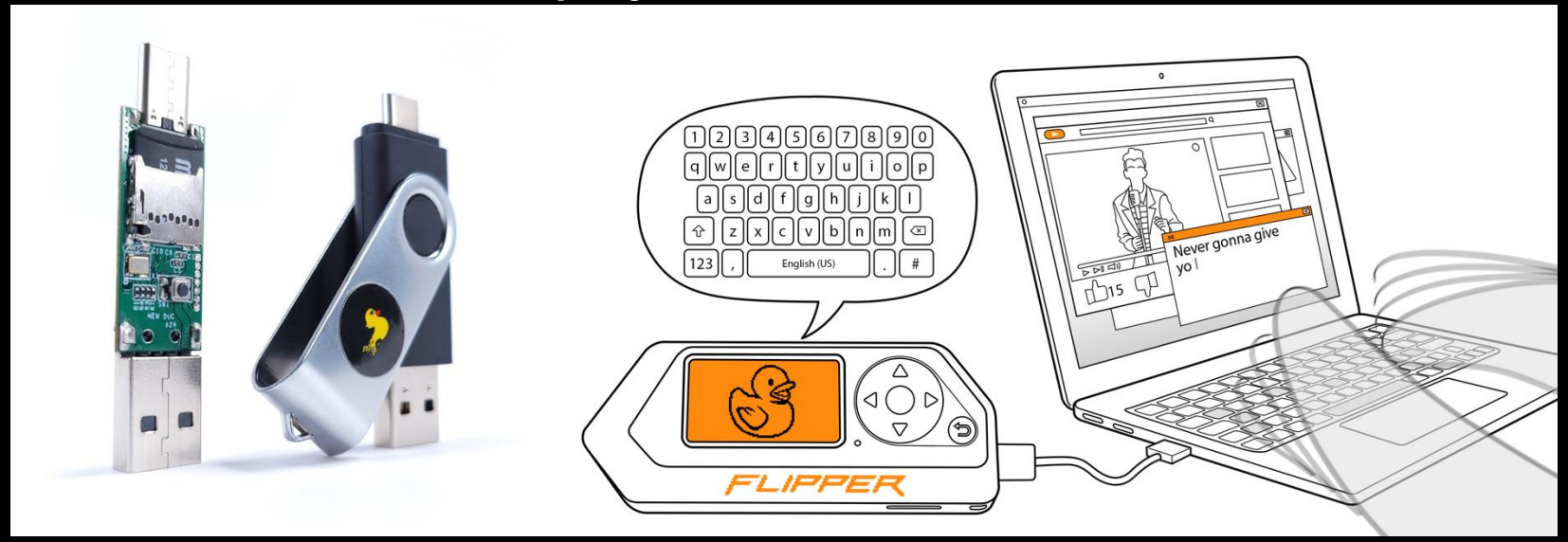
Flipper Zero supports a 1-Wire device communication protocol, which is implemented in small electronic keys known as iButton keys. These keys are used for access control, temperature measurements, humidity measurements, storing cryptographic keys, etc.

Flipper Zero can read, write, and emulate iButton access control keys with its built-in iButton module, which supports Dallas, Cyfral, and Metakom key protocols.



