

Securing a Home Router

Michael Horowitz

www.michaelhorowitz.com

@defensivecomput

last update: October 4, 2014





Defensive Computing

By Michael Horowitz



Subscribe



Follow @defensivecomput

Secure email in a hostile environment

Three ways to increase the security of email when in a hostile environment such as a computer hacker conference.

July 03, 2014 7:56 PM EDT  1

Comcast XFINITY WiFi: Just say no

By the end of 2014, Comcast plans on having enabled 8 million quasi-public XFINITY WiFi hotspots. Many of these hotspots will run off the home routers of Comcast customers (look for a network called xfinitywifi). Here I offer a long list of security issues with XFINITY WiFi.

Home is where the hotspot is



June 27, 2014 9:43 PM EDT  16

Level Set

- **Modem**: thing that connects you to the Internet
- **Router**: thing that shares a single Internet connection amongs multiple computers and tablets. It is also the source of Wi-Fi networks
- Modem and Router can exist as one device or two
- When combined, called a “**gateway**”
- **Firmware** is the operating system for the router

Level Set

TCP/IP Ports

Basic fundamental networking concept

Always used, seldom seen

<code>http://yahoo.com</code>	Works implicit port number
<code>http://yahoo.com:80</code>	Works explicit port number
<code>http://yahoo.com:82</code>	Fails, wrong port

Routers Make a Great Target

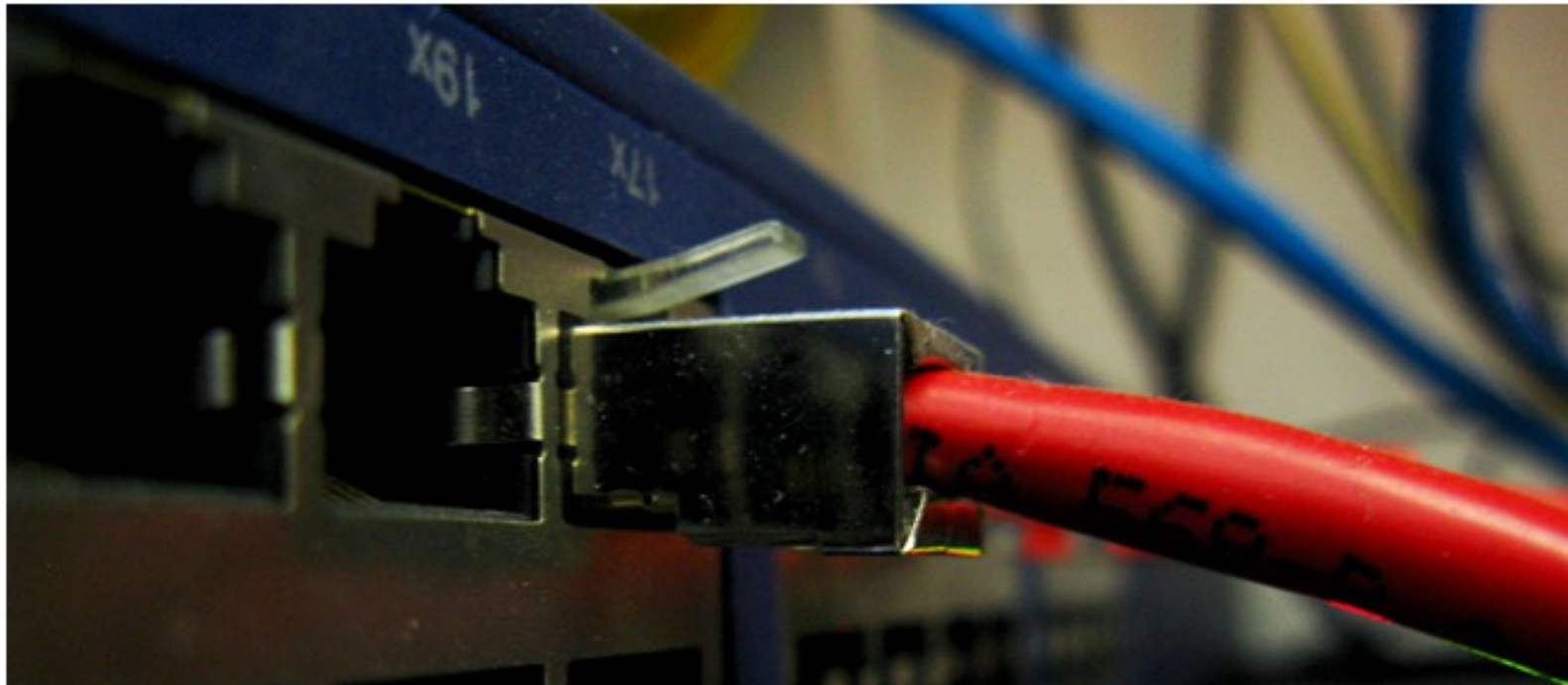
www.wired.com/2013/09/nsa-router-hacking/

WIRED

GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION

NSA Laughs at PCs, Prefers Hacking Routers and Switches

BY KIM ZETTER 09.04.13 | 6:30 AM | [PERMALINK](#)



Glenn Greenwald: how the NSA tampers with US-made internet routers

The NSA has been covertly implanting interception tools in US servers heading overseas – even though the US government has warned against using Chinese technology for the same reasons, says Glenn Greenwald, in an extract from his new book about the Snowden affair, No Place to Hide

- The explosive day we revealed Edward Snowden's identity
- Glenn Greenwald: 'I don't trust the UK not to arrest me'



Glenn Greenwald

The Guardian, Monday 12 May 2014 17.39 EDT

 [Jump to comments \(220\)](#)



POLICY > GOVERNMENT

Beijing to Washington: Ratted-out routers not welcome here

China announces vendor 'vetting' plan to keep out snoopware-infested kit

By Simon Sharwood, 23 May 2014

 Follow 3,512 followers

19

China has taken revenge on the USA for its Huawei ban and router-ratting actions alleged by Edward Snowden, by announcing a new “vetting” process for foreign technology providers.

RELATED



Why the United States Is So Afraid of Huawei

The threat may be theoretical—but compromised telecom equipment could quickly cripple a nation's civilian and military infrastructure.

By Tom Simonite on October 9, 2012

A compromised router

Can spy on you, of course

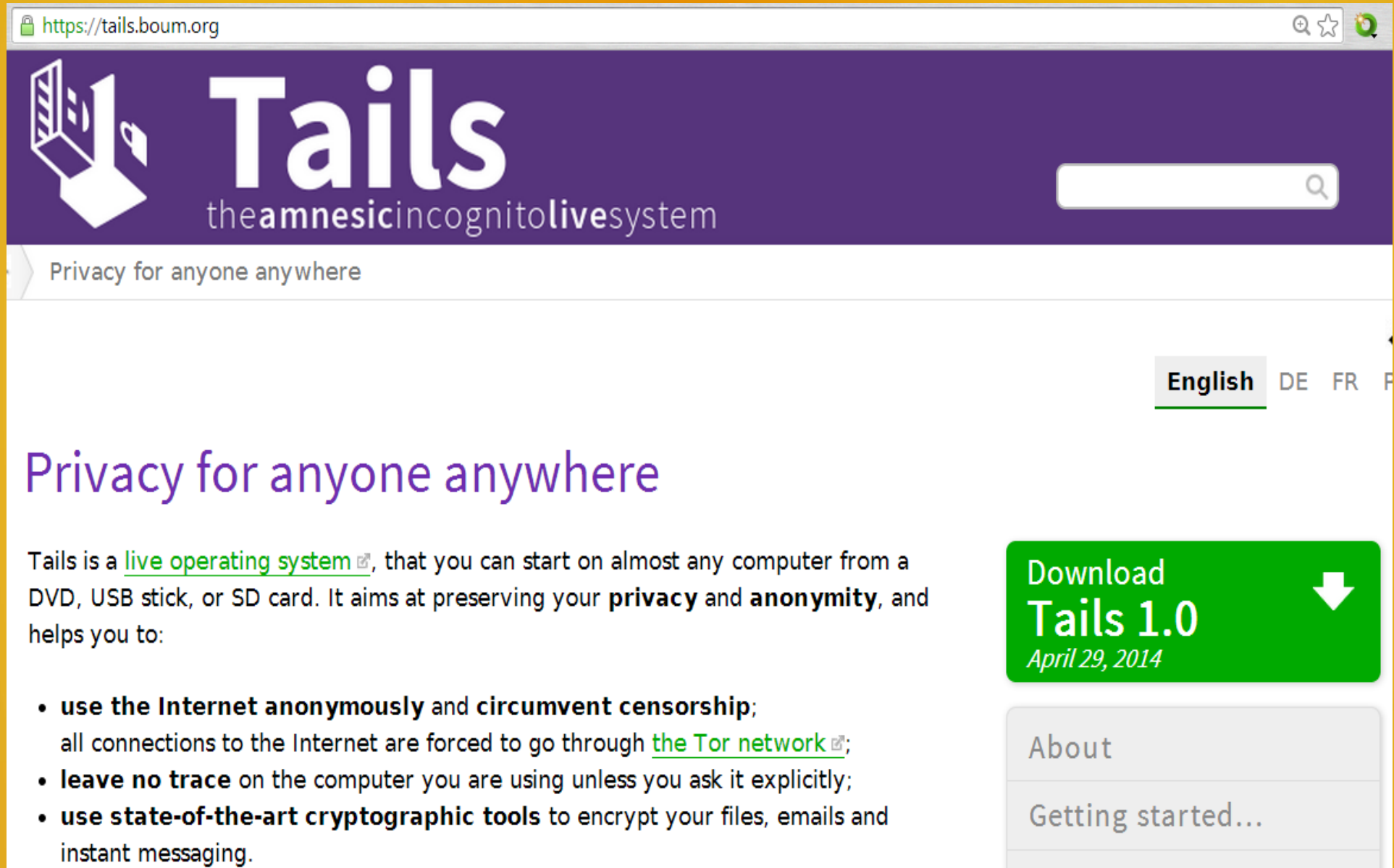
Can easily alter non-encrypted data in-flight

