

## Forum: [Hack Forums](#)

Thread: [What I do to try to stay safe](#)

**PhargedPhreak** - May 3, 2017, 9:21 pm

First of all keep all your patches up to date.

Also keep a backup - using something like sysinternals disk2vhd

<https://technet.microsoft.com/en-us/sysinternals/ee656415.aspx>

Don't use default passwords.

Don't use shitty passwords (i.e. password, 123456 etc - you can google a list of top 10 worst passwords).

Try to use long passwords (why? because rainbow tables and other methods of cracking are up to at least 12 characters - so use longer than 12 characters).

Don't re-use the same password on different sites over and over.

Have antivirus turned on.

Have an antimalware tool turned on.

Have a look at running processes to see if there's anything wierd looking there.

You can see them in task manager or various other tools like sysinternals process explorer.

To bring up task manager hit ctrl-shift enter.

Look at processes calling out to the internet to see if any of them are going to places you don't expect. you can use netstat -a at the command prompt for this. If you see something sketchy i.e. an IP address or site you don't recognize then you can go online and lookup the ip address on e.g. [iplocation.net](http://iplocation.net) to get more information if you think it's sketchy.

If you think it is sketchy, get the process ID and kill it. You can do that in task managers or sysinternals process explorer. tamosoft also has a good one called net essentials.

What else? You can set up your DNS to point to.opendns. that has some level of filtering of sketchy sites.

So what do you do if you want to go on sketchy sites?

Well this is kind of lame but on e.g. torrent sites, you can close the popups if you can click the x on the top right corner fast enough. You can also disable popups. You can also have something like malwarebytes realtime protection turned on which will save you against anything that's already been detected.

You can also run your machine from inside a VM - i.e. virtualbox. Cut yourself a copy of your main system using something like disk2vhd then copy it into virtualbox and go on the sketchy sites from there. Virtualbox will give you some degree of protection. You want to get even more paranoid you can run your browser inside a sandbox as well. Something like sandboxie. If you're going to do shit with really dangerous stuff like reverse engineer viruses, do it inside a sandbox inside a virtual machine. Or at the very least just a sandbox like cuckoo.

<https://cuckoosandbox.org>

[www.virtualbox.org](http://www.virtualbox.org)

[www.sandboxie.com](http://www.sandboxie.com)

Keep a recovery disk on a USB if you can so that if you do get infected and you can't fix it you can reinstall. That's where your backup is very useful.

If you're lucky and it's not a serious piece of malware you might get away with rebooting in safe mode and then trying to clean it with anti malware. There are a ton of good antimalwares. I try to use various different ones to get complete coverage if I think I'm infected.

[www.avg.com](http://www.avg.com)

[www.malwarebytes.com](http://www.malwarebytes.com)

[www.superantispyware.com](http://www.superantispyware.com)

So what if you want to download torrented stuff?

torrented stuff is often loaded with malware so it's not a good idea.

If you are still stubborn you want to take the risk, upload the torrented file to virustotal to see if it gets a hit.

virustotal.com is awesome because it has all of the major antivirus sites on it so it will often find stuff that the most common ones miss.

Worth noting though that if you're using for example crackme's or certain "hacker tools" they might be detected as viruses. Use your gut if you think something is a real malware or if you think it's a false positive.

Also if you're not sure, run some sketchy piece of software inside a sandbox or a virtual machine.

That's all I have.

**Slu5h** - May 3, 2017, 11:00 pm

Very nice summary.

For the last point I have a solution. If you wanna torrent evil shit on your machine, i use a VM, ok this is nothing new. But in addition I install HDGuard on my VM so after a restart everything is clean, it then works like a live OS with no persistence mode enabled. I have never encountered any problem with it.