Hello, I'm Roger Safian. Today is Friday, April 20, and you're listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

Today's podcast is pretty much gonna be entirely about the Macintosh Flashback malware that's out there right now. Let me start by giving sort of the updates as I know it. Apple does have fixes available so if you do the Apple update, you know to update your computer, you should get the update to prevent your machine being affected. Apple has also released a tool that will scan your computer and if it finds the infection and will remove it, so this is great. The tool is available only though for 10.6 and 10.7, so that's Snow Leopard and Lion of the Mac operating systems. And the reason is it's Apple's policy to only support the current version of the operating system, which is Lion, and the previous version, which is Snow Leopard. so if you've got an older machine and it's still running Leopard, which is 10.5.whatever, that machine is not going to receive any of the fixes and in fact you probably haven't received any fixes for quite a while. I would encourage you, if you are running an older machine you really might want to think about upgrading to the latest version. If you can run Lion, great, but Snow Leopard if you can't. I believe the update price is $30, I could be wrong about that but you can check. You definitely want to make sure that you're getting these updates if you need to continue to use this computer though, otherwise this problem is just going to get worse for you. Now Apple also has available, if you are running Lion, where you can download their tool and run it independently to see if your machine is infected, like even if you’ve applied the updates. They don't have that as far as I know for Snow Leopard, which is unfortunate. I think that what you're going to find here is, you know we've been talking about certainly for a while that Apple is no better or no worse than any other computer when it comes to security—everything's got its their issues and you need to be taking reasonable precautions. I think though that a fair number of Apple users have ignored that message and I suspect—or at least I hope—that we're going to get a change in that behavior amongst the Apple community so that they'll take their computer security a little more to heart because I think that what happened is they just kind of bought into the sort of hype that was going on about how malware is a PC problem and if I'm not running a PC, I don't have anything to worry about. And so what I find is there's a fair number of Apple users out there who do not update their machine on a regular basis and who are not running any antiviral software at all. So if that happens to be you, please change that behavior—update your machine, whenever it tells you there's an update, do it. And if it's not telling you there's an update, check regularly. You don't have to check once a week, but a couple times a month just to see if there are updates up there. and make sure that you update things not just that you got from Apple, but if you install other software on the machine, make sure that you're updating that as well. So for example it's pretty common for an Apple user to have Microsoft's Office on their
other on their Macintosh. Make sure that you update that as well, make sure you update all the other programs are on your machine so that you’re safe. And don’t forget you want good, strong, antiviral software which needs to be updated regularly as well on your computer.

I got a couple of interesting articles that I’ll put the links on the show notes for that kind of talk about this. One is kind of an interesting take, you know this was on information week, and basically what they were saying is this is the first time that Apple has ever come forward and even mentioned that they had a security issue. If you ever look at the Apple announcements when they do their updates, they’ll say “this fixes a security problem,” they never really go into any details, they never really talked much about it, they just kind of try to fly it under the wire. And that’s certainly not a good thing and I don't think it’s good for Apple, and I really don’t think it’s good for their customers. So I really hope that Apple changes that sort of behavior. One other thing that I think is really come out in this here, is the way that Apple handles their machines is perhaps—it works towards the detriment of their user community in some cases. In this case I think it’s one. And essentially what happened here is this vulnerability that was used for Flashback was found out and reported to Oracle—it's a Java vulnerability so it was found out and reported to Oracle last year, last summer in July or August—and then Oracle worked on getting out of fix, the fix was pretty rapidly deployed via Microsoft when they did their updates, but Apple doesn't just take—in other words, it'll get a fix for Java from Oracle and not just out it out there, they want to package and bundle it with their own updates. So they'd essentially delayed the deployment of this fix and I that's probably at least partially responsible for the spread of this virus. Now the other stuff that I've seen about the numbers has gone down. People were talking about you know half-million or a million or somewhere in that range. Now it turns out that people are saying that after the fixes have been out, maybe we’re down to 150,000, 250,000 infected machines. Still a lot, still a significant portion of Macs that are suffering from this issue, but not as bad as it was. And hopefully as more and more people apply the fix, we'll get more and more machines that are fixed and not vulnerable anymore. But I am still concerned about those people who were running 10.5. It’s not that old, you know I work here at a university obviously, it's very common for somebody to get a computer when they're a freshman to basically use it all through their school years. So four years is not that unusual. And Snow Leopard only came out a few years ago, there are a lot of people here that still have Leopard. To me it seems that they ought to be supporting more than what they just do, especially when it comes to security fixes. Other companies do tend to provide security updates for their software a lot longer than they do other updates and Apple just does not. They just completely cut the cord and I don't think that's good so I would encourage them to maybe revisit that policy. the other thing that's being reported is that there are variants of this out— there’s supposed to be at least two different new versions of this kind of malware out there so, it's not being detected by the Flashback stuff that Apple is done already. And you know once the floodgates are open, that’s it. I mean it’s always very difficult to get the
genie back in the bottle and I think that's the problem that Apple's gonna be facing right now. But you can help by protecting yourself. Again, making sure that the updates are applied in a timely fashion and making sure that you get good up-to-date antiviral software on your computer will certainly go a long way to help.

One more thing I wanna talk about with Apple, it looks like Apple is starting to update their Apple ID, the account information that they've got for the App Store—a series of security questions and things like that. I think all of that stuff will be good too because one of things I suspect it's going to happen pretty quickly is once people realize they can start compromising these Apples they will go for money which is essentially grab your iTunes account, or grab your Apple app store account and start using that as a way to get money. Because in the end I think that's what this is all about, it's all about money. That's all I want to say about that. I do want to end though with a link. There is a magazine GottaBeMobile, it's an online magazine, and they had a story about one of the Northwestern campaigns, the Reality Check campaign that we did. So I wanna put a link up in the show notes for that so you can take a look at that because I thought it was a pretty good campaign and it's kind of nice to be getting some positive press.

Anyway, thanks for listening. If you have any comments or suggestions, please feel free to send them to r-safian@northwestern.edu, and as always you'll find additional security information as well as the notes that contain the links for today's podcast at our website www.it.northwestern.edu/security/.