Hello, I’m Roger Safian. Today is Thursday, February 2, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

We’ll start with updates and the first thing we’ll want to talk about is updates for the Mac OS Lion. There’s an awful lot of updates that were just released and you should start seeing the update feature kick in on your Macintosh. If that’s not the case go ahead and do the update automatically because you know you don’t want to wait around too long after these updates are available. It looks like there’s a lot of different programs within the Mac OS that got updated so you’ll want to spend a little extra time because it might take a little longer than the normal updates to go through.

And while we’re talking about updates remember last week we discussed the Symantec product pcAnywhere and they suggested that you should disable it because there were some security issues that they could not address. They have got a hot fix available right now and my understanding is there are going to be some additional fixes, but according to Symantec if you install this hot fix it should be safe for you to run pcAnywhere. So if you are a pcAnywhere user you’re definitely going to want to make sure that you grabbed this update as quickly as you can.

And then we’ll talk about the HTC Android phones. It looks like some of them—not all the phones but some of them—have a vulnerability that looks like it might be able to expose credentials on the phone to malicious apps. Now HTC is supposed to be coming out with a fix—and in fact it’s possible by the time you hear this podcast that that fix will already be out—but if you’re using an HTC phone you might want to double check just to make sure that you’ve applied that fix. I’ll put a link to the in the notes for today show to the vulnerability alert that’s on search so that you can take a look at that determine for yourself if it applies to you.

And then there’s a bug in Sudo—Sudo’s an application that’s used on a lot of Linux systems and is also used on the Mac OS. And what Sudo allows you to do is run with privileges only for using that command—you would say like Sudo you know RM minus R* something like that and it turns out there’s a hole in it that would allow somebody to run commands as root without knowing the superuser password so that’s obviously very bad. So you’re gonna see updates coming out for this and I said this applies to the Mac as well—I don’t know if this was part of their recent updates to the Mac OS, but I hope so. At any rate, there’ll be definite new patches coming out for that.
And then I want to talk about a new drive-by spam and basically up until now it turns out that when—if somebody sent you some spam, you could look at the e-mail message and generally speaking you didn't have to worry about infecting your machine or doing something like that. Now that's not 100% true but that was true most of the time. It turns out now though there's some new techniques that are being used where they're taking and putting HTML in the spam and it turns out just looking at the spam is perhaps enough to cause the problems. The messages that are coming along are entitled "Banking security update" but I'm sure by the time you hear this there'll be lots of variations on a theme there. I'm not sure what's gonna be done about this—one would hope that your antiviral software will be able to catch this kind of stuff. Look for updates there and I'll try to keep you posted so that we can see what's going on.

We did just talk about the HTC error and it turns out there's a bunch of Android malware (and HTC primarily builds Android phones—now this is doesn't just apply to HTC) but that what they're saying is that it is many as 5 million users might've been duped into downloading infected apps from Google's Android Market. Now depending on your version of Android you might not be able to download from Google's Android Market but—without doing a couple of things to your phone which are pretty easy to do and Google talks you through how to do it—so you want to make sure that if you are downloading that you're all set. What I would recommend that you do is before you download any app at all—let's just assume you use straight-up Google Android, you’re not using Amazon or anything like that ‘cause then all bets are off—but if you use the general Google marketplace for Android look for the number of people who are reviewing that app, look for how long that app has been around, how many downloads has it had. A lot of this information can be forged but if you've got 100,000 people have downloaded the app and 15,000 reviews and crazy numbers like that it's probably not something that they're forging. If you've got at app that's got five stars and two people have said it's the best thing since sliced bread, maybe you want to be a little cautious there. You know just be careful. And then if you're not using the app store that's great—you know just because you have an Android phone doesn't mean that you have to use apps, but my guess is most people who are using the Android phone or the iPhone are certainly going to want to take advantage of the apps at some time, the apps really do make the phones massively useful I think. And then the thing about this is, another thing to keep in mind, is they did sort of target specific groups of people I would say—people who are looking for something for nothing. So for example some of the apps were called "sexy girls puzzle" or the "ground counter strike force" you know like a game or something like this here. What I would say is these are the types of applications that lend themselves to this so just be very careful—if this kind of application that you want, knock yourself out but just remember that's the kind of application that these people to be targeting and you know you need to be a little more cautious when you get this stuff.
There’s also a hole in Samba. Samba 3.63 is out now and that's gonna close a security hole in Samba (and my guess is a lot of people if you’re running a system like this, you probably know this already) but please if you’ve if you got the Samba running on your system, go and grab that latest update because you don't want exposure your users to this problem.

I have a article here from Twitter about how to protect your Twitter account and it's just sort of the basics and things like that but what I think is interesting is they use some of the very same suggestions that we've used all along—using a strong password, are you making sure using HTTPS, and keeping your operating system update—all the same sort of things that we've been preaching here at University for a long, long time is the very same stuff that is being said by our folks over Twitter. So I'll post a link to this in the show notes as well, give it a quick look if you are Twitter user you might want to take care some of these things. If you're not a Twitter user take a look at it anyway because there’s a lot of good information in this article.

And then we've got 15 open-source tools for Windows admins and some of them are things that you might be using already, some of them are things that you might not. My only sort of complaint about this whole thing is it's put together an kind of like a slideshow mode with a couple of advertisements in the middle that I really hate that, I just wish they would just give you the 15 tools and here’s where they are, here’s where to download them is what they do instead of this one at a time “click here click here click here”—gets really annoying after a while.

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/.