

Abusing Amazon Dash Buttons

Bob Igo

SSBBQ 2015

What Is It?



What's it Supposed to do?



Place it.

You can hang or stick Dash Button using a removable loop or reusable, washable adhesive on the back.



Press it.

When you are running low on your favorite products, simply press Dash Button and look for a green light.



Get it.

Once you see the green light, your order is placed automatically and delivered to your front door.

What's it Cost?



What if it did Something Cooler™?

- First, we need to know how it works.
- WIFI device.
- Button press
 - performs a DNS lookup of `parker-gateway-na.amazon.com` via `8.8.8.8`
 - Sends a message that says "buy me this thing"

The Plan

- If we convince it that 8.8.8.8 is actually *our* DNS server, we can send it wherever we want to.
- First, we need to set up the Dash button.
 - *Sort of.*

75° 8:07

amazon Prime

☰ 🔍 🛒

- Your Account ←
- Your Recommendations ↗
- Your Subscribe & Save ↗
- Back Up Your Photos ↗
- MORE
- Change Country 🇺🇸
- Notifications
- Contact Us
- Legal Information
- Help & About
- Not Robert W Igo? Sign out

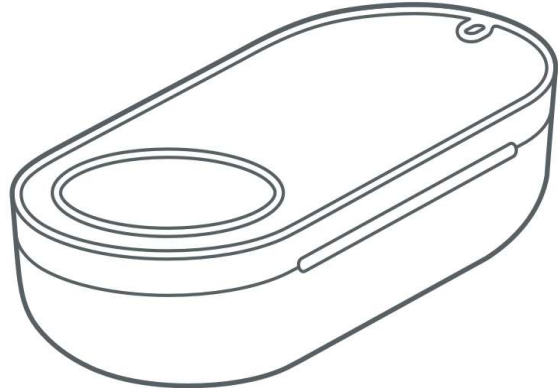
75° 8:07

amazon Prime

☰ 🔍 🛒

- My messages >
- Dash Devices**
- Manage devices >
- Set up a new device ← >
- Personalized content**
- Review your purchases >
- Your social settings >
- App Preferences**
- Advertising Preferences >
- Manage Voice Recordings >

Dash Button Setup



Reorder your favorite household product with the click of a button.

Getting started is easy. Your button connects to your phone for one-time setup, and then it's ready.

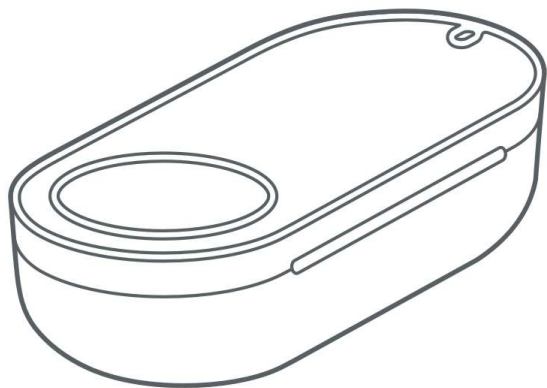
By tapping "Get started" below, you agree to the terms [found here](#).

Get started

Step 1 of 4



Press and hold your Dash Button until the light flashes blue, and then tap **Continue**.



Make sure you hold your Dash Button for 6 seconds before tapping continue.

Continue

Step 2 of 4



Wait for Wi-Fi to connect

We found your Dash Button and we are connecting via Wi-Fi. Your phone will be temporarily disconnected from the Internet.



