

Forum:[Hack Forums](#)

Thread: [\[GFD\] Guide For Dummies: Windows Security](#)

Tokyo ? - March 5, 2014, 3:49 pm

Meso's Guide To Windows Security Hey guys, I know many of you know the values of having security on your various Operating Systems and your computer in general, but this is a "Security Guide For Dummies" in a sense. I'll be discussing the importance of having security as well as some tips and tricks to ensure that you are truly secure. In this particular guide, I will be discussing the importance of security on WINDOWS operating system, hopefully these tips are easy to understand and after reading this thread you can walk away knowing more about your Windows Security.

Why Do We Need Security? First of all, I would like to point out that whether you like it or not, computers and other technology are slowly become an everyday thing and what some would argue to be a necessity in households. It is because of this fast growing "technological up-rise" that more and more people are becoming familiar with the security protocols of various Operating Systems and how to bypass and exploit them to enable themselves access to your software and potentially do some nasty things to it. This is why I am creating a Windows Security guide because quite frankly everyone needs to be familiar with techniques they can use to counter-act exploitation and other potentially harmful situations when using their PC. So, with that being said, why is security so important?

1) The number one reason as to why security is important is because of the fact we are incorporating it into our daily lifestyle, we tend to become lazy and leave sensitive information all over the place. Whether this information be E-Mails, Passwords, Phone Numbers, Addresses, Credit Card Numbers, or even Online Banking Details you are constantly leaving footprints on every single domain you enter or everything you do on your machine!

2) As I mentioned on the previous point, your footprints are everywhere, someone can find you from the gamertag you had in 4th grade or even just from your first name and your DoB, making sure you are being secure on the internet will LIMIT (not remove) the amount of footprints you have.

3) Lastly there are 3 main types for security (in my mind), the 3 types consist of: Operating Systems, Internet, and Software. I will be going into all of these types and analyzing what you can do to stay secure!

Security | Operating Systems: Operating Systems are the heart and soul of your PC, they link everything together, from the hardware to the software. You always want to keep your heart pumping and your soul in high spirits correct? So keep your Operating System the same way! How might you ask? Well one of the most important things you need to note about keeping your Operating System secure is to update it on a regular basis, if an Operating System is out of date then they are now vulnerable and easier to break into. Operating Systems do not update for no reason, usually there is a purpose behind the act and if you can not keep up with the new technology you will crash and burn. The main focus here is to ensure that you have turned on "AutoUpdate" for your Operating System, this will notify you when an update needs to occur and it is because of this notification that it is very hard to miss and update.

How do I turn on AutoUpdate?

- 1) Click the "Start" button in the bottom left corner of your screen, and/or press the "Windows Icon" on your keyboard.
- 2) Next go to your Control Panel and look for "System and Security".
- 3) After clicking on that you should arrive at a page that lists multiple selections to choose from, you will want to go to "Windows Update". Here you will see sub headings on the left side or in the middle of the pop-up, you will want to click on "Check for Updates" or "Turn automatic update On or Off".
- 4) Obviously if your updater is turned off, turn it on and set it to daily to ensure that you are being notified every day of the week, month, and year in case there is a sudden OS update!

Other security tips I would recommend would be to make sure you are running NTFS Disk Formatting as well as assigning passwords to all user accounts on the machine. Passwords are key to protecting your OS, one way to make sure you have a strong password is to go and enable "Strong Password Policies" on your PC. This will create a minimum length as well as a lockout time when a certain number of wrong passwords are entered. You can find "Strong Password Policies" by going to "System and Security > Account Policies > Password Policy".

Security | The Internet:

It's no secret that staying anonymous on the internet can be quite challenging at times, and you will or maybe already have left some footprints that allow people to attain information on you. How can you stay anonymous?

There are multiple ways, but a very easy way is to change your IP address every week or so and to do this you simply leave your router unplugged for 30 minutes to an hour which will change your IP address to a completely new one!

