Document name: Document date: Copyright information: CONFIGURING YOUR OWN FIREWALL (MAC) 2015 Content is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence INTRODUCTION TO CYBER SECURITY http://www.open.edu/openlearn/science-mathstechnology/introduction-cyber-security/content-section-0



OpenLearn Study Unit: OpenLearn url:

CONFIGURING YOUR OWN FIREWALL (MAC)

Arosha K. Bandara



Introduction to Cyber Security

Configuring your own firewall (Mac)

In this, we'll be enabling the firewall for Mac OS X on Mavericks.

Enabling the firewall

1. Open **System Preferences**, which can be found either in the Dock or via the Apple menu at the top left of the screen.



2. Choose Security & Privacy.

00			System P	references			
	show All				(٩	
General	Desktop & Screen Saver	Dock	Mission Control	Language & Region	Security & Privacy	Q Spotlight	Notifications
CDs & DVDs	Displays	Energy Saver	Keyboard	Mouse	Trackpad	Printers & Scanners	Sound
iCloud	(@) Internet Accounts	Network	Bluetooth	Sharing			
ш	1.				2	0	
Users & Groups	Parental Controls	App Store	Dictation & Speech	Date & Time	Startup Disk	Time Machine	Accessibility
*	1	<u>(</u>					
Apple Qmaster	Flash Player	Java					



3. Select the Firewall tab.



4. If necessary, click the lock icon and type in an administrator password in order to make changes.

Name: Password:	System Pro Security & password	ferences is trying to unlock Privacy preferences. Type your to allow this.
Password:	Name:	Ministra and Anna and
	Password:	•••••

5. If the firewall is not already active, turn it on by clicking the **Turn On Firewall** button.



6. The Mac OS X firewall will prompt you the first time all applications attempt to connect to the network, your choices are remembered so you will not be asked in future.



Firewall Options

The firewall has a number of options accessible through the **Firewall Options...** button. In each case options can be turned on and off by clicking the small check box next to each one:

temote Login (SSH)	Allow incoming connections
Remote Management	Allow incoming connections
Screen Sharing	Allow incoming connections
+ -	
+ – Automatically allow signed software signed by a valid cert the network.	ware to receive incoming connections ificate authority to provide services accessed from
+ - Automatically allow signed softw Allows software signed by a valid cert the network. Enable stealth mode	ware to receive incoming connections tificate authority to provide services accessed from

- Block all incoming connections stops remote computers sending data to your computer without having been asked to do so by your machine. You can add programs to an exclusion list, using the + button near the middle of the window.
- 2. Automatically allow signed software to receive incoming connections allows applications with a digital signature to bypass the firewall and receive data. In theory, signed applications come from trustworthy sources and are less likely to host malicious data.
- 3. Enable stealth mode stops your computer from responding to messages asking if it is connected to a network. These 'ping' attacks can be used to identify likely targets for attack.

If you make any changes to your firewall settings, click the **OK** button to confirm them and click the lock (if necessary) to re-lock your settings.