Setting up Tor in the Library: An Overview

By the FIMS Graduate Library, University of Western Ontario

To learn more about Tor, check these out:

- https://www.torproject.org/docs/documentation.html.en
- https://www.eff.org/pages/tor-and-https

The Library Freedom Project also has list of resources relating to Tor:

- https://libraryfreedomproject.org/allabouttor/

Tor Browser

You can find the install files, as well as instructions for the installation, here:

- https://www.torproject.org/projects/torbrowser.html.en
- https://ssd.eff.org/en/module/how-use-tor-windows

Tor has a list of warnings about how to best use Tor to stay anonymous, many of which your patrons should be aware of:

- https://www.torproject.org/download/download-easy#warning

Also note that giving out personal information through Tor, for example, via social media, will de-anonymize the session.

Tor Relays

To set up a Tor relay, aka Tor node, you will need:

1. A dual or quad core PC, preferably running Debian or Ubuntu
2. A high speed internet connection.
3. Intermediate knowledge of Linux

First you'll need to download and install Tor:

- https://www.torproject.org/download/download-unix.html.en

Then you will need to configure Tor to receive Tor traffic. Some resources explaining the configuration process, include:

- https://www.torproject.org/docs/tor-doc-relay.html.en
- https://unindented.org/articles/run-a-tor-relay-on-ubuntu-trusty/

The Tor Project has recommendations to keep your relay secure:

- https://trac.torproject.org/projects/tor/wiki/doc/OperationalSecurity

The Library Freedom Project has compiled resources for libraries deciding to run Tor exit relays (where Tor traffic exits the network to its final destination, unencrypted and accessible to other online actors):

- https://github.com/LibraryFreedom/tor-exit-package/blob/master/resources.md