Another way is to get a Virtual Private Network, also known as a "VPN". Virtual Private Networks essentially cover your IP with another, hence giving the viewer a false impression that they do in fact have your IP Address. Many of the good VPNs you have to pay for, which are worth it depending on how paranoid you truly are, so expect to spend a little bit of money when looking for a good VPN. Lastly, which is kind of a silly suggestion but if you live close enough to a neighbor, you can always use their network! This will show your "IP" as the IP Address of your neighbor and you won't have to worry about being tracked!

Free VPNs (Although Not Recommended):

- 1) HotspotShield: <http://www.hotspotshield.com/>
- 2) CyberghostVPN: <http://cyberghostvpn.com/>
- 3) VPNBook: <http://www.vpnbook.com/>

Now as I mentioned before, because of the fact you leave fingerprints all over the internet, some people are able to take those prints and track down your exact location and everything about you. This is called "Doxing" or attaining someone's "Dox". If you are unaware of what a "Dox" is, here is an example of information of what a Dox can consist of:

Spoiler ([Click to View](#))##### BASIC INFORMATION #####

Name:
Birthday:
Age:
Email:
Skype:
Facebook:
Twitter:
YouTube Channel:
Google Plus:

ADVANCED INFORMATION

Alias:
GT:
IP:
Address:
Country:
City:
State:
ZIP:
Postal Code:
Home Phone:
Cell Phone:

FINANCIAL INFORMATION

Amazon User:
PayPal User:
Ebay User:

As you can tell, if someone were to get your "Dox" they can do pretty much anything to you, including blackmail and harassment. So how can you prevent a dox? A very simple way is to use a VPN and to change your IP Address as I stated above, but you can also do something else. If you are trying to become anonymous on the internet and are still not satisfied with the techniques I mentioned earlier, try going to a public facility and using their internet. For example a library, a school, or even a gymnasium. Also try to not give out any personal information over the internet to anyone who asks for it, tell them you would rather stay anonymous and if they do not respect that decision, just move on and forget about them.

Security | Safe Software:

Software is the blood in your computer, it never goes away and carries/provides for your computer in multiple ways. One being the type of Browser you are using or the type of Anti-Virus protection you have. Typically you don't want to remove these items and without Software, your computer would just be blank and would be pretty boring. So lets now get into the topic of "Safe Software" and what are some things you should be looking out for when downloading programs and software off of the internet.

Let's go through my process of thinking when downloading software:

1) Assess what you are downloading - Could the software have other hidden features? Does it contain unwanted traffic ads and other annoying material? With these "hidden" features affect my PC's performance?

2) Review the source - Check to see if the domain/website in which you are downloading the software from seems legitimate and has positive reviews as a SAFE and RELIABLE source.

3) Who else has this? - Check to see if the software has good reviews and whether or not there are potential risks involved after downloading. Just search the product on Google and have "reviews" followed behind the name to get a list of some feedback others have had with the software.

4) Check Size & Type - How big is the file? How much memory will this software take up to run? What type of application is it, and is that type of application dangerous? (Look for .exe, .bat, .pif, .scr files)

5) Is the software signed? - When choosing to "Run" or "Install" the software, check the top left corner of the pop-up box to see if the software is licensed. Typically software that has a company name there is legitimate, but don't always trust this, double check the source. If the top left reads, "Open File - Security Warning", then you know it could be a potential risk to your computer and information.

Follow these steps for installing software and you can 99% guarantee a safe and trustworthy install, and you shouldn't have to worry about any malicious content coming onto your PC.

Thank you for your time, this has been my first guide in my new guide series "Guides For Dummies". Hopefully this educated you all, and please leave any feedback for me as a post reply below it would be much appreciated for improvements on my next guide!

~Meso~

?

Tesseract - March 5, 2014, 5:32 pm

This is a pretty cute guide. I like it, and it really is for dummies. Great stuff for those at the level of zero in computing.

