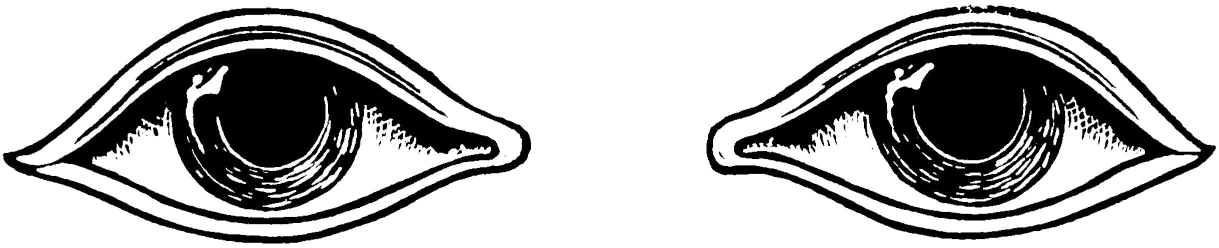


OCTOBER REBELLION LAPTOP LOCKDOWN

@xradmin, XR Global Tech / XR International Support, https://rebellion.global

You’ve just followed the Phone Lockdown guide. Great! Now lockdown your laptop.

Using a laptop for your XR work

It is quite natural, in some cases necessary, that some rebels will want to use a laptop for their work with Extinction Rebellion. Just like phones however, few laptops *only* have data belonging to their owner on them: most have many contacts, photos and videos of other people - the people in our lives. While you may feel little concern for losing the data on your laptop, others may not feel the same way, and may be harmed unless your laptop is sufficiently secured from data theft. This is especially pertitent to those engaging in civil disobedience, even more so those working in a coordination capacity, as they represent a Single Point of Failure (SPOF) within the branch, typically with contact lists and other information that can be used by an adversary to do deep harm. Logins to important accounts on the laptop can also be hijacked/compromised.

While laptops are rarely taken to actions, it is perfectly plausible that any rebel planning or participating in an action may find themselves under investigation before or after the event, whether that be an arrest at home, border seizure, or a warrant that mandates device seizure during the arrest period.

Activity: meditate on your laptop

Find a quiet place and put your laptop in front of you on the table, with the lid closed. Take your hands away from it. Imagine seeing that laptop taken from your hands at an action by a police officer, who then puts it in a bag. Imagine you will never see that device again, with experts at the police station sitting at that laptop and going through it, checking pictures and videos, and looking at contact lists, reading texts, opening up the browser to log into your social media and XR platform accounts. Beyond our work in XR, police and federal investigators have also been known to use personal information they have harvested from a compromised device or account to coerce and/or threaten arrestees.

In particular, meditate not just on *what* is on that laptop, but *who* is on it, and what other *accounts* (and information) that laptop can be used gain access. Think also about how all of this might implicate other rebels not just now, but in the future, even when they may no longer be part of our movement.

In summary, we don’t lock down our laptops solely for ourselves, but out of caring for each other, and our branch. Respecting privacy and anonymity is also essential to our regenerative culture in a time where such basic rights are so widely exploited by corporations and governments, used to control, disempower, and condemn.

GET EMPATHIC ABOUT DATA

- Photos, videos and audio recordings of rebels, especially A&L meetings
- XR account login details (Mattermost, Base, email, Pads, etc)
- Contact lists

Consider a 2nd laptop solely for your XR work

While it can seem unweildly to work across two laptops, it is considered best practice within frontline activism to completely partition your personal life from your activist work, starting with the devices you use. While travelling for XR, take your XR laptop, and imagine in all cases that your XR ‘world’ is separate from your personal life, such that one does not compromise the other. A second hand laptop can be sourced or bought very cheaply, at no cost to the environment, and considered effectively disposable, in use solely for your contribution to Extinction Rebellion.

If you choose to go this direction, something advised, consider your platform requirements for XR. Perhaps your ‘XR laptop’ does not need to be more than a browser and document editor, and so for this reason a cheap Thinkpad laptop with Ubuntu Linux installed is sufficient for your needs. A second-hand x230 Thinkpad can be bought for less than EUR150 on eBay, for instance.

IMPORTANT: Having a second laptop is not an option for everyone, especially those with little financial support or means. In either case, any laptop used for XR work should be *disk encrypted* to ensure it is safe to give to police and investigators.

Encrypting the disk of your laptop

IMPORTANT: Before you begin to encrypt your laptop, be sure to have in mind a strong passphrase. It absolutely should not be used anywhere else. It should never ever be generated using an online password generator, and should never be stored in the cloud (LastPass, and iPassword are examples). It is best to create a passphrase that is unique and that you can type out without ever needing another device or account to access it.

Strong Passphrase Guide

There are many methods for building a strong passphrase. Simply put, it needs to have a mix of letters (upper and lower case), numbers and special characters, and should be over 30 characters long. Here is an example (don’t use this!):

Fs%2M&`{xy^2I$!H:ze[MBW)oW8vEB9]X.e

Here is another example (don’t use this!):

PyimArcUkerb?Ogp3fDafCovgunyop*

Such passphrases are very difficult to remember, which can be quite a problem if your XR recommended offline encrypted password wallet (KeePass or KeePassXC), or other means of password storage, are innaccessible (for instance, on devices that have been taken by Police). *It’s for this reason it can be a very good idea to create a memorable passphrase from a nonsense sentence, one you make up, and in your language.*

Such a passphrase cannot be a citation from a book, song lyric or expression. Rather it should be entirely made up by you and closely rehearsed in memory to make sure you’ve got it. **Store it in your encrypted passphrase wallet anyway**, but be sure you can recall it from memory right when you need it, without assistance.