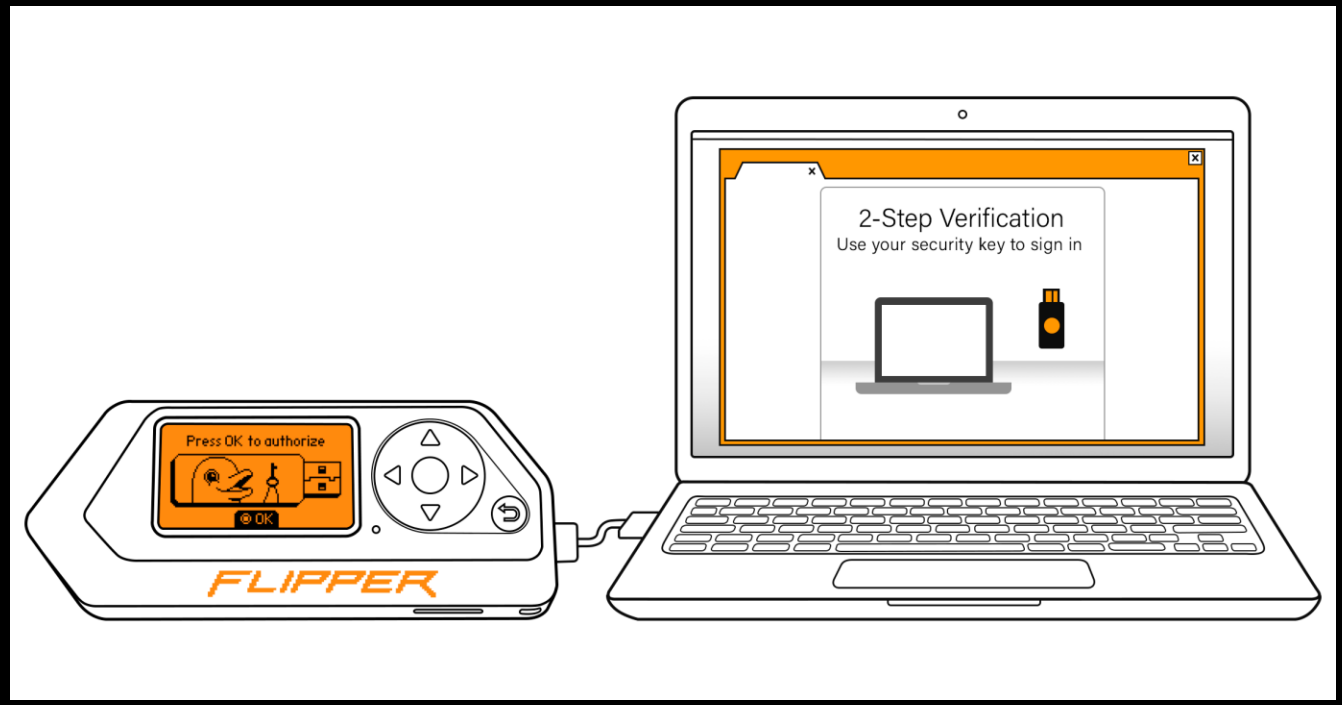
Flipper Technology(07/09) - BadUSB

Flipper Zero can act as a BadUSB device, recognized by computers as a Human Interface Device (HID), such as a keyboard. A BadUSB device can change system settings, open backdoors, retrieve data, initiate reverse shells, or do anything that can be achieved with physical access. It is done by executing a set of commands written in the Rubber Ducky Scripting Language, also known as DuckyScript. This set of commands is also called a payload.



