

# Forum:[Hack Forums](#)

Thread: [Home WiFi Key from WiFi Printer HP](#)

**SIM-46898** - August 6, 2019, 11:28 am

I connected to a HP Envy 5540 AIO printer which in turn is connected to a home network router. Is it possible to get the home router's WiFi key from the printer? It doesn't allow Internet access while connected to the printer.

**itzgame** - August 6, 2019, 1:57 pm

this is what I have found from a youtube video:

Steps for retrieving your wireless network password with the HP Print and Scan Doctor:

First, make sure your computer is connected to the wireless network from where you need to retrieve the password.

Navigate to the Print and Scan Doctor file that can be downloaded from [hp.com/go/tools](http://hp.com/go/tools).

The file name is HPPSdr.exe.

Double-click to open the file.

Click OK, Continue, or Yes to run the file.

Click Accept to agree to the terms.

From the menu bar, click Network, and then click Show Advanced Info.

From the Advanced Info screen, click Show Wireless Info.

In the Wireless Settings section, the wireless network the computer is connected to is listed under SSID.

The network key or password is listed under Network Key next to the network name.

**SIM-46898** - August 8, 2019, 10:21 am

(Aug 6, 2019 01:57 PM)itzgame Wrote: [\[CITE\]](#) this is what I have found from a youtube video:

Steps for retrieving your wireless network password with the HP Print and Scan Doctor:

First, make sure your computer is connected to the wireless network from where you need to retrieve the password.

Navigate to the Print and Scan Doctor file that can be downloaded from [hp.com/go/tools](http://hp.com/go/tools).

The file name is HPPSdr.exe.

Double-click to open the file.

Click OK, Continue, or Yes to run the file.

Click Accept to agree to the terms.

From the menu bar, click Network, and then click Show Advanced Info.

From the Advanced Info screen, click Show Wireless Info.

In the Wireless Settings section, the wireless network the computer is connected to is listed under SSID.

The network key or password is listed under Network Key next to the network name.

That only lists the AP's the current computer is connected to not what the printer is connected too.

**Phizo** - August 8, 2019, 7:35 pm

Modern printers (and many other devices) utilise Wi-Fi Direct, allowing devices to connect peer-to-peer without a wireless access point, and behaves as a virtual router by embedding a software-based access point (SoftAP). The connections are negotiated over WPS (a Wi-Fi standard which simplifies connections to WPA/WPA2-PSK networks); i.e., the network you are connected to is the one created by the SoftAP embedded into the printer which provides some version of WPS.

This is completely distinct from the network you are targeting but is often registered as a node in the target network so this negotiation process is unnecessary. I.e., Wi-Fi Direct is provided for printers generally for the purpose of allowing anyone to connect to it for printing regardless of being part of some LAN. The best you can do is to exploit the printer (if possible) such that you can perform remote code execution to leverage it to acquire access to the target network by targeting the router/gateway or any other nodes/APs if and only if the printer is a node on that network and not simply accessed via Wi-Fi Direct (which would leave it open to anyone who can perform the WPS negotiation). Note that while WPS is used in SoftAPs provided by printers due to complexity correlating with the device's role, so more complex devices such as smart phones which can perform data tethering can use the embedded SoftAP to access the Internet.

An aside: WPS can be exploited in some cases to recover the PSK (and thus the passphrase), but note that there is no correlation between the printer's PSK and the PSK associated with the network it is a node of (assuming it is). The PSK depends on both the SSID and passphrase of the network such that  $PSK = PBKDF2(\text{passphrase}, \text{SSID}, 4096, 256)$ . PBKDF2 is a key derivation function which requires a pseudo-random function as part of its implementation / derivation process. In the case of WPA, that is HMAC-SHA1, which is iterated over the input 4096 times continually to produce the bits which make-up the final 256-bit PSK.

**Mad76e.** - August 9, 2019, 4:17 pm

Hmm Phizo is right, not much to add

There exist some older wireless printer servers that are vulnerable, especially those that company's uses, that allow both for a wired and wireless connection. Reason for using both is that guests, consultants etc. shall be able to print wireless without getting access to the company's wired network. Often it's carelessness that a printer have "wireless" activated by default, that the admin forgot about or something. In worst cases might be a way in to the network from the wireless access point, but this is indeed very rare, often the printer servers are not monitored properly by the security personnel. Some of these vulns are connected to XSP (cross-site printing), and CORS spoofing (cross-origin resource sharing), and PjL to some degree. The problem here is that there's few people that actually care to update the firmware; these "as long as it works its good" attitude can be fatal. However most of the vulnerabilities regarding printer servers are manipulation with the actual printer itself, as example printing garbage/propaganda, and to display some childish messages in the printer display.

However there are some ways to get inside the actually printer file systems, and some ways to get the printer jobs as they are printed, which isn't good for a company, if secrets can be revealed and made public it can jeopardize the companies future. Also to pivot from the printer server direct in to the wired network (if there are any wired connection to the printer server, which also are rare), is hard, but it has happened before. (no i haven't succeed yet)

Some wireless printer servers are open for all to access and some are configured with a wpa2 key. The name usually is connected to the actual printer model or printer server model, some even use bluetooth to print

The PPrinter Exploitation Toolkit (PRET) is an interesting tool to use and explore, but unless you're out to troll someone or to do some sinister things, its more or less useless to the normal home brewed hacker, but deserves a mention