May be added to a botnet

Can run man-in-the-middle attacks to spy on
SSL/TLS traffic

Can send you to evil twin websites

Possible High Value Evil Twin Website



The screenshot shows a web browser window with the address bar displaying <https://tails.boum.org>. The website has a purple header with the Tails logo on the left, which consists of a stylized laptop with a padlock. To the right of the logo, the word "Tails" is written in large white letters, and below it, "the amnesic incognito live system" is written in smaller white letters. A search bar is located on the right side of the header. Below the header, a white banner contains the text "Privacy for anyone anywhere". On the right side of the page, there are language selection buttons for "English", "DE", "FR", and "P". The main content area features the heading "Privacy for anyone anywhere" in purple. Below this, a paragraph describes Tails as a "live operating system" that can be started from a DVD, USB stick, or SD card, aiming to preserve privacy and anonymity. A list of features is provided, including using the Internet anonymously, leaving no trace, and using cryptographic tools. On the right side of the main content, there is a green button labeled "Download Tails 1.0" with a white downward arrow and the date "April 29, 2014". Below this button, there are two buttons: "About" and "Getting started...".

<https://tails.boum.org>

 **Tails**
the amnesic incognito live system

Privacy for anyone anywhere

English DE FR P

Privacy for anyone anywhere

Tails is a [live operating system](#), that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your **privacy** and **anonymity**, and helps you to:

- **use the Internet anonymously** and **circumvent censorship**;
all connections to the Internet are forced to go through [the Tor network](#);
- **leave no trace** on the computer you are using unless you ask it explicitly;
- **use state-of-the-art cryptographic tools** to encrypt your files, emails and instant messaging.

Download Tails 1.0
April 29, 2014

About

Getting started...

Is this really Tails?

 <https://tails.boum.org/download/index.en.html>

3 Verify the ISO image

It is important to check the integrity⁺ of the ISO image you downloaded to make sure that the download went well.



Those techniques rely on standard HTTPS and certificate authorities⁺ to make you trust the content of this website. But, as explained on our warning page, you could still be victim of a man-in-the-middle attack while using HTTPS. On this website as much as on any other of the Internet.

As a consequence, **they don't provide you with a strong way of checking the ISO image authenticity⁺ and making sure you downloaded a genuine Tails.** In a dedicated section, we will propose you some more advanced techniques to check the authenticity of the ISO image.

All Tails ISO image are cryptographically signed by our OpenPGP key.

OpenPGP is a standard for data encryption that provides cryptographic privacy and authentication through the use of keys owned by its users. Checking this signature is the recommended way of checking the ISO image integrity.

Is this really Tails?

<https://tails.boum.org/doc/about/warning/index.en.html#man-in-the-middle>



Tails

the **amnesic** incognito **live** system



doc

about

Warning

Warning

Even though we're doing our best to offer you good tools to protect your privacy while using your computer, **there is no magic or perfect solution to such a complex problem.**

Understanding well the limits of such tools is a crucial step in, first, deciding whether Tails is the right tool for you, and second, helping you making a good use of it.

1. [Tor exit nodes can eavesdrop on communications](#)
2. [Tails makes it clear that you are using Tor and probably Tails](#)
3. [Man-in-the-middle attacks](#)
4. [Confirmation attacks](#)
5. [Tails doesn't encrypt your documents by default](#)
6. [Tails doesn't clear the metadata of your documents for you and doesn't encrypt the Subject: and other headers of your encrypted e-mail messages](#)
7. [Tor doesn't protect you from a global adversary](#)

Re-direct to evil twin websites

Classic attack: Malicious DNS servers

Instead of resolving tails.boum.org
to 204.13.164.188
resolve it to 6.7.8.9

How would you know?

Re-direct to evil twin websites

Think you won't fall for malicious DNS?

Your computer uses hard coded DNS servers instead of those offered by the router

- You still make easily detected DNS requests
UDP on port 53
- Compromised firmware can watch for DNS requests and answer some on its own without passing them through

Re-direct to evil twin websites

You avoid DNS altogether

Instead of tails.boum.org you go to 204.13.164.188

How do you know that is the correct IP address?

Game over: Even if it *is* the correct IP, a compromised ISP may still send you to an evil twin of tails.boum.org

Be a lesser target

Spy agencies can probably hack into Cisco and Juniper routers in their sleep

On the home front, bag guys and spies are more likely to pay attention to popular routers

→ Avoid consumer routers.

If a router is sold at Best Buy don't buy it

→ If a router is given to you by your ISP don't use it

→ ISP gateways can be converted to modems so that you can add your own router

How configure a router?

- Internal website
- Smartphone apps
- Cloud management via vendor websites
- Apple AirPort utility from OS X
- UPnP
- Telnet, SSH

IP address of router

To use the internal/administrative website of a router, requires that you know the IP address of the router.

See my Sept. 2013 blog

COMPUTERWORLD[White Papers](#)[Webcasts](#)[Newsletters](#)

[Topics](#) [News](#) [In Depth](#) [Reviews](#) [Blogs](#) [Opinion](#)



Michael Horowitz
Defensive Computing
[Read Bio](#) | [See Posts](#)

 [Subscribe](#)  [Follow @defensivecomput](#)

Find the IP address of your home router

By [Michael Horowitz](#)
September 09, 2013 1:45 PM EDT [12 Comments](#)

In an upcoming blog I expect to write about configuring a home router, which requires logging on to it. This, in turn, requires knowing the IP address of the router. Non-techies typically don't know anything about IP addresses, let alone the one assigned to their router. Since I expect the upcoming blog to be fairly long, I decided to start with this cheat sheet for learning the IP address of a router.

Rounding up the usual suspects

- Change the router password
- Update the router firmware – risky
- Eat your vegetables

Router Password

- Anything but the default (if not using remote admin)
- If using Remote Administration then *very* long
- Some routers let you change the userid too
this is great!
- Some routers offer a second read-only userid

New Firmware Notification

- Router may do nothing
- Router may offer a manual online check
- Router may check on its own and tell you when you login to admin website
- Router may send you an email notification of new firmware (Peplink does)
- Self-update automatically? Verizon FIOS
ActionTec *maybe*

Defensive Steps for new Firmware

- ✓ Download current firmware, if possible, to fall back to
- ✓ Download a file of the current settings, again for fallback
- ✓ Take pictures of the admin screens in case some settings get changed
- ✓ Have a spare router

Step up in class



Reboot System

Select the firmware you want to use to start up this device:

- ☐ Firmware 1: 6.1.0 build 1419
- ☒ Firmware 2: 6.1.1m46 build 1496 (Running)

Reboot

SSID (network name)

