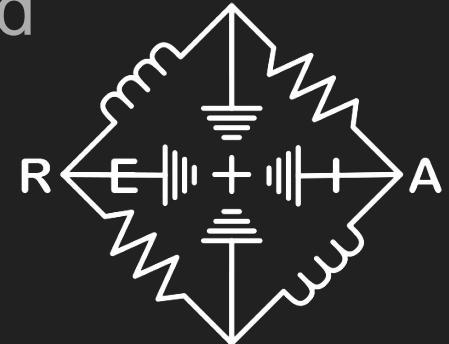


Wifi_Hacking_Self_Defense

4 Advanced Attacks Countered



Who Am I?

Hi! I'm Ash Wheeler:

- University Student in the US
- Primarily working on BioHacking using Open Hardware & Software
- Also exploring Wi-Fi and RFID Tools Based on Microcontrollers

Resources

- Example Github Repo: github.com/skickar/CatGotYourPassword
- Serial terminal: serialterminal.com
- Flashing Tool: nugget.dev
- Retia Discord: <https://discord.gg/rjVJbauAUX>

Attacking Yourself to Learn Defense

- Getting attacked in the wild
- Attacking Others to Learn What Vulnerable Systems Look Like

How do we Learn Safely and Ethically?

- ✓ Use Our Own Devices as a Lab
- ✓ Also Makes Your System More Secure

What are we learning?

- Covert Scanning of Wi-Fi Leaks & how to plug them
- Using Beacons to actively expose POI's & Travel History
- Evil QR Codes & Hidden Network dangers
- Wi-Fi phishing attacks & how to spot them

Wi-Fi Leaks - Learn what networks are stored in a phone

- We'll use passive Wi-Fi scanning to learn about a target Wi-Fi device
- This is undetectable and purely passive
- Nearby devices call out for recently joined networks
- This can expose a lot of information
- Requires no interaction with the target on our part

Beacon Swarms - Actively Extract Stored Networks

- We'll create many fake Wi-Fi networks
- If nearby Wi-Fi devices have a matching network name stored, they try to connect
- We can use this information to identify VIP's and where a person has traveled
- This is an active attack and can be detected

Poisoned QR Codes - Tag a phone for tracking & MITM

- This attack uses a QR code to inject an evil network into a Wi-Fi device
- The evil network allows a hacker to detect when you are nearby
- The hacker can also force your device to connect to an evil network at any time
- This allows for a man in the middle attack

Wi-Fi Phishing Attacks - Your Router Is Not Updating

- Wi-Fi Phishing is easy and effective
- Disable valid Wi-Fi network with deauth attack (we won't do this part)
- Create a fake AP pretending to be from the router with no password
- When victim connects, a spoofed router login page appears
- Claims to be the router updating, asks for Wi-Fi password

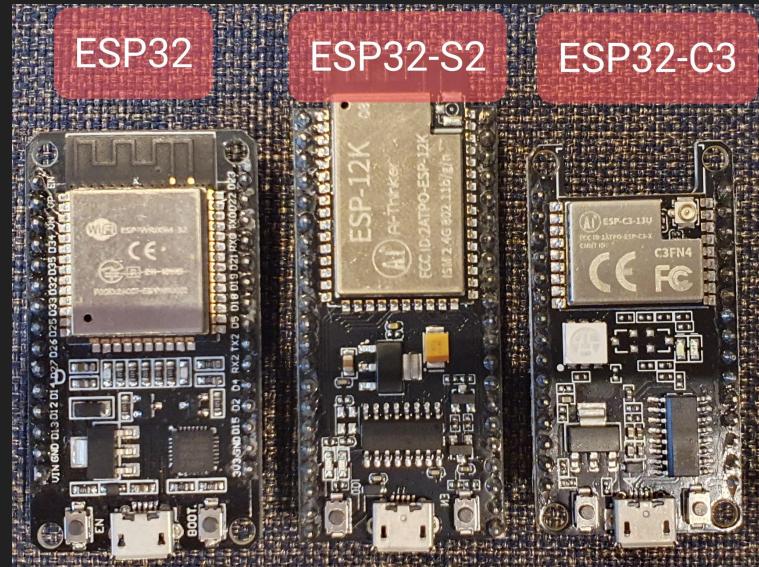
What is a Microcontroller?

