

Forum:[Hack Forums](#)

Thread: [\[TUT\] HUGE GUIDE to advanced online security | Computer protection](#)

?pth?n - May 25, 2014, 12:14 pm

Welcome

NOTE: This tutorial is for educational purpose only.

Table of contents

- I. Introduction
- II. Definition of dangers
- III. Antiviruses
- IV. Safe browsing
- V. Useful tools
- VI. Final words

I. Introduction:

Nowadays, everyone seems to know quite a bit on how to protect himself from the dangers of internet. Dangers such as viruses, trojans, phishing and scamming.

But the knowledge the majority of the people got, is outdated.

Blackhats are regularly updating their methods so they can find new „victims“ - victims like you and me!

My aim is, to make you alot more self-confident when traveling through the world-wide-web.

This tutorial is written for beginners and those who don't know how to stay safe on the internet.

II. Definition of dangers:

This chapter will tell you what a virus is, what it can do, and how it spreads itself (e.g. infects you).

A virus is an unwanted program, you can get while surfing on the web. Not every virus wants to steal your bank data!

There is a wide range of things the people who spread those viruses want to achieve. There are viruses who:

- Steal personal data
 - Steal passwords
 - Steal bank data
 - Scare you
 - Lock your pc
 - Destroy your PC
 - Delete files
 - Log everything you type in
- and so on..

Actually, the most common type of virus gives you full access to the victims computer.

So the hacker can see your pictures, documents, what you are doing right now, your IP, your Name, your passwords..

he can even shut down your PC or install new viruses on it!

So it is extremely important NOT to get such a virus.

There are only three main ways on how you may become a victim of a virus:

1) Opening an executable file. Viruses nearly always are .exe files (some more "harmless" ones can be .batch and such aswell).

If you get .exe from someone you don't know – DON'T open it!

Viruses don't hide in pictures like .jpeg (exception: read 3.)

So you are rarely getting infected by opening a picture or a song.

The most common executable you will meet are .exe files. However, there are some other file types that are executables aswell so you should deal with caution when finding one of these:

- .exe
- .scr
- .vbs
- .bat
- .jar
- .com
-

Number one rule: Don't open executable files you don't trust!

Make sure to go to your folder options and uncheck "hide extension for known file extensions". You can prevent falling for simple spoofing tricks this way.

2) Visiting a website. Yes, you can get infected by visiting a website. This works by exploiting a loophole in the Java application.

If you get infected, you won't even notice it. This kind of infection is called „silent java drive-by“ (SJDB).

This is a popular method, because most people will visit a website more likely than opening a .exe file.

However, this exploit was fixed some time ago. So if you're still using a old version of Java, update it NOW!

You may heard of people, saying they got infected on google or gmail itself. This is wrong, and they got the virus somewhere else.

Those big sites can't infect you, because for a SJDB, the site owner has to upload his virus to a site and change the site code so you will get infected with it.

No one can change the code from such a big site – unless it is

hacked. There have been cases in which a big website got hacked and a SJDB was uploaded to it.

So everyone who visited the site that day became the victim of a virus.

So in theory it's possible to get infected by visiting popular sites. But this is highly unlikely and JDBs have been patched.

3) Outdated plugins. In 2), I mentioned that an outdated version of Java gives hackers the opportunity to infect you while visiting a website.

There are also some other plugins you should always have updated. The most common plugins with security risks are flash player, adobe reader, acrobat, the browser itself, windows..

Always have your plugins and software updated! The companies usually fix exploits very fast, but this won't give you any advantage if you don't update your plugin regullary.

These so called „0-Day-Exploits“ are very dangerous when they are found in programs like Adobe Reader.

A .pdf can have a manipulated code, infecting you as soon as you open it.

The same can happen to other files, which are normally using a third-party-program (no windows

program) to open.

So always update your plugins and programs. It may be quite annoying, but it will increase your security alot!

2.1 Trojans (RAT's):

Today, the most common virus is a trojan. More exactly, a RAT. RAT means „Remote Administration Tool“.

It is extremely easy to build such a virus.

Even a 12-year old can follow online tutorials to build one.

They may be easy to create, however they are not less dangerous because of this. RAT's grant the hacker full rights to someones computer.

