SECURE YOUR COMPUTER

✓ **CREATE A STRONG PASSWORD.** It should be original, complex, use no personal information, and update it every three months. A good password uses a mix of letters, numbers and symbols and uses words that is unrelated to any personal information. This includes birthdays, family, friends, or pet names, even street addresses. For more on good passwords visit **https://securityinabox.org/en/guide/passwords**

✓ **CREATE USER AND ADMIN ACCOUNTS** for daily use to avoid digital attacks aimed at the root level of your computer. You can find this on a mac at **Apple Menu → System Preferences → Users and Accounts**. You can find this on a PC for Windows 10 at **Start → Settings → Accounts → Family & other people → Add someone else to this PC**.

✓ **ENCRYPT YOUR COMPUTER** and your hard drives On Macs this is done through the security panel in system preferences, turning on Filevault. You can find this at System **Preferences → Security & Privacy → FileVault**.

On Windows machines you can check if Device Encryption is enabled by open the Settings app, navigate to **System → About**, and look for a "Device encryption" setting at the bottom of the About panel. If you don't see anything about Device Encryption here, your PC doesn't support Device Encryption. In that case use **VeraCrypt** a free software that allows you to encrypt all your devices. Learn more at **https://veracrypt.codeplex.com/**

✓ **USE A STRONG ANTI-MALWARE SOFTWARE ROUTINELY** meaning once a week. We recommend **MalwareBytes** and check for updates frequently. You can find it here **https://www.malwarebytes.com/**

✓ **DON'T OPEN ATTACHMENTS!** This is the main way people get hacked. Don't believe us, ask the Democratic National Party! If someone sends you a file on any platform and it is a file that can be opened by Google apps then do it. This includes Word, Excel, PDF, and even some image files. This is because Google can handle malware that might be lurking in such files while your own computer cannot. If it is something you don't feel comfortable uploading to Google then download the file and scan it with your own anti-malware software. But make sure your anti-malware software is updated. Finally, you can also upload the file to **virustotal.com** and scan it against many anti-virus libraries as an alternative process.

✓ **UPDATE YOUR OPERATING SYSTEM FREQUENTLY.** On Macs you can find this at **Apple Menu → App Store**. On your PC in Windows 10 automate your updates by going to to Control Panel and check if your automatic updating is turned on. Otherwise follow these steps below:

1. Access the search box in your Windows operating system, type update and then Windows Update.
2. Select Change settings.
3. Click Install updates automatically (recommended), in case it is not already selected.

For more information go to Equalitylabs.org if you have questions or are in need of help contact us at Equalitylabs@riseup.net