The passphrase should be more than 5 words, and contain upper-and-lowercase letters. Once you have a passphrase, ‘sprinkle’ it with special characters and numbers. Here is an example (don’t use this!):

tHeir phuture refused to spe4k without the.presence.of.laught3r

Windows laptops

When a Windows laptop is bought, or Windows installed on an existing laptop, the contents of the hard disk are not encrypted. This means that even if your password is strong it will be trivial for law enforcement or investigators to make a copy of your laptop contents and study them. They do this by taking the disk out and connecting it to another computer to access it just as one would a USB stick.

It is for this reason that our first task is to encrypt the laptop contents so that they cannot be read without a special encryption passphrase that we set. Only then can the laptop be given to police and investigators in peace.

There are a variety of means to encrypt a Windows laptop. Two primary encryption tools will be covered here.

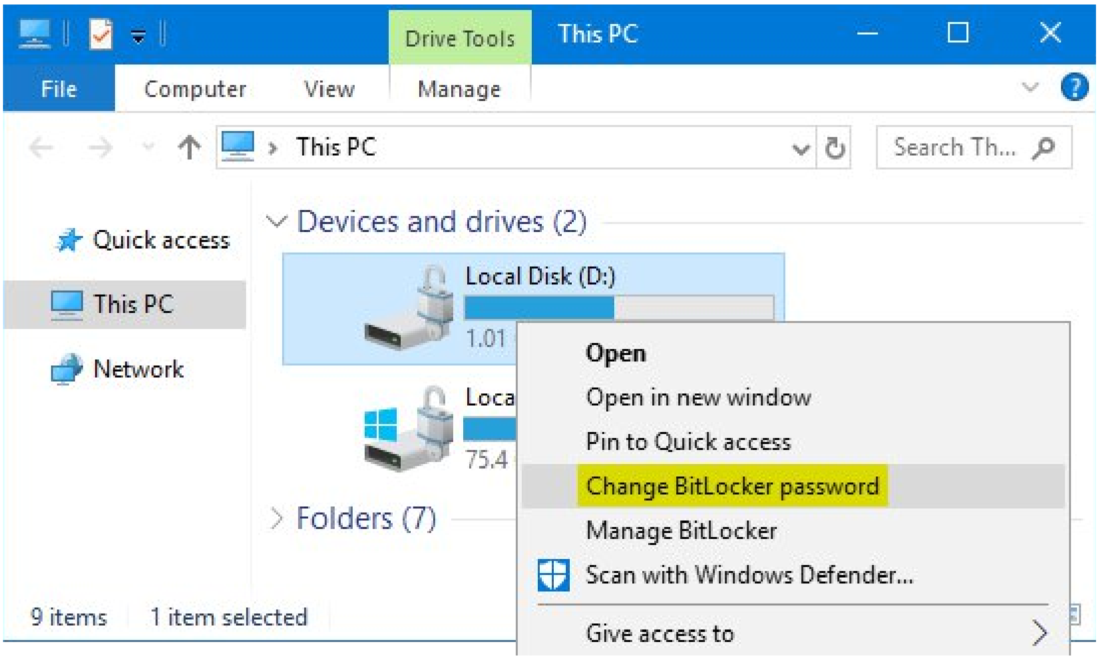
Option 1: Bitlocker

Bitlocker has the advantage that it comes preinstalled with most recent versions of Windows. While *closed source*, it does use very strong encryption, and has been broadly audited to meet FIPS (government and military) security regulations. If you don't have much time, and don't want to install extra software, choose Bitlocker. Otherwise, choose Veracrypt (below). Note also that Bitlocker isn't available on some versions of Windows, including Windows 10 Home Edition.

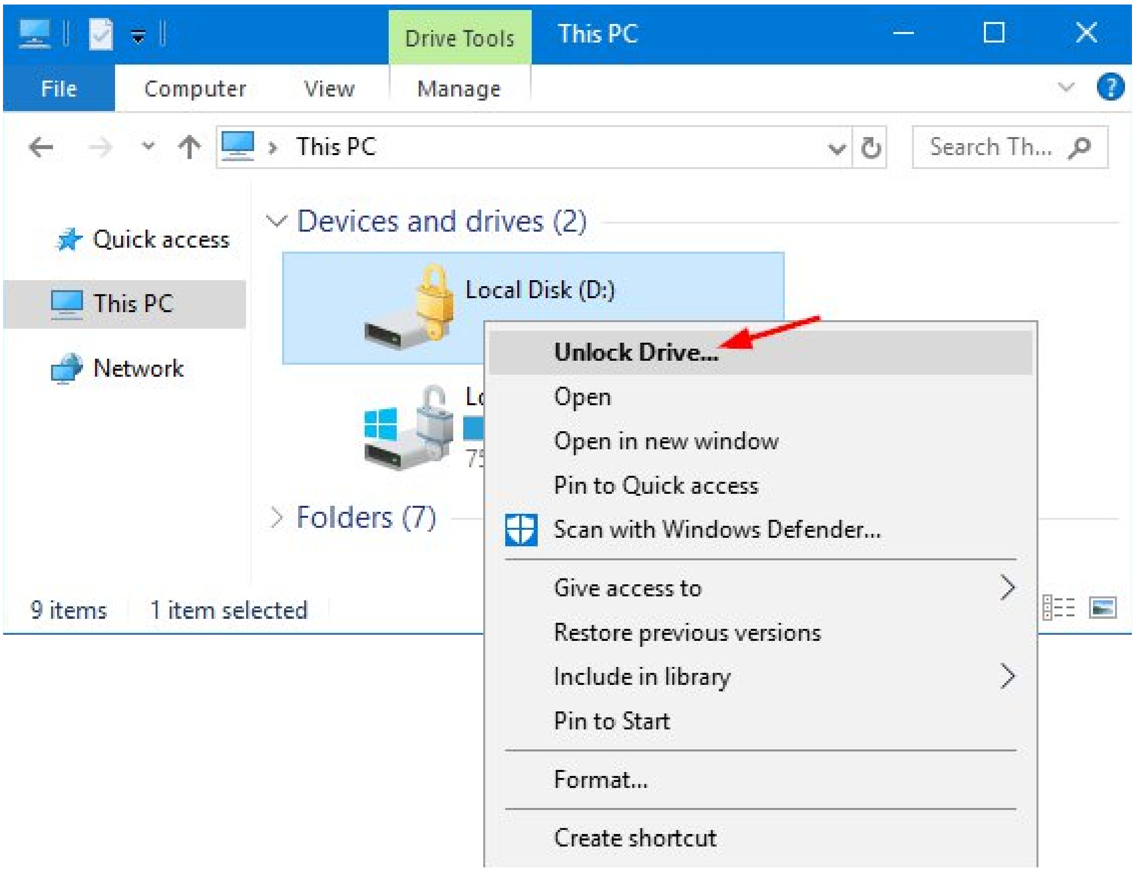
IMPORTANT: If you bought a new Windows 10 computer and signed in using your Microsoft account, your device will be encrypted by Windows and the encryption key will be stored automatically on *OneDrive*. This is not good, as Microsoft can be forced to quietly or openly provide that key to decrypt your laptop. Further, your Microsoft account could have been compromised by an attacker, *even s/he/them that has your laptop*, and so for this reason it is better to opt out of storing the key in OneDrive.