Step 2 of 4



Select your Wi-Fi network

- HP-Print-15-Officejet 6600  
- 5AV68  
- Igo-BGN  
- WILWIFI  

Enter a different network

Step 2 of 4

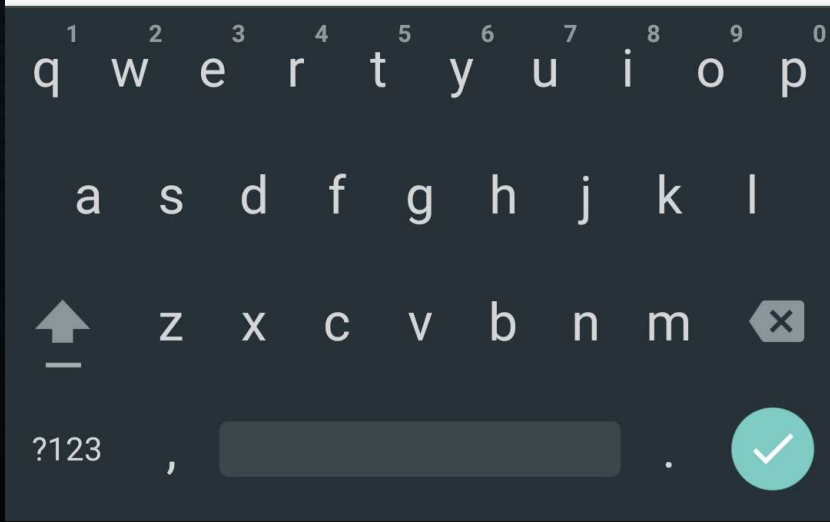
Enter the password for Igo-BGN

Network Igo-BGN

(case sensitive)
HIDE

Save password to Amazon
Helps connect other devices. [Learn more](#)

Continue



Step 3 of 4

What do you want to do when you click it?

Wellness CORE Natural Grain Free Dry Dog Food, Original Chicken Recipe, 26-Pound Bag