Inexpensive Systems on Chips With A Variety Of Strengths and Weaknesses

Examples:

Esp8266- Wi-Fi Injection Capable Mc with 10 GPIO Pins

Esp32S2- Wi-Fi Enabled Mc with HID and USB

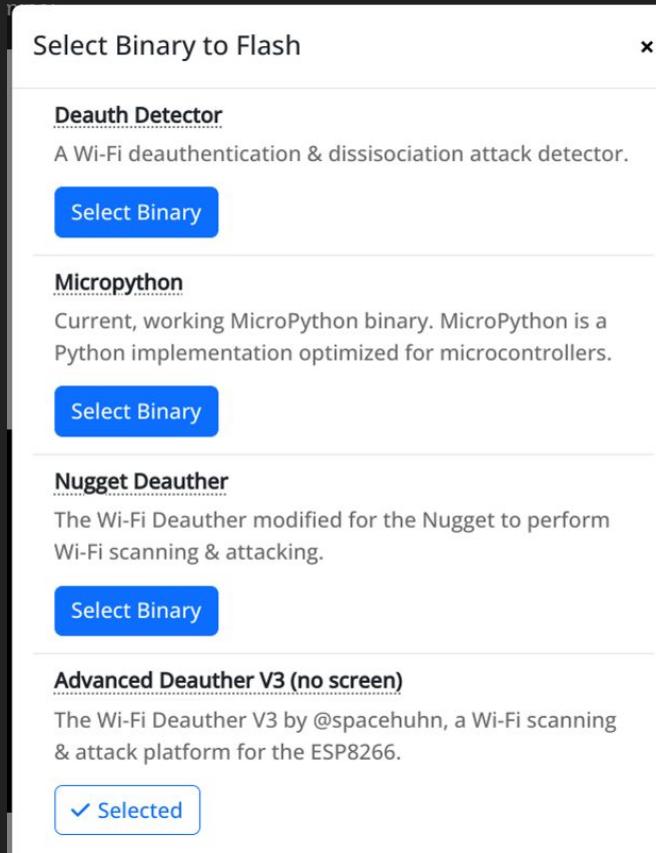


Setting Up the Wi-Fi Nugget

- Navigate to our flashing website www.nugget.dev in a Chrome based browser
- Plug in your Nugget via USB cable & click “Connect Your Nugget”
- Select your Nugget from the dropdown menu of serial devices



CONNECT YOUR NUGGET



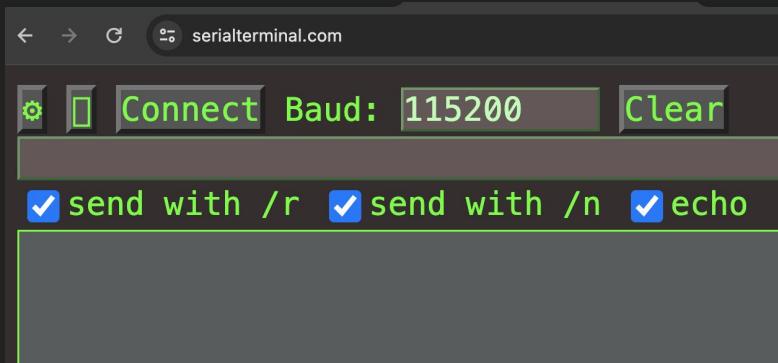
Flash the Headless Advanced Wi-Fi Deauther Binary

- Open a Chromium based browser and navigate to: nugget.dev
- Plug in Wi-Fi Nugget, Click “Connect Your Nugget”, Select Serial Port of Nugget
- Open Select Program Menu And Select Advanced Deauther V3
- Close Menu and “Program”

*Certain Systems may need to have Dialout Group added

Connect Via Serial terminal

- Navigate to serialterminal.com in a Chrome browser
- Unplug & Plug in your Nugget, set Baud to 115200, click “Connect”
- Select your Nugget from the dropdown menu of serial devices
- Type “help” and press return to test if the connection is working