Change Bitlocker Password if it is not strong

Right-click on the BitLocker encrypted drive in Windows Explorer, and select **Change BitLocker password** from the context menu.



Note: if the encrypted drive shows a gold lock on the icon, then you can't see the " **Change Bitlocker password** " option in the context menu, you will need to unlock the BitLocker drive first



Not using Bitlocker already?

- **Turn on device encryption**
- Sign in to Windows with an administrator account (you may have to sign out and back in to switch accounts). For more info, see Create a local or administrator account in Windows 10.
- Select the **Start** button, then select **Settings** > **Update & Security** > **Device encryption** . If **Device encryption** doesn’t appear, it isn’t available. You may be able to use standard BitLocker encryption instead. Open Device encryption setting.
- If device encryption is turned off, select **Turn on** .
- **Turn on standard BitLocker encryption**
- Sign in to your Windows device with an administrator account (you may have to sign out and back in to switch accounts). For more info, see Create a local or administrator account in Windows 10.
- In the search box on the taskbar, type **Manage BitLocker** and then select it from the list of results. Or you can select the **Start** button, and then under **Windows System** , select **Control Panel** . In **Control Panel** , select **System and Security** , and then

under **BitLocker Drive Encryption** , select **Manage BitLocker** . **Note:** You’ll only see this option if BitLocker is available for your device. It isn’t available on Windows 10 Home edition.

- Select **Turn on BitLocker** and then follow the instructions.

