



iDevices:

iPhone
iPod
iPad



September 2014

Welcome to Volume 5, Issue 9 of iDevices (iPhone, iPod & iPad) SIG Meetings



This SIG provides more opportunity for sharing of experiences than the more typically structured classroom, lecture or formal setting.

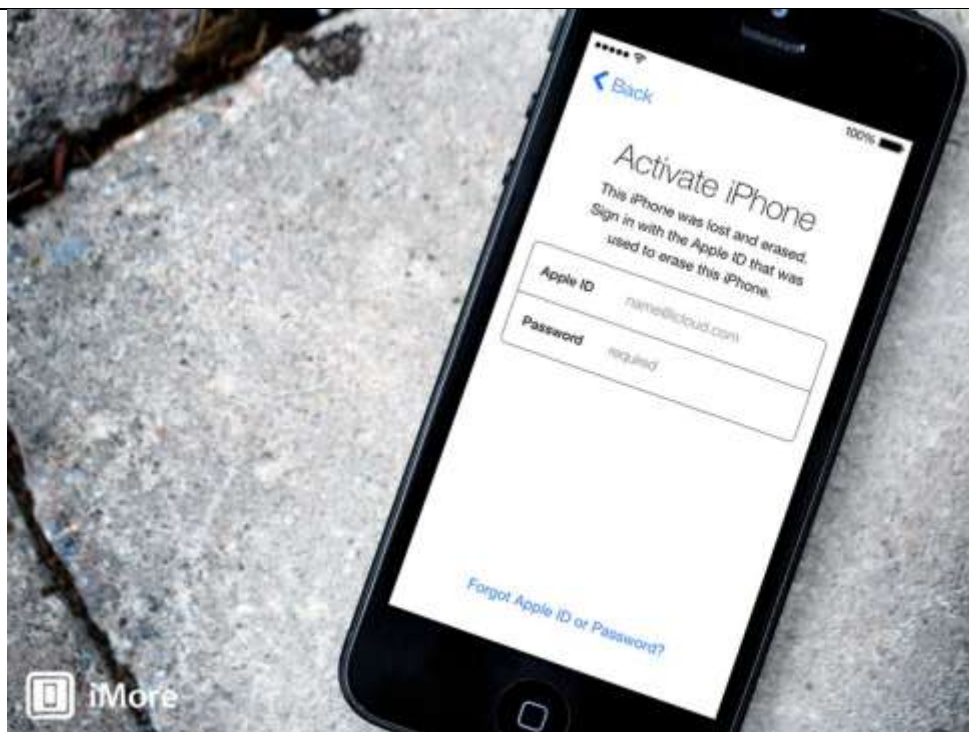
Need Help? Go to the **iDevice FORUM**, [click HERE](#)

To find Apps that are free for a short time, click these 2 icons:



Apple Sliced

iSnoops



The future of personal security

By [Nick Arnott](#), Saturday, Sep 6, 2014 a 5:55 pm EDT

Apple is [responding](#) to security concerns raised by many this past week as a result of [massive release of stolen celebrity photos](#). While this is a good move by Apple that will increase security for users, it's important to understand what these changes do and don't mean for us.

The more you know ≡≡≡★

Apple was heavily criticized this last week for its security around iCloud backups. iCloud backups can be downloaded with a person's username and password — no two-factor authentication required even for users who have it enabled. In response, Tim Cook announced some upcoming changes to iCloud account security. The first change is starting in a couple of weeks — two-factor authentication will be required when restoring backups from accounts that have two-factor authentication enabled. Additionally, when an iCloud backup is being restored, users will be notified via email and push notification. These are both welcome changes but it's important to remember our role and responsibility in security as users. Speaking to the [Wall Street Journal](#) on these new changes, Tim Cook said:

When I step back from this terrible scenario that happened and say what more could we have done, I think about the awareness piece. I think we have a responsibility to ratchet that up. That's not really an engineering thing.

I don't think that the importance of this observation can be overstated. With the iCloud accounts that were compromised in relation to the theft and release of celebrity photos, attackers were able to gain access to the accounts by answering security questions. If two-factor authentication had been enabled on those accounts, it would have been significantly more difficult for the attackers to access those accounts because the unique recovery key that users are given when setting up two-factor authentication would have been required before the attackers could have answered the security questions.

To be clear, the people who committed these crimes are the only ones responsible for them. I simply want to emphasize that there are steps we can all take to try and better protect ourselves. If people don't know about two-factor authentication, they won't use it. Even if they know about it, if it's easy to ignore then most will not use it. It's important that two-factor authentication be easy to use, and that people are informed about it.