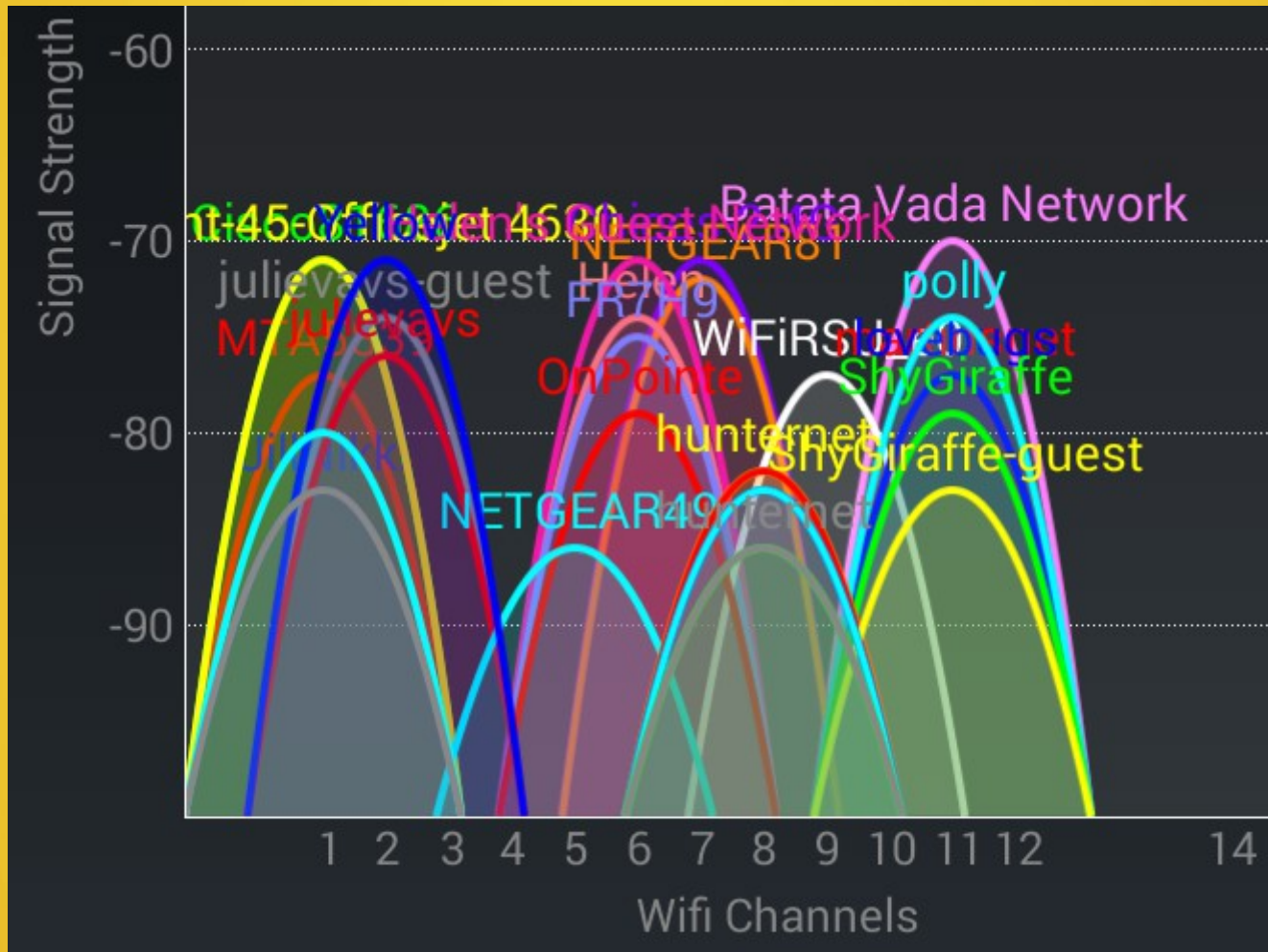
Change the default

Dont' give away personal information

Hiding is a waste of time



2.4GHz vs 5GHz



Wi-Fi Encryption

- WEP bad, WPA eh, WPA2 best
- WPA2: if asked, opt for AES (a.k.a.CCMP). Do not use TKIP
- Some routers do not have an option for only WPA2
- WPA2 needs a *loooooong* password

Wi-Fi Passwords

 **Gibson Research Corporation** • Security

Home ▾ SpinRite ▾ Services ▾ Freeware ▾ Research ▾ Other ▾



Perfect Passwords

GRC's Ultra High Security Password Generator

24,195 sets of passwords generated per day
14,072,116 sets of passwords generated for our visitors

Generating long, high-quality random passwords is not simple. So here is some totally random raw material, generated just for **YOU**, to start with.

Every time this page is displayed, our server generates a unique set of custom, high quality, cryptographic-strength password strings which are safe for you to use:

64 random hexadecimal characters (0-9 and A-F):

446A860AFF331FB1AEACD98AB668BA4549F825FB8F9186D71DFEFBA7D6295E37

63 random printable ASCII characters:

`PB=!E,b-!irF?EHxMv0^{~n5>hjIcULVq1]K{sOymMF&LB~Q,E^oc`#*<yM5;H

63 random alpha-numeric characters (a-z, A-Z, 0-9):

n3ouwdewsu591dgmXRGKKzW6uwqmDWae0MWXP6HeIlvowfpRZjA8aIhrSkeRWpR

Click your web browser's "refresh" button a few times and watch the password strings change each time.

Wi-Fi Passwords

BAD: **kyPeQ3!khx** (too short, can't remember it)

GOOD: **..new..york..yankees..** (long, easy to remember)

Other Good passwords

- ✓ Like red tulips? **red123TULIPS123**
- ✓ Like Shakespeare? **tobeornottobe-->THATisthe?**
- ✓ From New York City> **new-yawk-RULES!!!!**
- ✓ Like XKCD comics? **BatteryHorseStapleEtcEtcEtc**
- ✓ Like being a smartass? **>>>>>>>thisismypassword**
- ✓ Like to remember a date/place? **Denver///2009///**
- ✓ Want to remember HOPE? **HOPEX==hotel==statler**



The Hacker NewsTM

Security in a serious way

Smart LED Lightbulbs Can be Hacked too; Vulnerability exposes Wi-Fi Passwords

 Tuesday, July 08, 2014  Swati Khandelwal



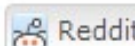
Share

1586



Tweet

552



Reddit

0



Share

92



ShareThis

2466



Topics ▾

News

In Depth

Reviews

Blogs ▾

Opinion

St



Michael Horowitz

Defensive Computing

[Read Bio](#) | [See Posts](#)



Subscribe



Follow @defensivecomput

Google knows nearly every Wi-Fi password in the world

By [Michael Horowitz](#)

September 12, 2013 10:44 PM EDT 193 Comments



Share

589



If an Android device (phone or tablet) has ever logged on to a particular Wi-Fi network, then Google probably knows the Wi-Fi password. Considering how many Android devices there are, it is likely that Google can access most Wi-Fi passwords worldwide.

Lock Down Local Admin

Worst `http://192.168.1.1`

Better `http://192.168.1.1:22999`

Better `https://192.168.1.1`

Best `https://192.168.1.1:22999`

And ...

Lock Down Local Admin

- If possible, change the admin userid
- Turn off wireless access to admin site
only Ethernet clients can make changes
- If possible, logon as a read-only user
- Log out when done
- Set a timeout in case you forget to log out
- Use private browsing mode for administration
- Turn off Telnet, SSH access

Lock Down Remote Admin

Local	http://192.168.1.1
Remote	http://auntsally.dyndns.org

Linksys calls it “remote administration”

Netgear calls it “remote management”

Asus calls it “Web Access from WAN”

Verizon FIOS calls it

“Incoming WAN access to Web-Management”

Peplink calls it “Web admin access”

Configuring Remote Admin on Asus

Authentication Method	HTTPS ▼
HTTPS Lan port	8686 Access setting page via https://router.asus.com:8686
Enable Web Access from WAN	☒ Yes ☐ No
Port of Web Access from WAN	HTTPS: 8558
Only allow specific IP	☐ Yes ☒ No

DDNS for Remote Admin

`https://auntsally.dyndns.org:22333`

WAN - DDNS	
DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to a dynamic public IP address, through its registered domain name. The wireless router is enabled for DDNS and other DDNS services.	
Enable the DDNS Client	☐ Yes ☐ No
Server	www.DYNDNS.ORG Free Trial
Host Name	b[REDACTED]dns.org
User Name or E-mail Address	[REDACTED]
Password or DDNS Key	[REDACTED]
Enable wildcard	☐ Yes ☐ No

DNS Servers

- DNS translates computer names to IP addresses

`www.hope.net => 207.99.30.200`

- Every ISP offers at least two DNS server computers
- I prefer OpenDNS.com
- They do more and offer more privacy
- OpenDNS offers free services without opening an account
- Family Shield blocks porn, no account needed
- Open a free account for more features, paid for more still

DNS Servers

- Regular OpenDNS 208.67.222.222 and 208.67.220.220
- Family Shield 208.67.222.123 and 208.67.220.123
- Audit OpenDNS at <https://store.opendns.com/settings>
- DYN, Norton and Comodo also offer free DNS services
- Google has the easiest to remember DNS server IP address

8.8.8.8

Auditing DNS Servers

- A popular attack is changing the DNS servers used by the router and/or provided to clients via DHCP. There are two websites that show your current DNS servers

<https://www.dnsleaktest.com> and

myresolver.info

Your IP address

208.67.217.13 (?)