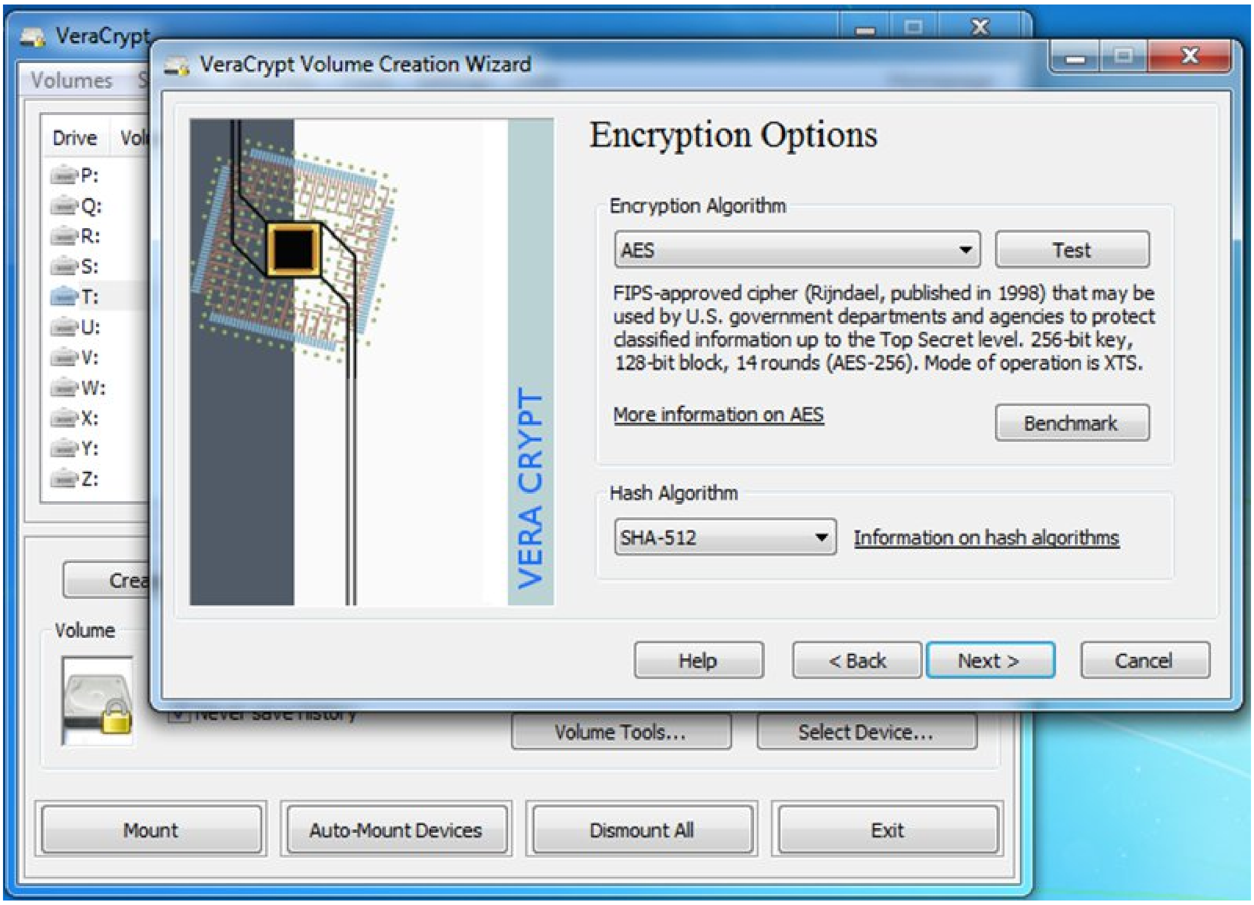
Option 2: Veracrypt

Veracrypt is a popular alternative to Bitlocker, based on the well known predecessor *TrueCrypt*, and offers many of the same strong encryption standards as Bitlocker. Unlike Bitlocker is it *open source,* which means it can be easily inspected by public security auditors. However, at this time, it has not undergone a complete audit. nonetheless, the encryption standards it uses are very good.

Importantly, it has the advantage that it will hide the fact the hard drive is encrypted, giving you *Plausible Deniability* in the event of device seizure: you can just say you don’t know the drive is encrypted.

Unlike Bitlocker you will need to download Veracrypt.

Follow the steps in this image to encrypt your drive. Choose the option shown.



VeraCrypt Volume Creation Wizard

Encryption Options

Encryption Algorithm: AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

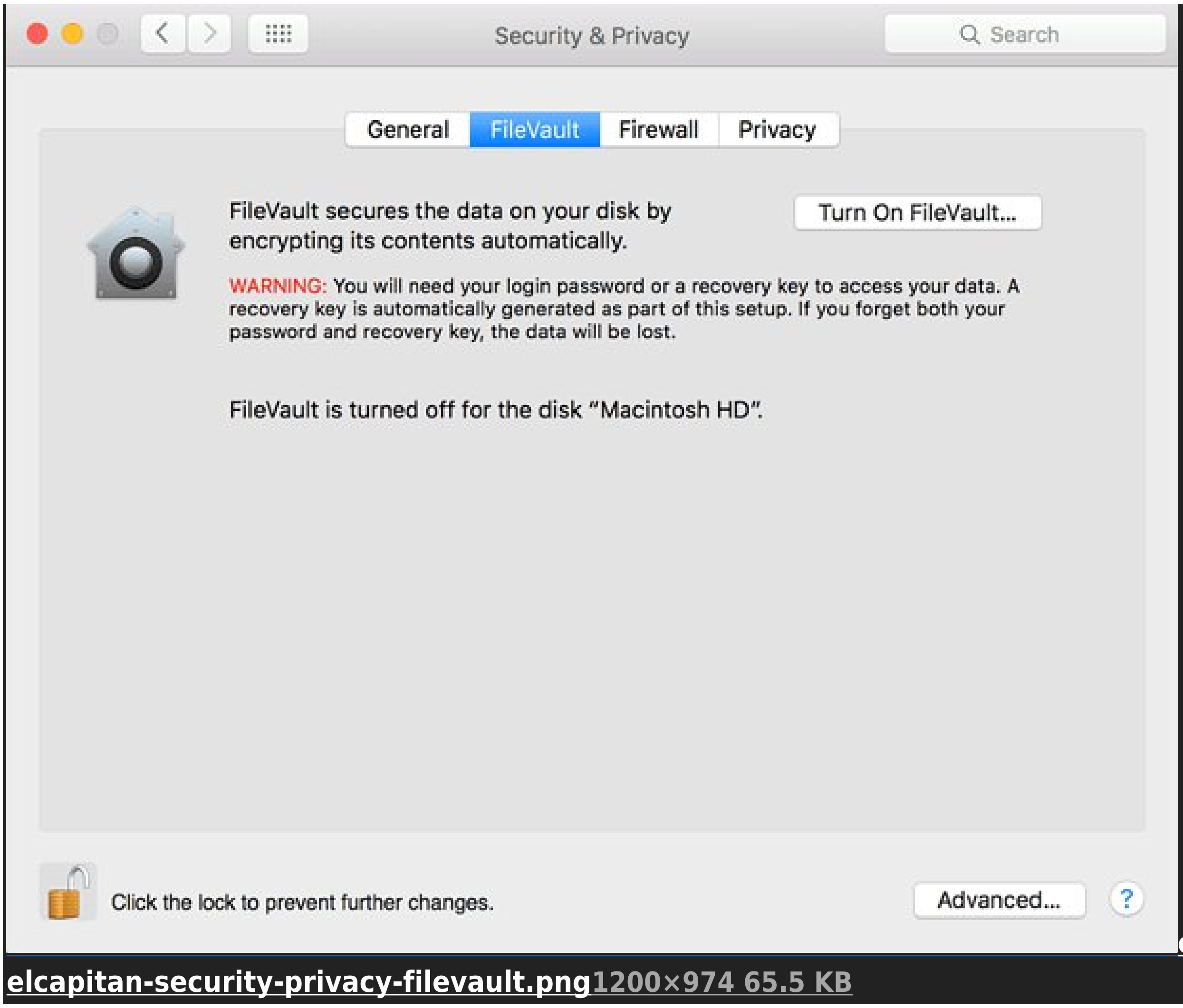
Hash Algorithm: SHA-512

Apple OS X laptops

As BitLocker is to Windows, *FileVault* is the de-facto disk encryption solution for OS X systems. Note however that FileVault does not encrypt your entire system (including the ‘startup disk’), solely the directory containing your user data (the ‘Macintosh HD’, in Apple speak).