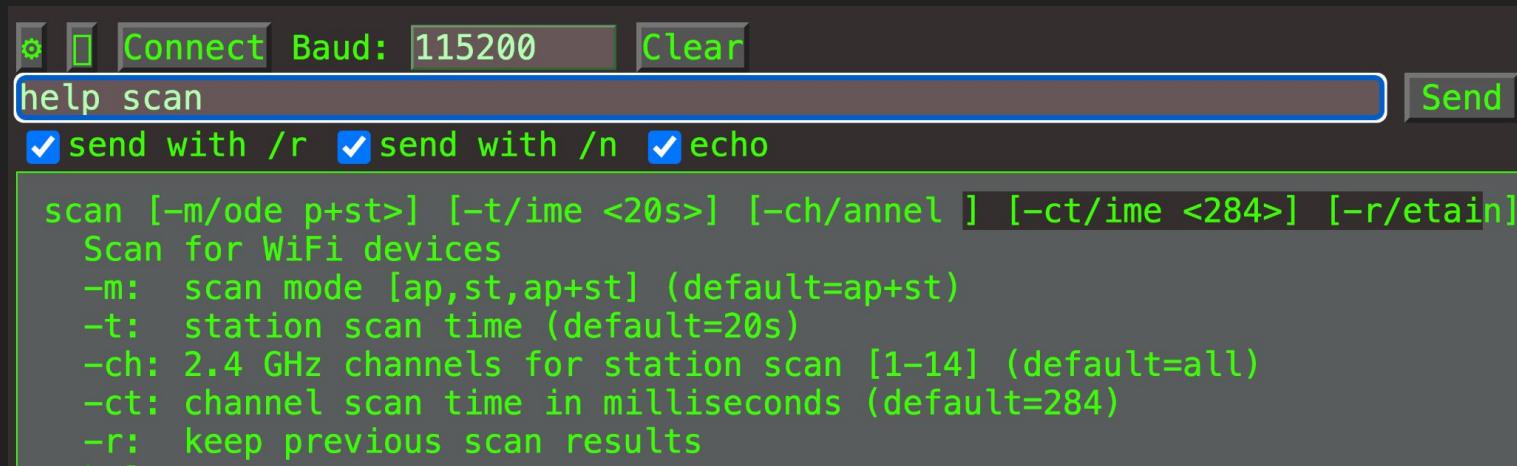
A screenshot of the same web interface after entering the "help" command. The header remains the same. The main content area now displays the help text for the "deauth" command:

```
✓ send with /r ✓ send with /n ✓ echo
deauth [-ap ue>] [-st/station] [-mac,manual] [-t/time/out <5min]
Deauthenticate (disconnect) selected WiFi connections
-ap: access point IDs to attack
-st: station IDs to attack
-mac: manual target selection [Sender-Receiver-Channel] for
-t: attack timeout (default=5min)
-n: packet limit [>1] (default=0)
-r: packets per second (default=20)
-m: packet types [deauth,disassoc,deauth+disassoc] (defaul
```

We're set up!

- Scan - search the airwaves for Wi-Fi signals, display devices & access points
- Beacon - create the appearance of Wi-Fi networks that can't be joined
- AP - create an evil Wi-Fi access point that can be joined

Use the “help” command to get more information on how to use each command:



```
⚙️ ⚡ Connect Baud: 115200 Clear
help scan
Send
 send with /r  send with /n  echo

scan [-m/ode p+st>] [-t/ime <20s>] [-ch/annel ] [-ct/ime <284>] [-r/etain]
  Scan for WiFi devices
  -m:  scan mode [ap,st,ap+st] (default=ap+st)
  -t:  station scan time (default=20s)
  -ch: 2.4 GHz channels for station scan [1-14] (default=all)
  -ct: channel scan time in milliseconds (default=284)
  -r:  keep previous scan results
```

