How to protect your Apple iCloud account

Worried about hackers destroying your iCloud music, pictures, and documents? Here are three things you should do right now.

By Steven J. Vaughan-Nichols for Zero Day | March 24, 2017 -- 19:41 GMT (12:41 PDT) | Topic: Security

Your Apple iCloud account may be open to attacks.

Maybe the London-based hacker group -- which goes by the name "Turkish Crime Family" -- doesn't have access to [250-million Apple iCloud account names and passwords](). But they do have access to some indeterminate number of accounts, and that's more than enough reason to exercise caution: Protect your iCloud password and data today or risk losing it tomorrow.

Here's how to do it.

Back up vulnerable data

First, you need to back up your iCloud data. Yes, I know Apple's idea was you could use iCloud to back up your Apple device data, and that's fine, but it's iCloud itself we're worried about today.

For your iPhone, iPad, or iPod, the easiest way to do this is to [back up your device's files to your Mac or PC with an iTunes backup]().

- Plug your device into your Mac or PC with iTunes on.
- In iTunes' top left-hand corner, under the play controls, there's a tiny phone icon. Click here and it will take you to your device's menu.
- Click on Summary in the left-hand column.
- You will be presented with three boxes. Choose Select Backups.
- Choose to automatically or manually back-up your device. If you choose automatic, every time you plug your gadget in, iTunes will start to back it up.

Backing up your Apple device locally, and not just to iCloud, is a good idea.

The only problem here is that [iTunes doesn't back everything up](). For example, it won't back up your Apple Pay information and settings, photos already on iCloud, or purchased iTunes and App Stores content.

So, to be safe, you really must change and secure your password.

Change your passwords

Apple could help here -- and not just by paying off the Turkish Crime Family. Other major sites -- like Amazon, Netflix, and LinkedIn -- buy cracked password lists, and use one-way hashing matches to check for existing passwords. They then reset vulnerable passwords and ask users to switch passwords. Apple hasn't done that, but it should consider doing it, given just how large the threat appears to be.

Since Apple isn't doing this, it's up to you.

One thing that has always annoyed me is that Apple talks as if your Apple ID and iCloud ID are different. They're not. They're the same, and they use the same password.

To [change your Apple ID password](#), sign in to your [Apple ID account page](#) with any web browser and follow the instructions to reset your password. I changed mine using Google Chrome from a Mint Linux system.

Your new Apple ID password must contain at least eight characters, a number, an uppercase letter, and a lowercase letter. You also can't use spaces, the same character three times in a row, your Apple ID, or a password you've used in the last year.

Whatever you do, [do NOT use dumb passwords](#) such as "abcdefgh," "qwerty," or "password." The easiest way to create a secure password that won't try your memory is to use passphrases instead of passwords.