FileVault 2 is available in OS X Lion or later. *If you’re using an earlier version of OSX, consider using Veracrypt.* When FileVault is turned on, your Mac always requires that you log in with your account password.

1. Choose Apple menu > System Preferences, then click Security & Privacy.
2. Click the FileVault tab.
3. Click 🔒, then enter an administrator name and password.
4. Click Turn On FileVault.



FileVault secures the data on your disk by encrypting its contents automatically.

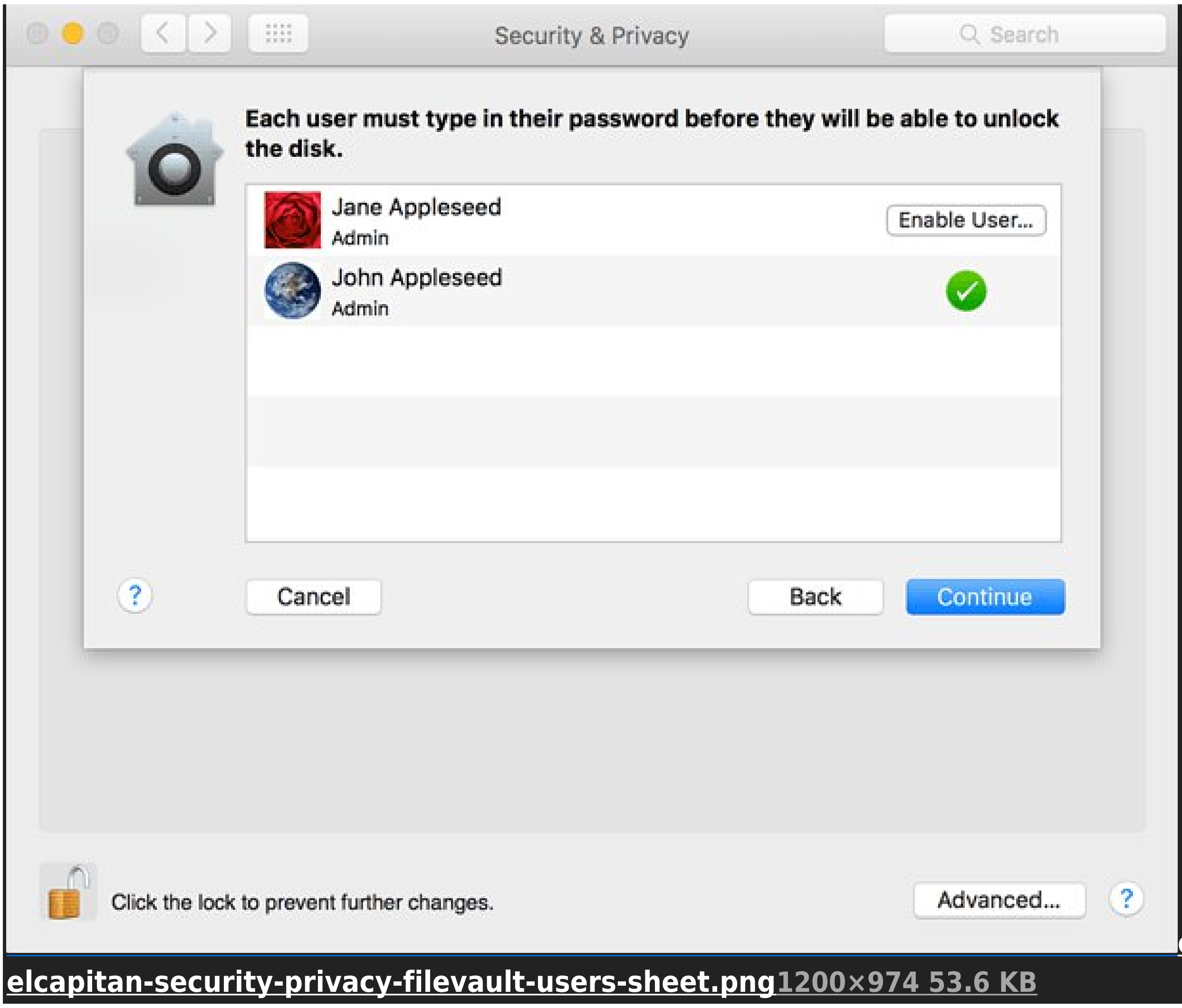
WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk "Macintosh HD".

Click the lock to prevent further changes.

osx-elcapitan-security-privacy-filevault.png1200×974 65.5 KB

If other users have accounts on your Mac, you might see a message that each user must type in their password before they will be able to unlock the disk. For each user, click the Enable User button and enter the user’s password. User accounts that you add after turning on FileVault are automatically enabled.



Each user must type in their password before they will be able to unlock the disk.