The source IP address of your DNS recursive resolver

208.67.217.13 (?)

m3.nyc.opendns.com

Guest Networks

- Secondary networks with different passwords
- Hopefully better separation from private network
- Change password frequently
- TURN OFF when not in use
- Look for scheduling of Guest networks

Who is on your network

- Consumer routers do a poor job
- FING runs on Android and iOS
- Nirsoft Wireless Network Watcher on Windows
- Skydog is no more. Eaten by Comcast

Fing

**Overlook WiFi**

Wireless network

18/20

12 hours ago

**192.168.0.1**

00:18:4D:CC:BB:F5

Router

Netgear

**192.168.0.5 (+4)**

00:17:F2:97:A4:5A

Desktop

Apple

**192.168.0.12**

00:0E:7F:96:D3:27

Printer

HP

**192.168.0.13**

00:12:FB:5C:93:C1

TV

Samsung

**192.168.0.14**

04:1E:64:45:4A:53

iPhone

Apple

**192.168.0.15**

00:13:A9:5C:93:C2

Laptop

Sony

**192.168.0.20**

04:1E:64:45:4A:54

iPod

Apple

**192.168.0.22**

04:1E:64:45:4A:55

iPad

Apple

**192.168.0.23**

00:12:FA:6C:93:C1

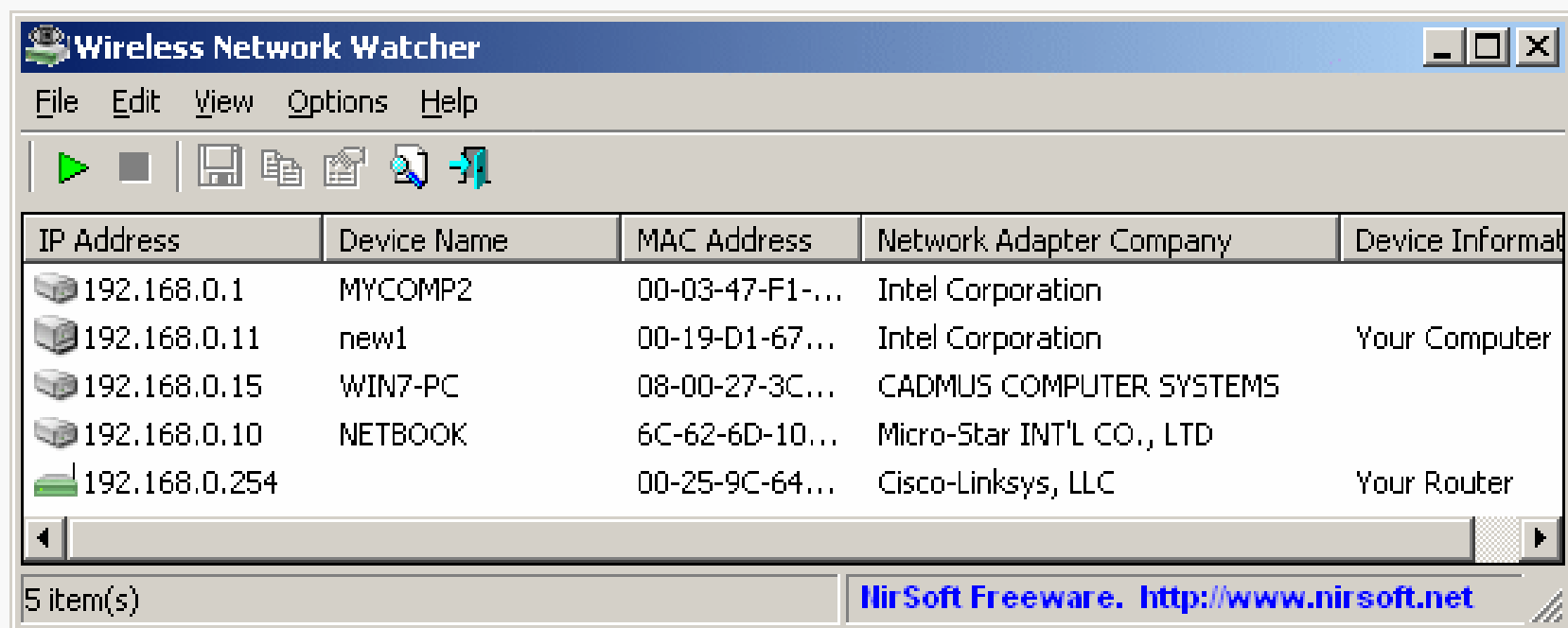
Media Player

THX

Description

Wireless Network Watcher is a small utility that scans your wireless network and displays the list of For every computer or device that is connected to your network, the following information is displayed name.

You can also export the connected devices list into html/xml/csv/text file, or copy the list to the clipboard.



Peplink Monitoring

Filter

☐ Online Clients Only

☐ DHCP Clients Only

Client List

	IP Address ▲	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal
	192.168.1.1	Mikrotik	0	0	F0:D8:00:00:00:00		
	192.168.1.2	VonageBoxy	0	0	90:68:00:00:00:00		
	192.168.1.3	Sar	0	0	28:98:00:00:00:00		
	192.168.1.4	SqueezeboxRadio	0	0	00:04:00:00:00:00		 -52dBm

Peplink Monitoring

Outbound

Protocol	Source IP ↓	Destination IP	Service	Interface
TCP	192.168.1.1	192.168.1.100:88:5228		WAN
TCP	192.168.1.1	192.168.1.100:25:5222	XMPP/Jabber	WAN
TCP	192.168.1.1	192.168.1.100:6:443	HTTPS	WAN
TCP	192.168.1.1	192.168.1.100:6:443	HTTPS	WAN
UDP	192.168.1.1	192.168.1.100:10000	SIP	WAN
TCP	192.168.1.1	192.168.1.100:9000	HTTP	WAN
TCP	192.168.1.1	192.168.1.100:7:3483		WAN
UDP	192.168.1.1	192.168.1.100:8	NTP	WAN
TCP	192.168.1.1	192.168.1.100:443	HTTPS/SSL	WAN

Total searched results: 9

Inbound

Protocol	Source IP	Destination IP	Service	Interface
No sessions				

Hiding on the Internet

- Ping response blocking
- HNAP
- Firewall and ports

Router is a computer

What might happen when unsolicited data packets from the Internet hit a router?



Hiding From Ping

How do bad guys on the Internet find you?

One way is the TCP/IP Ping command

All routers have an option to ignore Ping commands

```
C:\Users\me>ping yahoo.com
Pinging yahoo.com [98.139.183.24] with 32 bytes of data:
Reply from 98.139.183.24: bytes=32 time=29ms TTL=50
Reply from 98.139.183.24: bytes=32 time=38ms TTL=50
Reply from 98.139.183.24: bytes=32 time=54ms TTL=50
Ping statistics for 98.139.183.24:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 29ms, Maximum = 54ms, Average = 41ms
```

Hiding From Ping

Terminology for disabling the Ping response

- Netgear says “*Respond to Ping on the Internet Port*”
- ASUS calls this “*Respond PING Request from WAN*”
- Linksys calls it “*Block Anonymous Internet Requests*”
- Peplink calls it “*Reply to ICMP PING*”

HNAP Reconnaissance

Home Network Administration Protocol

Yet another way to access a router

Offers up technical details of the router

Designed for Hardware manufacturer to remotely manage devices

No password needed in next slide

← → ↻  ~~https://192.168.1.100/~~HNAP1/

This XML file does not appear to have any style information associated with it. The document tree is

```
▼<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  ▼<soap:Body>
    ▼<GetDeviceSettingsResponse xmlns="http://purenetworks.com/HNAP1/">
      <GetDeviceSettingsResult>OK</GetDeviceSettingsResult>
      <Type>GatewayWithWiFi</Type>
      <DeviceName/>
      <VendorName>Linksys by Cisco</VendorName>
      <ModelDescription>Internet Gateway Device</ModelDescription>
      <ModelName>WRT54GL</ModelName>
      <FirmwareVersion>v4.30.16</FirmwareVersion>
      <PresentationURL>/</PresentationURL>
    ▼<SOAPActions>
      <string>http://purenetworks.com/HNAP1/IsDeviceReady</string>
      <string>http://purenetworks.com/HNAP1/GetDeviceSettings</string>
      <string>http://purenetworks.com/HNAP1/SetDeviceSettings</string>
      <string>http://purenetworks.com/HNAP1/GetDeviceSettings2</string>
      <string>http://purenetworks.com/HNAP1/SetDeviceSettings2</string>
      <string>http://purenetworks.com/HNAP1/Reboot</string>
      <string>http://purenetworks.com/HNAP1/GetWanSettings</string>
      <string>http://purenetworks.com/HNAP1/SetWanSettings</string>
      <string>http://purenetworks.com/HNAP1/GetWanInfo</string>
      <string>http://purenetworks.com/HNAP1/RenewWanConnection</string>
      <string>http://purenetworks.com/HNAP1/AddPortMapping</string>
      <string>http://purenetworks.com/HNAP1/GetPortMappings</string>
      <string>http://purenetworks.com/HNAP1/DeletePortMapping</string>
      <string>http://purenetworks.com/HNAP1/GetMACFilters2</string>
      <string>http://purenetworks.com/HNAP1/SetMACFilters2</string>
    ▼<string>
      http://purenetworks.com/HNAP1/GetRouterLanSettings2
    </string>
    ▼<string>
      http://purenetworks.com/HNAP1/SetRouterLanSettings2
    </string>
      <string>http://purenetworks.com/HNAP1/GetConnectedDevices</string>
      <string>http://purenetworks.com/HNAP1/GetNetworkStats</string>
```

HNAP More Info

“...for devices that might potentially be deployed and managed by an ISP, or even by a corporation to remote sites, you want a management protocol that is on by default, and is difficult for the remote user to turn off. Or from some reports, on some devices this protocol stays enabled even after your turn it off”

More on HNAP - What is it, How to Use it, How to Find it by Rob VandenBrink Feb 214

<https://isc.sans.edu/diary/More+on+HNAP+-+What+is+it+How+to+Use+it+How+to+Find+it/17648>

See also

www.cisco.com/web/partners/downloads/guest/hnap_protocol_whitepaper.pdf

www.tenable.com/blog/hnap-protocol-vulnerabilities-pushing-the-easy-button

<https://isc.sans.edu/forums/diary/Linksys+Worm+TheMoon+Summary+What+we+know+so+far/17633>

Firewall and Ports

Firewall in router Lords Over all ports

Can be open, closed or stealthed

Stealth is the best, sends incoming data packets to the bit bucket. Suppressing Ping response is stealth

Open is usually a mistake for home routers, used to run a server

Closed means the incoming packet is not processed, but an error message is sent. Like answering a knock on the door with “go away”. Shows someone is home.



