

Forum:[Hack Forums](#)

Thread: [Apple Firmware Password question/help](#)

?Arc - May 24, 2016, 10:30 am

Hello, I was curious if apple would be able to fix my issue.

First I want to say before you read further, no, my macbook is not stolen, nor would I have ever steal something. (Truthful. But not that it matters to say on a forum or website. anyone could lie, i suppose.).

My Macbook I got a few years ago was working perfect. I bought it second hand because it was cheaper. Long ago from a friend in a different state because he didn't like apple's OS after trying it, or some reason like that.

Anyways... I put an efi password on it a long while back and I can't remember it. If you've read about these topics, then that's obviously what most of the people will say.

Anyways, I obviously know I can't get it unlocked without receipt, sadly. And my ssd inside was acting buggy. And now I can't boot into recovery mode to fix it due to forgotten EFI.

The Macbook is a 2013 Model, No disk drive. Its been registered to my Apple ID, would apple be able to fix it if that's all I got? I know you need a receipt, but if its been registered to my apple ID (the serial), I could just take the SSD out and put it in another Macbook but I only have one 2013 model and I don't have one I can put the pcie ssd memory stick into, otherwise I would.

Unless I could request the receipt from apple but I doubt it due to I'm not the original purchaser. I can't ask the guy/my friend because I moved and don't really remember his contact details, sadly. I'm only 25 so I didn't save or get what I should of when I bought it because I didn't think that far head. when i got it so long ago.

Thank you for reading.

Originally posted on the apple support pages, not many replied.

I used one because I didn't want my brother trying to mess with my PC because he always tries to overwrite my password or delete my whole OS. After a while I forgot it existed.

It's a retina, so there is no way to unlock it sadly. I just was curious if the macbook being connected to my apple ID since I had it would work as a type of proof. Because if it was stolen the thief would not have been able to register it. Mine has been registered on mine so I know it's not stolen.

Is there any actual way to fix this?

Or a website or something.

There is stuff on ebay where you ship it to them and they remove it and it says tons of people have done it but I'm afraid it's a scam or they'll steal my MacBook Pro.

Thank you for reading.

.eXe - May 24, 2016, 1:24 pm

Do not under any circumstance send your MacBook off. Now if I'm not mistaken, there is unfortunately no way past the EFI password. Not unless you were to go full hog and possibly reflash the chip on a hardware level, if that's even possible.

?Arc - May 24, 2016, 2:19 pm

(May 24, 2016 01:24 PM) Evil.eXe Wrote: [\[CITE\]](#) Do not under any circumstance send your MacBook off. Now if I'm not mistaken, there is unfortunately no way past the EFI password. Not unless you were to go full hog and possibly reflash the chip on a hardware level, if that's even possible.

I'm not. I just don't know if it was a scam or not, because ebay sellers for EFI removals have like 150 sellings and a ton of rep. So it looked okay but not at the same time.

Truthfully I'm going to have to reflash if Apple won't do it for me. I just don't want to drive all the way there just to be told no they can't remove it. Due to not original owner. Maybe they will if they check to see if it's registered to my Apple ID? (it is), just no receipt.

.eXe - May 24, 2016, 2:47 pm

(May 24, 2016 02:19 PM) Owner™ Wrote: [\[CITE\]](#) I'm not. I just don't know if it was a scam or not, because ebay sellers for EFI removals have like 150 sellings and a ton of rep. So it looked okay but not at the same time.

Truthfully I'm going to have to reflash if Apple won't do it for me. I just don't want to drive all the way there just to be told no they can't remove it. Due to not original owner. Maybe they will if they check to see if it's registered to my Apple ID? (it is), just no receipt.

Unfortunately that won't be enough. For example I could buy a stolen MacBook that already has an EFI password but a fresh install of Mac OS, so I go and set up my system, until the day comes that I

find out it has the EFI password.

?Arc - May 24, 2016, 3:07 pm

(May 24, 2016 02:47 PM)Evil.eXe Wrote: [\[CITE\]](#) Unfortunately that won't be enough. For example I could buy a stolen MacBook that already has an EFI password but a fresh install of Mac OS, so I go and set up my system, until the day comes that I find out it has the EFI password.

Bah. Would flashing the bios chip completely remove the password? I wish I could do it but sadly I'm not that savvy in tech. It would cost me 100 dollars just to remove my own password I forgot.

.eXe - May 25, 2016, 2:23 am

(May 24, 2016 03:07 PM)Owner™ Wrote: [\[CITE\]](#) Bah. Would flashing the bios chip completely remove the password? I wish I could do it but sadly I'm not that savvy in tech. It would cost me 100 dollars just to remove my own password I forgot.

I don't even know if it's possible, I'm just speculating here. If you have a steady hand I suppose you could probably buy a broken Mac of the exact same model, and re-solder the chip.

?Arc - May 25, 2016, 4:30 am

(May 25, 2016 02:23 AM)Evil.eXe Wrote: [\[CITE\]](#) I don't even know if it's possible, I'm just speculating here. If you have a steady hand I suppose you could probably buy a broken Mac of the exact same model, and re-solder the chip.

Sadly won't work because apparently the chips go to the motherboard are special to the serial numbers. You can buy them blank or filled online but still have to input dumped code, which I sadly can't do. I'm no coder and I don't have the stuff required.

In a fucked up way I could buy a macbook pro new of the same model from apple, and replace the motherboard and return it. But I couldn't do that. I'd feel bad.

.eXe - May 25, 2016, 12:51 pm

(May 25, 2016 04:30 AM)Owner™ Wrote: [\[CITE\]](#) Sadly won't work because apparently the chips go to the motherboard are special to the serial numbers. You can buy them blank or filled online but still have to input dumped code, which I sadly can't do. I'm no coder and I don't have the stuff required.

In a fucked up way I could buy a macbook pro new of the same model from apple, and replace the motherboard and return it. But I couldn't do that. I'd feel bad.

They'd probably know, anyway. Your only other option is to buy one with a dead screen/optical drive etc and just salvage the mobo.

?Arc - May 25, 2016, 2:25 pm

(May 25, 2016 12:51 PM)Evil.eXe Wrote: [\[CITE\]](#) They'd probably know, anyway. Your only other option is to buy one with a dead screen/optical drive etc and just salvage the mobo.

Alright, thanks. I'll check into it. I'm going to leave this thread open in case some random stranger somehow finds an exploit or related. That way if I have the broken motherboard still I can salvage it.

nined3z - May 25, 2016, 7:37 pm

if you used a 4 digit password you could brute force it with a teensy (micro processor) via USB from a script online. I actually have done this with success. It will take sometime tho.

?Arc - May 25, 2016, 8:22 pm

(May 25, 2016 07:37 PM)nined3z Wrote: [\[CITE\]](#) if you used a 4 digit password you could brute force it with a teensy (micro processor) via USB from a script online. I actually have done this with success. It will take sometime tho.

Thats the thing, I set the password so long ago I don't remember if I used a random password like I would, or a 4 or 6 digit pass. plus I'm stupid teensy wise and can't understand how it would work.

EDIT: I assume it isn't 4 digits because i would of had to set it with icloud and I don't use icloud. (well I have an icloud but I meant I never set one with icloud).

.eXe - May 26, 2016, 1:53 am

The only possible method I have found, is this:

<http://osxdaily.com/2009/10/19/bypass-mac-firmware-password/>

If you can remove the RAM in your system, there is a method to get round it, but I believe the 2013's have RAM soldered to the mobo.

EDIT: Buy yourself a Teensy 3. We can set it to act like a keyboard and automate a bruteforce attack. For \$24 it's about your cheapest option.