

Forum:[Hack Forums](#)

Thread: [How do you protect yourself ?](#)

Corrupt3d - April 13, 2017, 5:14 pm

i was wondering what kind of protection you all use or do against virusses dangerous links etc?

i use
vms
Malwarebytes
sandboxie
vpn
use virus total a lot
and glasswire(to see when my computer makes a new connection)

Soulmate~?? - April 13, 2017, 6:30 pm

Those are the basics but you could switch out MBAM with any top level AV or Malware Removal Tool. Also there are some extensions that come in really handy when you're browsing which protect your privacy. There are tons of them but some good ones are HTTPS everywhere, [Disconnect](#), LastPass (for passwords), and Privacy Badger. Adblock is also a must but I try not to run it on websites where I can support the creators through ad revenue. I think Sandboxie or a VM is the most important part.

?Ñâzg?! - April 13, 2017, 8:08 pm

I use linux ?
Dear admins: I have nothing else to say

Mr. Kim - April 13, 2017, 9:34 pm

I use windows firewall and my brain :)

Come at me <3

Evil Corp - April 14, 2017, 12:34 am

(Apr 13, 2017 08:08 PM)?Ñâzg?! Wrote: [\[CITE\]](#) I use linux ?

Dear admins: I have nothing else to say

I'm not sure if I should move to linux completely.....I do graphics design and video editing, that would be hard on linux if I'm not using windows software.

E1NH4ND3R - April 14, 2017, 8:33 am

Don't run .exe files from websites you don't know.
And don't visit websites that are suspicious.

?Ñâzg?! - April 14, 2017, 10:26 am

(Apr 14, 2017 12:34 AM)Evil Corp Wrote: [\[CITE\]](#) I'm not sure if I should move to linux completely.....I do graphics design and video editing, that would be hard on linux if I'm not using windows software.
lol I was just fucking with you guys
even on linux you do need security (not an AV but other things)
Noscript, an adblocker, self destructing cookies, firewall and app armor are the basics for linux security
and it's more than just that

ZwntanosNekros - April 14, 2017, 10:27 am

I use virtual machine always and never opening anything at main os.

Estonia - April 14, 2017, 11:11 am

(Apr 14, 2017 08:33 AM)4NN1H1L4710N Wrote: [\[CITE\]](#) Don't run .exe files from websites you don't know.

And don't visit websites that are suspicious.

If you have windows (no xp or anything end of life thing) how u can get infected by simply visiting website. I know there are java drive bys but they aren't working.

givevalue - April 14, 2017, 11:13 am

Communication and account registration

1. unique email account for all of my important services (not that gmail wildcard bullshit, a unique email!).
2. anonymous SMS verification (I use www.anonymousbtcsms.com) for services that require sms verification

IP protection

I don't trust (and am too cheap to pay for) privacy services so I setup a box on AWS and digital ocean for my own VPN system using docker.

How to:

docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html

www.digitalocean.com/community/tutorials/how-to-set-up-an-ikev2-vpn-server-with-strongswan-on-ubuntu-16-04

Social profile separation

Use Google Chrome's profiles to separate my online identities. Prevents my facebook leaking to my gmail or other activities.

Estonia - April 14, 2017, 11:18 am

I use windis 10 but i have only windos defnder and i cant click on bad links all time

Zenomhunter - April 14, 2017, 11:18 am

I sit in a RDP. LOL I have a mac so mainly use a RDP with sandboxie

mr robots hungry child - April 14, 2017, 10:37 pm

Virtual machine for just about everything. Worst case scenario, my VM gets infected, and nothing sensitive is stolen.

Rangers. - April 16, 2017, 5:34 am

Using a VPS to do all the stuff I need to.

Computerjul - April 16, 2017, 5:53 am

I am using NOD32 + Malwarebytes but maybe i will change from MBAM to Zemana. In addition i am using Ghostpress against low level keyhook. An additional layer of security would give Riot Isolator with AntiRemoteDesktop and RUNPE + Vodooshield AntiExecutable but i doubt that anyone is so fcking stupid that he needs such a protection.

Best regards

Fresh Khalifa - April 16, 2017, 2:23 pm

I use Malwarebytes, CCleaner & Bit Defender. Other than that I always clean my temp files to keep junk off my computer.

THC - April 16, 2017, 2:24 pm

I have a shotgun sitting by my desk, I think I'm pretty safe.

Corrupt3d - April 16, 2017, 3:10 pm

(Apr 16, 2017 02:24 PM)M.D. Wrote: [\[CITE\]](#) I have a shotgun sitting by my desk, I think I'm pretty safe.

i live in europe so i use vodka

if russian hackers wanna get me i just throw the vodka and they chase it ?

THC - April 16, 2017, 3:12 pm

(Apr 16, 2017 03:10 PM)Corrupt3d Wrote: [\[CITE\]](#) i live in europe so i use vodka

if russian hackers wanna get me i just throw the vodka and they chase it ?

Weaponize it- Keep a rag and a lighter near by so you can transform it into a molotov.

Corrupt3d - April 16, 2017, 3:16 pm

(Apr 16, 2017 03:12 PM)M.D. Wrote: [\[CITE\]](#) Weaponize it- Keep a rag and a lighter near by so you can transform it into a molotov.

naaa i just pull my pants down and rub it against the hackers till they feel awkward and go away

Jericho - April 16, 2017, 3:56 pm

Well myself I think the best way to protect your security is common sense. Don't click fishy links from a guy that calls himself root@hacker69. And don't download files that you don't %100 trust even then you should scan them.. everyone knows not to trust a random .exe but most people for some reason don't think a .jar can be malware. But they are hugely mistaken

Internet - April 16, 2017, 8:02 pm

Bitdefender, SonicWALL with gateway filtering, and common sense. My important home servers are completely isolated on their own VLAN. I see no reason to have multiple security solutions running side-by-side on a computer, waste of resources if you have half a brain.

