10 Additional Computing Tips and Tricks for Students

François Briatte

June 8, 2018

This document is part of the "Computing Advice for Students" series. It is a companion to "10 Computing Tips and Tricks for Students."

All software recommendations are for Mac, because this is what I know best and use most of the time. You can easily find alternatives and clones for Windows and/or Linux on alternativeto.net.

All software has been tested on OS X 10.9 only, and might not work properly on other systems. If you are running any of the newer versions of macOS, there might be better software available than that recommended below.

Part 1: Become mildly perfectionist

The advice in this section is productivity-oriented. In computing, "productivity" means doing things quicker, and possibly better. Very often, it involves keeping your hands on the keyboard, rather than having to click on a million different buttons.

1. Use a keyboard expander

We all spend a ridiculous amount of time typing the same words – our names, the polite parts of our emails, … – over and over again. Treat yourself:

> Install aText and enter your common phrases with shortcuts.

The shortcuts will work everywhere: in your browser, in your text editor, in your Finder, etc.

2. Optimise your window management

All modern operating systems let you hide or maximise windows easily, but to position the windows intelligently or to improve how you interact with them, you will need extra utilities.

> Install TotalFinder (shareware) or XtraFinder (freeware) to manage your Finder window tabs, and Spectacle to manage the location of your windows on screen.

Note – On a Mac, the keyboard shortcut to cycle through the windows of an application is Cmd-`. Surprisingly few people seem to know that shortcut.

3. Scrutinize your applications

Applications (executable programs) can take up unnecessary disk space, or hide malware and other harmful components, so make sure that you know what is installed on your computer, and what it does or might do.

> Use AppCleaner to list your applications and remove them if necessary.
> Use KnockKnock and other Objective-See tools to detect malware.

4. Supervise your computer maintenance

Your operating system silently performs many different maintenance operations, such as getting rid of temporary files, on a regular basis. Sometimes, you might be interested in controlling that process, for instance to clear up some disk space or to troubleshoot a software issue.

> Use OnyX to control a myriad of system maintenance operations and settings.

The same program will provide you access to semi-hidden features of your operating system.

Note – Many people seem to use CCleaner (also available for Windows) to perform some of the same tasks. CCleaner has been compromised in the past: it might, or might not, be safe to use, and I do not know what it does exactly.

5. Automate what can be automated

If you are managing a large quantity of files, it can be a good idea to use the `rsync` utility to backup your data. More generally, using command line tools like `rsync` and writing short scripts to program them can automate many tasks while making them much easier and quicker to perform.

> Three excellent command line utilities for general use:
> 1. `rsync` for (remote) file copying, as in backups
> 2. `wget` to download stuff (e.g. entire websites) with minimal effort
> 3. `cron` to schedule scripts to self-execute periodically

There are (literally) thousands of command line utilities, and tons of online documentation on how to use them to produce the most complex or idiosyncratic results. Many of those utilities are extremely useful to manipulate text or to process audio and video files.

Part 2: Become mildly paranoid

The advice in this section is security-oriented. In computing, "security" means minimising the risk of waking up one morning and finding out that your identity and bank account were used to buy drugs, forged passports or weapons.

Before taking any of the steps below, make sure that you always run up-to-date software provided by trustworthy developers, and that your data are regularly backed up. To reduce the attack surface on your computer, disable all "sharing" options in your system preferences, such as screen or file sharing.

6. Encrypt your hard drive

A skilled attacker (such as specialised governmental services) will almost always find a way to access your computer if it is connected to the Internet. Encrypting your data makes it impossible for that attacker to read from your hard drive without also stealing your user password, thereby creating a minimum layer of security on top of your data.

Use FileVault or anything like it.

If you want to go 200% paranoid because you are storing highly sensitive material, use encryption with plausible deniability, e.g. Espionage. Also note that neither FileVault or Espionage are open source software, which means that you need to make sure that you trust their developers before you start using any of them.

Note – If you are saving online backups of your data, then you need to also encrypt the backups, using a tool like Arq, which interfaces nicely with Google Drive and other cloud file storage solutions.

7. Install a thief tracker

Stealing laptops is a common form of attack that can result in data and identity theft on top of the cost and time of replacing your system. Installing tracking software might (just might) help you and the police to recover the laptop, if not the data.

Buy and install Undercover.

Note – If you need to protect devices (including phones) running other systems, then perhaps Prey might serve your needs, although I do not know if it can be trusted. The same goes for Hidden, which works only on Apple devices.

8. Monitor your network

As soon as your computer (or any other device) connects to a network like the Internet, every communication from and to that network becomes a potential liability. You should always be aware of what goes in and out of your computer onto the Internet, through which channel(s), and why.

Buy and use LittleSnitch. A free alternative by Objective-See, Lulu, is coming soon.

To get an idea at what your network traffic looks like and how busy it is, run Private Eye, which is free. What LittleSnitch provides on top of monitoring are blocking rules to reject unwanted connexions.

9. Use a VPN

A VPN caries all your Internet traffic through an encrypted "tunnel" that makes it difficult to identify where you are and what you are doing online for anyone but yourself *and* the VPN provider. It is commonly used as a protection against Internet Service Providers and governments (yet see note).

Buy a VPN subscription from a trusted provider, such as cryptostorm.

It is impossible to fully trust a VPN provider. I *tend* to trust cryptostorm, which is based in Iceland, ProtonVPN, based in Switzerland, IVPN, based in Gibraltar, and FDN, based in France.

Note – There are very good arguments *against* using VPNs, mostly to do with how much you can trust providers with your Internet traffic. Understand the risks, or build your own VPN.

10. Use encrypted email

It is highly likely that your current email provider (e.g. Google) does not let you send, receive or safely store encrypted communications. For that, you need a separate account:

Open an encrypted email account, like ProtonMail.

ProtonMail is free and based in Switzerland. Before using it, make sure that you understand what it encrypts, and how. More feature-rich encrypted email services exist, but they tend to be relatively expensive, or are located in countries that participate in global surveillance programs.

Final note – Using secure communications does not make you more anonymous online (quite the contrary), and none of the tips and tricks above will protect you against a skilled attacker or against other security vulnerabilities, such as phishing attacks. Running antivirus and other computer security software might help, but understanding existing threats and reducing your attack surface are essential.