Subject: Re: App Store Scam- Possibly credit card fraud - fake reviews - media would love this

From: Phillip Shoemaker <[redacted]>

Received(Date): Mon, 18 Jul 2011 12:01:51 -0700

Cc: CSR ASM <[redacted]> Anders Baecklund <[redacted]> Lisa Tyerman <[redacted]> Evayn Burns <[redacted]>

To: Marta Cervantes <[redacted]>

Date: Mon, 18 Jul 2011 12:01:51 -0700

These are FRAUD takedowns. FRAUD is not done through UTB nor through App Review.

But, agreed, these apps are all misleading, have always been misleading, and there's no way the reviewers actually checked to see if the app did what it said it did. This means we are not truly checking for core functionality, are we?

On Jul 18, 2011, at 11:53 AM, Marta Cervantes wrote:

From my investigation (and looking back through my emails), if these guys have been removed 4 times in the past few months, this information hasn't been broadly distributed. These takedowns have not gone through UTB.

The reviewers were looking at these apps in isolation, without the fraud context without the necessary rights hold policy for the Flash trademark.

We should roll this out asap, IMO.

thanks,

Marta

On Jul 18, 2011, at 11:22 AM, Phillip Shoemaker wrote:

> I want to be clear here: I hear the line " the marketing text was different at time of review " ALL of the time. However, in this case, the NAME of the app AND THE SCREENSHOTS, clearly indicate something different. in both of these apps, the reviewers made mistakes, and the issue is that these apps keep slipping by. These guys have been removed for fraud 4 times in the past few months, and they keep submitting these apps over and over. Not sure why they keep getting approved. This is not a problem with these two reviewers, it is with the entire review team thinking that these types of apps are OK. They are not.
> Adding these devs to the watchlist, when they're getting removed from the program is unnecessary. Rather, we need to keep an eye out for these types of apps. If we continue to let these into the store, we continue to have problems with the review team.
>
> On Jul 18, 2011, at 11:17 AM, Marta Cervantes wrote:

UTB investigation for

442875834 Flash Video Expose
Issues found: the app is misleading in that the MT claims it is a Flash reader and player but does not actually provide these functions.

At least one reviewer has confirmed that the current Marketing Text is different than what was originally submitted for review:

"The Marketing Text that is shown appears to be totally different from what I remember reviewing a couple weeks ago. Previously, I believe it was advertised as information on Flash, and it included a web browser. I thought it seemed a little sketchy so I made to sure check that it didn't have some hidden feature to actually watch flash videos (and it couldn't)."

While it is difficult to anticipate misleading MT changes, the app name itself is misleading if the app functions simply as a browser,so this should have been flagged by the reviewer. Additionally, the use of a third party TM (Flash is a trademark) in the app name is in violation of accepted usage.

Recommendation:

Remove from Sale. Developer needs to be put on notice that changes to MT that are fraudulent will have consequences. Developer also needs to be added to the watchlist.

Coaching for the team: Both reviewers were suspicious and took pains to ensure the app functioned as described. However, the app name wasn't itself a concern since the app provided Flash related information (see screenshot below), but I doubt that this is original content - probably just taken from an Adobe web site or other public site. So both the app name and the content contain TM violations. I think this issue might have been avoided with a rejection for 8.5 initially.

I would recommend evaluating whether it makes sense to add Flash to the list of TM holds as a way to prevent fake Flash readers. Adobe is already on the hold list so adding another of their TMs shouldn't be a huge impact - Evayn can confirm if that's the case.

Call ticket has been filed.

<PastedGraphic-2.tiff>

On Jul 18, 2011, at 8:59 AM, Phillip Shoemaker wrote:

These "Flash Player" apps are still hitting our platform, and for some reason unbeknownst to me, we're still approving them. THEY DO NOT WORK. I've tried each of these, and went to various flash sites to verify, and they do not work. Despite the reviewers comments stating that these are not misleading, they absolutely are.
Let's find out how these are continuing to slip through review and how we can educate the team

to keep these from happening again. Additionally, we need to UTB and remove these ASAP. Lastly, please explain why appreview@apple.com did NOTHING to alert us to these issues, despite the fact that multiple emails were sent to us.