Lab #1: Detect & plug Wi-Fi Leaks in your devices

- We'll scan the airwaves to listen in on networks devices are calling out for
- Try a basic scan - just type “Scan”
- We'll do a more advanced scan to learn more about what's around us
- What might we not see? Connected Wi-Fi devices that aren't being used

```
[ ====== Scan Results ====== ]
[ ===== Access Points ===== ]
ID SSID (Network Name)           RSSI Mode Ch BSSID (MAC Addr.) Vendor
=====
```

ID	SSID (Network Name)	RSSI	Mode	Ch	BSSID (MAC Addr.)	Vendor
0	*HIDDEN-NETWORK*	-85	WPA2	6	90:4c:81:fa:bd:e0	HewlettP
1	"POS411"	-84	WPA*	6	90:4c:81:fa:bd:e1	HewlettP
2	"CCA411"	-86	WPA2	6	90:4c:81:fa:bd:e3	HewlettP
3	"H-Rewards by IntercityHotel"	-85	Open	6	90:4c:81:fa:bd:e4	HewlettP
4	"CORP"	-86	WPA2	6	90:4c:81:fa:bd:e5	HewlettP
5	*HIDDEN-NETWORK*	-63	WPA2	1	90:4c:81:fc:03:80	HewlettP
6	"POS411"	-63	WPA*	1	90:4c:81:fc:03:81	HewlettP
7	"DHOffice"	-62	?	1	90:4c:81:fc:03:82	HewlettP
8	"CCA411"	-62	WPA2	1	90:4c:81:fc:03:83	HewlettP
9	"H-Rewards by IntercityHotel"	-61	Open	1	90:4c:81:fc:03:84	HewlettP
10	"CORP"	-63	WPA2	1	90:4c:81:fc:03:85	HewlettP
11	"CORP-IoT"	-63	WPA2	1	90:4c:81:fc:03:86	HewlettP

```
=====
Ch = 2.4 GHz Channel , RSSI = Signal strength , WPA* = WPA & WPA2 auto mode
```

How many networks are in your phone?

- Check your device's trusted network list
- I am the instructor of this class and I still had 4 vulnerable networks when I checked
- You should delete any open Wi-Fi networks or set them not to auto-connect
- Do this. We'll wait.
- ANY of these networks can sell you out, It only takes one



BW-Jamaica-Inn	None
BWButtePlazalnn	None
Caesars_Resorts	None
CafeCosmos	WPA2 Personal
CafeMak1	WPA3 Personal
CafeMak1_2.4g	WPA3 Personal
CafeMak2	WPA3 Personal
CafeMak5_2.4G	WPA3 Personal
CafeMak8_5G	WPA3 Personal
CapitalOneCafe	None
Carmen Miranda	WPA3 Personal
CFA-CO	None
Chicken_Easy_11	WPA3 Personal
Chickenbucker	None
CityBrew	None
ClientScape	None
Clyde Coffee	WPA3 Personal
Clyde Guest	WPA3 Personal
Coffeebean	None
CoffeeBeanWifi	None
COLTER COFFEE	None
COLTER COFFEE 2 (fa...	None
COLTER COFFEE 3 (fa...	None
ComfortSuitesAirport	None
Conference AV	WPA3 Personal
CRAVE Enjoy Wi-Fi	WPA3 Personal
cupcakes4u	WPA2 Personal
cupcakesforeveryone...	WPA2 Personal
Cyberdyne Systems	None
dd-wrt	None
DefCon-Open	None
Dennys Guest Wifi	None
DLab Guest	WPA3 Personal
Dolcetti	None
DoubleTree	WPA3 Personal
Evenstevens-Guest1	None
FakeNet	None
Firehouse Subs	None

Done

Let's Scan for Data Leaks

- Use this advanced scan: **scan -m st -ch 1-12 -t 60 -ct 5000**

```
# help scan

scan [-m/ode p+st>] [-t/ime <20s>] [-ch/annel ] [-ct/ime <284>] [-r/etain]
      Scan for WiFi devices
      -m:  scan mode [ap,st,ap+st] (default=ap+st)
      -t:  station scan time (default=20s)
      -ch: 2.4 GHz channels for station scan [1-14] (default=all)
      -ct: channel scan time in milliseconds (default=284)
      -r:  keep previous scan results
```

What do you see?

