# Threats of Physical Harm

Finally, understand that there is always one way that attackers can obtain your password: They can directly threaten you with physical harm or detention. If you fear this may be a possibility, such as if you are going to be travelling across hostile borders with sensitive information, consider ways in which you can hide the existence of the data or device you are password-protecting, rather than trust that you will never hand over the password. One possibility is to maintain at least one computer/email/keepass account that contains largely unimportant information, whose password you can reveal quickly.

If you have good reason to believe that someone may threaten you for your passwords, it's good to make sure your devices are configured so that it won't be obvious that the account you are revealing is not the ?real? one. Is your real account shown in your computer's login screen, or automatically displayed when you open a browser? If so, you may need to reconfigure things to make your account less obvious.

In such circumstances, you should also treat your password manager as a sensitive file, and hide/protect it as we describe in the [Protecting Files lesson](umbrella://lesson/protecting-files).