Thanks.

From: Jane Doerr <[redacted]
Date: July 18, 2011 8:25:15 AM PDT
To: "sjobs@apple.com" <sjobs@apple.com>, [redacted]
"appreview@apple.com" <appreview@apple.com>
Subject: App Store Scam- Possibly credit card fraud - fake reviews - media would love this
Reply-To: Jane Doerr <[redacted]

Its a Monday workday so wanted to follow up with this. If no one would bother to respond and take action, I think the media would love this. It is so wrong to let a scam like this go undiscovered and then reported with no action taken. This app is top 50 grossing in app store right now. Love Apple. Please do something right as you always had.

From: Jane Doerr <[redacted]>
To: "sjobs@apple.com" <sjobs@apple.com>; [redacted]
Cc: "appreview@apple.com" <appreview@apple.com>
Sent: Saturday, July 16, 2011 11:16 AM
Subject: Scam perpetuating in app store

Dear Steve,

I am an Apple fan and am thankful that Apple takes the approach to validate apps in the app store. Unfortunately, the system is not perfect and scams can still perpetuate in the app store where reviews can be gamed and short term and even possibly long term monetary gains can be made by unscrupulous developers. These apps may just be a small part of Apple's revenue, but it is like a disease that spreads and that only worsen user experience, embolden bad developers and discourage the legitimate developers.

In particular, I have been observing apps by Vietnamese developers that somehow were able to get past the approval process but yet misleads by fake description and lots of fake reviews. The lots of fake reviews may also be an indication of compromised credit cards which may be a much more serious issue for Apple.

In particular, look at

http://itunes.apple.com/app/flash-video-expose/id442875834?mt=8

http://itunes.apple.com/us/app/flv-explorer/id443432688?mt=8

and it is not hard to see the following red flags:

1) Fake reviews and stolen credit cards? - Flash Video Expose was just released and it has lots of 5 star ratings. Ditto for FLV Explorer which has been around longer. But sort through reviews based on "Most critical" for FLV Explorer and you will realize that users are complaining of a scam whereas the 5 star reviews seem to be fake. I would hypothesize that the developer is using either stolen credit cards, iTunes cards or prepaid cards. However, the economics make sense to cheat since they are only paying Apple's cut to write a review which cost $3 per review but resulting in a disproportionately increase in paid conversion and increase in ranking. Its better than using Pay Per Install scheme like Tapjoy which you have banned. Run the numbers to see the % of reviewers to downloads. The higher % can suggest fake reviews since I would assume that less than 10% of people downloading writes a review.

2) Apps look the same - FLV Explorer and Flash Video Expose looks like the same app with minor modifications, yet perpetuating the same scam of misleading consumers that this is a Flash player. Trick is to pass another app through when the old app has garner enough 1 star reviews and perpetuate the same scam.

3) Misleading Description - the app is not what the description says. Both apps have the same demo link: http://hdmediaplus.biz/flash which actually is nothing to do with the app and just another way to scam consumers of a HTML5 player on the app. Read the description and download the app and see for yourself.

The only way I can see this passing through the approval process is

a) Developer changes to a misleading description after the app is approved.
b) There is some breakdown in the approval process within the specific org approving the app.

I can go on and on and perhaps give recommendations and fraud detection algorithms for the app store. However, I trust Apple launch an investigation into these 2 apps and pull these developers off the app store before a small disease like that spreads. I respect the effort, quality and time put on my the approval team and can understand when things falls through the crack or developers game the system. Hopefully, this email does not fall on deaf ears and action is taken.

A loyal Apple Fan since Apple 2e.