- Try modifying the scan to stay on channels 1, 6 & 11

Lab #2: Tracking With Beacon Swarms

- Beacons - Advertisements To Devices For Wi-Fi networks
- Beacon Swarm - Creating Clones of Popular Networks en Masse
- Scanning for Requests to Join, We can Identify Users Of VIP Target Networks, Such as Government Employees

Other Networks	
	A_Guest
	admin-guest
	att-wifi
	Camden
	CCA411
	CityofLosAngelesGuest
	Comfort Inn
	CORP
	CORP-IoT
	Cricket-Guest
	DaysInnOnline
	DHOffice
	FBI-SurveillanceVan
	Guest
	Guestnet
	Hollywood Guest Inn
	Jacks_Guest
	LATTC-Visitor
	LAX-C guest

beacon "SSID_1","SSID_2"... -mon

- beacon - Loops sending of target beacons to create beacon swarm
- “SSID_x” - Sets the target names, works 20 or (sometimes)more networks
- -mon - Tells the tool to scan for devices attempting to join the advertised networks

```
> help beacon

# help beacon

beacon -ssid/s [-bssid,from ] [-receiver,to ] [-enc/ryption ] [-ch/annel <1>] [-r/ate <10>] [-auth,m/on/itor]
Send WiFi network advertisement beacons
-ssid: network names (SSIDs) for example: "test A","test B"
-from: BSSID or sender MAC address (default=random)
-to: receiver MAC address (default=broadcast)
-enc: encryption [open,wpa2] (default=open)
-ch: 2.4 GHz channel(s) [1-14] (default=1)
-r: packets per second per SSID (default=10)
-m: scan for authentications
-save: save probe requests from auth. scan
-t: attack timeout (default=5min)
```

```
[ ===== Authentication Scan ===== ]
```

```
Scan time: 5min
```

```
Channels: 1,
```

```
Channel time: -
```

```
Beacon Mode: On
```

```
Save stations: No
```

```
BSSID filter: 0
```

```
Type 'stop auth' to stop the scan
```

RSSI	Ch	Vendor	MAC-Address	SSID	BSSID
-74	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-72	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-74	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-71	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-66	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-71	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-68	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-70	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-69	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-70	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-67	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-68	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-67	1		fe:23:2d:09:0e:53	"Ace Hotel"	00:0a:73:a2:dd:d3
-48	1		06:06:e7:96:78:50	"Americas Best Value Inn"	00:0a:73:a2:dd:d4
-49	1		06:06:e7:96:78:50	"Americas Best Value Inn"	00:0a:73:a2:dd:d4
-50	1		06:06:e7:96:78:50	"Americas Best Value Inn"	00:0a:73:a2:dd:d4
-53	1		06:06:e7:96:78:50	"Americas Best Value Inn"	00:0a:73:a2:dd:d4
-52	1		06:06:e7:96:78:50	"Americas Best Value Inn"	00:0a:73:a2:dd:d4
-52	1		06:06:e7:96:78:50	"Americas Best Value Inn"	00:0a:73:a2:dd:d4
-49	1		06:06:e7:96:78:50	"Americas Best Value Inn"	00:0a:73:a2:dd:d4
-49	1		06:06:e7:96:78:50	"Americas Best Value Inn"	00:0a:73:a2:dd:d4
-50	1		06:06:e7:96:78:50	"Americas Best Value Inn"	00:0a:73:a2:dd:d4
-50	1		06:06:e7:96:78:50	"Americas Best Value Inn"	00:0a:73:a2:dd:d4
-52	1		06:06:e7:96:78:50	"Americas Best Value Inn"	00:0a:73:a2:dd:d4
-50	1		06:06:e7:96:78:50	"Americas Best Value Inn"	00:0a:73:a2:dd:d4

Example Attack Result

Lab #3: Wi-Fi Attacks with Evil QR Codes

- Let's make an evil QR code
- We can encode different information in QR codes
- For this example, we'll be making a Wi-Fi QR code
- This format is sneaky because we can add data the user can't see
- We're going to add the "hidden" flag to this QR code