ShieldsUP!!

Port Authority Edition – Internet Vulnerability Profiling

by Steve Gibson, Gibson Research Corporation.

- **For orientation and background**, please examine the page links provided below for important information about Internet vulnerabilities, precautions and solutions.
- **First time users** should start by checking their **Windows File Sharing** and **Common Ports** vulnerabilities with the "File Sharing" and "Common Ports" buttons below.
- For orientation and information about the Port Authority system, **click the Home or Help icons** in the titlebar . . .

[Click here](#) to check your router now...

**GRC's Instant UPnP
Exposure Test**

HOME

ShieldsUP!! Services

HELP

File Sharing

Common Ports

All Service Ports

Messenger Spam

Browser Headers

You may select any service from among those listed above . . .

User Specified Custom Port Probe

Lookup Specific Port Information

Or enter a port to lookup, or the ports for a custom probe to check, then choose the service. Your computer at IP 24.215.161.102 will be tested.

https://www.grc.com/shieldsup

PASSED

TruStealth Analysis

Your system has achieved a **perfect** "TruStealth" rating. **Not a single packet** — solicited or unsolicited — was received as a result of our security probing tests. Your system ignored and refused to reply to repeated probes of any hacker, this machine does not exist on the Internet. Some hackers reveal their presence by attempting to "counter-probe the prober", thus revealing themselves. But your system did not.

Port	Status	Protocol and Address
<u>20</u>	Stealth	ftp-data File Transfer Protocol (Default Data Channel)
<u>21</u>	Stealth	ftp File Transfer Protocol (Control Channel)
<u>22</u>	Stealth	ssh SSH Remote Login Protocol
<u>80</u>	Stealth	http World Wide Web HTTP
<u>8080</u>	Stealth	http-alt HTTP Alternate (see <u>port 80</u> and <u>port 81</u>)

Another Firewall tester works on TCP or UDP

<https://pentest-tools.com/discovery-probing/udp-port-scanner-online-nmap>

<https://pentest-tools.com/discovery-probing/tcp-port-scanner-online-nmap>

Router Software STINKS!

Perhaps developed by amateurs

Perhaps developed with spying in mind

Perhaps both

First thing EFF said in discussing their upcoming firmware

Asus password length bug

Netgear DDNS bug

July 2013 Independent Security Evaluators

EE BrightBox router http://1.2.3.4/cgi_status.js

<https://scotthelme.co.uk/ee-brightbox-router-hacked/>
securityevaluators.com/knowledge/case_studies/routers/soho_techreport.pdf/

Router Software STINKS!

This is the error that made me realize it was time to step up from consumer routers.

**A change has been made, causing disconnection to setting page.
You may made the change in changing IP address, changing port
number or disconnecting Wi-Fi to RT-N56U.
Please re-connect Wi-Fi and use modified IP address and port number to
access setting page of RT-N56U.**

Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0

Worng Worng Worng

thewirecutter.com



Jump to a category...



The Best Wi-Fi Router

Netgear R6250

It took months of research and in-depth testing to find our new best Wi-Fi router. The [Netgear R6250](#) has the best balance of speed, price, stability, and features compared to the competition. But depending on what you own now, you may want to wait to upgrade.

The Wirecutter backtracks

▼ Expand Previous Updates

April 28, 2014: The Asus RT-AC56U is no longer our pick for best Wi-Fi router because of severe connectivity issues on its 2.4Ghz band (and we're working on a guide detailing why Netgear's R6250 is a better choice). But if you do own the Asus already, you should download the router's latest firmware update as soon as possible. We don't know if it will fix the 2.4Ghz issues, but we will test it ourselves to find out.

April 15, 2014: Based on our hands-on testing with the Asus RT-AC56U, we have determined that the router can have severe connectivity issues on its 2.4GHz band. While this might not affect all RT-AC56U routers in all scenarios, it's prevalent enough to render this device ineligible to be our pick for best Wi-Fi router. We're recommending Netgear's R6250 in its place — look for a full analysis to come shortly.

March 28, 2014: If you buy this or another Asus router like the RT-N56U, RT-N66U, AC66U, or AC68U, update your firmware immediately to prevent attackers from accessing USB storage devices attached to your router. It's a good idea to download the firmware from the Asus website to ensure you get the very latest version.

▲ Collapse Previous Updates

The Woops of WPS



The screenshot shows a web browser window with the address bar displaying www.wi-fi.org/discover-wi-fi/wi-fi-protected-setup. Below the address bar is a header section with the Wi-Fi Alliance logo on the left and the text "The worldwide network of companies that brings you Wi-Fi®" on the right. The main content area has a heading "Wi-Fi Protected Setup" followed by two paragraphs of text. The first paragraph describes WPS as an optional certification program for ease of setup. The second paragraph states that WPS products have industry-standard security features provided by WPA2™ and gives consumers an easier approach to setting up a security-protected Wi-Fi connection.

← www.wi-fi.org/discover-wi-fi/wi-fi-protected-setup

 The worldwide network of companies that brings you Wi-Fi®

Wi-Fi Protected Setup

Wi-Fi Protected Setup™ is an optional certification program based on technology designed to ease the setup of security-enabled Wi-Fi® networks in home and small office environments. Wi-Fi Protected Setup supports methods (pushing a button, entering a PIN, or using NFC) that are familiar to most consumers to configure a network and enable security.

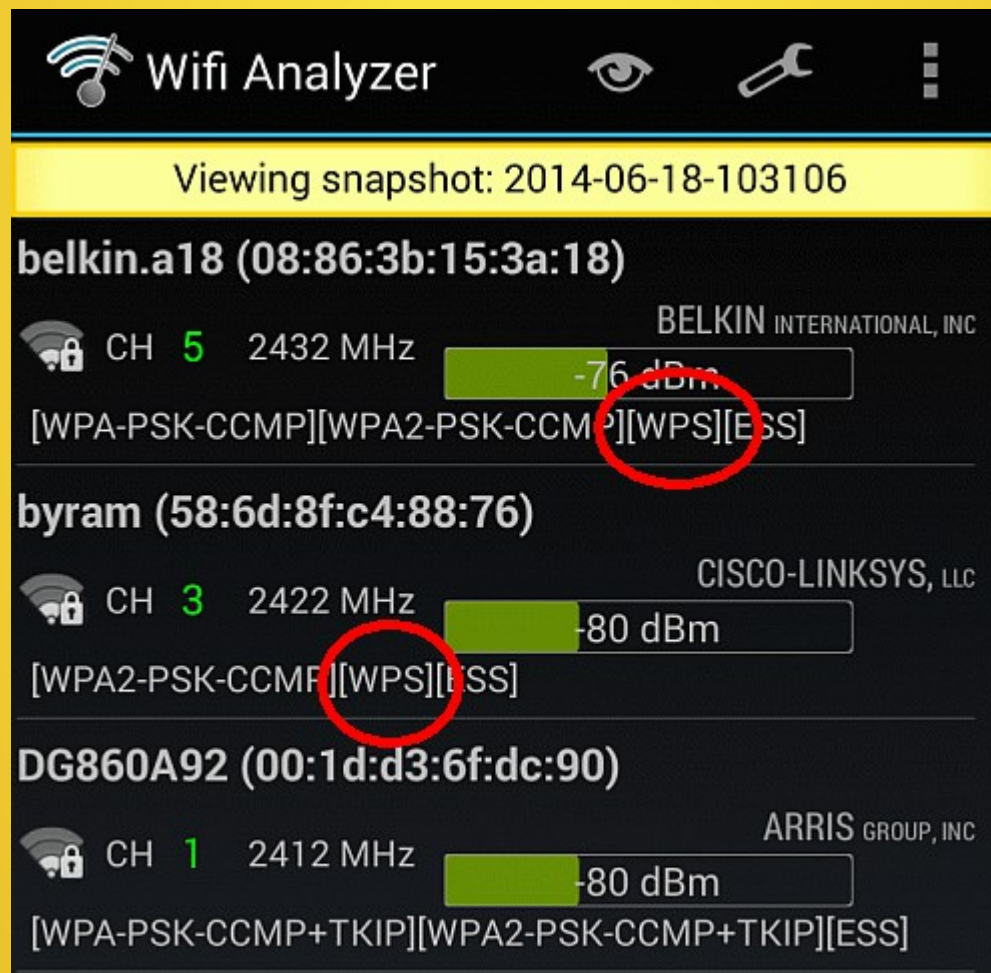
Like all Wi-Fi CERTIFIED™ products, Wi-Fi Protected Setup products have industry-standard security features provided by WPA2™. Wi-Fi Protected Setup gives consumers an easier approach to set up a security-protected Wi-Fi connection, either between devices or in a network configuration. Additional devices can be easily added to a Wi-Fi Protected Setup network over time.