He can see what the victim is doing, control his clicks, lock everything, view the webcam, read out passwords and keyboard inputs – basically he can does everything he wants.

2.2 Worms, Ransomware:

Worms are getting rare these days, but they still are the most dangerous virus when the hackers aim is to destroy your computer or infect it with alot of different stuff.

They can be a real pain to get rid of. If you are infected, they may spread through your LAN-network and even through your e-mail contact list or facebook account.

Not knowing that you are used, you will then send an e-mail with the virus as attachment to all contacts in your e-mail program.

Another shooting-star regarding viruses, is Ransomware. This is the software that locks your PC, telling you that the authorities found child porn, terroristic material and so on on your computer.

If you want to unlock your PC, you have to pay a small sum like 50\$ via Paysafecard or another online payment to the fake authorities.

They are easy to build (using a premade toolkit!), what makes them pretty common in the web. They are ridiciolous annoying to remove, but not impossible.

2.2 Spyware, Adware:

The name of these „viruses“ sound horrible, but they actually are one of the softer viruses.

You can get one of these, when installing normal tools (e.g. Yahoo) and clicking on the next-botton too fast.

You will then agree to install one of these programs. They are mainly looking at your online activity.

What sites you visit and what you are searching for on google. Knowing this, they will give you pop-up's with advertisments that are related to what you have searched before.

Adware often gives you simple pop-up's about betting and porn sites. They are not really harmful, but it still can be irritating when getting interupted by one of these pop-up's.

III. Antiviruses:

Normally every computer got an antivirus-program – most computers even have them preinstalled. An antivirus-program detects a virus on your system, and removes it right after. This is the theory. The common belief is, that if you own a good antivirus-program, you won't get any trouble because of viruses anymore.

That is...completely wrong!

An antivirus-program can be a good addition to give you more safety while surfing, but it doesn't gives you full security for your system.

Furthermore, if you are using the knowledge you will eventually have after fully reading this tutorial, you don't even need one anymore. (It is still recommended, of course!)

If you are looking for an answer on which program is the best, I can't help you.

Antivirus-programs are using databases of signatures (part of a code every program has), and comparing them to every file on your system.

If they find a signature on your computer that matches one of the infected signatures in the AV's database, then they will

evacuate/delete the infected file. This is why there is no best program. Every popular AV-tool has a big database of signatures, to check viruses with.

What points out a good AV, is how fast they upload new signatures to their database.

From my personal experience, I can suggest you Avast, Avira, ESET, Kaspersky and a few others (Note: These are only personal suggestions, feel free to use others).

They are updating their databases frequently – so always update your antivirus-program when there is an update available.

It is very important to read chapter 3.1 now, to see why you should update your program as often as possible.

3.1 Crypters:

Why are there still viruses that „bypass“ your antivirus-program? The answer to this question is simple, because the guys creating and spreading those viruses are not dumb.

There are so called „Crypters“. These Crypters have the ability, to change the code of a program, so antivirus-programs won't detect a virus as a virus.

When someone writes such a crypter, every virus "modified" with it will be undetectable for any antivirus-program.

It will take some time for the AV companies to find the new virus and update their database of signatures.

This can take a few hours, a few days or even weeks. That is why you should update (auto-update) your AV-program whenever an update is available.

Such Crypters are even getting sold very cheap on the web. So the 12-year old who built a RAT, can save up his money to buy a crypter, which will make his virus fully undetectable (FUD).

It is important that you understand how easy it is, to create and hide a virus. The 12-year old is no fictional story!

Those black-minded hackers who hide in the dark only appear in movies. The truth is, that everyone who can use google is able to build such a virus from scratch within 1 hour.

Everything needed is available as a toolkit, or purchasable for money.

As you can see, such a virus is no magic..

but staying safe while browsing isn't neither!

IV. Safe Browsing:

So far, you have learned that viruses only infect you when you open an executable file or when you browse through the web with outdated plugins like Java.

You now also know, that no AV-program can secure your system from a virus that was made very recently. But there are still some other tricks to stay safe while browsing, and I will show you them!

4.1 Updated plugins and Java

Since I mentioned this point before, I will only repeat it in short. Whether you are using Firefox, Chrome or Internet Explorer (I recommend you Firefox!) you need to stay updated regarding the plugins you are using.

