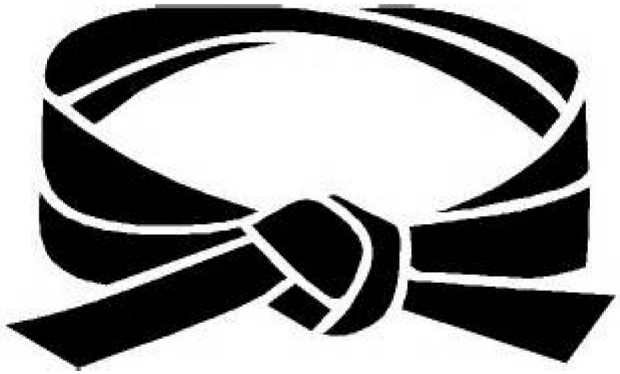
Online Self Defense – Black Belt Level

TAILS and Tor

Tails
theamnesicincognitolivesystem



Tor
TorProject.org

Review - White Belt Level

1. Do your updates
2. Use good antivirus/antimalware software
3. A long password is a strong password
4. Be suspicious of all emails, particularly those asking you to click on links, or that have attachments.

Review – Yellow Belt

1. Always verify that you are on the website you mean to be
2. Set browser to more secure settings
3. Use privacy enhancing browser plugins
4. Scan everything you download
5. Only download programs from the official website

Review - Green Belt Level

- Information is the currency of the internet
- Privacy has finincial as well as ethical implications
- Make sure that your connection is encrypted (HTTPS)
- Anonymizing web proxies can help
- VPNs are better
- Tor Browser is even better

Review – Brown Belt Level

1. Unencrypted email is like sending a postcard instead of a letter
2. To encrypt email use Mozilla Thunderbird with the Enigmail plugin
3. To encrypt chat use Pidgin with the OTR plugin

Threat Modeling

Decide what your most likely threats and plan your defense based on the following questions.

1. What is the most vulnerable/exploitable?
2. What is the most valuable?
3. How can I mitigate my vulnerabilities?
4. What can I do to limit damage if an attack is successful?

Segregation of Identity

- Limit ability of a third party to connect different aspects of your life. For example, casual web browsing and home banking.
- Group activities with similar security requirements.
- Be self disciplined about this segregation. It is hard!
- Segregation limits scope of damage in case of a successful attack against you.

Tor – What is it?

Tor Browser Bundle

- https://www.torproject.org/download/download
- Works on Windows, Linux, Mac, Android
- No installation is needed. Can even be kept on a USB drive

Tor

- What does it do?
- What does it not do?
- What should you not do with it?

The Amnesic Incognito Live System

TAILS is a secure operating system that is designed to do everything possible to ensure you privacy and security. By default it provides the following benefits:

1. It uses state of the art encryption for files, emails, and instant messaging
2. It leaves no trace on the computer it is used on.
3. It gives strong privacy protection by forcing all traffic through the Tor Network
4. It is a mobile operating system that can be carried on a keychain and used anywhere

Getting TAILS

- TAILS can be downloaded from **https://tails.boum.org/install/index.en.html**
- All instructions for installing TAILS are provided by the site
- TAILS can also be copied from any other TAILS drive