

By Jack Wallen

Out of the box, a Linux desktop is far more secure than most others. But this level of security doesn't necessarily involve typical security-focused software or techniques. Sometimes, the easiest means to security are those measures that are the easiest to forget. Let's take a look at 10 things you can do to secure a Linux desktop.

Note that we're talking about the desktop, not a server. Linux server security is another beast all together -- one that would confuse the average desktop user.

1 Locking the screen and logging out is important

Most people forget that the Linux desktop is a multi-user environment. Because of this, you can log out of your desktop and others can log in. Not only does that mean that others could be using your desktop, it also means you can (and should) log out when you're finished working. Of course, logging out is not your only option. If you are the only user on your system, you can lock your screen instead. Locking your screen simply means that a password will be required to get back into the desktop. The difference here is that you can leave applications running and lock the desktop. When you unlock the desktop, those same programs will still be running. Safe and secure.

2 Hiding files and folders is a quick fix

In Linux-land, files and folders are hidden by adding a "." before the name. So the file *test* will appear in a file browser, whereas *.test* will not. Most people don't know that running the command `ls -a` will show hidden files and folders. So if you have folders or files you don't want your co-workers to see, simply add the dot to the beginning of the file or folder name. You can do this from the command line like so: `mv test .test`.

3 A good password is a must

Your password on a Linux PC is your golden key. If you give that password out, or if you use a weak password, your golden key could become everyone's golden key. And if you're using a distribution like Ubuntu, that password will give users much more access than, say, on Fedora. To that end, make sure your password is strong. There are many password generators you can use (such as [Automated Password Generator](http://freshmeat.net/projects/apgd/) (<http://freshmeat.net/projects/apgd/>)).

4 Installing file-sharing applications is a slippery slope

I know many Linux users are prone to file sharing. If you want to run that risk at home, that's your call. But when at work, you not only open yourself (or your company) up to lawsuits, you open your desktop machine up to other users who might have access to sensitive data on your work PC. So as a rule, do not install file-sharing tools.

5 Updating your machine regularly is a smart thing

Linux isn't Windows. With Windows, you get security updates when Microsoft releases them (which could be many months away). With Linux, a security update can come minutes or hours after the security flaw is detected. With both KDE and GNOME, there are update applets for the Panel. I always recommend having them up and running so you know when updates are made available. Don't put off security updates. There is a reason they come out.

6 Installing virus protection is actually useful in Linux

Believe it or not, virus protection in Linux has its place. Of course, the chances of a virus causing problems on YOUR Linux machine are slim to none. But those e-mails you forward to others' Windows machines could cause problems. With a good virus protection, like [ClamAV](http://www.clamav.net/) (<http://www.clamav.net/>), you can ensure that e-mail going out of your machine doesn't contain anything nasty that could come back to haunt you (or your company).

7 SELinux is there for a reason

SELinux (Security-Enhanced Linux) was created by NSA. 'Nuf said? What SELinux does is help lock down access control to applications. And it does it very well. Sure, SELinux can sometimes be a pain. In some cases, it might take a hit out of your system performance. Or you might find some applications a struggle to install. But the security comfort you gain using SELinux (or Apparmor) far outweighs the negatives. During the Fedora installation, you get the chance to enable SELinux.

8 Creating /home in a separate partition is safer

The default Linux installation places your /home directory right in the root of your system. Sure, this is fine, but 1) it's standard, so anyone gaining access to your machine knows right where your data is and 2) if your machine goes down for good, your data might be gone. To solve this problem, you can place /home on a different hard drive or partition all together (making it a partition in and of itself). This is not a task for the weak of heart, but it is one worth employing if you're uber-concerned about your data.

9 Using a nonstandard desktop is worth its weight in gold

Not only do the alternative desktops (Enlightenment, Blackbox, Fluxbox, etc.) give you a whole new look and feel for your PC, they offer simple security from prying eyes you may never have thought of. I have deployed Fluxbox on kiosk machines when I wanted a machine that could do one thing: Browse the network. How do you do that? Simple. Create a single mouse menu (or desktop icon) for the application you want to use. Unless the user knows how to get back to the command line (by logging out or hitting Ctrl-Alt-F*, where * is a desktop other than the one you are using), they will not be able to start up any application other than the one offered. Since most users have no idea how to move around in these desktops anyway, they aren't going to have the slightest idea how to get to your files. Simple pseudo-security.

10 Stopping services is best

This is a desktop machine. It's not a server. So why are you running services like httpd, ftpd, and sshd? You shouldn't need them and they only pose a security risk (unless you know how to lock them down.) So don't run them. Check your `/etc/inetd.conf` file and make sure that all unnecessary services are commented out.

Simple but effective

You might find these suggestions to be pure common sense -- but maybe you'll see a means of security you never thought of before. And if you're a new Linux user, these tips are a great place to start to ensure that your Linux experience is a good one.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for the [Downloads at TechRepublic](#) newsletter
- Sign up for our [IT Leadership Newsletter](#)
- Check out all of TechRepublic's [free newsletters](#)
- [10 common mistakes to avoid when you're installing Linux software](#)
- [10 things to consider when choosing a Linux distribution](#)
- [Cut down on Linux command-line typing with these 10 handy bash aliases](#)

Version history

Version: 1.0

Published: May 28, 2008

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Content Team