

Quick Internet Security Guide

By Ron Killian

www.theplrstore.com

WARNING: I am Not a security expert! This is Not a complete end-all-be-all guide to internet security. It is just a quick guide for some tips on improving security.

First things first... I know I shouldn't need to say this, but it does seem to slip most people's minds, including myself 😊

Preventive Measures

Keep your passwords safe!

It's a no-brainer, but people miss it every day. The first mistake is to store your passwords on your computer. I use to do that myself. Sadly it seems to be a growing trend of hackers and "bad people", to break into people's computers and obtain their passwords. It's happened to me and others I know. It's probably not that difficult to get into your computer.

There are two solutions that come to mind.

First is to keep your passwords on a removable device. I use USB Thumb drives myself, I have two, one being a backup. I also only keep them plugged into my computer, only then I need a password.

I also opted for USB drives that can be encrypted, double the power. Harder for hackers to get to them, plus, if you ever lose one out in public, there is less chance of any one accessing your information. I think I paid around \$8 each at Walmart and worth every penny as far as I am concerned.

Another solution is to use a anti-virus software that encrypts your passwords. They say it's very safe, but I still use the USB drives instead. It's an option, your choice.

It is also a good idea to change your passwords on a regular basis.

Back up Your Stuff!

I will admit, I am bad at this myself. You should always back up your data on a regular basis. You can do this manually, or better just a back up program to do it, so you won't forget. Tech's will tell you it's best to have two external back up drives. One plugged in and the other is not, the second one is not plugged in, in case of a lighting strike.

A anti-virus software can also go a long ways to protect the data on your computer and keep out “spies”, that might be logging what you do. What software you use is your choice, every one as a different opinion.

As for your Websites...

Again, backing up the data for your is very important! Most hosting services provide back ups as a part of their service, if yours does not, you might want to look for a new host, as it’s a very basic and necessary feature.

Back ups vary per hosting company, they are usually daily or more commonly, weekly. How often your site needs to be backed up depends on how often your site changes, or how often you update it. It also depends on how much you are willing to lose. I personally prefer daily back ups because my sites change quite often.

Obviously a back up is very important if you get hacked because you can “restore” your site. It could be the only way to fix your site.

If you need to do daily back up’s and you use something like Wordpress, you can use phpMyAdmin in cpanel, to export (back up) your database. This can also be set up to run automatically, speak with your host if you want to go this route, they can explain it better than I can.

An important thing to remember is, you don’t want to back up a database that is already hacked. Just something to keep in mind.

You should always keep a copy of all your files, so they are there if you need to re-upload them. They should also be backed up to an external device.

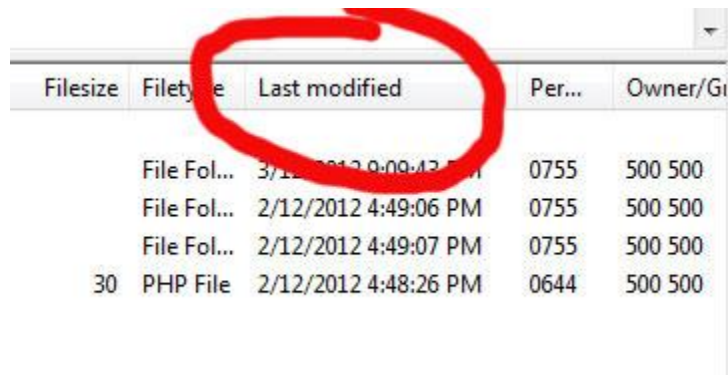
If you've been hacked...

The first step should be to see if new files have been uploaded to your site. You should also check to see if any files have been modified recently, that you did not modify.

As mentioned before, you should already have a copy of all your files, and you should also have a pretty good idea what files are right and which are not. If you're not totally sure, compare them to your local copy, to see which ones should not be there.

One note, some files are modified automatically, such as a site map, so a recently modified file might be all bad.

One trick I use to watch for changes to my sites, including WordPress, is to use FileZilla. With FileZilla, you can sort your server's files per "Last Modified". See the image below:



Filesize	Filetype	Last modified	Per...	Owner/Gi
	File Fol...	3/12/2012 9:09:42 PM	0755	500 500
	File Fol...	2/12/2012 4:49:06 PM	0755	500 500
	File Fol...	2/12/2012 4:49:07 PM	0755	500 500
30	PHP File	2/12/2012 4:48:26 PM	0644	500 500

That is a screenshot of the server side (or Remote Site:) of FileZilla. Clicking on the "Last Modified" bar will sort your server files by the last time they were uploaded or modified, which could be a clear indicator of what was changed or hacked. It's a much faster way of finding bad files. Folders will also show the date modified, even if one file is changed.

Once you find some files that are "not right", the best way to fix it, is to upload your local copy of the file and Over-write the bad file. Of course as long as your local copy is not hacked.

Remember though, over-writing a file will erase what is there, which is usually way you want to do, but be warned you could over-write something you need. So make sure you know what your re-uploading.

For Wordpress users...

If your using Wordpress to run your site, you need to make sure everything is always up to date. Be sure Wordpress and all your plug-ins are completely up to date. One of the biggest reasons wordpress or plug-ins are updated is for security reasons.

If your wordpress site is hacked, you just need to follow the procedure outlined above, about re-uploading files, over bad hacked ones.

Another important issue with Wordpress is that you do not have any files or folders that have to high when it comes to file permission settings. The highest file or folder permission setting is 777 and is way to open for hackers. At the very least, the permission settings should be at 755 minimum. Of course, the lower the setting, the more security your files are. I have some myself that are set to 400, which is pretty much the lowest settings. Problem is, some files need to be set at a certain level for everything to work correctly.

If parts of your Wordpress site have to be set to 777 to run correctly, you might want to think about finding a new host, I've had to do it myself before.

With most every hacked site, it almost always just a matter of finding files that should not be there and delete them (make sure you know what your deleting), or finding bad files and re-uploading and over-writing those bad files.

In conclusion...

As I said, this is not a complete internet security guide. I just wanted to get something out that might be of help.

You also have to realize that sadly these day's it not a "if" you get hacked, it's "when". Seems it's a part of doing business on the internet.

The best course of action is to keep an eye on your files, to catch things while they are happening. I usually check my files several times a day. It's easy with FileZilla.

I hope this helps. I encourage feedback, so you please let me know if I've missed anything, or if there is anything I can do to make this guide better.

I wish you the great success!

Ron Killian

<http://www.theplrstore.com>

<http://www.rakwebsites.com>

<http://www.upgradedtraffictactics.com>

<http://www.quickimvideos.com>