

Forum:[Hack Forums](#)

Thread: [Guidelines to Staying Safe](#)

Once Timeless - May 14, 2010, 5:02 pm

Guide to Staying Safeby WMM - with help from other members

Antivirus:

As most Microsoft Windows users know there are such things as [Antivirus](#) which is a program and virus removal tool that allows your computer to be scanned for malware infections and Trojan viruses. When you are downloading things or sending email, also opening files or sites. Mainly sites like torrent finding sites or sites with loads of ads. Now some Antivirus softwares are really neat and allow you to do some awesome things to keep your computer stay clean. Not saying that all anti-viruses are good though. There are some pretty crappy ones out. I will not discuss this debate though all I will say is that there are good ones and bad ones. Usually when you use anti-virus programs you pay for what you get. All the good ones that are out now usually require you to pay for the good ones. No doubt there are free ones, like [Avast](#), [ESET \[Nod32\]](#), [Kaspersky](#) and several more. I could go on and on, about anti-viruses but there is no need for me to. But mainly when you get a good AV you should probably make sure you are always updated to the most recent database and most recent version of the anti-virus. All I can really say is you should have a AV if you use "Windows." For any more info you can check out the [Wikipedia](#) site which talks all about anti-viruses and goes into details. I would prefer that you don't send me a PM asking about programs and whatnot when you can just press the "New Thread" Button.

Antivirus List

[Panda™ Big Antivirus List](#)

Downloads:

About 65% of the time infections will come from things you download. That is why it is very important that you always check to see if what your downloading is coming from a legit source before you even touch the file or preferably start the download. You can find more info below if you are curios about staying safe when downloading torrents. Now [Downloading](#) files from unknown sources. Especially from here, for example if you download something from a user with very little posts and no rep you should probably find a better source; that is mainly up to you though. Windows is very exploitable and easily hacked now adays XP moreover then Vista and or Windows 7 not with the right anti-virus program though. Since windows is so exploitable you should simply like I am saying a million times watch what you download because that is where most viruses come from. If all members here read this thread and applied it I am sure the White Hat Section would be more dead (not saying that section is bad but usually posts in there are for bad reasons). Now lets consider websites.

Websites:

Lets discuss websites. Getting infected with a AV from a website is not likely with the correct and working AV. Many of the times you won't get infected from a website unless but you will with a non working or without a AV. Lets say about 20% of the time is when you get infected from a website. Most websites would include sites with several annoying ads or even sites that are not very popular. Not saying all sites that are not popular have Viruses embedded in them but some do. Most of the time though sites like Torrent Pond for example with all those annoying ads without the appropriate anti virus it will not go so well. Just saying unless you know people that use the site often and site looks good not very annoying or anything it will be safe. The content that inside the website is another question. Most of the website owners put java drive-by's in the site to mask it and look like some sort of a game. Which when you click accept from the Java it automaticly runs their Trojan/server virus. Or some of the owners use iFrames to bind their website's source with a script

that will automatically download/execute a file on your machine. Kaspersky is best in these cases with iFrames, as he blocks them before you even have the chance to see the actual index.php/html file.

Torrenting:

This guide will be about how to find the right torrents when posting or downloading.

Definition: [Wikipedia](#)

Being Safe: As you know for some reason hackers like to infect hacked or pirated software, also known as "WareZ". Since that is the case you have to be extra careful especially if you are a Windows user. But not do hackers just like to infect files they also like to be tricky and embed "Trojans" and whatnot in the site. That is when you run into trouble, there are several good sites and bad sites. Some good sites could be: [Demonoid](#), [The Pirate Bay](#) and [ISO-Hunt](#). Don't get me wrong just because I posted that does not mean all the files on those sites are 100% completely clean. The best thing to do is to read the comments, I know you like but that is boring and a waste of time. But honestly would you rather download a big ass file then get it and all it does is infect you and doesn't work? I will tell you what 99% of people would not. So save your time and bandwidth you used up by downloading a file that you are at least over 50% sure it will work. Here are a couple of examples. Now look at [this](#) torrent for example you scroll down and you see no comments, correct? Well that means several things. There are not many seeders so your download speed may take a little longer, but that also means you could download it and it may not work since there are no comments it means no one is there to confirm it so that would be a torrent that is not recommended to download. I would only suggest downloading torrents like that if the file you're trying to download is hard to find. Just because there are no comments does not mean it won't always work. It's also good to check and see what the file type is. If it's a .iso file like the previous one is then it should be alright, unless there is a virus or something crazy thing that happens when you open setup.exe. Now let's take a look at a different situation. Now look at this file [here](#) and scroll down to the comments. I am not sure exactly why but hackers love to embed viruses into a key-generator (KeyGen) file. Probably because it's easy to trick people into doing it. But if you read the middle comment it states "the program is fine, the key gen contains a Trojan horse. so use caution" so that means 99.9% of the time it will have what they say people just don't go say there is a virus because they like to piss the people off no, they say it either because they almost got infected or they know the member usually has uploaded infected files in the past. So don't download that file!