Fortunately, the WSJ also said that Apple plans to more aggressively encourage people to enable two-factor authentication in iOS 8. If I had to guess I would say this change might look similar to Apple's change to setting a passcode in iOS 6. Prior to iOS 6, during setup, users would be given two options: Set a passcode on the device or not. Both carried equal weight. In iOS 6, users were instead presented with a keypad to set their passcode. In the upper-right hand corner was a small "Skip" button. People still have the option to not set a passcode, but Apple did a nice job of steering people strongly toward setting one. I would not be surprised to see something similar for two-factor authentication in iOS 8.

Even if more people enable two-factor authentication as a result, it's important that they are educated about it. Starting in two weeks Apple will send you a notification when a user attempts to restore an iCloud backup from your account. This notification is a critical piece of informing us as users that somebody could be trying to access our data, but that's all it's doing: informing us. So now what? To some it may seem obvious that it means you should change your password, but to many a simple warning won't mean much. Once again with a bit of good news, Apple also told the WallStreet Journal that the new notification system they will be rolling out in a couple of weeks will give people the chance to take action when they receive a notification, such as changing their password and alerting Apple's security team.

As with most things security, this does have a potential negative impact on convenience. If you only have a single device that you've set as a trusted device on your account — let's say your iPhone — and something happens to it — like it's stolen or falls into a river — it will be absolutely essential that you have the recovery key Apple gave you when you enabled two-factor authentication. I think this is a perfectly fair trade-off on Apple's part and I don't think we'll see a large number of people who completely lose access to their iCloud data as a result of two-factor authentication, but I'm guessing the number will be greater than zero.

Token security

Of course we're still not entirely safe (nor will we ever be). Apple's two-factor authentication only uses 4-digit codes. You only get 10 attempts to enter the code before you're locked out for 8 hours, but consider the following. Let's say an attacker has obtained a large number of iCloud account credentials – for the purposes of this exercise we'll say they have 1,000 compromised accounts. Four-digit codes only leave us with 10,000 possible codes. If an attacker can attempt 10 codes on each of those 1,000 accounts, that means they stand a 1 in 1,000 chance of guessing the correct code on any given account. With 1,000 accounts, the attacker has a good chance of correctly guessing the code on at least one of those accounts.

This isn't a reason to panic. It's no small feat to obtain credentials for 1,000 iCloud accounts. And even if your account was one of the thousand, there's only a 1 in 1,000 chance that yours would be the one that they would compromise. But still, this is a plausible scenario. Most other services utilizing two-factor authentication seem to use longer codes (6 digits or more). Given the infrequency with which a two-factor authentication code needs to be entered, and how quick it is to enter a numerical code, it would be great see Apple extend the length of their two-factor authentication codes.

No silver bullets

Even with the upcoming changes, two-factor authentication does not guarantee our safety. One of the best things we can do to protect ourselves is use complex, hard to guess, and hard to crack passwords. Just because you have an alarm on your house doesn't mean you should leave your front door unlocked. Two-factor authentication is not intended to replace passwords; it's meant to supplement them.

It's been said countless times before, but I'll say it again here: You need to be using long, complex, hard to guess passwords. For most websites and services, I have 1Password generate a long, random password for me. Since your iCloud password is something you need to type in on a fairly regular basis, this may not be the best way to go, *but* you still need to make it secure. While character complexity is good (mixed case, special characters, numbers), length generally has a greater impact. A phrase like "My dog's name is Scott." is significantly more difficult to crack than a random password like wJM2=.Vkn7 (assuming your dog's name isn't actually Scott, in which case that phrase could be easier to guess). Phrases also have the benefit of being easier for our human brains to remember. If you're not sure how to come up with a secure password, there are some [great articles out there to help you](#).

If you're one of those people who sees this advice time and time again and thinks "I know I should, but it just seems like too much of a pain", please give it a try. You'd be surprised how quickly you can get used to typing a more complex password.

Insecurity Questions

One final weakness that anybody using iCloud (as well as many other services) should be aware of is security questions. Which do you think would be harder for an attacker to figure out: a password like Ci<s}e)Ob+noks or the answer to the question "What was the name of your first pet?" The problem with security questions is they are significantly easier to learn or guess than good passwords. Often times the answers to security questions can be discovered through casual conversation, or by Googling or looking at your Facebook page. Your account will only be as safe as the weakest link defending it. In order to not have security questions be a weak link, it's a good idea to treat them as passwords.

As Rene has [previously said](#), security questions should be avoided when possible, and when they can't, use randomly generated passwords for the answers (or a long phrase as mentioned above). Just be sure to store these passwords in your favorite password manager so you don't inadvertently lock yourself out of your account.

Looking to the future

Security is a war with no end in sight. It's a cat and mouse game. New vulnerabilities will be discovered, software vendors will patch them, and more new vulnerabilities will arise. As more people around the world continue to use smartphones, more services pop up to store our data, and we continue store more information than ever before on electronic devices, the potential payout for exploiting, and therefore the number of interested criminals, will continue to rise.