Qifi.org: Browser Based QR Generator

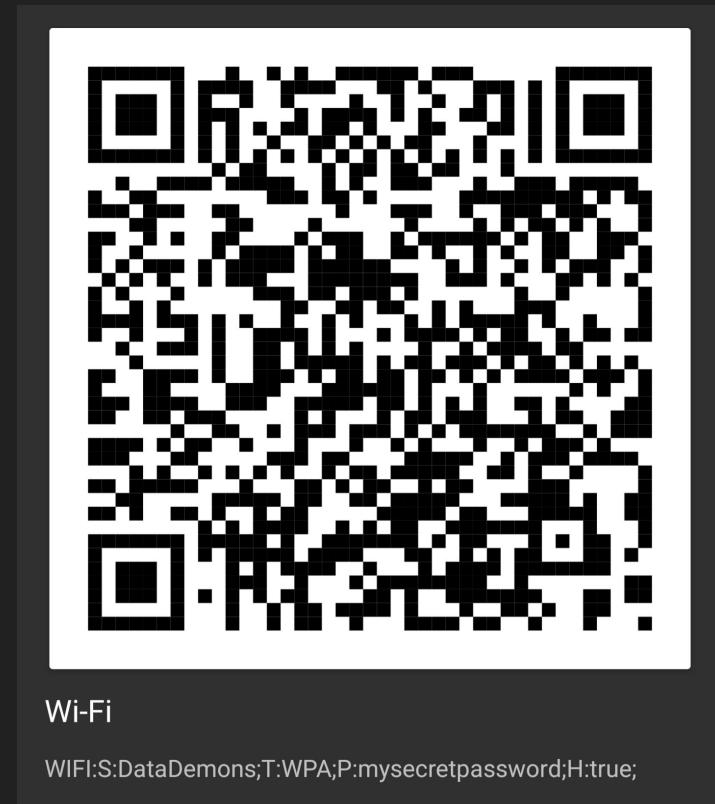
pure JS WiFi QR Code Generator

SSID
 DataDemons

Encryption
WPA/WPA2/WPA3

Key
 Is your SSID hidden?
Hidden

Generate!



Let's Tag Our Device - Create Your Own QR Code

Run this while scanning your QR code:

scan -m st -ch 1-12 -t 60 -ct 5000

Remediation

- Don't scan QR codes you don't trust
- Regularly check your saved networks and delete any unrecognized nets to ensure System Security

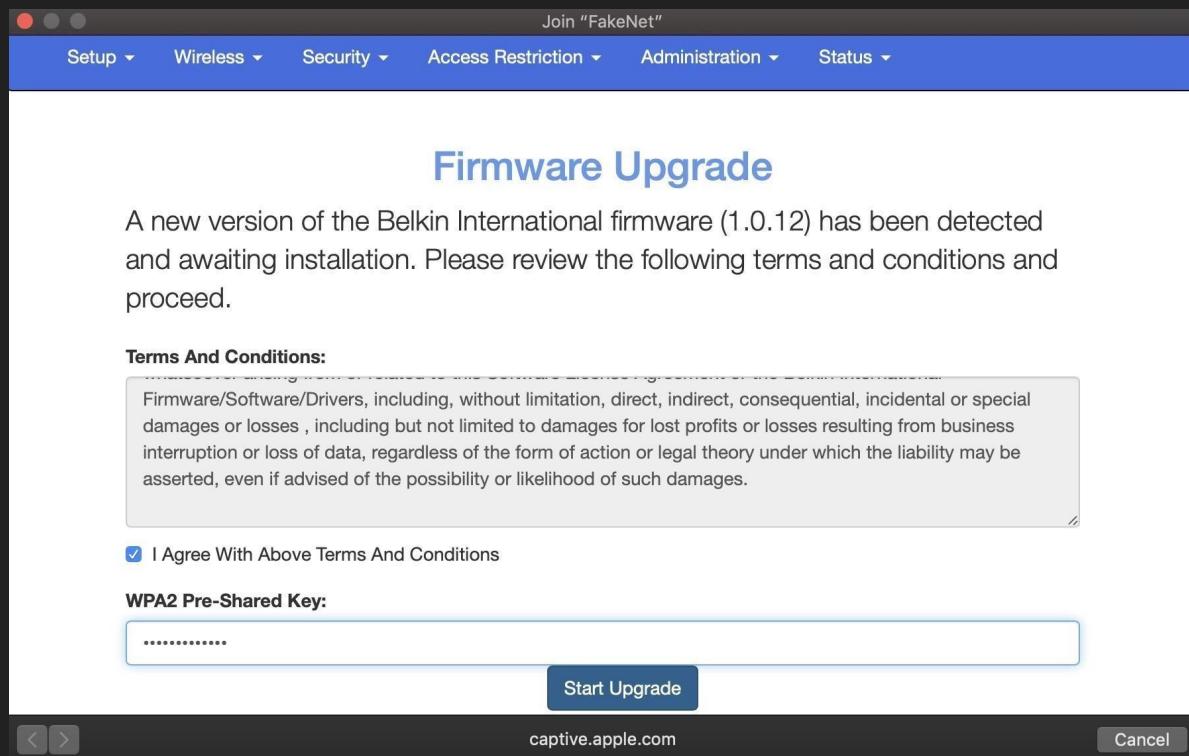
! You Just Infected Your Device, Clear that Tracker out