Viruses:

This guide will be about viruses and how to keep your self protected from them.

Definition: [Wikipedia](#)

As you know today in our world there are 'hackers,' hackers will want to infect you with a virus in many ways that if you do not protect yourself you can become one of their 'victims'

To be safe from a hacker all you mainly have to do is watch what you download from websites. When going to a website to see if it's a real file you should judge the site. If it's a brand new site then some times it's not a clean file your about to download. If the site has been there for a while and you've checked the poster and his/her information on the file/program and it's feedback and it looks safe you can download it and take it to a online scanner to check and see if it's clean. Here's a very good online scanner you can use. "[Virus Total](#)". Once you've scanned the file/program you downloaded and the website did not pick anything up it's okay to use it. If the file gets detected then I suggest you not to open it because it can harm your computer. Some people like to listen to music, play games, use programs and things such as that and the stuff they use may not be free so they go to a warez/torrent based site and download it. If you just buy the program then there is no way you can get harmed unless the original copyright owner has infected it which in most cases they will not.

Trojan Horses:

Definition: [Here](#)

Now we are going to get a bit more specific. We are going to start with "Trojan Horses." Now Trojan horses is the most common virus. I would have to say that since they are easily applied and probably easier to make. What a Trojan does is basically gives unauthorized access to a persons computer. Not all do the same thing but nearly all do something similar things. So practically they

are designed to give a hacker remote access to someones computer. Once one is installed or applied it allows hackers to do things with the computer likely to harm it more and make it more vulnerable. If you want to get more specific about Trojan Horses and what they can do check out the definition it gives a list of what they tend to do.

D.D.O.S:

Definition: DDoS stands for Distributed Denial of Service, in which you control several hundreds computers known as zombies which will simultaneously attack a single network or computer so that there internet crashes.

Preventing a DDoS Attack:

If you want to protect your apache webserver against DOS, DDOS, or brute force attacks use mod_evasive module. mod_evasive is an evasive maneuvers module for Apache to provide evasive action in the event of an HTTP DoS or DDoS attack or brute force attack. It is also designed to be a detection and network management tool, and can be easily configured to talk to ip-chains, firewalls, routers, and etcetera. mod_evasive presently reports abuses via email and syslog facilities.

Phishing:

[Full guide about phishing](#)

Phishing is basically a fake login page to which you're usually brought to by links you click. Usually, an attacker pretends to be a person of high authority of the website the phisher is about, or takes the form of any notification message that website might send to you. Experienced crackers can make these messages appear pretty legitimate, hard or even impossible(in some cases) to differ from the real thing. They can even use a compromised account of any friend of yours to bring you to their fake login page. So being alert on whether or not the messages you open are legit, or if the people you're chatting with are really who they claim they are, doesn't really seem practical much.

What is practical is to follow one simple rule. Whenever you're logging to a page whose url you didn't write yourself(meaning, you were led there by clicking a link), always check the url in your browser. If its part before the .com is any different than the page you're logging in, it's probably a phisher. So instead of facebook.com, a phisher would look like facebook.t34.com, facebo0k.com, facebook.cjb.com... you're getting the point. Have in mind that xxx.facebook.com wouldn't be a phisher, because xxx in this case is a subdomain of facebook.com. And subdomain can be anything before the main domain name, separated by a . from it. Now that you know how to differ phishers from non phishers, don't put your login info in the phishers ;)

Staying Safe Using Proxies:

Definition: http://en.wikipedia.org/wiki/Proxy_server

Nowadays you have to be careful at where you make your 'IP' visible at. Many people nowadays can initiate DOS/DDOS attacks just from knowing your Internet Protocol address. One of the best ways to prevent your IP from being visible to the public is using a proxy when you surf the web. A proxy basically runs the information you want to view, through the providers server and at the other end it will seem that you are connecting from a completely different Ip/location.

