

## The Short List of Mac OS X System Security:

The short list for Mac OS X System Security is intended as a quick one page list of things to consider about securing a single Mac OS X install. It is not a full blown technical explanation but a short list, and is intended to talk about securing a single computer and not the complexity of a full network. The concepts behind this paper are to the point but will be explained in a paper entitled "Mac OS X System Security Checklist", to be finished and available later.

-----  
The Short List :  
-----

01. Setup the administrative users account and don't use it for general purposes. Also DO NOT EVER ENABLE ROOT AND DISABLE IT IF ENABLED. This is addressed in the NSA/CSS Guidelines for securing Mac OS X located:

<http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/apple/mac/331-009R-2004.pdf>

02. Choose a Secure System Password - Passwords should be relatively long, relatively random and should contain alphanumeric and non-alphanumerics. Most importantly is should be memorable. If you do need to write it down, put it on a piece of paper that always goes into your wallet for safe keeping. Passwords should be changed from time to time as well. You may find an article on creating strong passwords at this link:

<http://netsecurity.about.com/cs/generalsecurity/a/aa112103b.htm>

03. Firewalls - Mac OS X 10.4 has one that starts from install. One should disable everything that is not being used and consider looking at it periodically to make sure it is proper.

04. Set the "Software Update" system preference to check on at least a weekly basis (default.)

05. Anti-virus software - ClamXav is a good freeware anti-virus software that has received high marks from users and can be found at:

<http://www.markallan.co.uk/clamXav/>

06. Spyware, Keystroke Loggers, Trojan Horses and Administrative Applications - MacScan is considered the best out there. It costs \$24.95 and can be downloaded from:

<http://macscan.securemac.com/>

07. Anti-Spam software - Spam Assassin is a freeware anti-spam software for the Mac OS X that can be found:

<http://spamassassin.apache.org/>

08. A Disaster Recovery Plan and Business Continuity Plan should include a back up system. A definition of this can be found here:

[http://en.wikipedia.org/wiki/Disaster\\_recovery](http://en.wikipedia.org/wiki/Disaster_recovery)

09. Outbound Firewall - Little Snitch costs \$24.95 and can be downloaded from:

<http://www.obdev.at/products/littlesnitch/index.html>

10. Securing Microsoft Windows or Linux running on Mac OS X. Once again you can find a system configuration "Guide to Securing Microsoft Windows XP" from the NSA/CSS located at:

<http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/winxp/C44-026-02.pdf>

Or one might look at the many security guides for securing Microsoft Windows 2000 from the NSA/CSS located at:

<http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/winxp/C44-026-02.pdf>