Lab 4: Catching Wi-Fi phishing attacks

- Wi-Fi phishing is part social engineering, part hacking
- First, the hacker kicks the victim off their real network
- Then, the hacker makes an evil AP with the same name as the target network
- The evil AP has no password and pretends to be the router updating
- If the victim connects, the evil AP asks for the Wi-Fi password
- It claims to need this for a security update, but is actually the opposite

Real Phishing Page

- A Security researcher was compromised by this Phishing Network Page in the wild
- OS “sign into Network” Serve on mobile makes this look authentic



The image shows a screenshot of a web-based interface titled "Firmware Upgrade". The header includes navigation links: "Setup", "Wireless", "Security", "Access Restriction", "Administration", and "Status". A "Join 'FakeNet'" button is also present. The main content area has a title "Firmware Upgrade" and a message stating: "A new version of the Belkin International firmware (1.0.12) has been detected and awaiting installation. Please review the following terms and conditions and proceed." Below this is a section titled "Terms And Conditions:" containing a detailed legal disclaimer about damages and liability. A checkbox labeled "I Agree With Above Terms And Conditions" is checked. A "WPA2 Pre-Shared Key:" field contains several asterisks. At the bottom right are buttons for "Start Upgrade" and "Cancel". The URL "captive.apple.com" is visible at the bottom of the browser window.

Join "FakeNet"

Setup ▾ Wireless ▾ Security ▾ Access Restriction ▾ Administration ▾ Status ▾

Firmware Upgrade

A new version of the Belkin International firmware (1.0.12) has been detected and awaiting installation. Please review the following terms and conditions and proceed.

Terms And Conditions:

Firmware/Software/Drivers, including, without limitation, direct, indirect, consequential, incidental or special damages or losses , including but not limited to damages for lost profits or losses resulting from business interruption or loss of data, regardless of the form of action or legal theory under which the liability may be asserted, even if advised of the possibility or likelihood of such damages.

I Agree With Above Terms And Conditions

WPA2 Pre-Shared Key:

Start Upgrade

captive.apple.com

Cancel

Let's create a phishing network

- Wi-Fi phishing is part social engineering, part hacking
- First, the hacker kicks the victim off their real network
- Then, the hacker makes an evil AP with the same name as the target network
- The evil AP has no password and pretends to be the router updating
- If the victim connects, the evil AP asks for the Wi-Fi password
- It claims to need this for a security update, but is actually the opposite

Let's create a phishing network

```
# help ap

ap -s/sid  [-p/password ]  [-hidden]  [-ch/annel <1>]  [-b/ssid >]
Start access point
-s:  SSID network name
-p:  Password with at least 8 characters
-h:  Hidden network
-ch: Channel (default=1)
-b:  BSSID MAC address (default=random)
```

Let's create a phishing network

Type this command, replacing the SSID with your own:
ap "RotSehenAberGehen"

Now, connect with your phone to the AP.
Do you get a popup?

