Flipper Zero Demo

Infrared Spam

Test: Can you Turn the Light On?
Can you Change the Colors?

Most common household devices use Infrared remotes, often with overlapping codes. Your TV, Air Conditioning, LEDs, Fans, Projectors, Speakers/Soundbar, Blu-ray/DVD player, Computer Monitors, Digital Signs, and more - all use similar remotes.

Turn on the Flipper Zero and navigate to Infrared

Select a library of codes

ATTACK

Hint: The LED library works worse than expected for this experiment. Our home TV remote control power button does turn our LED lights red though…

When you are done please press the power button on the light to turn it off for the next person.

Flipper Zero Demo

Infrared - Read a Remote

Test: Can Read the Infrared Remote and Emulate It?

Flipper Zero (top), Infrared Remote (middle), Infrared-Controlled LED Bulb (bottom)

On the Flipper Zero, navigate to “Infrared” and then “Learn New Remote”

Aim the remote at the Flipper and then press a relevant button to test

The Flipper Zero should recognize and capture the signal

You can then replay the signal with the Flipper Zero aimed at the light to test whether it was successful

If you have issues, try changing the settings (left to change from Infrared to Manual mode, right to change from Decode to Raw mode)

In the Field: This can be used to capture, emulate, or otherwise mess with a variety of devices while on an engagement. From shutting off security’s CCTV monitoring screens, to messing with AC units and coming in as AC repair personnel, to simply causing distracting chaos - this can be used to support physical breaches in a variety of ways.

Flipper Zero Demo

Steal and Emulate a Badge

Goal: Clone a working badge and emulate it with a Flipper Zero

Hint: There are both low and high frequency badge options in this exercise

Step 1: Identify Working Badge

In the Field: Look for employees who successfully swipe into doors and target them. Security badges, facilities, and high-level employees often have global access.
In the Lab: Swipe a badge and see if you are granted (green bar) or denied (red bar) access.

Step 2: Grab & Emulate Badge Data

In the Lab: 1) Navigate to the main menu (hit back a few times)
2) Select 125 kHz RFID or NFC
3) Select Read & hold it against the badge (may take 1-3 seconds)
4) If it doesn't work, select the other frequency option
5) Success involves a noise and green LED lighting up
6) On the Flipper Zero select "More" and then "Emulate"
7) Swipe the badge on the reader and look at the badge number (lowest row on reader display)
8) Compare the badge numbers. Does your Flipper Zero now provide you access to this badge reader, door, and building? If so, you can save it on the Flipper and use it anytime you want.
9) Success!

***Note**: In the field, you can often write the badge data to another card. If you have a badge printer and photo of the original employee badge, you can print a fake one and encode it with the Flipper to work accurately.*

In the Field: *Grabbing badge data is done easiest with a long range reader, however a Flipper Zero can read the badge from within 0-2cm. You may need to social engineer your way into holding or borrowing the target's badge, or you can find a way to hold a Flipper directly against their badge. A Flipper Zero can read a badge through a thin piece of fabric but typically not a thicker backpack or other material.*