Firefox is a safe, fast and comfortable browser, so I suggest you getting it. Most of the Plugins or in-depth steps I will mention are using Firefox.

If you want to update your plugins and addons, you simply need to click on Extras -> Addons in Firefox. You can auto-check if your plugins are up to date there. If they are not, then please update

them as soon as possible.

Most plugins also have an auto update possibility. I suggest you checking this, as it will save you a lot of time.

4.2 Useful addons for Firefox

There are some really useful addons for Firefox. In fact, Firefox is known for thousands of addons that can be handy in all situations.

Some addons are also helpful to make your browsing more secure. I will show you the most useful ones!

NoScript:

Every website is using so called scripts for different actions on their site. If you are using Java or Flash applications for example, then you are using such a script.

Behind such a script, a hacker could hide his malicious file. You can't get hacked by visiting a website without any scripts and just text.

NoScript blocks all scripts, on every site! This makes it extremely handy, and I suggest everyone to download it.

It will be annoying the first few days, since every website uses scripts and you need to allow scripts for the site first.

After the first week, you then will have a decent „white-list“ of websites, which won't have any scripts blocked.

AdBlock:

This awesome addon helps you to block all pop-up windows that interrupt you from surfing. You can also allow pop-up's for a specific site if you need to.

These advertisements are not only annoying, they can also sometimes contain viruses. If you are using these two addons, your experience while browsing will be a new one.

You can feel quite safe (don't click obvious scam links, especially on FB) and won't be annoyed by pop-up's any longer!

Other nice addons you should have a look into are Ghostery or Lightbeam.

4.3 DOX and Anti-Dox

Doxing is the gathering of personal information of someone on the web. Doxing is not done by many, however, if someone is good at it and has some luck, he can get into your online accounts.

If someone is doxing you, then he is browsing through all search machines, social networks and so on to find information about you.

Most of the times this only happens when there is an enemy you got in real life, who wants to harm you.

Information about you can be used in multiple ways, but the most common one, is to access your email account. If you create a new email account, you have to set recovery

questions. Often, answers to these questions (e.g. My grandfathers first name) can be found while doxing. How can you prevent that someone doxes you?

It is very simple. Stay away from posting all your personal data in the web! Facebook is the worst you can do. I don't mean that you are not allowed to use FB.

But if you do so, have in mind that everyone can see what you are liking and posting. Use the privacy settings on Facebook, and make everything as private as possible.

Google yourself! What can you find out about you? „What is in the internet once, will stay there forever“

Have this in mind when you are giving out your personal data anywhere.

Quote:PRO TRICK (Facebook):

1. Set your facebook language to Indonesia, log out
2. Use a proxy to get an IP from Indonesia
3. Login, delete your last name! You can keep your surname only
4. Change the language and IP back
5. You now will only have your surname on facebook!

?pth?n - May 27, 2014, 10:02 am

4.4 Emails and security questions

Spam is annoying! But there is a common misunderstanding regarding spam emails. Opening a spam email is harmless.

In fact, sometimes I just open these emails to read them - this can be quite amusing! You can only infect yourself when opening the attachment in the email, or following a link within the mail.

Links in emails do look real sometimes, but don't follow them!

It is easy to „spoof“ links, so the real link is hidden behind the one you will see. Another trick of hackers is, that the email header can be spoofed aswell!

And this is childsplay! You can do it within 2 minutes. Spoofing a email, will make it look like someone else send it. Basically everyone can send you an email from, for example:

„gates@microsoft.com“ or „smith@cia.gov“

The mail wont be send from that mail, but it will look like that. If you have read the latest chapter about DOXing, you will know that your personal data doesn't need to be in the internet.

A common mistake the most are doing, is setting very easy security questions for their email accounts. Security questions are safe when the information cannot be found in the internet, or obtained from other persons easily.

A perfect security question for example would be: „What was my first word“ or „What was the first gift from grandma“ As long as it is very personal, it is fine!

4.5 Choosing the right password

Having strong passwords for your internet accounts is recommended! But most people don't understand why. There are two reasons on why you need a strong password:

- Guessing:

If someone who knows you wants to guess your password, he will try passwords, that you could have chosen. For example if you like football, he will try „football“ „Football“ and maybe even „football1“.

So don't use your name or anything related to you as your password. Noone should be able to get into your account by guessing it!