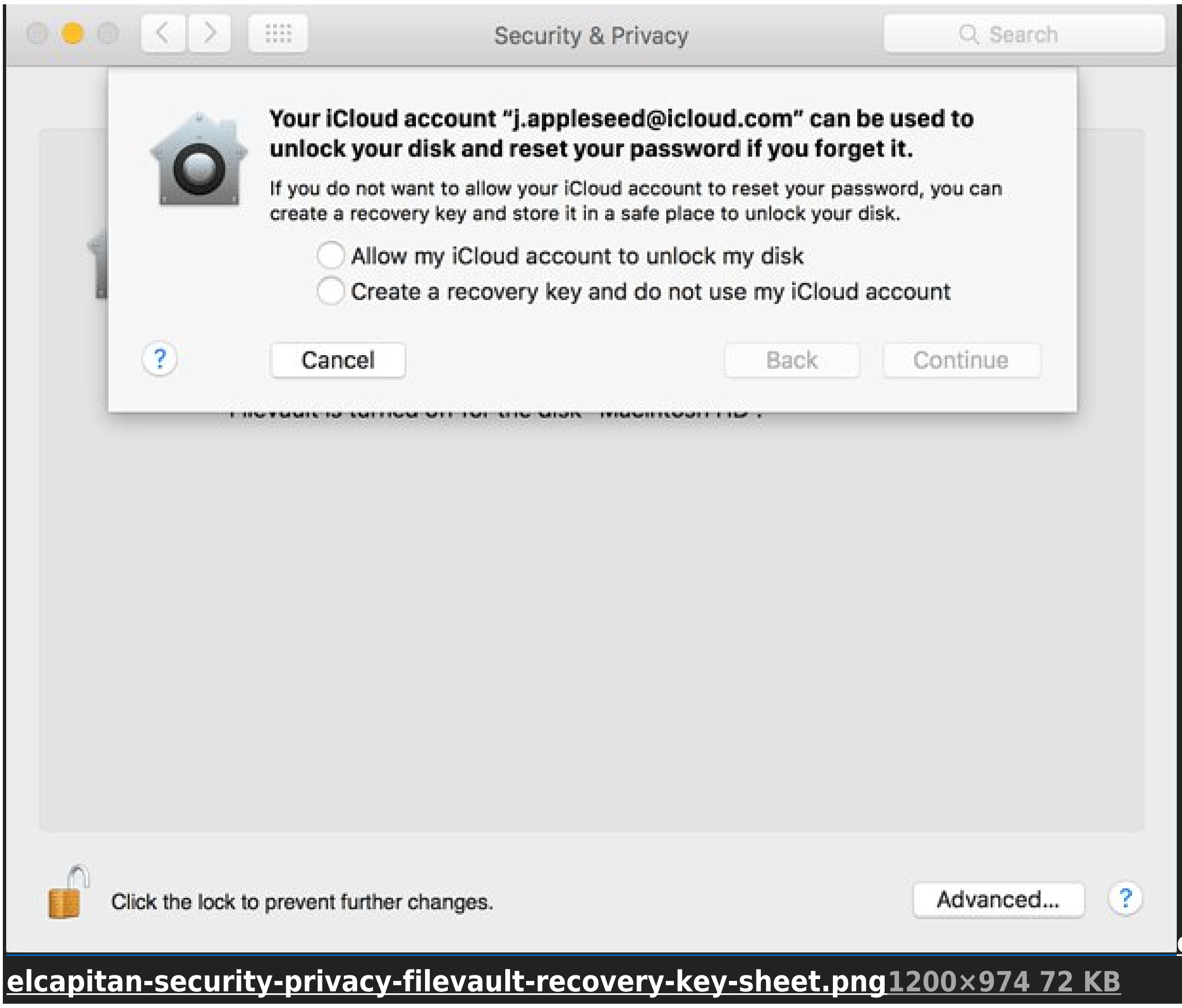
Jane Appleseed
Admin

John Appleseed
Admin ✓

osx-elcapitan-security-privacy-filevault-users-sheet.png 1200×974 53.6 KB

Choose how you want to be able to unlock your disk and reset your password, in case you ever forget your password:

IMPORTANT: If you're using OS X Yosemite or later, you can choose to use your iCloud account to unlock your disk and reset your password. **Don't do this**. If you're using OS X Mavericks, you can choose to store a FileVault recovery key with Apple by providing the questions and answers to three security questions. **Don't do this either**.



Your iCloud account "j.appleseed@icloud.com" can be used to unlock your disk and reset your password if you forget it.

If you do not want to allow your iCloud account to reset your password, you can create a recovery key and store it in a safe place to unlock your disk.

○ Allow my iCloud account to unlock my disk
○ Create a recovery key and do not use my iCloud account

Click the lock to prevent further changes.

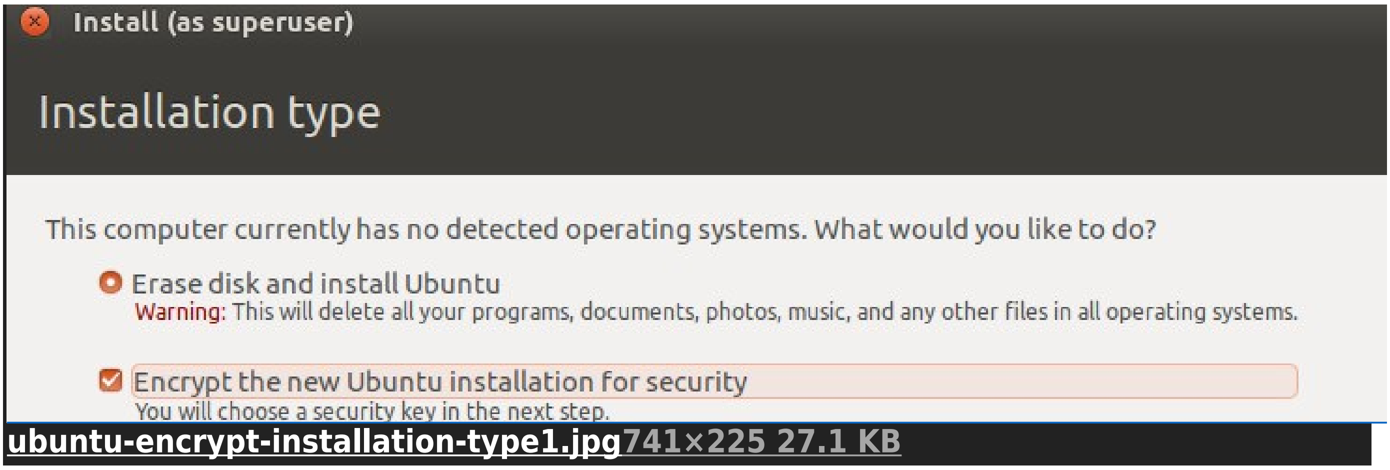
osx-elcapitan-security-privacy-filevault-recovery-key-sheet.png1200×974 72 KB

