HOW TO PROTECT YOUR PRIVACY ON LINUX

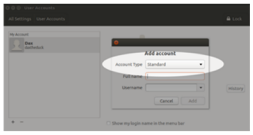
1 Don't be complacent because you're running Linux!

It's easy to have a false sense of security, thinking that other operating system might be more targeted than Linux, but there are plenty of risks and vulnerabilities for all types of Linux devices. Keep your guard up regardless of your OS.

2 Ensure you use a password to protect your user account.

This should be required, but even so, make sure you always use a strong, lengthy password.

3 Don't use an admin account for daily activity.



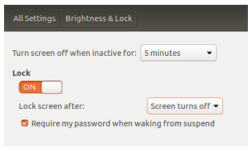
For everyday computing, log in with a basic or standard user account. This is likely to be the default behavior when creating a new account, but it's worth double-checking your account's status. Note that some system-wide actions will require you to log in with the administrator account because of restricted permissions.

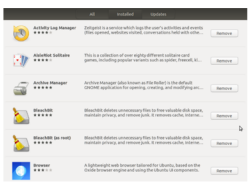
4 Encrypt your data.

Full disk encryption is ideal, but it's also possible to encrypt just your home directory, for example on a shared machine. This is usually done during installation, and is difficult to do afterwards. In that situation, the easiest solution is to backup your data (always a good thing!) and then re-install the OS selecting encryption options. If you really want to try encrypting an existing system, the process varies depending on your distribution and disk partition setup so it's best to search for instructions relevant for your environment.

5 Activate your screensaver when idle with screen lock.

Reduce the time for the lock to take effect once the screensaver starts.

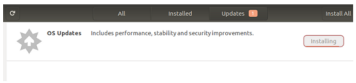




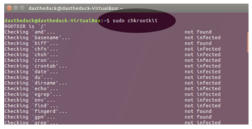
6 Review your installed applications.

It's good practice to keep installed applications to a minimum. Not only does this keep your machine lean, it also reduces your exposure to vulnerabilities. As well as looking through your application list manually, there may be tools available for your distribution to make it easy, such as BleachBit.

7 Keep your system updated.



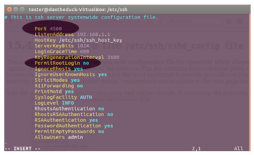
It's usually easy to keep both Linux and installed applications up to date. At the very least make sure updates for security are installed automatically.



8 Periodically check for rootkits.

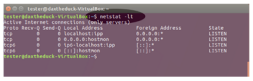
This can be done by installing a rootkit detector such as chkrootkit, which is easily run with the command sudo chkrootkit.

9 Lock down remote connection settings.



If you use SSH for remote access, there are some simple steps to reduce the risk of attack. The easiest is to use a port other than the default port 22. You can also prevent remotely logging in as root with PermitRootLogin no in the SSH config file. This article has more tweaks for securing SSH.

10 Turn off listening services you don't need.



Some daemons listen on external ports. Turn these services off if not needed, for example sendmail or bind. This could also improve boot times. To check for listening services, use this command: netstat -lt

11 Make sure you have a firewall running.

Your OS may have a built-in firewall already, probably iptables. Firewalls can be confusing to configure with the command line, but there's likely to be a GUI frontend available for easier control such as Gufw.

12 Restrict privileged access with SELinux or AppArmor.

These may be installed in your system by default but if not, it's worth adding and configuring them. They both enable users to define rules that limit how applications can run or affect other processes and files. The benefit is that in the event of an attack, the damage to your system is limited. You can read more here about how to use SELinux and AppArmor.

Congratulations! You've just taken a big step to increasing privacy and protecting the data on your Linux system.

https://spreadprivacy.com/linux-privacy-tips