Instead of working your nerves into a frenzy trying to memorize what the cat wrote when he jumped on the keyboard (e.g. "sdf9usdf"), use an easy-to-remember but nonsensical phrase instead. For example, "Plump/Trotting Pups:" or "UNC?Win!Duke?Lose!" or "AC!DC!Tesla! Edison?" These are easy to recall and hard for crackers to break.
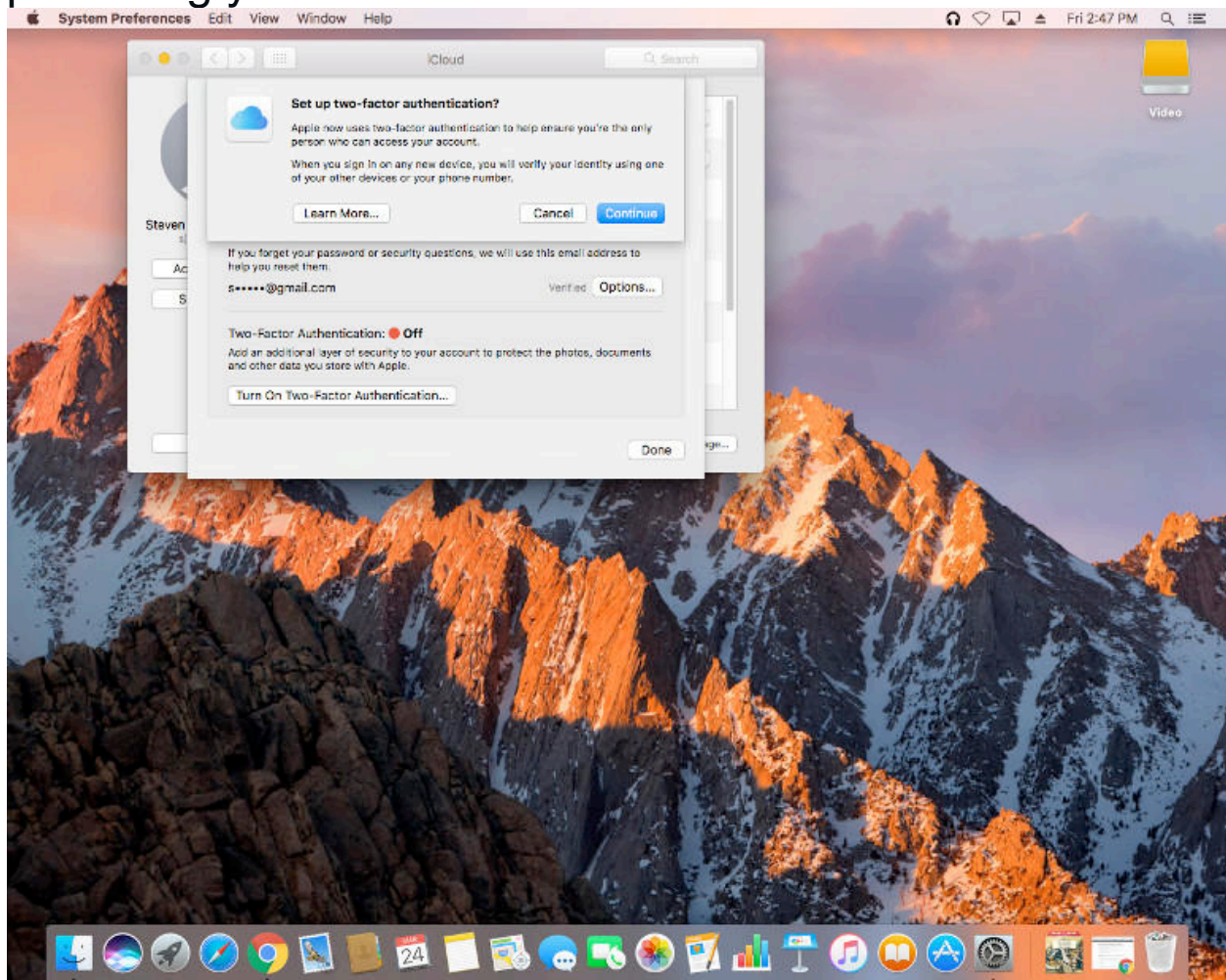
Once you've changed your password, you'll need to change it on all your Apple devices.

Then, you're going to want to add another layer of protection: Two-factor authentication (2FA).
2FA

[Apple's 2FA is clunky](#), but it still does a great job of protecting your account.

For additional protection, turn on Apple's two-factor authentication.

When you activate 2FA, you can access your account only from trusted devices such as your iPhone, iPad, or Mac. When you want to sign in to a new device for the first time, you'll need to provide two pieces of information. These are your Apple ID password and the six-digit verification code that's automatically displayed on your trusted devices.

To use Apple 2FA, you'll also need a trusted phone number so you can receive verification codes. To add a trusted phone number, take the following steps:
1   Go to your Apple ID account page
2   Sign in with your Apple ID
3   Go to the Security section and click Edit
4   Click Add a Trusted Phone Number and enter the phone number

Now, you're ready for 2FA. For a trusted device, you need an iPhone, iPad, or iPod touch with iOS 9 and later, or you need a Mac running OS X El Capitan or later that you've already signed into with 2FA.

To turn on Apple 2FA, take the following steps.

On your iPhone, iPad, or iPod touch with iOS 9 or later:
1   Go to Settings > iCloud > tap your Apple ID
2   Tap Password & Security
3   Tap Turn on Two-Factor Authentication

On your Mac with OS X El Capitan or later:

1. Go to Apple menu > System Preferences > iCloud > Account Details
2. Click Security
3. Click Turn on Two-Factor Authentication

Yes, this can be a lot of work. On the other hand, how much work would it take you to replace your important photos, music, books, or documents if your Apple iCloud account goes up in smoke? Take the time, do it now. You'll be glad you did.

Related Stories:

- [Apple iCloud ransom demands: The facts you need to know](http://www.zdnet.com/article/how-to-protect-your-apple-icloud-account/)
- [The worst passwords of 2016 are as lazy as ever](http://www.zdnet.com/article/how-to-protect-your-apple-icloud-account/)
- [We're stuck with passwords: Here's how to make them work better for you](http://www.zdnet.com/article/how-to-protect-your-apple-icloud-account/)

Original article:
http://www.zdnet.com/article/how-to-protect-your-apple-icloud-account/?loc=newsletter_small_thumb&ftag=TRE17cfd61&bhid=2340584768728644737557973 7817622