

Forum:[Hack Forums](#)

Thread: [Encrypting Hard Drive is it Worth it?](#)

ST4RL0RD - July 23, 2017, 10:20 am

Doing a lot of investigative journalism, getting around 4,5k genuine views per article I write now and I'm touching on some very touchy/sensitive stuff.

Considering encrypting my hard drive in case the feds every bust me.

What are the pros and cons of doing such a thing?

I've read that it can cause your system to crash and cause loads of problems so a lot of the time isn't worth it, is this true?

sdk - July 23, 2017, 10:22 am

(Jul 23, 2017 10:20 AM)R!CK3O Wrote: [\[CITE\]](#) Doing a lot of investigative journalism, getting around 4,5k genuine views per article I write now and I'm touching on some very touchy/sensitive stuff.

Considering encrypting my hard drive in case the feds every bust me.

What are the pros and cons of doing such a thing?

I've read that it can cause your system to crash and cause loads of problems so a lot of the time isn't worth it, is this true?

If you're actually worried, for whatever reason, move it to an external bay and have a hammer, best encryption ever.

PizzaFox - July 23, 2017, 10:32 am

In my experience with Bitlocker I've had zero problems or noticeable slow-downs. I use 128 bit AES full-disk encryption on both of my drives. I decrypt them with a key on my USB drive I carry everywhere. Just smashing a hard drive won't always work, they can piece together fragments. Best way to destroy an SSD is to microwave it. For an HDD, super strong electro magnet.

Sheeple - July 23, 2017, 10:41 am

Use veracrypt if you plan on encrypting your drives. I have all of my HDDs in my PC currently encrypted with AES(Twofish(Serpent)) as well as my OS Boot SSD. The boot time is a little longer ~ 21 seconds, however; security > speed. You should use an absurdly long passphrase, mine is > 30 chars. Wouldn't recommend Bitlocker.

Also, not really too sure that encryption will protect you from the feds but I guess it's worth a shot. If you have the FBI after you for breaking some serious laws, they may charge you for withholding information or some other bullshit. You should read up on laws regarding cryptography or even talk to a lawyer and try to not get yourself in any obvious trouble.

ST4RL0RD - July 23, 2017, 10:53 am

(Jul 23, 2017 10:41 AM)Sheeple Wrote: [\[CITE\]](#) Wouldn't recommend Bitlocker.

Why, out of curiosity?

coco69 - July 23, 2017, 10:59 am

Get a networked drive and hide it somewhere in between a wall or the ceiling or something, run a line to the ceiling and add a switch, and make it look as if the cable is directly running to a tv or something. run a power line somewhere close and disguise it as a power line for a lamp or something, if anything simply disconnect the power source and your golden.

Sheeple - July 23, 2017, 11:00 am

(Jul 23, 2017 10:53 AM)R!CK3O Wrote: [\[CITE\]](#) Why, out of curiosity?

Closed source and owned by microsoft. Don't trust it at all, matter of opinion. It could be backdoored and the feds could just access your "encrypted" data with no trouble at all while VeraCrypt is open source and consistently updating their security. VeraCrypt is just more secure it pretty much every aspect compared to bitlocker.

archangel.dmitry - July 23, 2017, 11:40 am

You need start with the weakest point - you. If you encrypt the drive and a judge orders you to unlock, you will have to. If you don't, you will be held in contempt of court. For civil cases, you can be held indefinitely. In case of criminal charges, you will have to prove that the drive has self incriminating evidence to rely on 5th amendment to avoid providing the key. But it is hard to pull off and requires a good lawyer.

THC - July 23, 2017, 11:46 am

(Jul 23, 2017 11:00 AM)Sheeple Wrote: [\[CITE\]](#) Closed source and owned by microsoft. Don't trust it at all, matter of opinion. It could be backdoored and the feds could just access your "encrypted" data with no trouble at all while VeraCrypt is open source and consistently updating their security. VeraCrypt is just more secure it pretty much every aspect compared to bitlocker.

I think at some point there was a bitlocker related leak revealing that it was relatively easy for the federals to gain access to the data? I thought it was something snowden related however I might be wrong.