WPS is being used

Sophos scanned London in April 2014

Total Networks: 81,700 WPS enabled on almost 28,000

www.sophos.com/en-us/press-office/press-releases/2014/04/london-warbiking.aspx



WPS push button mode

SLASH GEAR REVIEWS COLUMNS FEATURES TEGRA HUBS

D-Link WiFi Smart Plug Review

4

May 22, 2014

 Tweet 25  22

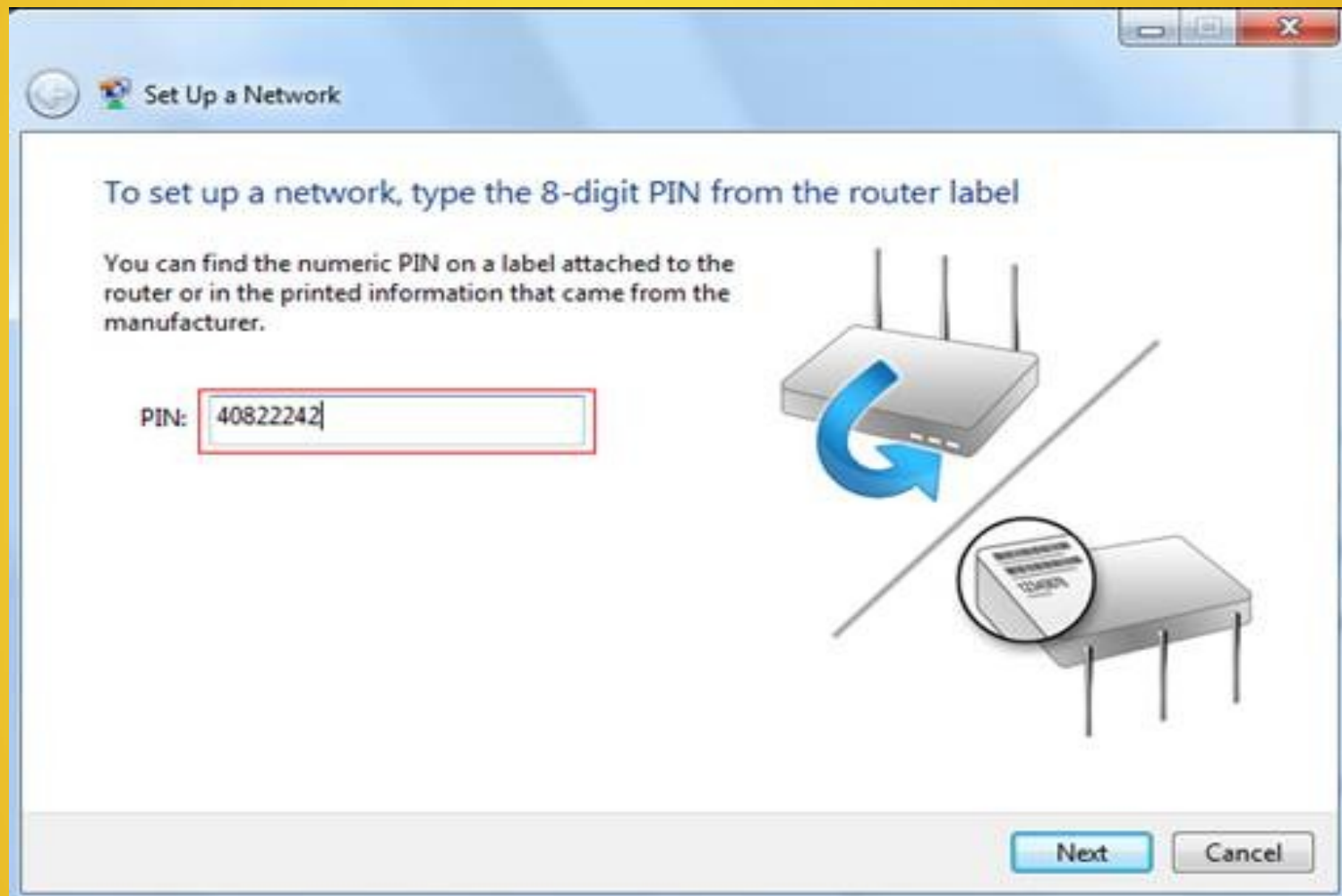


Piecing together your own **smart home** used to be a headache; now, you can buy products off-the-shelf, like **D-Link's new WiFi Smart Plug**, and be up and running from your smartphone in minutes. We're not just talking remote control over lights, either: D-Link's system allows for power and heat monitoring, for the frugal and safety-conscious among us. Read on for our full review.

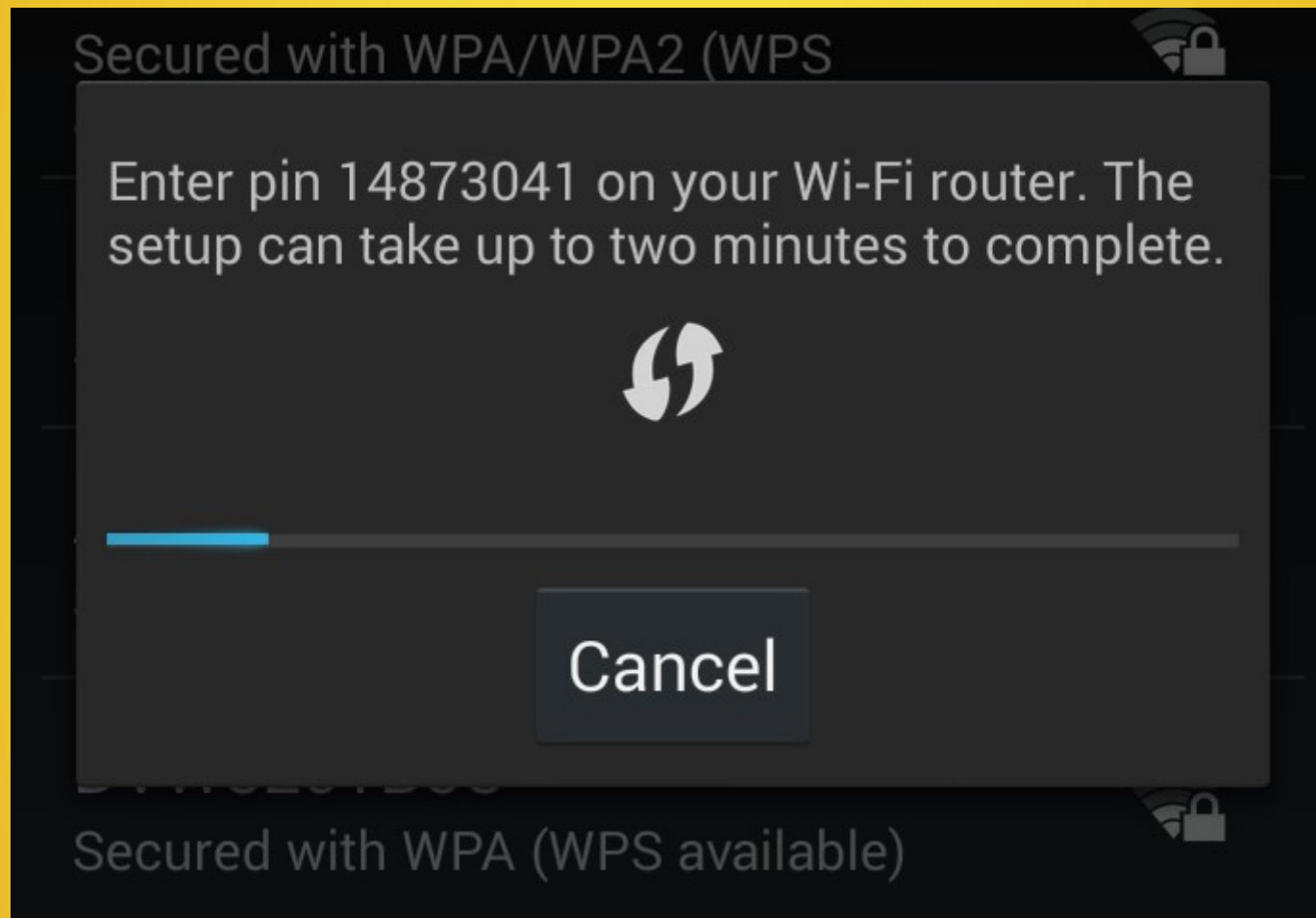


Chris Davies

WPS initial router setup



WPS Entering a PIN



WPS 4th mode of operation

Every consumer router has a hard wired WPS PIN code

8 digits. See it on label on the router

Wireless client provides the PIN code and gets onto network



The s--- hits the fan

KrebsonSecurity

In-depth security news and investigation



BLOG ADVERTISER

29 New Tools Bypass Wireless Router Security

DEC 11

Security researchers have released new tools that can bypass the encryption used to protect many types of wireless routers. Ironically, the tools take advantage of design flaws in a technology pushed by the wireless industry that was intended to make the security features of modern routers easier to use.