IMPORTANT: Be sure to create a local recovery key. Keep the letters and numbers of the key somewhere safe—other than on your encrypted startup disk. You may, for instance, store them using MiniKeePass on your iPhone or using KeePassDX on Android or on another device.

GNU/Linux laptops (Debian, Ubuntu, Mint, etc)

While Linux systems are in general far more secure than Windows systems, and much less likely to compromise user privacy with built-in off-laptop storage solutions (like Windows 10 and OS X system), there is no singular way to wholly encrypt a GNU/Linux laptop *after* installation. You can however create another UNIX account on the system, login and encrypt the home directory of that user from another account, then copy in the data you need to keep safe.

The better solution, however inconvenient, is to simply copy off all the important data to, say, a large USB stick or external drive - ideally encrypted - and reinstall the laptop. As you do, choose the option for full disk encryption. Here, for example, is how it's done on Ubuntu:



Install (as superuser)

Installation type

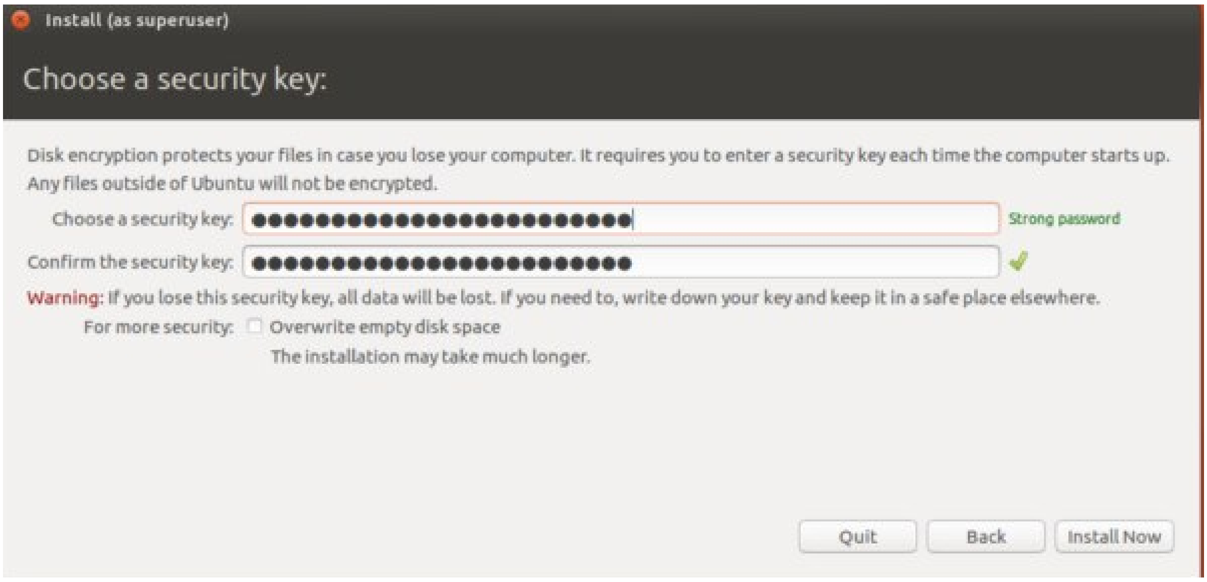
This computer currently has no detected operating systems. What would you like to do?

● Erase disk and install Ubuntu
Warning: This will delete all your programs, documents, photos, music, and any other files in all operating systems.

☑ Encrypt the new Ubuntu installation for security
You will choose a security key in the next step.

ubuntu-encrypt-installation-type1.jpg741×225 27.1 KB

Clicking “Install Now” with the encryption options selected in Ubuntu will bring up a configuration page. This page allows the user to set the encryption key for the installation.



Install (as superuser)

Choose a security key:

Disk encryption protects your files in case you lose your computer. It requires you to enter a security key each time the computer starts up. Any files outside of Ubuntu will not be encrypted.

