

# Forum:[Hack Forums](#)

Thread: [\[GUIDE\]The Intermediate user's Security guide](#)

JavaMachine - June 11, 2012, 3:17 pm

Welcome to my Security and Guide. I consider this guide to be an intermediate user's guide because I will not be explaining such terms like "Heuristics" and such.

This guide is to be used for reminders and tips. This guide will not hold your hand through everything described. Much of the guide is personal opinion. Keep in mind I do not simply recommending 1 program for each angle of infection and attack.

## Table of contents

### 1.Anti-Viruses

#### 1.1:What they are for

#### 1.2:The top 10, and my reviews

#### 1.3:My personal favourites

### 2.Fire-Walls

#### 2.1:What they are for

#### 2.2:My recommendation

### 3.Browser Protection

#### 3.1:Why you need this

#### 3.2:The Browser

#### 3.3:The addons that you need

### 4.MalwareBytes

#### 4.1:MalwareBytes

## Misc. tools

## Physical Protection and Methods to prevent infection

### Anti-Viruses

#### What Anti-Viruses are for

These programs are meant to be doing the work of scanning files in your system for infection, scanning every file downloaded. They are your main defense against downloading malicious files, some may have other features, however, I recommend other specialized programs for these features.

#### The top 10, and my reviews

Now, in no particular order, these are 10 anti-viruses, and what I experienced when I used them:  
BitDefender-Nothing remarkable

Kaspersky-EXTREMELY User-Friendly, there is a advanced user option and that allows for a semi-extensive customization of the program. I recommend this if you are not the intermediate user meant to be reading this guide

Panda Antivirus Pro-Nothing remarkable

F-Secure AntiVirus-Incompatible with some other programs that will be mentioned later in this guide

AVG Anti-Virus-Does not come with firewall in the free version. One of the top 3 most popular.

Avast! Pro Antivirus-This comes with a sandboxing feature which I approve of, easy to use. However, it has failed me in the past and allowed me to get a minor infection. It is one of the top 3 and detection rates will improve.

G Data Antivirus-Nothing remarkable

Avira Premium-This was hard as hell to install, very little support for the free version. It required me 2 restarts and 1 hour just to get the free version to work, and it was a virus database from 2011 and wouldn't allow me to update. Hopefully this has been fixed.

Norton-Feels very resource demanding, slow interface, although it attempts to be quick and easy to use.

ZoneAlarm-Although not my personal experience, the firewall on this program blocks many games and such.

I know there are probably some that I missed, but these are the ones requested of me. Some of them say "Nothing remarkable" as in they were quite average, no overwhelmingly simple interface, no low-end or high-end detection rates.

### 1.3:My personal favourites

My personal favourite would have to be Avast, although it has failed me and allowed me to get infected, it has a nice sandbox feature which will come in handy if you suspect the next page you click on will be infected, or that next file.

Although I use AVG, which has a noticable performance change when you move the slider in it's scan. It's premium version is incompatible with COMODO Firewall, it will simply not allow you to install it.

### 2:Fire-Walls

#### 2.1:What Fire-Walls are for

Now while the Anti-Viruses guard against file-based attacks, like executables, the Fire-Wall will prevent viruses from uploading or downloading without permission. It is your connection protection(rhyme).

#### 2.2:My recommendation

I personally recommend COMODO firewall, this firewall is easy to install, comes with active customer service(It only took me 3 minutes to get a LIVE user in a chatroom, at PEAK times). It also comes with a handy Sandbox, although this gave me a BSOD. The nice Paranoid Mode is EXTREMELY handy when executing suspicious files or entering suspicious websites, it blocks every action going on in your computer unless you press the "OK" button. You can easily see all your connections, how much data is being transmitted, and you can end it if you want to. The only thing I don't like is the faulty Sandbox mode.

### 3:Browser protection

#### 3.1:Why you need this

Just having an anti virus and firewall are not enough, although this is partially the anti-viruses job, files processed through the browser must also be regulated, this includes Scripts, Pictures, Websites. After just an hour browsing HF, you may find alot of talk on Java Drive-Bys, this section will ehlp you protect against most everything.

#### 3.2:The recommended browser

My recommended browser is Mozilla Firefox. However, as this is not a biased guide, I will also mention that Google Chrome has the same level of security capability as Firefox, but I prefer Firefox because Chrome is gaining popularity and will become a higher target of vulnerabilities.

### 3.3:The required Addons

There are quite a few addons you should have on Firefox, I may be missing a few, but these are the ones I have on my computer.

1.WOT(Web of Trust), this is an addon that allows users to vote on websites, adding points to things like Vendor Reliability, Privacy, Child Safety. Malicious sites will generally be voted poorly upon in every category, this is a very basic addon but goes a long way.