\$54.99

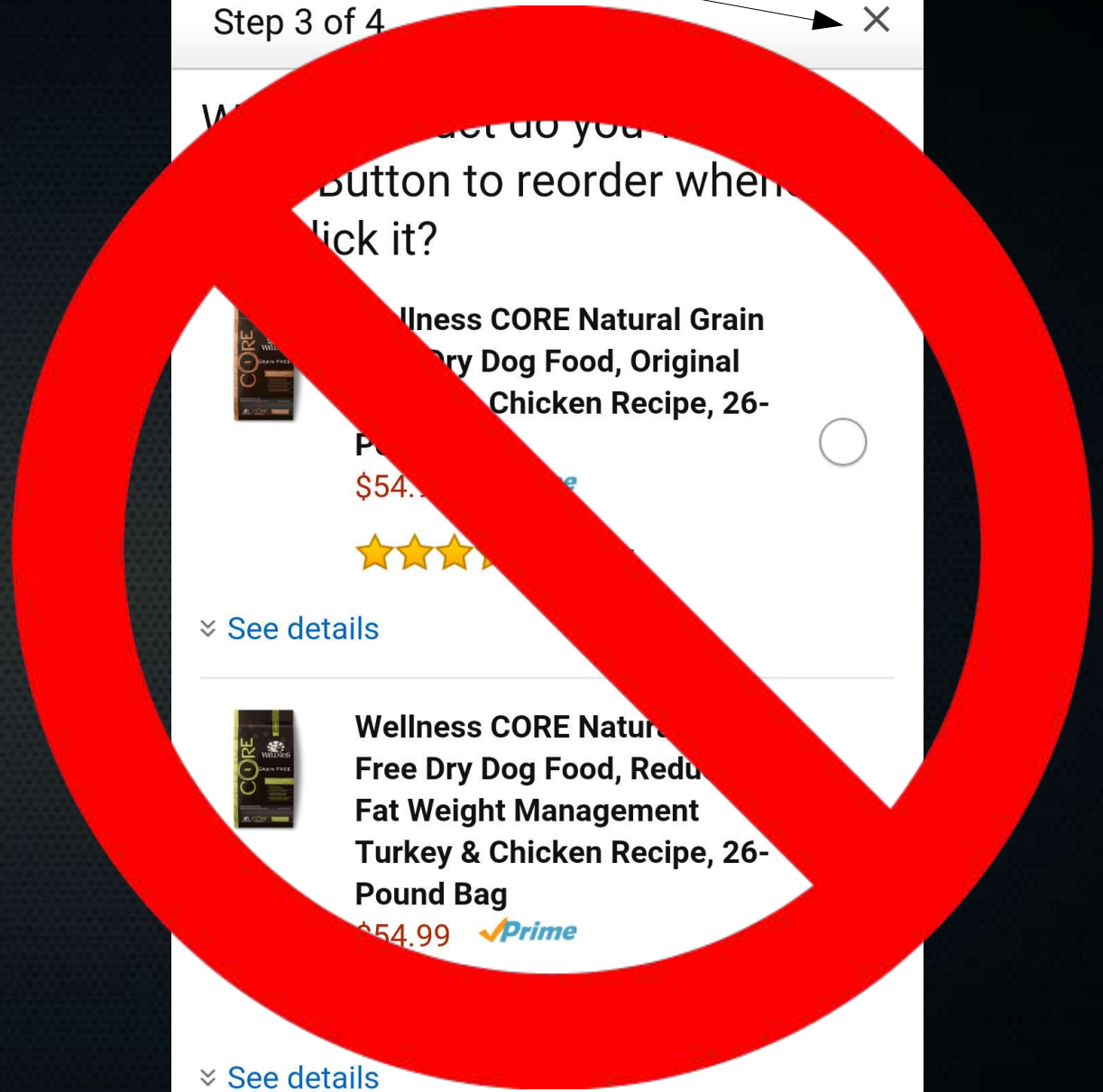
★★★★★

[See details](#)

Wellness CORE Natural Grain Free Dry Dog Food, Reduced Fat Weight Management Turkey & Chicken Recipe, 26-Pound Bag

\$54.99

[See details](#)



Now Put a Bag Over its Head

- It knows your WIFI password, but it doesn't know how to buy anything.
- Confuse it
 - add this to `/etc/hosts` on your router at `192.168.0.1`:
`192.168.0.XYZ parker-gateway-na.amazon.com`
 - Add this to `/etc/firewall.user` on your router:
`iptables -t nat -I PREROUTING -j DNAT --destination 8.8.8.8 --to 192.168.0.1`
`iptables -t nat -I PREROUTING -j DNAT --destination 8.8.4.4 --to 192.168.0.1`

Restart Services

- `/etc/init.d/firewall restart`
- `/etc/init.d/dnsmasq restart`
- Now the Dash button will ask 8.8.8.8 for the mothership's IP address, but it'll get 192.168.0.1

One Final Step

- The Dash buttons aren't always on.
- They send an ARP packet when you press the buttons as they connect to WIFI.
- Any software on your LAN can look for these packets, extract the MAC address, and uniquely identify each Dash button.

Example Python Script

```
def arp_display(self, pkt):
    if pkt[ARP].op == 1: #who-has (request)
        if pkt[ARP].psrc == '0.0.0.0': # ARP Probe
            if pkt[ARP].hwsrc == '74:c2:46:54:41:cf': # Bounty
                #print "Pushed Bounty"
                print "toggling",self.item
                state = self.get_status(self.item)
                print "it's in state",state
                newstate = self.toggle(state)
                print "toggling to",newstate
                self.post_command(self.item, newstate)
            elif pkt[ARP].hwsrc == 'a0:02:dc:e4:fc:8c': # Tide
                state = self.get_status("Pantry_Ceiling_Light")
                newstate = self.toggle(state)
                self.post_command("Pantry_Ceiling_Light", newstate)
            elif pkt[ARP].hwsrc == '74:75:48:8d:7f:9b': # Glad
                pass
```



**What's In
The Box?**

\$1.75 battery



~\$19 components



- *"It also happens to be exactly the same chip used inside the \$19 Spark Photon."* --Matthew Witheiler @ Bit of Cents

Compare To...



\$34.00




This item will be released on October 31, 2015.

Pre-order now.

Ships from and sold by Amazon.com.

Qty:

 Pre-order: Add to Cart

or 1-Click Checkout

 Pre-order with 1-Click

Not yet released

Free shipping once released

Ship to:

DIY Options



WiFi Module - ESP8266

WRL-13678

\$6.95

★★★★☆ 1



SparkFun Electric Imp Breakout

BOB-12886

\$12.95



Edimax WiFi Adapter (EW-7811UN)