- Bruteforcing:

The main reason on why you need a strong password, is to be secured from so called „bruteforce“ attacks.

Bruteforce is a way on how to hack an account. The attacker will automatically try to use every possible combination of signs as your password!

Most websites are secured against bruteforce attacks, so this is kind an old method on how to hack someone. Also, if the password is more than 9+ signs long, it will take a very long time to hack it.

The time needed depends on the computer used, but in general a password with 10+ signs will take more than 1 year to hack.

A similar method is a dictionary attack. This doesn't try out all possible combinations, it will rather have a premade dictionary that tries all words and checks if the password is a word that is in a

dictionary.

This method is much faster than bruteforcing! Because of this, make sure that your password is LONG and can't be found within a dictionary!

A perfect password is memorable, uses upper- and lowercases, signs, numbers, 10+ cases and is not found in a dictionary.

An awesome password would be a sentence you can remember! Use the first letter of every word, and you get a strong password.

4.6 Phishing and https

When you login into any bigger site, especially online shops likeamazon, you will be browsing on a https connection.

This will make it alot harder for anyone who is on your network or tries to find out your password, to success.

If the website you are login in or browsing at uses https, your traffic will be secured way better than while browsing on a http site.

Most phishing websites, e.g. a fake amazon site, are not using the https protocol. If you are unsure or want to check if the billing site you are redirected at is safe, just take a look if it uses https.

You can't do that in general, because there are alot sites without https. But especially when doing online banking, check if its a secured connection.

On facebook you might want to check out the security settings for your account.

You can set, that you always want to browse facebook on a https connection. This gives you no disadvantages, so just set it.

V. Useful tools:

5. Useful tools

There are alot of dangers in the internet, but there are even more tools to safe you from them! Some are really handy, and the regular internet user doesn't even know about them.

That is a shame, because with the right tools and some usage of your brain, you won't need an AV-program anylonger! I will give you some overview for the most useful tools in my opinion.

These tools are easy to understand, and safe downloads of them can be found on the internet easily (most of them have their own website).

5.1 Sandboxie / VM

Everyone already had a file once.. and was wondering if it is safe to open or if it's a virus. If you were unlucky, it was a virus and you got infected right when opening it.

With Sandboxie you don't have to worry about this any longer! Sandboxie will make you a „special place“ within your computer - when you open something with sandboxie, you can work with it like on your normal system.

But the advantage of sandboxie is, that you can delete the whole sandbox with just one click! So if you opened a virus, you can just delete your sandbox and the virus will be gone aswell.

What happens in the sandbox, stays in the sandbox.

Because of this, it is the best testing-area for suspicious files. Virtual machines (VM) are working the same way. There are plenty VM out there.

Just google for them. You can set up a virtual computer, and test things out on it.

If you want to change it back, you only need to do one click and everything will be deleted on your VM.

Sandboxie (www.sandboxie.com) is free to use, and will give you alot of self confidence when browsing the web – because you can even start your browser with sandboxie!

5.2 Comodo, KeyScrambler, TCPview, STM

Comodo

Every windows user has the windows firewall preinstalled. The windows firewall got better with time, however there are still better firewalls which are free to use.

One of these additional firewalls is Comodo. If you install Comodo, every program that wants to communicate with the internet, has to ask for your permission first.

You will notice, when a program on your computer, for example a RAT, wants to communicate with the internet.

Seeing all in- and outgoing connections, is a great way to see if you are infected with a virus. Imagine, every RAT / Keylogger / Trojan has to send data back to the hacker – but it won't be able to, because the Comodo Firewall blocks it.

KeyScrambler

Keyloggers are still a common tool, to get someones password. Also RATs are using the technology of a keylogger, to log everything you are typing on your keyboard.

KeyScrambler is a free tool, that will encrypt everything you type into your browser. If you type in a website adress or write an email, KeyScrambler will encrypt your input with random numbers and signs.

Don't worry – you can write and use the internet as always. It just leaves a weird combination of signs for any program that wants to record your keystrokes.

That means, even if you are infected: When not storing passwords in the browser and using KeyScrambler, your passwords are very secured against hackers.

TCPview

You may don't want to use TCPview as a regular internet user. It is a tool from microsoft, that shows you every connection on your computer.

