Hello, I’m Roger Safian. Today is Thursday, April 5, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

I’m going to start with patches as we usually do and the updates for Microsoft were just announced today. These are the updates that will be coming out next week on Tuesday and it looks like a little bit of everything is gonna get updated—a couple patches that apply to Windows, there's one patches that applies to Internet Explorer, looks like maybe a couple for Office, there's one I think for MySQL—so the odds are pretty good if you've got Microsoft equipment, you've got something that's can need to be patched on Tuesday. So make sure that when Tuesday, Wednesday rolls around you grab those patches right away 'cause you wanna make sure that you get them applied, especially the patches for Internet Explorer. If you're using Internet Explorer as your browser and a patch comes out, you can pretty much bet that that means there’s gonna be trouble for it. And it probably goes for just about any browser you’re using—Firefox, Opera, whatever—when there’s a patch for your browser, you definitely make sure that you get that patch applied right away.

And then the big story in the on the patches market is got to do with Apple. And we’ve been talking about security issues with the Apple systems for quite a while but they're finally reaching kind of epic proportions I would say. Problems not as necessarily as bad as what you might find in the PC world but it's getting up there. There is an exploit out there, it's called Flashback, and it looks for old versions of Java and then it attacks your system same exact thing that we would see happen in the PC world. Now there are reports that there's already between 500,000 and 1 million machines Macintoshes already infected. Just before I came in I saw a report that said now it’s up to 1.2 million Macs are affected. And I think this is partially because—my guess is anyway—a lot of Macintosh users do not have antiviral software on the machine. You kind of buy into “I have a Mac and I don’t have to worry about this” and we've been trying to dispel that for a while but you know that's obviously not been widely received, the message there. So really you need to fix this vulnerability. If you've got a Macintosh make sure that you apply this update. I'll put a link to the Apple release on the show notes, make sure you apply this. You might also consider just turning off Java. A lot of people report to turn off Java for the most part doesn't really cause them any problems; they’re not using it when they browse. If that's the case, why don’t you at least give it a whirl right? Open Safari, go to Preferences, Security, and deselect Java, and you should be all right from that point on. Unless you’ve been affected already, but that doesn't mean you shouldn't update Java anyway; if it’s on the machine you should update it, so please make sure you get this taken care of. if you're using Firefox, it may be taken care of for you automatically because Firefox has blocked the old version of Java so that you won't be able to use it anymore so that might be causing you some trouble. On the other hand if you not using Java anyway you might not even realize that's blocked on your machine.
Then the other big story that I want to talk about is this Global Payments and the credit card theft. Now right now they're saying that 1.5 million cards are affected in this. I would not be a bit surprised to find out that those numbers are going to climb. Now Global Payments is company that sits between you, your bank, and credit card companies and my understanding of what they do is basically help route the money to the right parties: they route money to the banks, they route money to the credit card companies, things like that. And what they're saying is that some of the track two data on the machines may have been stolen. And this track two data doesn't always contain the same amount stuff but it does contain things like your account number and the expiration date. Now there's other data that's probably not there amongst the things that I don't believe is there are those little security codes that they put on the cards, that's not supposed to be on the track two data. So I don't know how big this good bit story that came out over the weekend and for some reason is not getting a lot of play. But to me it seems like a pretty big deal. And as I said I would fully expect to see the number of cards rise higher than 1.5 million but we'll see what's going on with them.

In another story that came out that—again not getting a lot of play but seems like a big deal—is got to deal with social security cards that have been hacked. And essentially what they're saying is the Social Security Administration was hacked and that details of Social Security card holders—which means pretty much everybody, at least everybody in the US—were compromised. Now the story apparently first broke and was confined strictly to Puerto Rico but it looks like it's larger than that. Now I just started to follow up on this before putting this podcast together so I'll probably have to do some more work next week, but it looks like right now they're saying, at least the headline of this article is $30 billion. Now that's huge. Now the numbers that I were reading in the Wall Street Journal were much smaller but they were still in the billions of dollars, that's a pretty big deal. It looks like the IRS is dealing with this by creating a form—the IRS has on their website form 14039 which is the identity theft affidavit from December 2011. And just putting a form on the websites of the IRS seems pretty inadequate for something of this scope. And we will follow up on the story and I'll put a link in the shown notes so you can read about it yourself.

Another thing we'll talk about is Facebook and it looks like at least some of the applications—that the apps that are on your iPhone or Android, not all of those could be released by Facebook, but these appear to be the ones that were released by Facebook—are holding onto information about your login credentials so that somebody can get ahold of your Facebook information by getting ahold of your phone. Now this is certainly Facebook not taking security as seriously as they should, certainly not something new, although I think they have been trying to make strides in the right direction. But I don't think this is strictly a Facebook problem, this is why I think it’s very important when you’ve got a smartphone that you have to have your security code on, you have to make sure that you’re putting information into the phone that if it was compromised you could deal with it in a timely fashion—maybe if your phone gets stolen or lost, you want to change your Facebook password maybe bank accounts. I'm personally against using any sort of banking information on your smartphone just because I think it's too easy for the smartphone to go missing. And this stuff is gonna just be happening more and more so,
please, if you got a smartphone take every precaution in order to make sure that you're protecting the phone so that your data and you are safe.

Then there's a guide that I found for hardening the IOS. And this is from Australia and it deals with the iPod, the Touch, the iPhone, the iPad, any IOS system 5.01 and higher. And it's a pretty interesting guide, kind of comprehensive, it's probably geared to somebody who really wants to take their security seriously so you may not want to do all the stuff that they're talking about here but there’s a lot of good information but I would encourage you to give it a look-see if you're using those devices.

And then the last thing I want to talk about is Xboxes. And basically it turns out that the Xbox, like a lot of these systems, has got a hard drive in it and when you get rid of the Xbox, what happens to that hard drive? And the same sort of thing applies when you've got a computer to get rid of, when you've got your office copier machine, your TiVo maybe, who knows? A lot of these devices have got hard drives in them and what happens to that hard drive and all the information that's on it when you get rid of that device? Personally I never get rid of the device with a hard drive without removing the hard drive and just destroying it because I want to make sure that that data is gone. Now it turns out that with the Xbox, Microsoft is good about getting rid of the stuff that's on it—the games and stuff like that—so that somebody else couldn’t use it but they're not very good about getting rid of your personal information. And so somebody has done little forensics work and they were able to recover the credit card date of the person who had the drive before they got a hold of it, which is certainly not a very good thing. So I would encourage you really don't worry about what the costs are, if you can go trade your Xbox in and get $50 or something like that, $50 is not gonna cut it if your information gets stolen. Any of these devices, just remove the hard drive. If you want to give it to somebody you could always go by am another hard drive, hard drive drives are cheap these days especially older, slower, lower capacity hard drives which, if you’re getting rid of a device, that's probably the hard drive that's in it. Go out and buy them a hard drive, put it in there, and give it to them. Then just make sure you take that hard drive out and take it apart, drill some holes in it, or just get rid of it. You don't want allow this to follow into somebody else's hand.

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/.