From: james | personal genius <[redacted]>
To: [redacted] <[redacted]>, "jeffrey E." <jeevacation@gmail.com>
Cc: [redacted] <[redacted]>, Richard Kahn <[redacted]>
Subject: Re: Possible unauthorized sign in
Date: Thu, 30 Aug 2018 17:48:40 +0000

Hi,

I checked out the machine for explanations of this message or signs of intrusion / cloning. The details are below; the tl:dr version is that there is no evidence to suggest anything untoward happened or that there was any kind of "security compromise." It is most likely that a bug in Apple's notification system delayed the sending of this alert since the July 17th macOS update on the iMac.

Findings:

- The 5th Floor iMac was ON, and logged into [redacted] account & her iCloud (I've turned off the machine).
- The iMac was in Sleep mode and does not appear to have been disturbed (or "woken") for quite some time.
- The name DOES match exactly as the name listed in the alert.
- The iMac appears only once on the list of devices signed into her iCloud account—along with:
  - her AppleTV,
  - iPhone X,
  - iPad Pro,
  - TWO MacBook Pros, and
  - Lesley's iMac (which was probably during a guest account session, I checked that computer & it's not logged in now).

**

→ [redacted]:
→ To remove any of those devices from your iCloud account:

1. On your phone open Settings > Your Name (at the top)
2. Tap the device to be removed (i.e. Lesley's iMac)
3. Tap Remove this Device at the bottom

→ Devices removed will be logged out of your iCloud account, so if anything is removed accidentally, you can just sign them back in. It's preferred to have this list be current so there aren't any ghost machines floating around that could authenticate logins to your account.

**

The log files in the 5th Floor iMac show NO software installs since August 15th (those were Office updates that happen automatically), the last OS update was July 17th, and the machine has been in sleep mode for the last week.

I can't explain why [redacted] would suddenly get this message yesterday, other than it was undelivered by a system bug on Apple's backend and queued until it finally delivered yesterday.

**

[redacted] iCloud account DOES have 2-factor authentication enabled; so one of the devices listed above would need to approve any logins to a new computer/device. Those authentications are push-notifications, NOT SMS, so they're very secure and can't be spoofed.

It is theoretically **possible**, if an attacker had (1) one of the approved devices above, (2) the iCloud password, and (3) were VERY lucky in the timing of the attack, that they could log into Messages & FaceTime separately (without iCloud) on a new computer that they had intentionally named "5th Floor iMac", and approve & dismiss the sign-ins from the device they have before [redacted] saw the requests. That would give them the ability to read any blue bubble iMessages [redacted] sends or receives.

BUT…. That's extremely unlikely because:

1. The FaceTime and Messages alerts would come separately; they only show up combined like that when logging into iCloud after a software update.
2. Had they logged into iCloud instead of Messages & FaceTime individually, the malicious computer would display in the iCloud device list.
3. They would have to have physical control over one of the other approved devices; if they had that, [redacted] already have access to [redacted] Messages & FaceTime messages on that machine.

If you are still concerned [redacted] iCloud account might be compromised, changing the password will log out all existing sessions and require each device to reauthenticate.

**

I do have a list of security suggestions that are tangentially related, but I will compile those and send separately.

Thank you,

James Ce
your own Personal Genius
□ Certified Support Professional 10.6
http://personalgenius.co