At issue is a technology called “Wi-Fi Protected Setup” (WPS) that ships with many routers marketed to consumers and small businesses. According to the [Wi-Fi Alliance](#), an industry group, WPS is “designed to ease the task of setting up and configuring security on wireless local area networks. WPS enables typical users who



Recent

Thieves

ATMs

True Good

Not Secure

Backdoor

Surveillance

Complex

Security

Expert: B

Bitcoin B

Pro and

The shame continues

www.pcworld.com/article/2141540/need-wi-fi-access-re

Need Wi-Fi access? Just reach out and touch your router



Yardena Arar
@dennyarar

Apr 9, 2014 5:00 AM



Networking devices that don't have conventional user interfaces is one of the bigger barriers to realizing the Internet of Things. To make that process easier, the Wi-Fi Alliance has added support for NFC (near-field communication) technology to its WPS (Wi-Fi Protected Setup) security standard. Instead of typing characters or pushing buttons, you'll soon be able to add an NFC device to your network by simply tapping it against your router.

WPS Gets Worse

In August 2014, Dominique Bongard of 0xcite in Switzerland reported that rather than make brute force guesses, he can calculate the correct PIN code after a single guess. Does not work on all routers.

<http://www.slideshare.net/0xcite/offline-bruteforce-attack-on-wifi-protected-setup>

Offline bruteforce attack on WiFi Protected Setup

Dominique Bongard
Founder
0xcite, Switzerland
@reversity

Port 32764 *issue*

Routers are spying on you





How Sercomm saved my Easter!

*Another backdoor in my router:
when Christmas is NOT enough!*



Released 18/04/2014

By Eloi Vanderbeken - Synacktiv

So you can reactivate the backdoor again...



- If you're on the LAN
- Or if you're an Internet provider (if you're one-hop away, you can craft Ethernet headers)
- It's **DELIBERATE**
- You can also use the 0x200 packet type to ping the router (it will respond with its MAC address) and 0x202 to change its LAN IP address

Port 32764 Coverage

Good writeup on this by Sophos April 2014

nakedsecurity.sophos.com/2014/04/23/the-soho-router-backdoor-that-was-fixed-by-hiding-it-behind-another-backdoor/



Yet Another Open Port

UDP port 53413 open and listening on WAN side

More than a million vulnerable Netcore routers in China

The fix here too, left the code and closed the port in a way it could be re-opened

Netis Routers Leave Wide Open Backdoor

by Tim Yeh at Trend Micro Aug 25, 2014

blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/

Netis Router Backdoor “Patched” But Not Really

by Tim Yeh Oct 3, 2014

blog.trendmicro.com/trendlabs-security-intelligence/netis-router-backdoor-patched-but-not-really

UPnP

Protocol to simplify the discovery and configuration of network devices without user involvement

UPnP is everywhere: Routers, printers, computers, NAS, IP cameras, Smart TVs

Designed for internal LAN use only – no security to speak of

Can be used to poke a hole in the firewall of a router

Turn it off in your router (If possible. Then test it.)

CERT warned in 2011 of devices exposing UPnP **on the Internet**
WTF?

UPnP

Security firm Rapid7 scanned the entire Internet every week for five months in 2012 and found

- Over 80 million unique IPs responded to UPnP discovery requests
- 17 million devices are remotely configurable
- 23 million devices vulnerable to a remote code execution flaw
- Vulnerable devices from 1,500 vendors

You can't make this stuff up

There are two online tests for UPnP on your router

Rapid7 offers free Windows software to test other routers

UPnP

Sophos: “Nearly ever vendor you have ever heard of in the home/SOHO business has routers on the list of vulnerable products. How a router manufacturer could ship a product that lets you configure the firewall without authentication on the outside interface is beyond me.”

nakedsecurity.sophos.com/2013/02/05/upnp-flaws-turn-millions-of-firewalls-into-doorstops/



Again: If a router is sold at a retail establishment, you don't want it

ShieldsUP!!tm

Port Authority Edition – Internet Vulnerability Profiling

by Steve Gibson, Gibson Research Corporation.

SAMPLE
Click HERE to test

Universal Plug n'Play (UPnP) Internet Exposure Test

be sends up to ten (10) UPnP Simple Service Discovery Protocol (SSDP) M-SEARCH UDP packets to your visitor's current IPv4 address (**10.1.1.1**) in an attempt to solicit a response from any public UPnP SSDP service. The UPnP protocols were **never** designed to be exposed to the public Internet. Equipment which does so should be considered defective, insecure, and unusable. Any such equipment should be disconnected immediately.

Your equipment at IP:

10.1.1.1

Is now being queried:



**THE EQUIPMENT AT THE TARGET IP ADDRESS
DID NOT RESPOND TO OUR UPnP PROBES!**

(That's good news!)



Universal Plug and Play

Router Security Check

Universal Plug and Play (UPnP) is a protocol standard that allows easy communication between computers and network-enabled devices. This protocol is enabled by default on millions of systems, including routers, printers, media servers, IP cameras, smart TVs, home automation systems, and network storage servers.

Recent research from Rapid7 revealed that at least 40-50 million of these devices are at risk due to security flaws in the UPnP protocol. These issues potentially expose millions of users to remote attacks that could result in the theft of sensitive information or further assaults on connected machines such as personal computers.

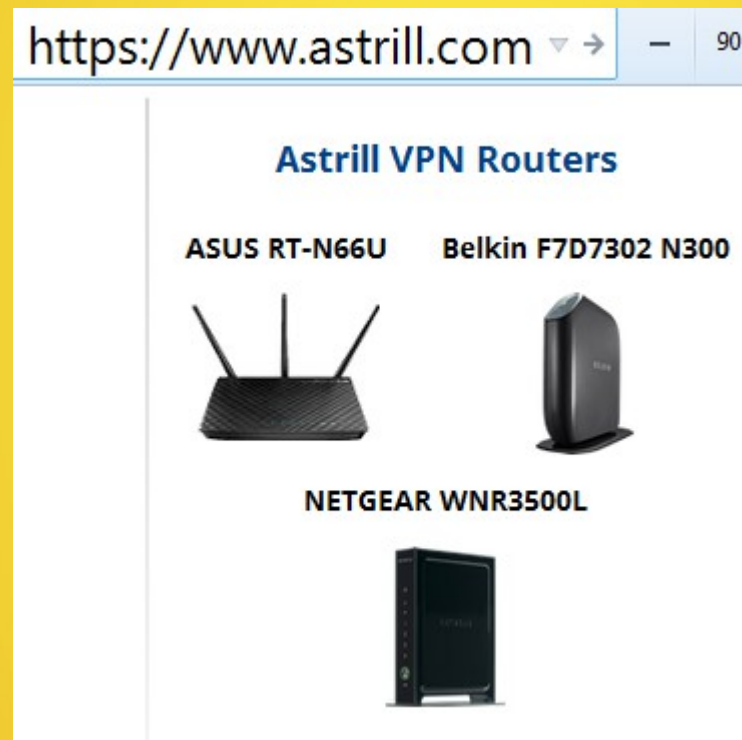
This service can test your router and determine whether it is vulnerable to attack. Clicking the Scan My Router button below will start the test. To learn more about UPnP vulnerabilities, please see [this blog post](#).

This service is only suitable for identifying whether your UPnP is exposed to the internet. To check for internal exposure, we recommend downloading the [free ScanNow for UPnP tool](#). We particularly recommend this for business users.

[Scan My Router](#)[Download ScanNow](#)[Frequently Asked Questions](#)

