Hello, I'm Roger Safian. Today is Thursday, February 16, and you're listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

We'll start with the updates. And of course it's Patch Tuesday was just this past Tuesday, so there's lots of updates from Microsoft. Looks like they're releasing nine separate patches but these nine separate patches patch a variety of different programs so you might update 10, 15, 20 different things on your machine because of these here. When I did apply the updates, it took a while—I mean of 10-15 minutes or so—before the patches were completely applied and you had to do a reboot. Now I think that it's important these things get applied as quickly as possible but there is one—if you if you can only afford to do one right now, go over and apply the one for Internet Explorer because that's probably the one that's can keep you at the most vulnerable, and apply the others when he get a chance. but don't let it go too long because you know how it is when these things come out, they're out there attacking all the time so you want to get them fixed as quickly as you can.

And then while you're taking care of the updates, Adobe came out with a new version of Flash. Looks like it supplies to just about everything, I see Android, Windows, the Mac, Linux, Solaris, so pretty much everything is getting a new version of Flash. and Flash is another one of those things that gets attacked quite a bit so make sure that you've got the latest version on there. It doesn't update itself automatically just go to the Adobe website and you'll be able to get a new version of it there.

We talked about Twitter last week and in particular their security guide and it turns out this week that twitter is going to make the HTTP S connections the default on their system instead of allowing people to use HTTP or HTTPS. Now this is great, I like this a lot and Facebook currently allows users to choose and I hope Facebook does the very same thing—makes everybody use HTTPS so then you got a secure encrypted connection to send your data back and forth. Google in case you're interested already does this so that's great. It's time for Facebook to join the crowd that's the whole point of this story.

And then I know that, myself, I always feel like during the holidays the spammers and the phishers and all these things just increased drastically. Turns out company's actually done a report (I don't know where they gathered the data from) but what they're saying is that yes, it's true, during holidays phishing attempts go up and I think we've all kind of instinctively just known that but what they're saying is the holiday with the biggest increase is Labor Day with a
whopping 1353% increase which, boy it seems like crazy amount, followed by Columbus Day which is 549, so boy, that Labor Day stat really stands out. I'll post a link to this article, you can read it on the Web site, it's kind of interesting.

And then the U.S. Senate is coming out with a cybersecurity standards bill, which I hope actually passes. We need to have some sort of standards and at the moment it concerns me that just anything can happen. people can use standards if they want, they can they can use whatever standards they like, maybe they use NIST or maybe these one of the ISO standards, or maybe they use nothing, and I think this is part of the reason why we have the number of breaches that we do have is there's no standardization, right? People just kind of run it however they feel and that's never a good thing, I don't think, in this kind of an industry.

Now a couple things, I'm a little disappointed that the bill doesn't say “Look, you have to use this standard as a minimum or something else,” right? I mean, if you just—the bill is very open which is—can be good, can be bad but if you just allow people to say anything is a standard, well they're gonna choose a pretty poor standards. So I really wish they would beef that up a little bit. and then just to be clear this is only going to be applied to systems that they consider critical, so maybe the system where you read your favorite blog or something might not be part of this set of standards, but maybe the service that they get their connection from would be. Now what I would hope is, once this set of standards gets out there, is that other organizations, even if they're not—this doesn't apply to them by default—would just adopt this as their standard. That would be great, love to see that. So kudos to the Senate.

And then Google is having problems with the Google Wallet again. They had some problems last week and it looks like it's continuing. Hopefully they're getting it address soon. It looks like that this is a way where somebody could clear the data that was in the wallet which, I don't know if that's necessarily a bad thing. I guess what it says is when they do that then you're forced to reenter the pen again and so that they could I guess if you have a key logger or something like that—it sounds a little convoluted but nonetheless it's an issue and I'm sure that Google needs to address it and it's gotta be serious enough because Google did take the wallet down again for because of this hear so that's not good.

Let's see, what do we got? Oh, the Apple. A couple stories about the Apple here. And the first one is something in Mac OS X and it looks like Safari is actually the culprit doing this here. and basically there is an event called Quarantines Events and it's keeping track of all the downloads that you make on the machine, even if you clear your download queue this log file that is written is just sitting there. And I hate it when they do stuff like this. I don't mind if you create some sort of log file because something's happened unexpectedly, something crashed or you need an error report about something, or you need to create a log file about just generic information, performance sort of information things that, when you log specific things—URLs that were visited or in this case files that were
downloaded, that sort of stuff—should only be done on the rarest occasions. Users should certainly be given notice about it and they should be given the option to clean this sort of stuff off of their machine easily. And Apple hasn't done that. Apple wants to portray themselves as being a good noble, fair company—well they should not be spying on their users that way. And so I hope they clean this up and my guess is Apple will address it and I hope they do soon.

Then there was talk recently about Apple's iPhone address book and how apps might use that address book in ways that you might not necessarily be aware of. And I think in some cases apps tell you—Facebook for example says when you when you try to load the mobile version of their app, “Hey, I'm gonna use the address book to see if you've got people” and I believe they even give the option to say like “yes” or “no” there. But some places don't and that's not a good thing. And so again I'll a post a link to this article on the news site so that you can take a look at it. but it worries me that there's so much information—I mean I don't have an iPhone, I have an Android myself—but there's so much information in your address book these days, I find myself putting more and more stuff and my guess is you do as well, and so that becomes something that you really need to protect.

And then there’s a great article that was in the New York Times and this is about—it’s called “Traveling Light in the Time of Digital Thievery." And basically it's “when I go overseas, what should I take with me and how should I protect it?” and the author’s primarily talking about trips to places like China, but you could use this information for anywhere, and it's really pretty interesting. Now what I would say is I love the idea of when you're going overseas, taking a loaner laptop or something like that with you especially an older, if you've got some older laptop that you're not using anymore, you could just wipe it out and put the stuff on it that you need so you keep in touch via e-mail and stuff like that. That's great but don't just take everything with and give this article a quick perusal. and then remember when you are—no matter where you're going, you could be just out of state—always do things like use the VPN in order to make sure that your connections are safe, make sure you're up-to-date on the patches in your antiviral software, turn off things that you don't need on your computer like maybe Bluetooth or cameras, things like that. If you got encryption, make sure that you're using encryption, a variety of different things. So take a look at this article, hopefully you'll find it pretty interesting.

And then I read what I thought was a very disturbing article about Nortel Networks and—Nortel is out of business, they've declared bankruptcy and their chief executive officer’s on trial right now for fraud—and what it turns out is that Nortel had a data breach several years ago and they knew about it and it sounds like they basically did nothing. Some stories are suggesting they tried to contact the Royal Canadian Mounted Police about this but didn't really get very far and just never followed up. Not sure if that's the part of the fault of the RCMP or Nortel, my guess is there's a little blame to go around both sides. but then what
they did is later on they sold, to the tune of $4.5 billion, patents on items that they knew or should have known, anyway, had been compromised in this breach. And for me this is kind of disturbing. I know when a breach happens, it's not a good thing; it's happened here at the University and in other places it's happened, nobody looks forward to this here. But when it does happen, you have to think, you have to be open about it, you have to make sure that you address it, and you have to do so in a very transparent way so people can trust you. When you read about this stuff after the fact, I think it really sullies your reputation. In this case it doesn't matter, the company’s out of business, but for other companies certainly I think it will matter.

Anyways, 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/.