At this very moment, we have a record amount of digital information stored on servers and in devices, and tomorrow will be a new record. For most of us, simply not using these devices and services is not a viable option. So we move on the best we can. Researchers will continue to promote best security practices, and we should do our best to follow them. Make smart choices.

Do everything you can to make yourself a difficult target. Lastly, security is constantly changing and evolving — keep an eye out for changes that take place and new best practices. This will help you stay one step ahead.

How to keep all your private photos off iCloud

By [Allyson Kazmucha](#), Saturday, Sep 6, 2014 a 12:03 pm EDT



While what happened to Jennifer Lawrence, Kate Upton, and many other celebrities could arguably happen on any cloud storage service, many folks are pointing fingers at [iCloud](#). While we don't believe iCloud is any less safe than any other backup service, we understand people wanting to take precautions. So if you'd prefer to not have *any* of your photos on iCloud, we can walk you through how to safeguard all your pics, nudies or not!

How to prevent iCloud from backing up or storing photos

In order to make sure none of your photos end up in iCloud, you first need to understand how iCloud stores your photos. There are a few different places iCloud could be storing your photos, so depending on how keen you are to get them off, you'll want to perform one, if not all, of the steps laid out below.

1. Disable Photo Stream

Every time you snap a photo, iCloud can back up your last 1,000 photos to Photo Stream automatically. They then become available on all devices linked to your iCloud account. People that use shared devices may not like this behavior and would rather have it turned off.

- [How to quickly enable and disable Photo Stream on iPhone and iPad](#)

Remember that you'll need to disable Photo Stream on every device you've got linked to your iCloud account. Also keep in mind that you don't need a password in order to re-enable it. If you're concerned about that, it's best to sign out of your iCloud account completely on shared devices.

2. Turn off iCloud Camera Roll backups

If you back up your Camera Roll to iCloud, anyone that would restore from one of your backups would have access to all of your photos. The easiest way to prevent that is to not back up your Camera Roll at all. Just make sure that you're periodically saving your photos someplace safe in case you were to lose or break your

iPhone or iPad.

1. Launch the **Settings app** on your iPhone or iPad.
2. Tap on **iCloud**.
3. Tap on **Storage & Backup** — it's all the way at the bottom.
4. Tap on **Manage Storage**.
5. Tap on your current device under **Backups**.
6. Under **Backup Options** turn **Off** the option for **Camera Roll**.
7. Tap on **Turn Off & Delete** to confirm.





You'll need to repeat this process on every device you have backing up to your iCloud account.

Apple sends email notifications when users sign into iCloud.com

By [Joseph Keller](#), Monday, Sep 8, 2014 a 11:05 am EDT



Apple has added a new layer of security to [iCloud](#), notifying users when someone logs into iCloud.com using their email address and password. When you log in to the site, Apple will send you an email notifying you that someone has your credentials have been used on iCloud.com, and instructing you either to ignore the email if you did this yourself, or what steps to take if you didn't.



Dear Joseph Keller,

Your Apple ID ([REDACTED]) was used to sign in to iCloud via a web browser.

Date and Time: September 8, 2014, 7:52 AM PDT

If you recently signed in to [iCloud.com](#), you can disregard this email.

If you have not signed in to [iCloud.com](#) recently and believe someone may have accessed your account, you should reset your password at [My Apple ID](#).

Apple Support

[My Apple ID](#) | [Support](#) | [Privacy Policy](#)

Copyright © 2014 Apple Inc. 1 Infinite Loop, Cupertino, CA 95014, United States. All rights reserved.

This is similar to emails that Apple sends out when you make purchases on a new device for the first time. It's a fairly standard security practice, but it's good to see that Apple is taking security more seriously in light of [recent events](#).

Additional links you may be interested in:

[How to reset a forgotten iCloud, iTunes, or App Store password on iPhone or iPad](#)

[How to view all the photos you've liked with Instagram for iPhone](#)

[How to find the owner of a lost or stolen iPhone](#)





[Apple offers free replacement program for defective iPhone 5 batteries](#)

[Photos in iOS 8- Explained](#)

[Manual camera controls in iOS 8- Explained](#)

[Can't delete photo albums on your iPhone or iPad- Here's why!](#)

Free Reference Materials For your iDevices

Apple iPhone User Guide	Apple iPad User guide	Apple Support Pages	Apple iCloud
			
<u>Click here to view</u>	<u>http://Click here to view</u>	<u>Click here to view</u>	<u>Click here to view</u>

[Want to trade in your old iDevice? Click on this link to compare prices](#)

The next meeting will be on
Wednesday, October 8, 2014 at 3:00 p.m.

Special Note: These pages contain links to third party websites. I cannot guarantee any third party website that you may access through the links. Also, it does not mean that I endorse those websites, or that I accept any responsibility for the content or use of those websites.