

Filtering tips on Linux with Pluckeye

Posted by greenland55 - 26 Mar 2020 20:55

For a while I have been using Pluckeye, which is a filter mostly notable for protecting Linux machines. It looks like it's been discussed here a couple times. Here are some things I have learned from my experience. Implementing this stuff has caused me to not have a fall from my Linux machine in several months (I have, sadly done so, but its been from other devices).

Their website, pluckeye.net has good resources. For installation information, www.pluckeye.net/how-to-install.html has good information. Also this forum has good stuff by looking up "pluckeye" in the forum.

A few points and pointers that weren't emphasized on that website or this forum:

1. You shouldn't usually have root access to your machine. You'll need root access to set it up but not afterwards. What I did was go onto one of the many random password generator websites, generated 64 characters of gobblygook, printed that out and put it in a box outside of home. If I need to install software I can retrieve it, but usually I use a non-admin account. If you are one of those people with a photographic memory you might need to do something else.

Second: You really need to use a Ubuntu-like distro if you are on Linux. Debian, Pop OS etc all work but Ubuntu is by far the best. Fedora, Arch, etc will not work. I feel Jon, the developer, is a bit too equivocal on this point. Maybe you like something else, but it's not worth it.

If you use anything that is not Ubuntu, even Debian, you may need to delete your recovery partition. To do this: format the recovery partition (you will need to be root to do this)

Then, before shutting down, edit `/etc/fstab` and remove the line that has the phrase "RECOVERY" or something like that. (If you shut down first, you can still do it but will need to go into recovery terminal mode).

By default it blocks all images but does not block access to any websites. This solves by default the majority of the problem. I have found it is best to use a whitelist still, because of time wasting and inappropriate reading material.

(the following setup commands do not need root, so you can send that paper to your Chaver in North Korea now or wherever you will keep it)

To set up a whitelist.

type in to terminal, once it's installed:

pluck add "Deny"

After that, think of all the websites you know that are good.

pluck add "Allow simpletoremember.com"

pluck add "Allow work.biz"

etc. These sites will be totally allowed.

Once you've done all of this, Set it to really work :

pluck level 2

pluck set "delay 1 Day"

Now it's blocking all of your apps and any setting that you

If you need to make things more lenient by allowing a site etc you don't need root, just type in the change, wait for the delay and you'll be set.

If you find some loophole, try typing "pluck nhb" to increase protection even more although it might cause some problems. Otherwise email him.

Finally, ssh can cause some issues with this. If you have an account me@hackercentral-server.su just type:

pluck add "Block hackercentral-server.su"

Also, the X-tian branding on some of it does not affect use of the software and you really should pay the suggested amount even if he doesn't make you.

This software works on Windows and Mac too, but haven't tried it on any of those. There's lots of stuff on their website at "www.pluckeye.net/faq.html" and examples of syntax at "www.pluckeye.net/eg.plu" Anyway, let me know if you have any questions and Hatzlichia to all programmers/nerds/free software enthusiasts!

=====
=====