2.Adblock, this addon blocks 95% of advertisements, this includes Youtube advertisements, this will be useful as many ads these days may redirect you to malicious pages. Besides, do YOU want to know how to lose weight in 3 easy steps, I know I don't, just let me be fat and read my manga.

3.NoScript, this addon, like the title implies, disables JavaScript on pages that you do not enable it on. Although this seems tedious, if you only visit 10 - 20 sites, it is easy to enable scripts on them, it only takes 3 seconds. If you step out of your routine 10 - 20 sites, this will protect you if it is Malicious.

4.KeyScrambler, This program will protect you in case your anti-virus misses a keylogger, or if it is installed physically. The only downside is it does not allow typing speeds of 110 words per minute or above, as it will mess up whatever you type at those speeds.

This is VERY troublesome for an Asian such as myself as I love typing long rants or guides like this one. However, you are most likely a non-Asian, so the only problem you will have is probably when typing a password, as this is a phrase/combination that you regularly type out.

### 4:MalwareBytes

Probably the most popular anti-virus on HF because it does not remove files without asking, thus allowing you to test your created viruses and other Frankenstein creations. I feel it has a pretty powerful scan but does not do much in terms of passive protection, even in the paid version. I simply had to put this in here because I hear it so often around the forums.

### Misc. Tools

- 1.Spybot Search&Destroy - This is highly recommended around the forums.
- 2.Advanced System Care - General System Cleanup
- 3.Auslogic's Disc Defrag - Will help your virus scans run faster
- 4.CCleaner - As the title implies, it cleans up your hard drive
- 5.A sandboxing tool - Although from your time in HF, you should have heard of Virtual Machines, the one I use is Oracle's VirtualBox, these VMs are separate from your machine and running files there with a sandboxing program like Sandboxie is recommended if you are prepared or suspicious of infection.

### Physical Protection and Methods to prevent infection

Physical protection - This only happens when either a friend comes to your house with the intent of infecting your computer. This is VERY effective as they have the ability to disable all your protection, and install their RAT or whatever they wish to infect you with. Here are 2 effective ways to prevent this

- 1.Disable Autorun, this is something that should be done anyway
- 2.Disable your USB drives, this might inconvenience you, but if you do not use them often, like me, this will buy you precious time in the washroom while your friend tries to figure out why he cannot access his USB/disc. This can obviously be done by going to Device Manager and disabling the port. I am 100% certain this works for disc drives, but there's a 50% chance it is listed in your device

manager.

Methods to prevent infection:

These are some of the senses you develop once you have browsed the internet as much as me. I will cover the most common way people get infected. This way is through youtube, and blogs(found through google),

-Youtube-

- 1.Check if the youtube video has comments made in seperate times, and also check if you can actually post a comment without it saying "Comment pending approval"
- 2.Approach websites in description bars cautiously by enabling NoScript and paranoid mode in COMODO

-Blogs/Google-

- 1.Check WoT, it is probably a unremarkable site with no rating though
- 2.Check comments on this blog(using the same method as the youtube one)
- 3.Paranoid mode and NoScript

If you have any questions, please post replies below, DO NOT PM me as I am not Ub3r/L33t and cannot hold many PMs. I am certain I may have missed some points. Please post replies in order to keep this thread alive. I spent an hour drafting this out.

**Eric21** - June 11, 2012, 11:35 pm

Good thread, but you might have used it attractively, this colour is too bright.

**JavaMachine** - June 12, 2012, 2:27 pm

(Jun 11, 2012 11:35 PM)Eric21 Wrote: [\[CITE\]](#) Good thread, but you might have used it attractively, this colour is too bright.

Colors are for organization purposes.

**Dynasty@HF** - June 12, 2012, 4:26 pm

thanks for the tutourial. some good advice and programs

**JavaMachine** - June 13, 2012, 3:01 pm

(Jun 12, 2012 04:26 PM)dynasty1987 Wrote: [\[CITE\]](#) thanks for the tutourial. some good advice and programs

Thank you for the compliment. This isn't really the full list of programs I use though.

**kenedy123** - June 14, 2012, 10:56 pm

Thanks for sharing the user's Security guide

**?Đ?vee?** - June 15, 2012, 8:44 pm

Thanks for sharing this man. Btw, some of the colors is making it hard to read :/

**JavaMachine** - June 17, 2012, 7:30 pm

(Jun 15, 2012 08:44 PM)?Đ?vee? Wrote: [\[CITE\]](#) Thanks for sharing this man. Btw, some of the colors is making it hard to read :/

Just highlight it, or tell me which specific colors were hard to read.