WRL-13677

\$14.95



SparkFun WiFi Shield - ESP8266

WRL-13287

\$14.95

★★★★☆ 5



SparkFun ESP8266 Thing

WRL-13231

\$15.95

★★★★☆ 11



SparkFun Electric Imp Shield

DEV-12887

\$19.95



XBee WiFi Module - U.FL Connector

WRL-12570

\$25.95

★★★★☆ 1

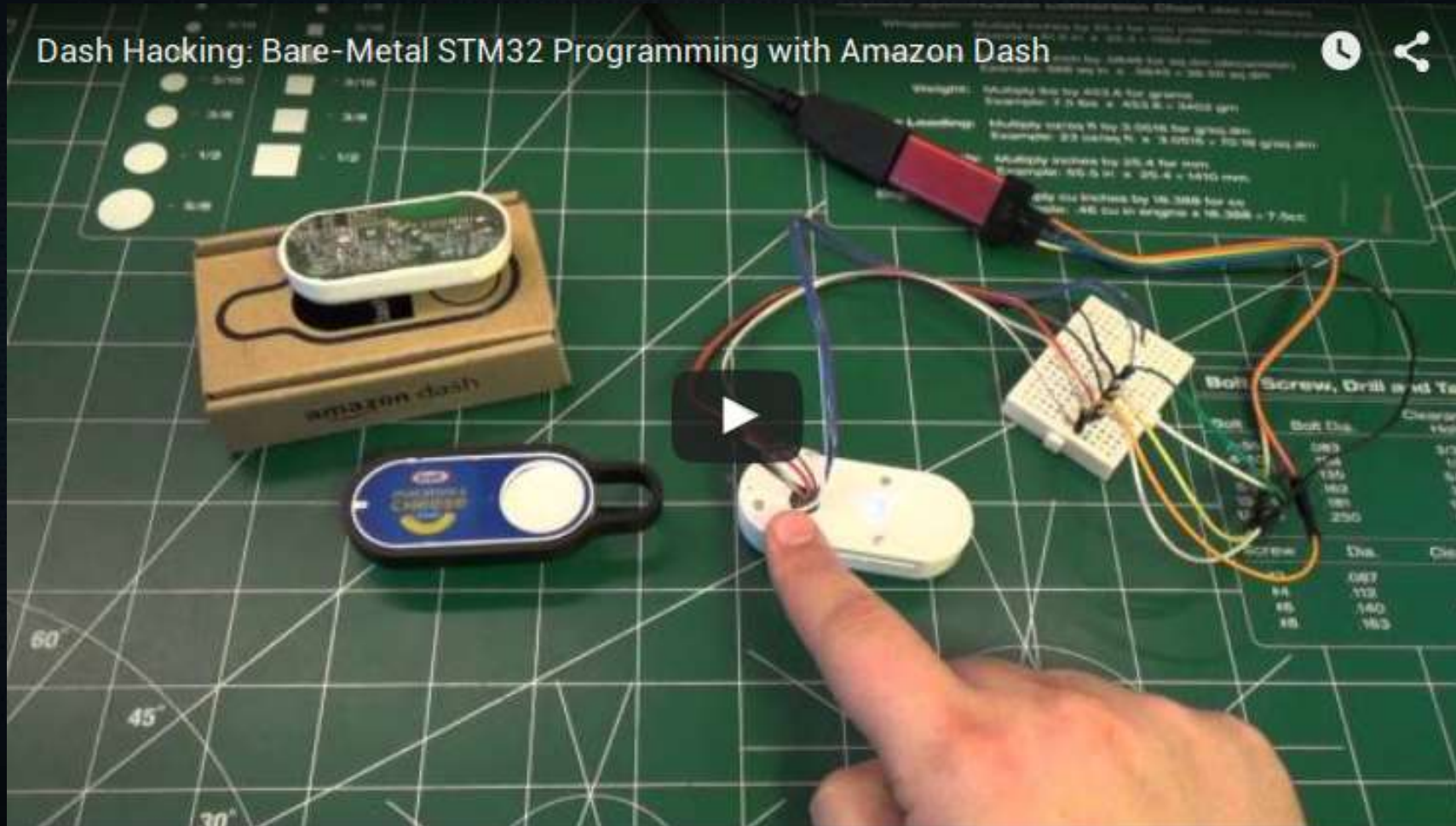


WiFi SMD Module - CC3000

WRL-12820

\$26.95

Future Efforts



References

- <http://blog.nemik.net/2015/08/dash-button-corral/>
- <https://learn.adafruit.com/dash-hacking-bare-metal-stm32-programming/overview>
- <https://community.smartthings.com/t/hack-the-amazon-dash-button-to-control-a-smartthings-switch/20427>
- <http://www.amateurradio.com/inside-the-802-11-bgn-amazon-dash-button/>