

What is UPnP? Why should you disable it on your router?

UPnP is a network protocol (or set of network protocols). These protocols outline a specific communication method that all kinds of devices can use to instantly communicate with each other on a network.

Technology in the computer age has been plagued with insecure features, security holes, and general oversights in software architecture. Flash drives can carry keyloggers. Browsers can have backdoors. Windows still requires constant security patches. The good always comes with the bad, and there is no end in sight to this problem.

Universal Plug and Play (UPnP) is a technological advancement that comes with its own set of drawbacks. It is a convenient technology, but that convenience can leave your system vulnerable to certain problems if you don't keep an eye on it. Read on to learn what UPnP is and how it can jeopardize your network security.

What is Universal Plug and Play?



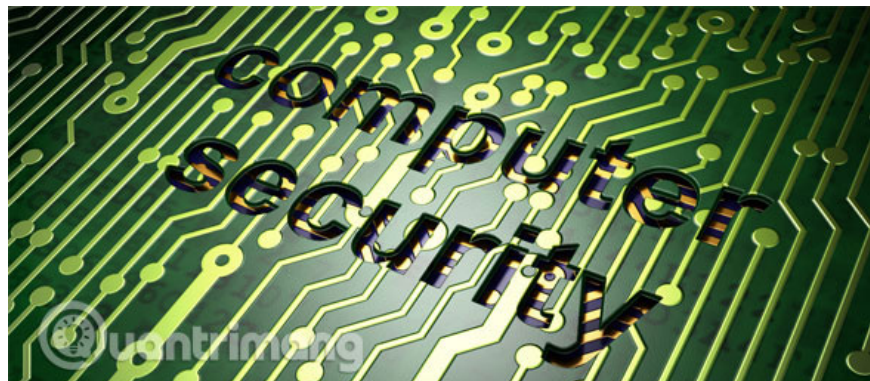
Technically, UPnP is a networking protocol (or actually a set of networking protocols). These protocols outline a specific communication method that all kinds of devices can use to instantly communicate with each other on a network. In most cases, UPnP is used by devices to discover other devices on that particular network. UPnP is so ubiquitous today that it would be surprising if you have never used it.

If you're still confused about what UPnP is, think of a printer. The first step is to physically connect the printer to the network (although these days this can be done over WiFi). In the past, you had to manually search for it and set it up so that other devices on the network could find it. Today, this happens automatically thanks to UPnP.

Once connected, devices on the network can continue to communicate with each other by sending and receiving data. Computers can tell printers to print documents. Media centers can transmit audio data. Mobile devices can connect to computers themselves. The possibilities are endless.

The term 'plug and play' is becoming more and more popular. You plug in the device and start using it immediately without having to go through the 'nightmare' of setup and configuration. UPnP is one of the most convenient networking technologies available today. UPnP is mainly used on residential networks rather than business networks.

The Dangers of UPnP



UPnP has been criticized for a number of security flaws over the past decade. The FBI previously recommended that users disable their UPnP settings to reduce the risk of damage. This has happened again, although the specific flaw this time is different.

What exactly is the problem with UPnP? There are two main vulnerabilities that have been exploited recently:

1. Programming errors - There are bugs in the actual code, which makes the UPnP implementation exploitable by bad actors, allowing them to execute malicious code via .
2. Unintended Exposure - The purpose of UPnP is to make devices on a network easily discoverable by other devices on that network. Unfortunately, some UPnP control interfaces may be exposed to the public Internet, allowing bad actors to find and access your private devices.

The US Department of Homeland Security has had to recommend that all users disable this protocol, due to these security holes. The holes have left about 40 million devices worldwide vulnerable to hackers. A worrying fact.



Don't panic, though! There's a silver lining to all of this. These bugs mostly affect older devices, but even they can be patched without having to buy new hardware.

Most UPnP implementations use an open source solution called **lilupnp**. Technically, any device running a version of lilupnp prior to 1.6.18 is vulnerable to this threat. However, since most manufacturers won't disclose that information to the general public, you'll have to wait until your device manufacturer releases an update that addresses these issues. Until those patches are available, you can prevent the problem entirely by disabling UPnP on all of your devices.

There are so many devices that use UPnP and so many manufacturers for each type of device that **TipsMake.com** cannot include disabling instructions for all of them here, so you should run a Google search for your device and include the phrase 'disable UPnP' in the search query.

As far as security holes go, this is one of the easier ones to fix. You'll have to wait for a fix, avoid using the internet, or reboot into Safe Mode and clean up the problem system. For this one, all you have to do is disable UPnP and you'll be safe for a long time.

Are UPnP attacks practical?

It sounds scary, but what are the chances of you encountering an attack via UPnP?

If your router is good, it won't have UPnP over WAN, which eliminates the possibility of hackers remotely accessing it. You'll be vulnerable to attacks over your LAN (Local Area Network), where one device gets infected with malware and spreads it across the network.

However, if you keep your device safe from malware, browse the web safely, and install one of the best antivirus programs, then you can most likely trust that your device won't spread viruses. If you want to be extra sure, you can disable UPnP on your router.

What happens if you disable UPnP?

If you disable UPnP, your router will no longer automatically manage ports for each device connected to your router. This means you will need to manually forward ports so they can communicate with each other.

So you'll need to make a decision. Do you like the convenience of UPnP, allowing you to easily connect devices to your LAN? Or are you worried about someone using those channels to cause damage and steal data? If you

like the convenience, use UPnP and keep your devices secure; if you like the security, handle port forwarding manually so they can't be exploited.

How to disable UPnP

If you decide to disable UPnP, you will need to access your router. You will need to do this frequently because you will need to access it every time you need to forward a new port (i.e. when you connect a new device to your network).

TipsMake.com has mentioned disabling UPnP in the article 8 steps to increase security for wireless routers, so be sure to check it out if you want to maximize the security of your router.

UPnP is a useful feature, but it can be exploited by cybercriminals. While you can disable it and manually perform port forwarding, some people may never encounter a UPnP attack due to good browsing habits and strong security. Therefore, you should consider both reasons when deciding whether to keep UPnP enabled.

You finished reading the article "**What is UPnP? Why should you disable it on your router?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.