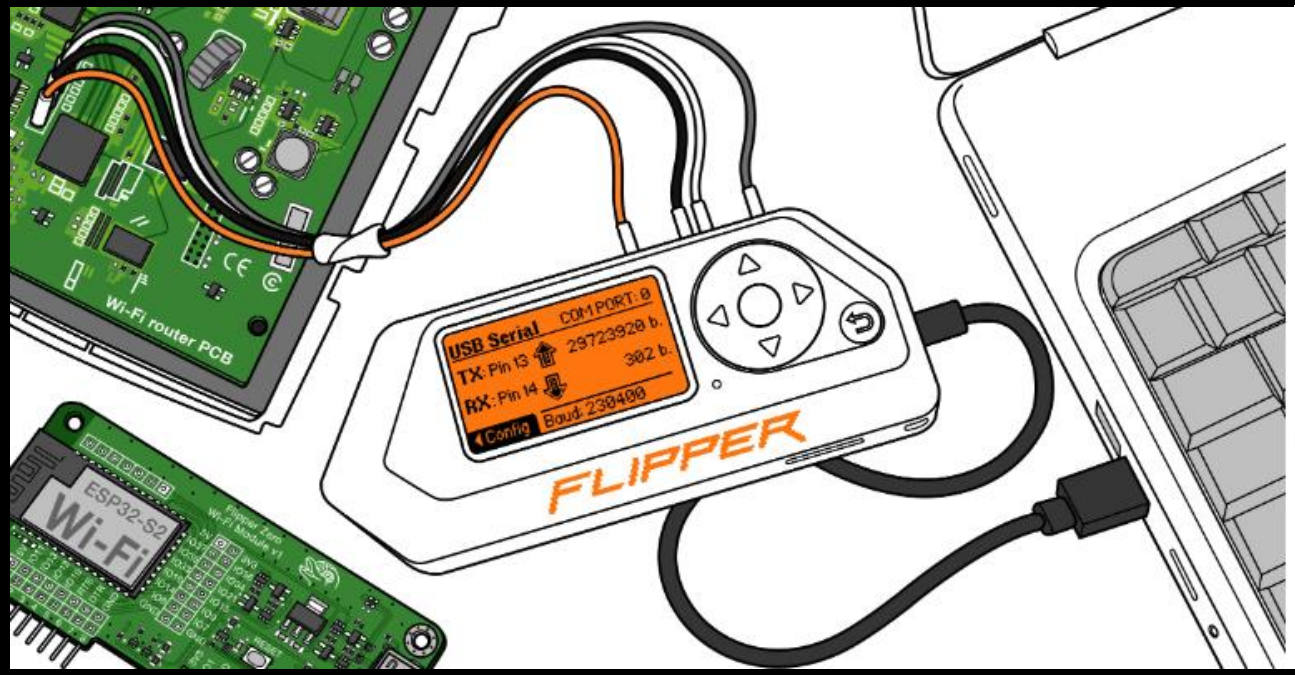
Flipper Technology(08/09) - U2F

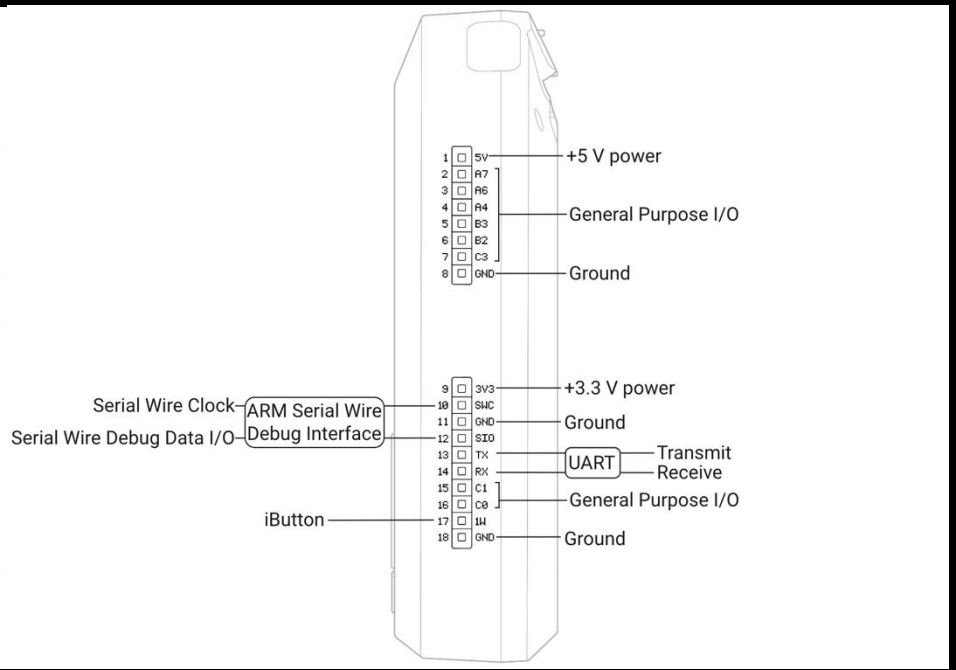
Flipper Zero can act as a USB universal 2nd-factor (U2F) authentication token or security key that can be used as the second authentication factor when signing in to web accounts. A security key is a small device that helps computers verify that it is you when signing in to an account. The use of this feature increases the security of your accounts.



Flipper Technology(09/09) - GPIO & modules

You can use your Flipper Zero for hardware exploration, firmware flashing, debugging, and fuzzing. Flipper Zero can be connected to hardware using its built-in GPIO pins, control hardware with buttons, run your code, and show debug messages on the screen. Flipper Zero can also be used as a USB to UART/SPI/I2C converter.





WHERE TO START? (01/02)

- Buy a Flipper Zero.

  - Interesting fact: It was first announced in August 2020 through the Kickstarter crowdfunding campaign, which raised $4.8 million. The first devices were delivered to backers 18 months after completion of the crowdfunding campaign.

- Install a micro SD card.

  Insert the microSD card into your Flipper Zero before updating the firmware.
  Flipper Zero supports FAT12, FAT16, FAT32, and exFAT file systems and is compatible with microSD cards up to 256 GB, but a 4 GB microSD card is sufficient to store all the necessary data.

- Update Firmware.

  - Update via qFlipper
  - Update via Flipper Mobile App

- Join the Community.

  - Official Forum, Discord, Blog, Repository, Telegram chat and more.

- Do your own research and have fun.

WHERE TO START? (02/02)

- main site - https://flipperzero.one/
- e-shop - https://shop.flipperzero.one/
- Documentation - https://docs.flipper.net/
- Firmware update - https://flipperzero.one/update
- Custom Firmware and comparison - https://awesome-flipper.com/firmware/
- Flipper Devices Official Repo - https://github.com/flipperdevices
- Flipper Lab - https://lab.flipper.net/

DEMO TIME

- Sub-Ghz
  - Doorbell
- NFC
  - Read/decrypt cards
  - Arduino reader
- Infrared
  - Air conditioner
  - Projector
- BadUSB
  - MacOS demo
  - Reverse shell
- GPIO (General Purpose Input/Output) & modules
  - WiFi Board
    - Evil Portal
- Bluetooth
  - BLE SPAM
  - Camera control

- The main reason of buying a flipper zero

FLIPPER ZERO

BRIDGEFEST

SAT 25.05.24

THANK YOU