I would just be careful with how you set up your encryption. Keep in mind if you forget your encryption key then RIP your data. I would keep an encrypted backup of important data somewhere.

ST4RL0RD - July 23, 2017, 1:04 pm

(Jul 23, 2017 11:40 AM)archangel.dmitry Wrote: [\[CITE\]](#) You need start with the weakest point - you. If you encrypt the drive and a judge orders you to unlock, you will have to. If you don't, you will be held in contempt of court. For civil cases, you can be held indefinitely. In case of criminal charges, you will have to prove that the drive has self incriminating evidence to rely on 5th amendment to avoid providing the key. But it is hard to pull off and requires a good lawyer.

I'm not a US citizen but I do believe the laws in the UK are just as harsh.

archangel.dmitry - July 23, 2017, 2:23 pm

"feds" are usually called US federal law enforcement agencies. I thought UK was a kingdom and not a federation. By the way you still can be a subject of US laws if you commit a crime against US based companies or individuals.

Uriel - July 23, 2017, 2:26 pm

(Jul 23, 2017 11:40 AM)archangel.dmitry Wrote: [\[CITE\]](#) You need start with the weakest point - you. If you encrypt the drive and a judge orders you to unlock, you will have to. If you don't, you will be held in contempt of court. For civil cases, you can be held indefinitely. In case of criminal charges, you will have to prove that the drive has self incriminating evidence to rely on 5th amendment to avoid providing the key. But it is hard to pull off and requires a good lawyer.

Haven't there been cases where individuals have gotten away by saying that they have forgotten the password? I think there was an individual that was held for some time (less than a year) and said that the stress of the situation & being that he had not thought about the password in so long he

forgot it.

BadBoy - July 23, 2017, 3:11 pm

If I recall properly, encrypting a hard drive/thumb drive makes read and write really slow. If you use veracrypt and set really long passwords or try to make the encryption strong by placing a really strong passphrase, mounting it will take quite a while.

I do recommend Aegis Secure key thumb drive. They come with a built-in keypad to enter your password with, the build quality is really nice, plus its hardware-based encryption.

Sheeple - July 23, 2017, 4:11 pm

(Jul 23, 2017 03:11 PM)BeatNode Wrote: [\[CITE\]](#) If I recall properly, encrypting a hard drive/thumb drive makes read and write really slow. If you use veracrypt and set really long passwords or try to make the encryption strong by placing a really strong passphrase, mounting it will take quite a while.

I do recommend Aegis Secure key thumb drive. They come with a built-in keypad to enter your password with, the build quality is really nice, plus its hardware-based encryption.

Security > Time

My passphrase > 30 chars and takes 20 seconds to mount

Voqet - July 23, 2017, 4:14 pm

Bitlocker has been decrypted before, without using the Recovery Key. Obviously many exploits still exist with-in Bitlocker and can be found if you focus time into it.

archangel.dmitry - July 23, 2017, 4:30 pm

(Jul 23, 2017 02:26 PM)Madness Wrote: [\[CITE\]](#) Haven't there been cases where individuals have gotten away by saying that they have forgotten the password? I think there was an individual that was held for some time (less than a year) and said that the stress of the situation & being that he had not thought about the password in so long he forgot it.

Yes, there are some cases but you need to convince the judge that it is indeed the case.

coco69 - July 23, 2017, 6:07 pm

I felt my solution was a solid one, but looks like no one even considered it, fine by me that's what I would do lol

Eternal. - July 23, 2017, 7:15 pm

(Jul 23, 2017 10:22 AM)sdk? Wrote: [\[CITE\]](#) If you're actually worried, for whatever reason, move it to an external bay and have a hammer, best encryption ever.

You'd be amazed what the Feds can gather from a broken hard drive. Encryption is probably necessary since you are asking.

slrslr - July 24, 2017, 2:25 am

Advantage of an encryption is that quite no one can steal your data physically.

Disadvantage is tiny slowdown of the disk operations and possibly boot time in case of system partition encryption.

But in my case it is not noticeable to rethink if i should stop using it.

I am using Truecrypt.ch, whole disk encryption. i decided for it, because one do not need to worry about unencrypted parts, leaked data into unencrypted.