macOS Security

Basic recommendations

- I always install the latest updates for the macOS System software as soon as they are available, including new versions of the OS.
- I do not use Word, or for that matter any MS product. If you do, make sure Macros are disabled.
- I do not use Flash player. I cannot caution you strongly enough against its use.
- I do not use Adobe Reader. I cannot caution you strongly enough against its use.
- You must be **certain** that any app you do use can be trusted. If you enter a username and password for a bad actor, you are probably *pwned*, and there is no reliable recovery from that save wiping the disk, reinstalling the OS and retrieving your data from offline storage.
- I use and highly recommend LittleSnitch, which monitors network connections. I am careful not to allow connections that I don't know the reason for.
- I am also currently running BlockBlock.
- I do not have Sharing enabled, and do not login in remotely. If you need such capabilities you should learn to `ssh`.

Antivirus

I do not have antivirus software running on my Mac.

I have occasionally scanned with ClamXav and not found anything. I do not know of a virus for OS X, but one can pass on Windows viruses in emails or Word docs. If you would like to check for this, ClamXav should detect it.

The basic problem with antivirus protection is that it cannot cope with new threats fast enough.

Furthermore, Macs have not been targeted by virus writers, for reasons that are debated.

I am always looking for new threats on the web by monitoring sites like

- hacker news
- Brian Krebs

- malwarebytes

The history of threats on Mac is instructive, here is a write-up of one.

In this exploit, the download site for DVD-ripping software **HandBrake** was hacked. For a period of four days, a version that installs ProtonB was what you got with your download.

The first thing the malware did was to ask for your password, so it could upgrade its priveleges. The next thing it did was to steal your Keychain.

As an aside, I frequently remove all website info from Safari, and clear the history as well, but that's more so I can read interesting NYT articles.

Passwords

I classify passwords as low, medium and high security.

- Low are held in the Keychain.
- Medium are held in an encrypted file which I decrypt for each use with a master password. **Disk Utility** can do this for you.

I generate long random passwords, e.g.

- `cohacrtztnlkinlaiemilrbrhrvvwr`

using a utility that I wrote.

Length and randomness are important, while a large character set is not so important. Here is a good discussion of several password issues. Requirements that encourage use of weak passwords (like resets every 3 months) are a bad idea.

The eternal question is how to backup such data securely, since the two requirements conflict. I store my encrypted password file on Dropbox. I also have backups stored on various hard drives.

Someone I trust recommends 1Password (see discussion).

I use random text (basically, a password like the one above) for secret questions, though I did once give my mother's birth year as 1809. Obviously, this needs to be saved securely so it can be copied and pasted.

For extra security, your everyday account used to surf the web should be a non-priveleged user.

I used to write high security passwords (banking) down on a piece of paper. Now I recommend that you set up a separate User for banking. My Dropbox is only available from that account.

Actual Mac security threats.

It may be helpful to review recent actual security threats observed for macOS.