On this USB drive: TAILS & the CIJ Infosec handbook

Tails stands for 'The Amnesic Incognito Live System'. It is an open source, Linux-based operating system that protects users' privacy and anonymity.

Amnesic: because no trace of your computer use is left on the system after shut down
Incognito: because it is privacy and security orientated, accessing internet anonymously by default, and thus circumventing any attempts at censorship

Using TAILS for the first time

To start TAILS you will have to make your laptop ignore the usual startup process (knows as 'booting') from it's internal hard disk. On most laptop this is done by pressing a specific button during startup. Usually the startup screen will specify the button to press such as <F1>, <F2>, <F12>, <Delete> or <Enter>. Pressing this menu in the first few seconds will bring up a selection menu where the USB-drive that contains TAILS can be selected as an alternative startup drive.

(TAILS will *not* work with Apple laptops – this in being worked on and will improve over the next year)

When you use Tails for the first time, you will see a screen load up with options 'Live' and 'Live failsafe'. You can hit Enter to choose Live immediately if you like, or it will be chosen automatically after 5 seconds.

When you boot up via a Tails stick for the first time, you will be asked one question: 'More options?'. In most cases you can select 'No' and then 'Login'. If you need to configure Tails to circumvent Tor censorship then select 'Yes' and you will see:

- '*Administrative password*'. It is unlikely you would need to create one unless you want to access the internal hard disk of the computer (which is not recommended, and can lead to unnecessary security risks).
- '*Windows camouflage*'. If you activate '*Microsoft Windows XP camouflage*', Tails looks more like Windows XP. This may be useful in public places if you think the Tails OS may be recognised or attract suspicion.
- '*Spoof all MAC addresses*', which should be automatically selected. This is a good option to hide the serial numbers of your network cards, which helps to hide your location.
- '*Network configuration*', under which you have two options: *connect directly to the Tor network*, or '*This computer's internet connection is censored, filtered or proxied. I need to configure bridge, firewall or proxy settings*'. *The latter option may be required if you are using a network connection that blocks certain types of connections (such as at a large company or some universities). Places like cafés will usually provide an open connection.*

Once you are logged into TAILS you will find a detailed handbook on how to use it and much more on the desktop as a PDF and ebook file. This ebook is also online as a series of webpages on the CIJ website:

http://www.tcij.org/resources/handbooks/infosec TAILS is described in detail in chapter 2

Given the rapid developments in the field of information security this book is under permanent development. Feedback is most welcome. Please mail us:
infosec@tcij.org

PGP KeyID :0x7EF8DE32
Fingerprint: D0C5 A200 A49B E194 7AE4 A7C8 4DD6 A68E 7EF8 DE32