# Why Someone Else Will Get Your Digital Photos

**Author :** Cat

**Date :** September 10, 2014

I'd like to talk about the safe places to store your digital pictures that you DON'T want seen. Spoiler Alert: there aren't any. Once you have captured a digital photo on a device that is connected to the internet, there are no guarantees that it will stay where it belongs.

When we hear about compromising photos, the reference is often to nudes. According to recent studies, 20% of all teens have taken some kind of nude or semi-nude photo on their phones. Statistics are even higher amongst adults. Warning to teens: just having them may be against the law - possession of a nude photo of someone under 18 is illegal in most western countries, even if the possession is consensual.

You may be thinking that you don't have any of *those* photos, but a photo could be compromising in other ways. You may have captured photos of you or your family but the background reveals details about your house. Or maybe it is an intimate, but not sexual, moment that was not meant to be shared. For example, on my phone I have a picture of my husband asleep in our bed with our infant daughter. I would not want that picture of our bedroom splashed across the internet even though there is nothing scandalous about it.

*I won't tell you to stop taking pictures with your phones, that is not realistic. I will tell you how they are at risk if ending up in someone else's hands.*

## Culprit one: The Software Bug

I am a little jaded here because I spent 12 years working on software for a handheld device company. I know how easy it is to have a software bug. I also know that sometimes weird things happen where the error in the software does not reveal itself on the first time you use the feature but maybe the 347th, and only after you have just made a phone call to your 3rd contact. These are the scenarios that aren't always tested. The scary part of a bug is that you are not aware of the issue until it is too late.

My friend sent his wife a photo recently using a popular chat software. It didn't work. He sent it again. It still didn't work. After 3 times a male friend of his sent him a message and asked why he kept receiving this picture. So the user sent the right photo to the right person but the software sent it to someone else.

We want to trust in the magic of technology but ultimately software was written by a human and is prone to errors.

## Culprit 2: The Screen Capture

Every device has the ability to screen-capture. What that means is that anything that crosses someone else's screen can be recorded by the device or computer. Where this is important is in the false security that a picture will be temporary. The purpose of applications such as Snapchat is that pictures self-destruct after they are received. That means the picture can be seen only briefly then they disappear from the phone. This has become popular for teens to use for 'safe' sexting. However, there no reason why the recipient can't screen-capture the image thus saving it indefinitely. And it happens often.

In speaking with a policeman on the matter, he said the #1 issue in high schools today is video capture. People feel safe in exposing themselves in a Skype or Facetime chat because it is live. Again, the video participant has the ability to capture stills or streams of that video, and in his case nude screen captures were being distributed within the high schools.

So there is no such thing as a temporary picture. All images, once posted or shared online, are permanent.

## Culprit 3: The Hacker

On August 31st, 2014, there was a massive hack in to iCloud, the Apple cloud storage. Pictures were taken from over 100 celebrities' accounts. Clearly the hacker had targeted the celebrities because they were all young and beautiful women. The photos were then posted on a popular anonymous forum called 4Chan. Within hours, they were reposted to several other sites including Reddit and its image hosting app, Imgur. Many people admit to having downloaded them to their own computers. Once an account has been broken in to and the pictures are taken, the damage cannot be undone.

This time it was iCloud but next time it could be Instagram, Facebook or Dropbox. No matter what storage and viewing systems you use, if it is connected to the internet, it is vulnerable to attack.

## Culprit 4: The New Setting

Last year Facebook made a change in their status box where if you altered the audience of a post (friends, public, etc), all subsequent posts went to the same audience. This was not well publicized. The result was that people were posting pictures that they intended for just friends, but were now being posted publicly. This particular setting has since been reverted but consider how many other times this could come in to play. If you use storage like iCloud, do your photos sync automatically to the cloud? If you update the software on your handheld device, this setting could revert to automatically syncing them all. Or maybe it uploads all device photos to Instagram.

It pays to check through all your settings routinely to make sure they are what you expect them to be. At the very least, double check after any kind of upgrade of software or an application because that is when they tend to revert back to 'defaults'.

## Culprit 5: The Returned Device

If you have ever returned a device to a store to get a new one, then you may also be handing in your passwords and your photos. Very few people completely wipe their devices of all their personal data. In an extreme case, one woman handed in a device last year in the US to exchange for upgraded hardware. The employee of the store where it was returned managed to uncover her Facebook password and her private semi-nude photos, both still accessible to him using software that the carriers have. This scrupulous employee decided to post her private photos on her Facebook account for all her friends and family to see. He was arrested and the woman was humiliated.

Make sure your device is completely empty before handing it over to anybody. I cannot list the instructions to wipe your device here because every software version and hardware combination is different. What you can do is type "how to wipe a device" in to Google and it will give you links for the instructions. I did this and found Android, iPhone and Blackberry listed right at the top.

### The lesson here: Photographer beware. Take your photos with your phone. Share your photos. But acknowledge there is a always a risk someone else may end up with it. If that is too big of a risk for *that* photo, delete it.