10 Ways to Make Computing More Secure

François Briatte
June 9, 2018

This document is part of the "Computing Advice for Students" series.

It complements Part 2 of "10 Additional Computing Tips and Tricks for Students", and also slightly overlaps with "10 Ways to Make Web Browsing Faster and Safer".

Its aim is to make you less vulnerable attacks that will extort money from you (ransomware), or make money from your devices (botnets), or extract valuable information from them for e.g. identity theft. Even if you are not a particularly valuable target, you are at risk if you are an easy one.

Caveats:

- This document assumes that you have encrypted your hard drive, as recommended in Tip #6 of "10 Additional Computing Tips and Tricks for Students".

  The other tips in Part 2 of that document are: "Install a thief tracker", "Monitor your network", "Use a VPN", and "Use encrypted email."

- 'Secure' does not mean 'private' or 'anonymous' – secure devices can also be identified and localised, sometimes even more easily than less secure ones.

  Similarly, 'more secure' does not mean '100% secure' or even 'most secure' – there are other options out there, but they tend to be less practical for low-tech users.

Sources:

- This document draws on the *Security Guide* published mid-2017 by Tech Solidarity, which has been extensively discussed online. It is targeted at similar low-tech audiences.
- Another resource is the *Surveillance Self-Defense* guide by the Electronic Frontier Foundation, which comes with a handy glossary. Some of its advice, however, is debatable (e.g. using Tor).

Part 1: Reduce the attack surface

The attack surface is anything that can be exploited in your computer setup to access your data. Your aim is to keep it as small as possible by anticipating possible attacks.

1. Keep *all* software up to date

Your operating system (OS) and your Web browser are first in line here, but all your software (i) should only come from trustworthy developers, (ii) should not return malware warnings when provided to VirusTotal, and (iii) should always be up to date.

Some important notes regarding software:

- *Operating systems* – OS popularity and vulnerability are highly correlated: in terms of security, { Android, Microsoft Windows } < { iOS, Apple macOS } < { Linux }.

  Remember to disable all 'sharing' options in your system preferences, such as screen or file sharing, and make sure that you know what software runs when you start up your computer.

- *Web browsers* – Use Google Chrome, which is the one that is most likely to be secure at this time. See "10 Ways to Make Web Browsing Faster and Safer" for additional related recommendations.

- *Antivirus software* – You probably should not use any, in order to lose the false sense of security associated with that kind of (actually risky, since it runs at administrator-level) software.

2. Do not trust email and attachments

Email is not a secure communication protocol, and is simple enough for almost anyone to be able to design phishing attacks. Since your email account holds immensely valuable information, the potential bounty for attackers is huge.

Use the most secure email provider, which right now is Google Mail, and use Google Drive to open suspicious attachments, which is far safer than opening them locally (on disk).

3. Do not trust cloud services

First, remember what Tip #2 of "10 Ways to Make Web Browsing Faster and Safer" says about HTTPS (encrypted) Web connexions:

> An encrypted *connexion* can still lead to an insecure *website* – do *not* assume that a website is secure just because it can be accessed via HTTPS.

Many cloud-based services like Dropbox or Evernote might be secure (or even very secure) right now, but are likely to be breached or compromised one day.

Check "Have I Been Pwned" for a practical demonstration, and do not store sensitive or personal data (such as your credit card details or your real date of birth) in such services.

4. Do not connect to insecure networks

Tip #5 of "10 Computing Tips and Tricks for Students" says:

> Your passwords do not protect you against network attacks: *never* log on to a sensitive website, such as one that stores your credit card details, from an insecure connexion like airport or hotel Wi-Fi.

This applies to virtually all Wi-Fi networks offered in cafés, hotels, public parks, trains and transport hubs such as airports and train stations. Using a network monitoring tool, as recommended in Tip #8 of "10 Additional Computing Tips and Tricks for Students", will show you how 'invasive' those 'free, open' networks can be, in which case using a VPN (Tip #9 of the same document) might help.

N.B. The Tor network is not necessarily secure itself, and the Tor Browser is *very* risky to use. If you are going to use Tor, learn enough about it to use it from Google Chrome instead.

5. Do not connect to insecure devices

Some insecure devices that you might own:

1. *USB sticks* (and *USB chargers*, unless you are using a USB data blocker).
2. *An Android phone* – iPhones are much more secure (although do not use Siri).
3. *An out-of-date home router* – find out how to update your router firmware.
4. *'Internet of Things' (IoT) devices* like Amazon Echo – just do not use those.
5. Any device gone through borders (see next tip).

And yes, the threat caused by USB sticks is hard to circumvent in practice – although it is easy to set up a shared Google Drive folder.

Note – The USB data blocker recommended above comes from the previously cited *Security Guide* published by Tech Solidarity. An alternative one is sold by SyncStop.

6. Do not travel with your data

Do not travel with any sensitive information: you will be going through transport hubs and borders, where you are at risk – not just from law enforcement – of getting your data broken into.

When travelling, use a travel kit – a computer that you can wipe out easily, after crossing the border and/or when coming home. A cheap Chromebook laptop is a reasonable option here.

7. Get rid of Web trackers

Although privacy is not the main topic of this document, avoiding your Web traffic getting tracked by third parties will limit how much attackers might learn about you, and how many attacks might be directed at you.

See "10 Ways to Make Web Browsing Faster and Safer" for recommendations on how to get rid of (most) Web trackers.

Part 2: Go beyond passwords

Tip #5 of "10 Computing Tips and Tricks for Students" and Tip #4 of "10 Ways to Make Web Browsing Faster and Safer" both recommend that you use the Dashlane password manager to store your (different, complex) passwords in a (local, encrypted) file.

However, passwords do not protect against typing under observation or against more elaborate attacks, so examining higher security options is recommended for sensitive (email, social media) accounts.

8. Use long passphrases

When you are going to use a password, e.g. to encrypt your disk or for your email account, make sure to use a long, random passphrase.

Two useful websites about passwords are:

- How Secure Is My Password, to compute rough password strength against brute-force attacks.
- Strong Password Generator, to generate strong passwords (to be stored in a password manager).

9. Avoid 'easy' two-factor authentication (2FA)

When offered to 'harden' your account security with something on top of your passphrase, a.k.a. two-factor authentication (2FA), avoid the 'easiest' options, *fingerprints* and *SMS* (texts on your phone).

Both fingerprints and SMS are easily retrievable by law enforcement and by other parties, and SMS is highly insecure, which is why encrypted text messaging through Signal or WhatsApp is thriving.

If you are going to use 2FA via mobile phone, a reasonably secure 2FA option is receiving a one-time password via a dedicated secure app, a.k.a. TOTP. Otherwise, see the next tip for a better solution.

10. Use a physical security key (U2F)

A physical USB stick serving as a Universal 2nd Factor (U2F) for your email and social media accounts is currently the best protection against getting those accounts hijacked.

The most well-known U2F security key is the YubiKey sold by Yubico, a company based in Sweden and in the USA. Its cheapest model currently costs $20 (around 22€ in Europe).

Final note – Computer security changes quickly, but as of today and for audiences that are unlikely to use Qubes OS or Tails, the advice above should make sense and help prevent low-skilled attacks.