Once you connect, you should see a
notification like this.

```
# ap RotSehenAberGehen
[ ===== Access Point ===== ]
SSID:      RotSehenAberGehen
Password:
Mode:      Open
Hidden:    False
Channel:   1
BSSID:    00:00:2c:c6:14:cd

Type 'stop ap' to stop the access point
[ ====== Connections ====== ]
IP-Address  MAC-Address  URL
-----
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /favicon.ico
192.168.4.100 92:f6:99:15:ba:2f /generate_204
```

Password Stealing Time

This example page is not weaponized

Type in a fake password.

The attacker can easily receive it!

Sign in to RotSehenAberGehen
connectivitycheck.gstatic.com

Password:

Submit

```
# ap RotSehenAberGehen
> Stopped access point
[ ===== Access Point ===== ]
SSID:      RotSehenAberGehen
Password:
Mode:      Open
Hidden:    False
Channel:   1
BSSID:    00:03:2a:b6:78:cd

Type 'stop ap' to stop the access point
[ ===== Connections ===== ]
IP-Address  MAC-Address  URL
=====
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /favicon.ico
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /generate_204?password=ILoveToJaywalk4Lyfe
192.168.4.100 92:f6:99:15:ba:2f /favicon.ico
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /generate_204
```

Self Defense Tips

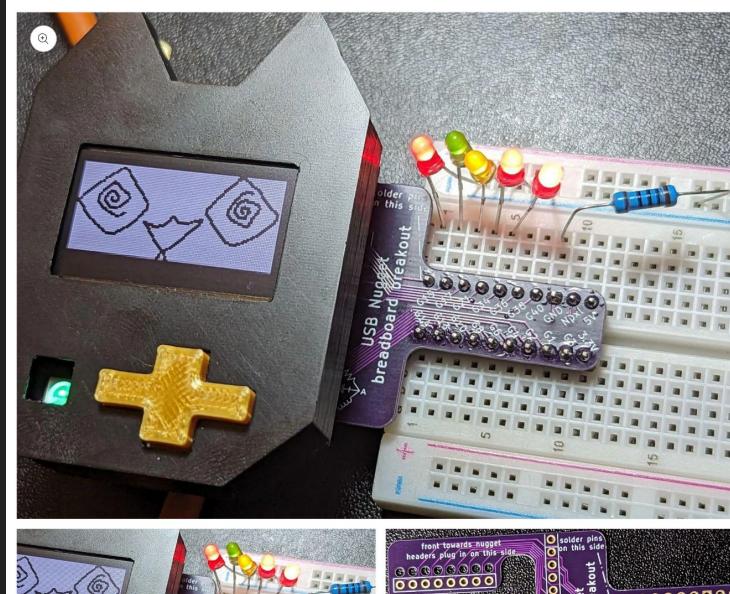
- Never join an open network with the same name as your home or work Wi-Fi network
- Never type your Wi-Fi network password into a website
- Delete any open Wi-Fi networks & set other networks to not auto-join
- Use a VPN to prevent an evil network from snooping or modifying traffic
- Do not add networks via QR code. Use a QR scanner that shows the raw text and verify it isn't a hidden network
- Don't use hidden networks



Teach a friend!

We have kits on Retia.io and discounts for instructors teaching classes!

- Nuggets
- Add-ons
- Online classes



RETIA.IO

**USB Nugget
Breadboard Tail
Breakout**

\$15.00 USD
Tax included.

Quantity

Add to cart

Buy with  [Shop Pay](#)

[More payment options](#)

This cute Breadboard tail breakout allows for easy connection to a breadboard for electronics prototyping. It was designed to be used with CircuitPython or Arduino to prototype hardware with the USB Nugget

Keep in Touch

Want to learn more? You can find us here:

- Discord: <https://discord.gg/rjVJbauAUX>
- Store: Retia.io
- Nugget Flasher: Nugget.dev
- Livestreams: youtube.com/@SecurityFWD