If you want to find out where I can get a decent Proxy? I would suggest "Hot Spot Shield" or a simple online one.

I don't mind this being a community project so if you want to add something let me know. I got the start I will add you to the credits if you do send me something to add.

Credits:

[Braco22](#)

[Detective Rootz](#)

[Sk8Plague](#)

[Crow](#)

[Livewire](#)

[Panda™](#)

Braco Asshole - May 14, 2010, 6:24 pm

Thanks for giving me some credits WMM. Altho that guide looks really nice!

Once Timeless - May 14, 2010, 6:57 pm

No problem.

It will be updated this is just the beginning.

Irelandrulz2 - May 14, 2010, 11:06 pm

Perhaps include safe internet browsing programs? I heard Chrome views everything to do on Chrome.

Once Timeless - May 14, 2010, 11:22 pm

If you want to make it then make it.

I am not going to be adding everything people tell me to.

If you do help you can be added to the credit list...

Would you like that or not?

I would prefer if I were you to just make a simple little section and then be added to the credit list.

--([S7N-])-- - May 15, 2010, 12:10 am

Very well written. Care to add a section in the guide for Trojans?

Once Timeless - May 15, 2010, 12:23 am

Sppecifically? Well in the morning I will. It's 1 am here.

--([S7N-])-- - May 15, 2010, 12:47 am

(May 15, 2010 12:23 AM)WMM Wrote: [\[CITE\]](#) Sppecifically? Well in the morning I will. It's 1 am here.

Yes. No hurries, take your time.

Once Timeless - May 15, 2010, 9:27 am

There you go.

Added a couple more detailed terms.

Legit Dude - May 15, 2010, 11:44 am

Great guide. Got right down to the point. And thanks for the positive reply on my DDOS Protection Guide. :)

Once Timeless - May 15, 2010, 3:19 pm

No problem.

Hope this comes to use.

Braco Asshole - May 15, 2010, 3:23 pm

Wow nice positive comments on this wonderful thread.

Once Timeless - May 15, 2010, 3:30 pm

I am glad there are.

I hope people refer more new computers users to this thread could help them out. If I saw this when I was just getting started and read it my knowledge of virus based things would have nearly doubled.

Legit Dude - May 15, 2010, 4:24 pm

Sick, thanks for the add to your post. :)

Once Timeless - May 15, 2010, 4:26 pm

No problem, like I said in the thread.

"I don't mind this being a community project."

Once Timeless - May 16, 2010, 2:24 pm

Thanks Crow for adding the section about phishing!

Once Timeless - May 18, 2010, 9:21 pm

Bump...

Good info here.

More members should read this.

nathan.505 - May 19, 2010, 2:27 pm

Thanks for the guide. It really helped me.

Once Timeless - May 19, 2010, 2:30 pm

No problem enjoy it :)

Can come in use.

Livewire - May 20, 2010, 4:05 am

Looks great! Pm'd you (:

Keep up the good work!

Once Timeless - May 20, 2010, 2:15 pm

"Livewire" info has been added.

Thanks for spending the time on it.

Livewire - May 21, 2010, 7:17 am

Thank you. (:

This is turning out pretty nicely. I like that it's a community project...so to speak

:D

Paradoxum - May 21, 2010, 8:48 am

I suggest you watch out for minor spacing issues. ?

Once Timeless - May 21, 2010, 2:14 pm

There you go picky people.

I believe the info is more important then the format.

Paradoxum - May 22, 2010, 6:01 am

(May 21, 2010 02:14 PM)WMM Wrote: [\[CITE\]](#) There you go picky people.

I believe the info is more important then the format.

True, but the format attracts the eye which convinces the brain to keep on reading.

Once Timeless - *May 22, 2010, 9:52 am*

I am sure it is but spaces usually don't harm the eye the just make it harder to scroll. So, not worth arguing about.

Glad you like it enough to give some feedback.

Once Timeless - *September 30, 2010, 6:34 pm*

There is a rule against bumping threads with low quality replies that are irrelevant to the topic. First warning; don't let it happen again. - Valiant