Even those that aren't connected to the internet right now. If you see an established connection from a program you don't know, you should immediately check this.

TCPview can be an awesome tool, to check if you are infected.

STM (Security Task Manager)

This tool can be quite handy, if you want to check all running processes on your computer. It will tell you which processes are safe, and which aren't.

You can't fully rely on the tool, because it's only looking for special suspicious features of a process. However, STM will rate every process and will tell you within seconds, if the process could be dangerous.

If the process is potentially dangerous, don't loose your head. It could be a false positive. Research about it a bit, and find out what it could be.

Since every virus is running as a process, this is an awesome tool for someone who is not that experienced with task manager, to quickly find out if there is anything unwanted going on.

5.3 Truecrypt

UPDATE: Strange things are going on with Truecrypt. It is unknown if the site got defaced or if they actually found a vulnerability that makes Truecrypt unsafe.

Stay away from version 7.2 and continue using an old version until it gets clear what happened.

This has nothing to do with online security anymore, but with general computer security. Truecrypt is a free tool used by the secret service and other companies.

It is able to put a password on a file, on a partition or even on the whole operating system!

Truecrypt is by far the best tool out there, that can make your whole computer extremly secure.

It won't help against hackers, but it will help against anyone who is physically trying to get into your computer.

It uses some awesome military-level encryption methods, making it impossible for anyone to be cracked, as long as you choose a hard password that can't be found in a wordlist (15+ chars).

Not even the FBI or CIA will be able to decrypt the file, if it has such a strong password. The more chars, the better. If you are scared someone could use your PC or you want to put a password on some specific file(s), Truecrypt is your best deal!

Truecrypt is an open-source project and gets regular updates.

Please visit www.truecrypt.org for more information.

VI. Final words:

Thanks for reading my tutorial!

I hope someone learned something new while reading it. If you got any questions, feel free to PM me or post on the thread.

This turned out to be a huge tutorial and I wrote it in my spare time. So leaving a simple "thanks" would be nice :)

If you found any bigger mistakes, let me know.

You may want to check out my other tutorials and lists as well:

Spoiler ([Click to View](#))- [\[TUT\] Improve your RAT spreading with worms](#)

-[\[Spreading\] How to infect your community or a company](#)

-[List of webcams with light](#)

- [List of sites that don't distribute](#)

- [\[FREE\] File Pumper | Boost your file size](#)

- [\[How to\] decrypt a hash | Beginner friendly](#)

- [\[TUT\] How to use a password profiler](#)

-[\[How-to\] use WhatsApp in "stealth mode"](#)

Have a nice day everyone ?

Aura - May 27, 2014, 10:05 am

OP, instead of posting your tutorial in different posts that have posts between each others, I suggest you to contact a Mentor or Staff member that will help you post your tutorial in one go so all your posts are after each other and it looks good. For now, save the two tutorials posts, delete that one and create a new thread. That's usually how people that creates tutorials in group subforums do before asking a Staff member to move the threads out of it.

?pth?n - May 27, 2014, 10:13 am

(May 27, 2014 10:05 AM)Aur? Wrote: [\[CITE\]](#) OP, instead of posting your tutorial in different posts that have posts between each others, I suggest you to contact a Mentor or Staff member that will help you post your tutorial in one go so all your posts are after each other and it looks good. For now, save the two tutorials posts, delete that one and create a new thread. That's usually how people that creates tutorials in group subforums do before asking a Staff member to move the threads out of it.

I know about that and that will be done when it's complete.

But since you help me out and I need to edit the post, this is the only solution for now.

Can't edit the post otherwise ;)

Aura - May 27, 2014, 10:27 am

(May 27, 2014 10:13 AM)?pth?n Wrote: [\[CITE\]](#) I know about that and that will be done when it's complete.

But since you help me out and I need to edit the post, this is the only solution for now.

Can't edit the post otherwise ;)

Alright well finish posting this tutorial, then close it and junk it (have all of it saved in a .txt file, divided in parts) and then send me a PM and I'll act as your place holder when you'll report it, alright ?

lorraine walsh - *August 17, 2016, 3:18 am*

Great helpful post, but you my friend missed something important. In the safer browsing category you did not mention about the neccessity of vpn services. They have become the requirement for modern day browsing. But only the authentic and genuine ones like PureVPN and Ivacy to some extent.