Tokyo ? - March 5, 2014, 5:41 pm

(Mar 5, 2014 06:32 PM)Radix Wrote: [\[CITE\]](#) This is a pretty cute guide. I like it, and it really is for dummies. Great stuff for those at the level of zero in computing.

Thanks for the feedback, much appreciated! ? And this right here:

(Mar 5, 2014 06:32 PM)Radix Wrote: [\[CITE\]](#) it really is for dummies. Great stuff for those at the level of zero in computing.

Music to my ears, considering that is exactly what I was going for! ?

Boog663 - March 5, 2014, 6:31 pm

Great guide, thanks for posting it.

Tokyo ? - March 5, 2014, 6:39 pm

(Mar 5, 2014 07:31 PM)Boog663 Wrote: [\[CITE\]](#) Great guide, thanks for posting it.

Thanks very much, appreciate the feedback! ?

Entropyon - March 5, 2014, 7:01 pm

I'm unsure which section. But this is general threat to windows security as you cover it. The security settings of java should have been set for maximum and readers should have been told not to install java if not necessary. Same with flash, especially now when you have html5 available on youtube.

Null Byte - March 5, 2014, 7:01 pm

Very simple but effective guide, this is information that everyone needs to know.

Entropyon - March 5, 2014, 7:02 pm

Forgot to mention that this tutorial is good because it's short. Don't try to extend it to size of a book

Tokyo ? - March 5, 2014, 7:05 pm

(Mar 5, 2014 08:01 PM)Null Byte Wrote: [\[CITE\]](#) Very simple but effective guide, this is information that everyone needs to know.

Thanks for the feedback Null. I think I'll keep making guides like this one, maybe some more advanced!

Ventures - March 5, 2014, 8:19 pm

Great guide for the general user who's looking to increase his knowledge on security. Thanks for posting this.

Aura - March 5, 2014, 9:08 pm

(Mar 5, 2014 08:01 PM)Entropyon Wrote: [\[CITE\]](#) I'm unsure which section. But this is general threat to windows security as you cover it. The security settings of java should have been set for maximum and readers should have been told not to install java if not necessary. Same with flash, especially now when you have html5 available on youtube.

Youtube isn't running completely on HTML5 yet, there's still in a transition phase, just saying.

But yes, keeping Java and Adobe Reader AND Flash up-to-date would be a good add-on.

Tokyo ? - March 5, 2014, 9:12 pm

(Mar 5, 2014 10:08 PM)Aur? Wrote: [\[CITE\]](#) Youtube isn't running completely on HTML5 yet, there's still in a transition phase, just saying.

But yes, keeping Java and Adobe Reader AND Flash up-to-date would be a good add-on.

Sounds good, I can definitely look into adding those on. Thanks for the input guys, really appreciate the feedback! ?

Par4ni - April 6, 2014, 4:21 pm

This is a well written, thanks for posting this.

Tokyo ? - April 7, 2014, 7:38 pm

(Apr 6, 2014 04:21 PM)Par4ni Wrote: [\[CITE\]](#) This is a well written, thanks for posting this.

Hey, thank you for the kind words there mate! Glad that you learned something and got enjoyment out of reading this. I hope to pick up this series once again here within the next week! ?

Warm Regards,

-Redic

Eeluminati - April 17, 2014, 5:57 am

You should include Dox stands for Documents.

Tokyo ? - April 18, 2014, 8:02 pm

(Apr 17, 2014 05:57 AM)Eeluminati Wrote: [\[CITE\]](#) You should include Dox stands for Documents.

Dox Stands? What do you mean specifically? ?

Jagster™ - April 19, 2014, 8:39 am

One thing I will critique:

You mentioned that to avoid being dox'd you should change your Ip (VPN) or use a public location... really the more important issue is to never give out real information or share your profiles

containing your real information. That is by far, more important than your real Ip being resolved seeing how a lot of users have dynamic IP's and can also request IP changes almost instantly from most ISP's.

Other than that, great little guide and very well written.

Computer Forensics - *April 24, 2014, 9:36 pm*

Amazing guide keep up the good work.