VPN Routers

ISPs co-operate with Spy agencies of the US government

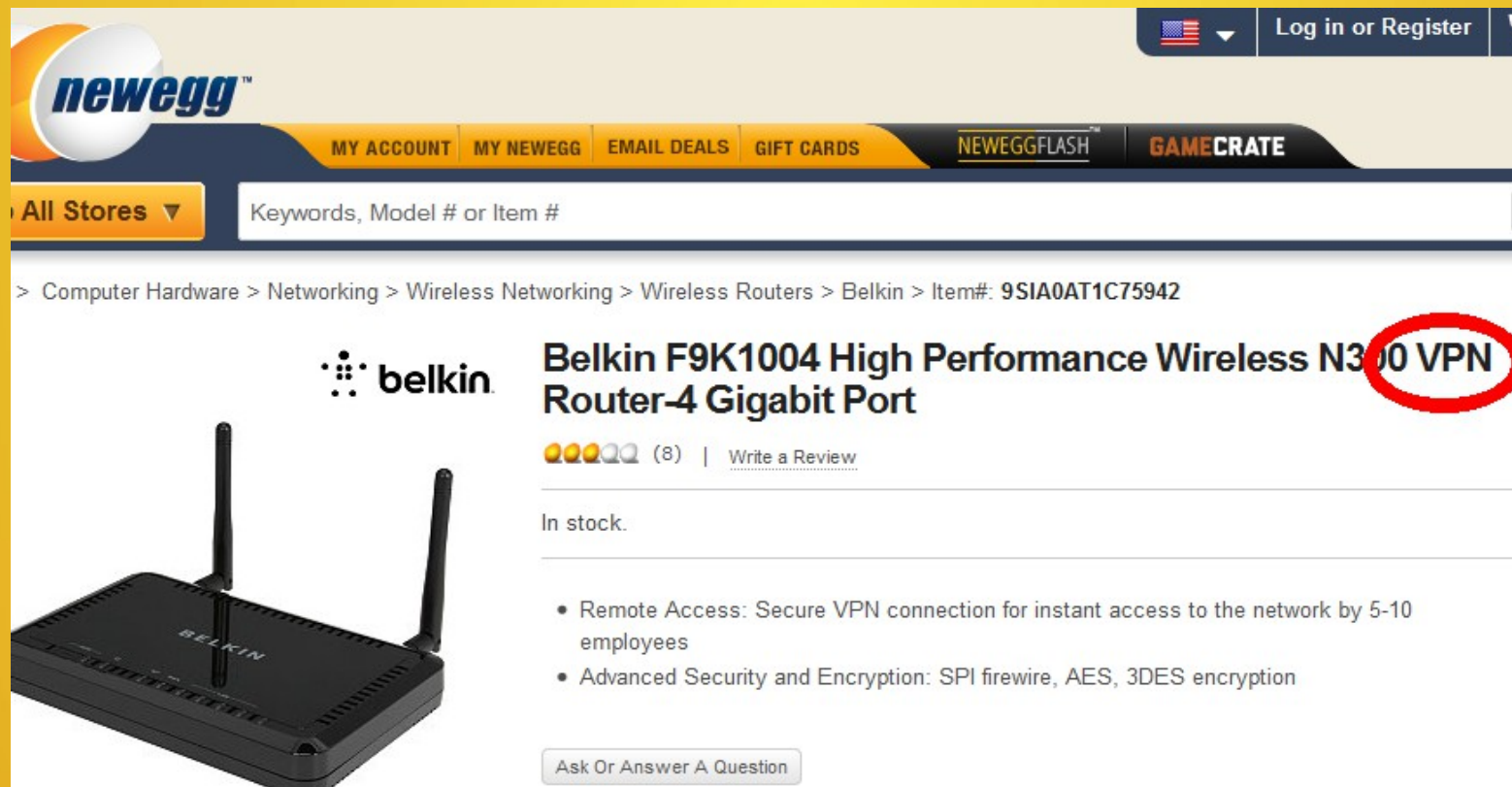


VPN Routers

Look for a VPN client router

Consumer routers claiming to be VPN are mostly VPN servers

Some VPN references may be to VPN passthrough



The screenshot shows the Newegg website interface. At the top, there's a navigation bar with the Newegg logo, a US flag, and a 'Log in or Register' link. Below this is a secondary navigation bar with links for 'MY ACCOUNT', 'MY NEWEGG', 'EMAIL DEALS', 'GIFT CARDS', 'NEWEGGFLASH', and 'GAMECRATE'. A search bar is present with the placeholder text 'Keywords, Model # or Item #'. The breadcrumb trail indicates the product is in the 'Computer Hardware > Networking > Wireless Networking > Wireless Routers > Belkin' category, with item number 9SIA0AT1C75942.

The product title is 'Belkin F9K1004 High Performance Wireless N300 VPN Router-4 Gigabit Port'. The word 'VPN' is circled in red. Below the title, there are 8 customer reviews (4 stars) and a 'Write a Review' link. The status is 'In stock.'.

On the left, there is an image of the Belkin F9K1004 router, a black device with two antennas.

Key features listed include:

- Remote Access: Secure VPN connection for instant access to the network by 5-10 employees
- Advanced Security and Encryption: SPI firewall, AES, 3DES encryption

At the bottom, there is a button that says 'Ask Or Answer A Question'.

Maybe Use Two Routers

VPN connected and what you now have

Wired: Roku box, Vonage box switch as needed

Wireless: Each router has its own Wi-Fi network

Secondary VPN Router Benefits

Hides your IP address and physical location

Connect to VPN server in a country where the ISP does not co-operate with US government

VPN router can encrypt traffic from devices that do not themselves support a VPN

Saves hassle of configuring VPN on multiple devices

Connect a TAILS computer to VPN router for added security

If main router is compromised, all it sees is encrypted VPN traffic

Secondary VPN Router Downsides

- Cost for router and service
- VPN will slow things down a bit
- Initial setup is non-standard.
Connect VPN router into existing router
- Finding a reliable VPN company
- Get up to speed on types of VPNs – anything but PPTP

VPN Client Routers

Some consumer routers can be VPN clients

Install DD-WRT, OpenWRT or Tomato

Buy a router pre-configured to work with a VPN company
Astrill sells 3 routers, HideMyAss sells 4

Flashrouters.com sells a handful of consumer routers customized to work with one of 18 different VPN providers

PunchVPN.com sells 4 consumer routers with OpenWRT installed customized by them to support five types of VPN
may be out of business?

EFF firmware for OpenWireless.org in the future

Asus Router

VPN client and server



Tor Routers

Safeplug from Pogoplug -ng

DreamPlug - for techies only

Portal – Personal Onion Router to Assure Liberty
not yet available..

Onion Pi from AdaFruit.com

Turn off ...

- DMZ
- Port Forwarding
- NAT-PMP
- SNMP
- Telnet and SSH access to router (already mentioned)
- UPnP and WPS (already mentioned)
- Disable access to router via the normal ports
- Disable HTTP access to router

And ...

- Turn off wireless networks at night
some routers have a button for this
- Use non-standard IP addresses 192.168.x.* where x >3 and <253
- Do not connect USB storage devices to a router
- If router has a log, look at it
- Note the status of the router lights when things are working
- Forward port 80 to a non-existing IP address
- Wake-on-LAN available in some routers (just cool)
- Plug modem/router into a line-interactive UPS

Step up from consumer routers

- DD-WRT, OpenWRT, Tomato
- Peplink/Pepwave
- PfSense
- Ubiquity?
- Cradlepoint?
- Smoothwall?
- ClearOS?
- Vyatta?
- MicroTik?



Step up from consumer routers

- SonicWALL TZ 105 UTM
no Wi-F \$210, with 2.4GHz Wi-Fi \$300 (as of July 2014)
- Check Point Software 620
no WiFi \$317 \$350 with Wi-Fi (as of July 2014)
- WatchGuard Firebox T10
no Wi-Fi, one LAN port \$190 (as of July 2014)
- Untangle boxes start at \$800

Step up from consumer routers

Sophos UTM Home Edition is free

www.sophos.com/en-us/products/free-tools/sophos-utm-home-edition.aspx

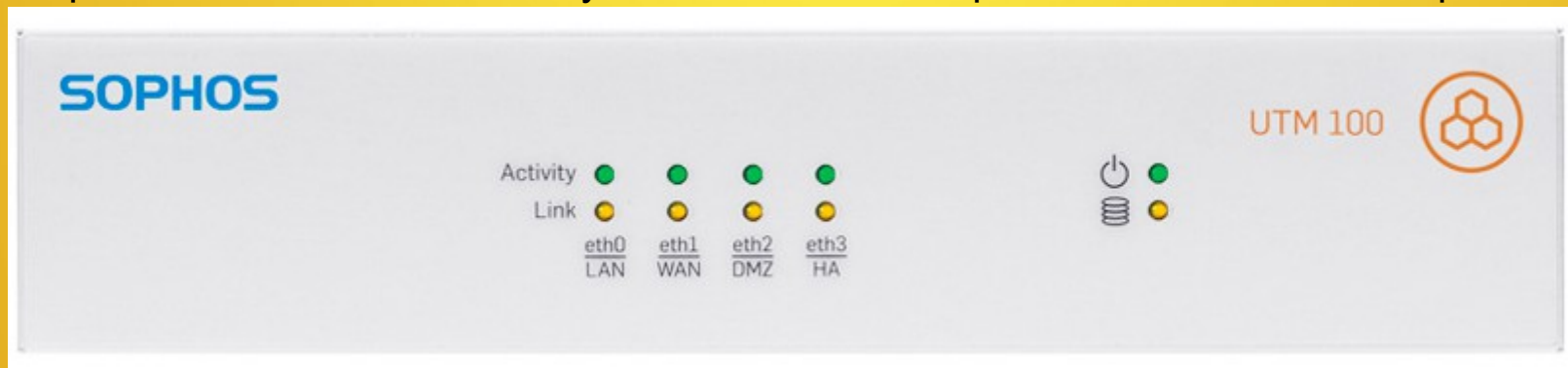
Installs on PC hardware

It is the operating system. Two Network adapters needed.

Used to be Astaro

They sell hardware too, but they don't publish prices
and would not talk to me

sophos.com/en-us/medialibrary/PDFs/factsheets/sophosutm100110120dsna.pdf



Comcast XFINITY WiFi

Has serious security issues - see

blogs.computerworld.com/mobile-security/24073/comcast-xfinity-wifi-just-say-no

money.cnn.com/2014/06/16/technology/security/comcast/

Comcast is turning your home router into a public Wi-Fi hotspot

By Jose Pagliery @Jose_Pagliery June 16, 2014: 11:08 AM ET



PHOTO-ILLUSTRATION: SHUTTERSTOCK/CNNMONEY

Thanks

Michael Horowitz

www.michaelhorowitz.com

Handout is posted here

@defensivecomput