In light of celebrity hacks, how to protect data (Update)

2 September 2014, by Mae Anderson

The circulation of nude photographs stolen from celebrities' online accounts has thrown a spotlight on the security of cloud computing, a system used by a growing number of Americans to store personal information over the Internet.

On Tuesday, Apple acknowledged the security breakdown and blamed it on intruders who were able to figure out usernames and passwords and bypass other safeguards. The company said it found no evidence of a widespread problem in iCloud or its Find my iPhone services. But the theft of the photos raises questions about the protection of information stored beyond a person's own computer or mobile device.

If celebrities' photos aren't safe, then whose are? Some key questions and answers about information that is stored remotely:

Q: What is the cloud?

A: The cloud is a way of storing photos, documents, email and other data on faraway machines. Amazon, Apple, Google and Microsoft all offer cloud-based storage. Smaller companies like Dropbox and Evernote do, too.

The practice saves space on computers, smartphones and tablets and allows users to access the same information from any device. And if you lose your phone, for example, you don't lose your vacation pictures. The drawback is that you are putting your information somewhere else, so you run the risk of a hacking attack on those systems and accounts.

Q: Is it secure?

A: For the most part, yes. Companies invest a lot to ensure that customers' private information stays private. "The short answer is the cloud is often more secure than other storage," says Rich Mogull, CEO of security research and advisory firm Securosis.

But that doesn't mean the system can't be compromised. "There are a lot of attackers who have a lot of time," Mogull says.

Q: How can individuals make their data more secure?

A: You need passwords to access your accounts, so choosing a strong one is important.

Tim Bajarin, an analyst at technology research firm Creative Strategies, recommends having different passwords for each account you hold online, so a breach in one system won't compromise another. It is also important to have a number and punctuation mark in each password or a creative spelling of a word to make it harder to guess. Also, avoid using common words or notable birthdays as passwords. A strong password is particularly important if you store sensitive information online.

Another way to make your information harder to hack is called multi-factor, or two-step, identification. That means the first time you log onto an account from a new device, you are asked for a second form of identification. Usually, that involves getting sent a code as a text on your phone or an email. A hacker who has your password would still need physical possession of your phone to get the text.

Most major cloud services, including Apple's iCloud, Google Drive and Dropbox, offer this kind of protection. Amazon's Cloud Drive is the notable exception. But you usually have to turn this on.

Apple is urging its users to switch to stronger passwords and to enable the two-step authentication feature in the aftermath of the celebrity hacking attacks.

Q: How can I tell if my phone or computer is

uploading information to the cloud?

A: You had to have signed up and agreed to the cloud services' terms, but that might have happened long ago, as you were setting up your device. If you are not sure if you have opted in, check your phone's settings.

With iPhone photos, for instance, if you have Photo Stream turned on, that means you are storing your photos on iCloud. Check your settings under iCloud. On Android phones, check the Auto Backup settings under Google+ in Google settings.

A: Is my financial information at risk?

Yes, if you use the same password for online banking that you do for other sites, and if you don't have multi-factor identification on your banking website.

But generally, financial information is among the most protected online. Information is encrypted, or scrambled, in transit. You can tell if a site does that if you see "https" rather than "http" before the website address.

Q: Will my photos and other information remain on the cloud even after I delete them?

A: They should not. Settings vary for different cloud services, but most of them delete information from the cloud when you delete something from your phone or computer, at least once the device has had a chance to sync with the online service.

You can check online, however. All the cloud storage providers have websites you can sign into to check out what information is being stored.

"If you want that extra feeling of being safe, make sure it's deleted online," says technology analyst Patrick Moorhead of Moor Insights & Strategy.

Q: How do I opt out of cloud storage?

A: Check your phone or computer settings if you don't want your photos and documents stored online. There are other ways to store information, including using an external hard drive or your device's own storage.

"If you really want to be safe, keep confidential information off your service provider and back it up to an external hard drive the old-fashioned way," Gartner analyst Avivah Litan says.