I may run second-opinion scanners like Super Anti-spyware (very underrated solution) and MBAM every-so-often.

?Ñâzg?! - April 16, 2017, 11:09 pm

(Apr 16, 2017 03:56 PM)WatchingJ Wrote: [\[CITE\]](#) Well myself I think the best way to protect your security is common sense. Don't click fishy links from a guy that calls himself root@hacker69. And don't download files that you don't %100 trust even then you should scan them.. everyone knows not to trust a random .exe but most people for some reason don't think a .jar can be malware. But they are hugely mistaken

anything can be malware

MP4, MP3, Doc, PDF

the list goes on and on

however it requires a vulnerability in the software that you use

so for example if you use VLC the attacker will need an exploit designed for the version that you use but once he finds the exploit he can craft a MP3 file with a backdoor once the mp3 is executed

<http://www.gnucitizen.org/blog/backdooring-mp3-files/>

(I'm just saying don't trust any files regardless of them being .exe or not)
best way to protect from this is running with very limited rights and constantly updating your software

taylor8806 - April 17, 2017, 12:47 am

There are various ways that will help you to protect your PC from malicious malware program. Very firstly install best security program and update it time to time. You need to be aware while installing anything from the web as downloading any free software brings nasty virus or malware with itself. Here check out some tips that will help you prevent virus and malware while downloading anything.

- Apps that function as an Explorer plug-in: These are very dangerous as they directly hook into the shell and will also make the entire PC slow or in the worst case, crash repeatedly.
- Antivirus applications: These are dishonorable for slowing down your PC, and you should never , ever use more than one real-time antivirus application at a time
- Anything ads that say it wills "Speed Up Your PC" or "Optimize Your RAM" will most likely slow it down, or damage the system, these are like the plague. So try to avoid all that as far as possible.
- Be certain to install official system drivers from the manufacturer website. Drivers play a very important role and have a huge impact on performance, so have stable, updated drivers.

These are very helpful tips for protecting your PC/laptop. You can make use of the best Virus Removal Tool this is best to remove any type of malware/virus program from your PC. This is the most advanced tool designed to automatically scan your PC and remove the malicious program easily. It also optimizes the performance of the PC/laptop and enhances the speed of the PC, and application installed.

To know more visit: fixwindowerrors.biz

5chn4pp - April 18, 2017, 3:44 am

FRST
JRT
Adwcleaner
Combofix
Hitmanpro
Rkill
Roguekiller
Tdskiller
Gmer
aswmb
And my brain

holyraider - April 18, 2017, 7:00 am

brain.exe, firewall, noscript, adblock, https only

if i suspect something happened i use mbam or kaspersky to check, but i never have any AV software running by default.

havnt had an infection in like 5 years..(i think h3h3 :D)

SIM-2501407 - April 18, 2017, 7:05 am

I simply don't trust people.

5chn4pp - April 18, 2017, 7:10 am

(Apr 18, 2017 07:05 AM)Act of Valor Wrote: [\[CITE\]](#) I simply don't trust people.

You trust HF with your personal info

You trust your email service with your personal info

You trust the brand of your hardware to not be backdoored
You trust many things in this world

SIM-2501407 - April 18, 2017, 7:11 am

(Apr 18, 2017 07:10 AM)Satudarah Wrote: [\[CITE\]](#) You trust HF with your info
You trust your email service
You trust the brand of your hardware
You trust many things You apparently do not trust punctuation.

ZuGgY - April 18, 2017, 7:14 am

I have avast, Malwarebytes, JRt, unlock origin, AdwCleaner, sandboxie, vpns, and logic.

5chn4pp - April 18, 2017, 7:14 am

(Apr 18, 2017 07:11 AM)Act of Valor Wrote: [\[CITE\]](#) You apparently do not trust punctuation.
Eh, that's something I normally don't use as I expect users to understand it.

LNO BoSS - April 19, 2017, 11:52 am

Your best bet is to stop running your mouth to me

Corrupt3d - April 19, 2017, 11:54 am

(Apr 19, 2017 11:52 AM)LNO BoSS Wrote: [\[CITE\]](#) Your best bet is to stop running your mouth to me
what you going to do shit talk in every thread of me ?
after that gonna lie you have another site and some software you dont own ?

dude your pathetic

Riggs - April 19, 2017, 12:04 pm

Surprised nobody has mentioned using SHA1 hashes and checksums yet. Verifying a sig confirms ownership and checksums ensure software integrity. These steps should be common practice for any vigilant user, but like most crypto-mechanics are often overlooked as rocket science.

Maeko - April 19, 2017, 12:29 pm

By not visiting suspicious sites or open any executable files that I have no idea of.

?Anarch - April 20, 2017, 3:27 pm

Use a virtual machine and dont really use things without running them in it first

cypherdemon - April 20, 2017, 3:53 pm

Bitdefender Total Security
Malwarebytes
Adw Cleaner

Currently got my eyes out for a VPN so I'll have one soon :)

Corrupt3d - April 20, 2017, 4:03 pm

thx for responses im going to use these answers for a school project :)

lucky. - April 20, 2017, 4:06 pm

Malwarebytes and occasionally using a VPN is all I need.

Byte-Array - April 22, 2017, 5:18 am

MBAM+Eset+VPN. Hopefully the combination would kept my PC safe....But as all says- "Security is a Myth"...

Agent A - *April 22, 2017, 8:07 am*

Fully encrypted disk + critical file 4 layer encryption [AES[blowfish[threefish[shacal-2]]]]. VM ware + deep freeze + sandboxie + ESET endpoint security + VPN + Malverbites.