Hello, I'm Roger Safian. Today is Thursday August 30 and you're listening to the information security news podcast brought to you by Northwestern University Information Technology.

I'm gonna start with the story about Oracle and Java and you know if you haven't been following this, sort of the short story is there is a vulnerability in Java 7 and Oracle comes into play because Oracle purchased Sun which made Java so Oracle has now taken over Java. and you know basically what it boils down to is there's vulnerabilities here, they're being exploited but not widely yet, but you know the assumption is that the exploits will spread and the number of machines that are being affected will go up. now there's workarounds for this here and I'll post a link to an article that's got some ways that you can protect your machines, but these are they're not easy workarounds. It's not that you couldn't do them but they're not easy. probably the one that seems like maybe the easiest to me if I had a recommend to my mother or somebody who's maybe not a very savvy person what's the best way to protect yourself for this particular thing, I might suggest using the two browser method that they'll talk about in this article. And basically what that is is you have one browser with Java and you only use that browser for going to a specific well-known trusted websites. You know and everything else you use this other browser that doesn't have Java. I don't how practical that is but it seems like one that would work and it's relatively easy to convince people just use that link when you want to go to say your bank or enter your hours at your automatic payroll at your employer. Anyway this vulnerability is out there, there is a fix for it right now but Oracle's not releasing it. Oracle releases their patches on a quarterly basis which means the next time Oracle is going to put out a patch is going to be October 16. And that's just way too much time for us to be waiting here. So I really do hope that Oracle steps up to the plate here, modifies their patching program, and at least for Java puts out the updates on a more frequent basis. that's certainly what Sun used to do and with a program like Java that's used in so many different things—when you think about it you know probably the average person must have half a dozen devices at least that use Java, I know it’s on my TV at home, it in my Blu-ray player, I'm sure it’s the phone, my computers, it's all over the place. Java’s something that needs to be updated and they need to updated on a more regular basis than just quarterly and it turns out that Oracle’s known about this problem for a good four months so they should have fixed this problem when they release their last set of updates which was I believe just earlier this month, I think right around the beginning of the month they put out some updates but maybe it was late in July but certainly they've had plenty of time to address this problem and they should've done that but they did not and you cannot have millions of machines all over the world vulnerable for you know six weeks, that's just unacceptable in my opinion. So Mr. Oracle if you're out there listening please changes your policy because it's pretty annoying for me and a lot of other people. I posted the links to
several articles about this particular story and you guys can read them when you've got a chance, it'll be in the show notes section.

Then I want to talk what the Dropbox service. Dropbox is one of these things were you put a file up there and you share the URL or login information with other people can go grab the file too. So it’s convenient for a whole bunch of things whether sure vacation you know pictures or your tax return, it’s a nice site. And Dropbox has had some issues and a lot of sites had issues and Dropbox is recently then upgraded to two factor authentication which is great. Now it's not an ideal situation as far as I'm concerned but it works reasonably well. one of the ways that you can do this is they’ll send an SMS to your cell phone so in other words what you'll do is log on to a site you put in username and password and whatever this code is that they would send to your cell phone. That’s alright but you know I don’t even travel that much and I travel enough to know that when I’m out of the country my cell phone typically doesn't receive SMS messages. Maybe there’s a way where we can do with e-mail as well but I don't know, they don't mention that. They do have some other options that looks like it might be able to also use, some of these tokens that you might get from your bank or your employer. But sort of the downside with it is what happens when you lose the token or your phone? You know they've got some recovery information here and that's where a lot of people are having their issues. What they're doing is they're issuing US what is a 16 digit backup code that can be used to unlock the account. So this requires the somebody is gonna put that code someplace where it's been a be safe. and I think for a lot of users that's a pretty big assumption, in fact I bet most users put it up on Dropbox so as soon as they lose their two factor they won't have the code either because it's on Dropbox in the first place. so I don't know what the solution is here, I applaud them for trying to come up with the two factor thing that's great but I really do think they need to find some way of ensuring that somebody doesn't get locked out of their account, this is a real issue for a lot of different sites not just them.

And then Websense really recently released some information about malware that's targeting BlackBerry users. Now I know I ignore the BlackBerry users out there and you know I occasionally see stories about the BlackBerry it’s relatively secure. Unfortunately BlackBerry’s market share has fallen really dramatically over the last few years and my guess is they’re not to be around for very much longer. But if you are using a BlackBerry I think we might be hitting a point now where those BlackBerry users out there are used to the security that they've always had an that may be eroding a little bit now and that allows the bad guys to take advantage of it. so this particular case what they’re seeing is spam that's sent to your BlackBerry that looks genuine, e-mail that's coming from BlackBerry, but it's not. and so you know what I would just encourage the BlackBerry users you know if you're still using your BlackBerry device, and it's a great secure device, that’s the one thing BlackBerry always had going for it was really it was a pretty secure device, so don't just rely on that security, rely on your own good
sense as well and check those messages and those links before you before you click on it.

And then a couple last stories that I've got. one is about Facebook spam and basically you've probably seen stuff like this here you know what “you've been tagged in a photo” or “is this a new photo of you.” this is spam going around and it kind of looks like a message from Facebook you know I get messages from Facebook that I've enabled on my accounts, you may as well. So just be cautious again similar to the BlackBerry story out there, it's similar to other stories that we've had in the past, you need to be very careful about links in e-mail messages that are easily forged, it's done a lot, and it's just not a problem that could go away so you really need to be careful before you click on those links.

And then we've talked a lot about password security and Wi-Fi and some of the issues that are out there with WEP and WPA and things like that. so there's a great story here in Ars Technica about a guy breaking into his neighbor's Wi-Fi network and breaking in is loosely used, I mean he asked his neighbor “can I try cracking your stuff over here” and it's just pretty interesting to read how long it took to do it. and this is not necessarily you know uber-hacker over here this just a regular guy, you know a pretty sharp guy, but using common tools he was able to get off the net for free or for very low price. So especially I'd say if you're living in an apartment building you might wanna look at this here and give some thought to your own Wi-Fi security.

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.