

Forum:[Hack Forums](#)

Thread: [Pirating - Surviving To Seed \(Definitive Guide\)](#)

camelCase - October 23, 2010, 7:48 pm

Hello Hackforums,

Steal this tutorial.

Yes, I'm back :) Keep seeding! In this tutorial I will be guiding you to downloading torrents & other illegal or copyrighted software while bypassing anti-p2p networks. The first question you might have is, "Why do I care if an anti-p2p network is watching me", or even "How do they watch me". We will address these common questions first.

Anti-P2P networks such as "Time Warner Telecommunications" and "Media Defender" are out to log downloaders. They first find material that shouldn't be seeded, such as material you're required to purchase. They download that and seed it. They then log all users who are downloading from them, which is nearly everyone. If you are not familiar with how p2p networking works, please [read an article](#).

After locating a user who is pirating their material, they log the IP address. By having that information they then contact your ISP (internet service provider) by tracing it and usually try to implement a seize and desist contract. If you then are caught pirating again (depending on ISP) you are usually fined or removed entirely from that ISP and put on a black list. A black list to ISP's means your a troubled user. Civil suits are possible, but rare.

At this point I would like to note: Most civil suit cases against pirates are thrown out of court immediately due to poor anti-p2p techniques. (See: Entrapment)

"So how do I prevent myself from falling prey to anti-p2p networks?"

1.) Peer Blocking software: Peer blocking software monitors network connections and tests them against a black list, or even sometimes using heuristics. This software will see your router/modem has requested resources from xxx.xxx.xx.xx and will check a blacklist or test the octets for known suspicions It will then decide whether the IP address is safe to connect to.

Software & Blocklists:

[Peerblock 1.0](#)

[Peer Guardian](#)

[Bluetack](#)

[Trusty Files](#)

[Blocklist software - does it really work? \[Study\]](#)

2.) Choosy Downloading: Be picky when it comes to downloading. Read comments to see if a few people have been caught. Only download from trusted users (or VIP) to be sure not just on quality, but safety and reliability.

3.) Encryption & SSH tunnels: Apply encryption to your traffic. Search Google to see if your bit-torrent client allows you the functionality of encryption, if it doesn't - you should probably recycle it. There are plenty of tutorials here on Hackforums.net to teach you how to use SSH tunnels. You

could also use proxy lists & a VPN for added security. By leaching bandwidth from someone else, it also adds a layer of security (See: Packet scrambling). [>How to apply encryption to your client<](#)

4.) Choose a local ISP: Choosing a somewhat obscure ISP is beneficial too. For reasons such as a.) It's harder to tie an IP address to the ISP and b.) Smaller ISP's tend to NEED their customers, henceforth are much more reluctant to warning/removing any of their users.

5.) Hail marry! You may also use a private torrent network, such as TorrentPrivacy.

6.) Oldies are goodies! Stay away from newer material, as this attracts the most attention from anti-p2p networks and the RIAA. Always try to pirate/download older material (usually a year or older is safer) [Credits to: jdcx95]

This tutorial comes due to a large amount of RIAA civil suits. Have an idea for anti-p2p privacy & security? Tell me in a comment! I strongly recommend you watching "[Steal this film](#)" documentary about piracy and its history.

-- I am currently planning the development to a bit torrent client with privacy & security in mind. This software will be coded by what I feel is the most competent developers around. The actual coding hasn't yet been initiated, but stay updated.

-camelCase

Deferment - October 23, 2010, 8:10 pm

Nice tutorial! Thanks for sharing, I'll be sure to follow this tutorial in the future to prevent from being caught.

*** Converter** - October 23, 2010, 8:24 pm

Hey thanks for this, but it really depends on your isp if they monitor your connection mine doesn't and i haven't been emailed or caught yet

camelCase - October 23, 2010, 8:31 pm

(Oct 23, 2010 08:24 PM)* Converter Wrote: [\[CITE\]](#) Hey thanks for this, but it really depends on your isp if they monitor your connection mine doesn't and i haven't been emailed or caught yet

If your ISP is determined to assure that their users are not pirating, they'll get you. After all, the data MUST pass through them too. Some ISP's [even small ones] will stop you without a contract of seize and desist to prevent from gaining a "pro-piracy" name.

I have gained friends in my community that work for my ISP, whether that has been the deciding factor of my freedom I suppose i'll never know.

*** Converter** - October 23, 2010, 8:35 pm

lol ive been a pirate for 5 years still luckily not caught, trust me this isp im with doesn't give a shit, if they get there money they are happy :)

jdcx95 - October 24, 2010, 5:48 am

Good guide. Another way to stay safe is to stay away from newer materials, especially movies. The DMCA loves to fuck people that download new movies. You have less of a chance of getting caught if you're downloading a movie that isn't brand new/not in theaters yet.

Or you could just download through a VPN (offshore with no logs of course). Then you're safe lol

camelCase - October 24, 2010, 10:54 am

(Oct 24, 2010 05:48 AM)jdcx95 Wrote: [\[CITE\]](#) Good guide. Another way to stay safe is to stay away from newer materials, especially movies. The DMCA loves to fuck people that download new movies. You have less of a chance of getting caught if you're downloading a movie that isn't brand new/not in theaters yet.

Or you could just download through a VPN (offshore with no logs of course). Then you're safe lol
Added w/ credits, much thanks!

Valof - October 24, 2010, 1:12 pm

This helps a lot! Thank you CamelCase!