Choose a security key: ●●●●●●●●●●●●●●●●●●●●●●●●●● Strong password

Confirm the security key: ●●●●●●●●●●●●●●●●●●●●●●●●●● ✓

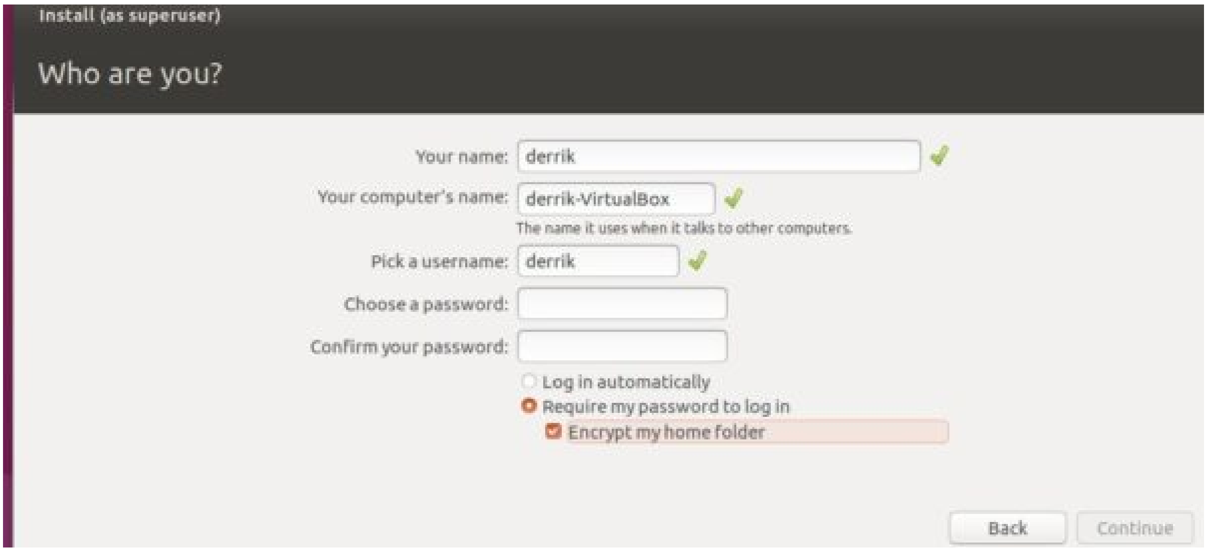
Warning: If you lose this security key, all data will be lost. If you need to, write down your key and keep it in a safe place elsewhere.

For more security: □ Overwrite empty disk space
The installation may take much longer.

Enter the security key. The security key window will grade the effectiveness of the security key, so use this tool as a barometer and try to get a security key that says “strong password.” Once chosen, enter it again to confirm it, and then write this key down on a piece of paper for safekeeping.

Additionally, check the box that says “Overwrite empty disk space.” This is an optional step. Select install now once everything is entered.

Select the time zone, and create a username along with a secure password.



Install (as superuser)

Who are you?

Your name: derrik ✓

Your computer's name: derrik-VirtualBox ✓

The name it uses when it talks to other computers.

Pick a username: derrik ✓

Choose a password:

Confirm your password:

○ Log in automatically

● Require my password to log in

☑ Encrypt my home folder

Along with creating an encrypted hard drive on Ubuntu, select the “require my password to log in” box and the “encrypt my home folder” box during the username creation process. This will add yet another layer of encryption for data on the system.

Rebel checklist

1. DO NOT USE A PASSPHRASE USED ANYWHERE ELSE TO ACCESS YOUR LAPTOP

If you use the same log in with your bank that you use to unlock your laptop, and a federal investigator is granted access on a warrant to all data related to your bank account (very common), your laptop can be unlocked by police. For this reason it is always a good idea to use a different passphrase.

2. DO NOT USE BIOMETRIC LOGIN (LIKE FINGERPRINT)

If you are arrested it is assumed that police will have access to your body, under force, to log into your device if you have chosen to set your device to use biometric login. These login methods should be avoided by activists.

3. NEVER STORE PASSWORDS UNENCRYPTED, OR IN THE CLOUD. ONLY STORE THEM ENCRYPTED AND/OR IN YOUR MEMORY

It is advantageous to have a backup of the password to your laptop, but very disadvantageous if your adversaries have access to it. Do not use services like *LastPass* or *iPassword*, as they store your password remotely, with the former being catastrophically hacked, compromising countless trusting members. Even though iPassword state they do not have the ability to decrypt your password and so read it, you have to trust them. This is putting your wellbeing in the hands of those you've never met, a business in a country under its own jurisdictional obligations to cooperate with law enforcement and federal investigators.

Rather, be sure to use an offline password manager, like KeePass, which stores passwords encrypted and on another device (like a laptop), or on an external USB stick, and under your control.

There is no problem storing a backup of your password on your encrypted phone, but know that very often all devices are taken by police during a home arrest. It is for this reason best to have a password stored in your memory and to have a USB stick with a backup of your KeePass database on it in a hidden location away from your home or work such that you can retrieve later.

4. STUDY THE LAW

All branches should assign a legal team to work *specifically* on rebel rights at the point of arrest. **Rebels can only be safely arrested when they are arrested knowing their rights**. A rebel that doesn't know it is illegal to be physically forced or threatened to hand over the login details to their laptop probably will. Part of caring for each other is ensuring that we are all on the same page, and can stand strong in full confidence we know our rights, and are not being lied to to compromise the safety of our peers.

IMPORTANT: it is very important to determine, within your operating jurisdinction, if it is against the law to withhold a passphrase from law enforcement at the point of arrest. If this is the case, it is essential all rebels are aware of this, and that all devices with any sensitive information are not taken to an action, whether encrypted or not. Withholding information from law enforcement - ‘obstructing legal process’ - is generally an offense much more serious than blocking a road, and in some jurisdictions can result in being imprisoned for many years, or worse.

5. PRESS THE POWER BUTTON ON YOUR LAPTOP AND ENSURE IT IS POWERED OFF BEFORE HANDING IT OVER

If you have reason to believe there is any risk of your laptop coming into the hands of law enforcement or investigators, be sure to hold down the power button and power it off. **Only when an encrypted laptop is off is it truly (practically) invulnerable to data extraction.** Do this when crossing a border, or when your laptop is in your bag and you are out and about in the city. While inconvenient, do it anyway.

IMPORTANT: If Police do return your laptop to you and your laptop is not encrypted, it should be considered compromised and so totally wiped. Malware implants in activist devices are increasingly common, allowing investigators to spy on you, activating your microphone or copying data from your device.