Hello, I’m Roger Safian. Today is Thursday, May 31, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

The first thing we’ll start with is updates and all I want to talk about is a new release of Chrome. So if you’re a Chrome user out there, make sure that your version of Chrome has been updated yet. By the way, you can check to see if you've got the latest version of Chrome if you go to the About box, it'll tell you right at the bottom with your current or not. If you're not, just do the update you'll be fine because it does fix some security problems and it's always good to keep the browser up-to-date. Browsers are certainly one of the big methods of attack on the network these days.

and the speaking of Chrome this makes me think—don't ask me how I jumped this way, my mind works in mysterious ways—but iOS. I just saw an interesting document that I haven't completely gone through but had a ton of great information and it was from Apple on iOS security just released a few days ago. So if you've ever wondered just how do things work on the iOS operating system, this is your opportunity to really get a good view of that stuff. So please take a look at it if you’re interested in iOS security. I’ll put a link in the show notes, just go there and click on it and you'll be fine.

And then I saw an interesting report, now this is from McAfee so I'm sort of jaded when an antiviral company talks about issues with people not using antiviral software, but it's an interesting report nonetheless. Basically what they're saying is that a large percentage of PCs here in the United States—they're saying nearly a fifth, 19%—of the PCs here in the United States either have no antiviral software at all or the licensing for the antiviral software has expired and has not been renewed, so effectively the antiviral software is not been updated for some period of time. Now that's bad. I mean, antiviral software, while I concede it's certainly not doing the job that it did years ago, it's still a critical component keeping your machine secure. And this is true whether you're running a PC or Macintosh. You know that antiviral software is really important these days, so make sure that you got it. Now there’s free software available for Macs, there’s free software available for the PC. So there's really no excuse not to have antiviral software on your computer. If you do happen to fall into this 19% and you have no antiviral software on your PC, then just go to Microsoft, grab their Microsoft Security Essentials, it's actually pretty decent program and it'll do just fine for you. Sophos has got free antiviral software for the Mac, this particular study doesn't talk about that but my guess is the number of Mac users who don't have antiviral software is significantly higher than this number. So please get antiviral software.
Speaking of antiviral software, there was a notice of the FBI about us some malware—RanSomewhere, they call it. Essentially what this is is you get a message on your machine and it’s sort of threatening—in this particular case I think it says we found suspicious files on your machine, we’re reporting you to the FBI, you have to pay a fine, the files or child pornography. They make it seemed pretty bad and you know they basically dupe you into giving them some money. Don’t fall for these types of things. What you can do a lot of times is you go to website and that's where these things pop up. You’re not to get this type of notification typically through a browser, whether you've got child porn on your machine, or you got a virus, or any of these types of things, you’re going to get it through something else. So when you do get these things, if you want to assume the possibility that maybe it’s legitimate, just try the operation again, but try it with something else and see if you get the same results. If your antiviral software is telling you that there is a virus, if you open up your antiviral software it should find it. Don’t rely on, for example, something that you see that looks like your antiviral software that's actually not.

And then we talked about this story a while back but it's come out with some hard numbers. And this was the Thrift Savings Plan, this is a plan that's available to primarily I believe the military folks who were out there. So if you were in the military or you're still the military, you probably have a Thrift Savings Plan account. And they had a breach last year and what they're saying now is that 123,000 accounts might've been exposed, they're saying they're not seeing any data that suggests that anything happened. We've had incidents along those lines as well but what I would say is interesting about this here is it doesn't seem like they’re doing a lot of notification to the folks out there who are doing this here. And what I would encourage you to do is if you are in the military or you know somebody who is or was in the military, might be a good idea to just give them a heads up, let them know that there was an issue with their savings plan last year, to just keep in an eye on their statements, just make sure there’s nothing unusual going on. Better safe than sorry.

Oracle gets beat up here about the way they handle Java security and this is a report from Kaspersky, and there's a part of me who really wants to beat up on Oracle as well but I won't. What I will say is that there's certainly room for improvement in the way that Java handles things and I do hope that they'll look at this here. If I've gotta beat up on Oracle for one thing in particular, it's gotta be in the way that they handle their updates. The quarterly updates for Oracle is—they're just atrocious, and I certainly hope they're not start doing that with Java as well because Java—I just don’t even want to think about it.

I saw good guide here about Facebook. And whenever I see this kind of stuff, I figure most people, certainly most people probably listen to this podcast, are using Facebook and Facebook security is pretty important. A lot of personal information is out on Facebook these days. And so every time I find something I think is interesting about Facebook, I try to bring it forward. Anyway this is the
“Inside Facebook Security” and it talks about how Facebook works on these things, and it’s pretty interesting reading I thought. So again I'll have the link in the show notes, please give it a whirl if you're interested in that.

And then I found something for passwords and the title here's “How Long Would It Take To Crack Your Password?” And it talks about password security, and password myths, and things like that, and a lot of these are things that we've discussed especially since we changed our password policy here at the University a year or so ago. What's interesting about this is they do have a little tool that you can use—and I am somewhat reluctant about these things but this came from a good source, so it's Sophos, an antiviral company, I guess I'm cutting them a little slack—but what they've got is tool on this page where you can pop your password in and you can get an idea of how long it would take crack that password. And it doesn't tell you exactly “I could crack that password in 3 minutes,” what it tells you is “I could crack that password in less than a day, or less than a week, or centuries.” I think that's the one that you're really looking at, I did a little poking around and it doesn't take that complicated of a password before you get into the “century.” So if you're thinking about password security at all, go ahead and play around with this a little bit and create a password where it’s gonna take centuries. I think they're pretty easy to fall into that and it's a good thing.

And you know how I'm always picking on mobile banking? I really do have lots of concerns about people who use these apps do their banking from their cell phones, it just kind of really gets me. And it turns out there's a story 8 out of 10 mobile banking apps are vulnerable to hacking. Now that may be high and certainly hacking in the mobile world, I'm not quite so sure that's an accurate term. But be that what it is, what it does say is that mobile banking apps are not secure, certainly many cases. So please, I'll continue to harp on this, be very cautious about using mobile banking apps. I think it's just dangerous, it's a dangerous activity to be involved in.

And then we don't often talk about Linux and malware, but it's out there. And somebody's put together something called Linux Malware Detects, so if you're running a Linux system you can use this to see if there's any malware on your system. And essentially what it does is it creates an MD5 hash of the files on your system and then compares those to the empty five hashes of known malware. So if you get a match, probably that's the malware package that you might want to look at getting rid of from your system. And I think it's kind of interesting and I believe that it's using hashes from several of the different antiviral packages so you get kind of a cross section there which I think is pretty useful.

And then a couple stories that I read the kind of got me thinking—and that's never a good thing. But the first one is “Words To Avoid Using Online If You Don't Want The Government Spying On You,” and basically what this is is
supposedly these are words that the government is searching for on the network. When you’re using a word like “nuclear device” or something like this, you could see how that might be something that might be interested in. But it turns out that the words that they’re searching for are much broader than something like “terrorist” or “nuclear devices” or something like that. So for example the word “pork” is one of the words that they’re supposedly searching for. It just seems like this is—if this is true, I’m not sure exactly why they care about the word “pork.” I like pork chops, I like pork ribs, yeah I mean, Porky Pig, is that a problem? I don’t know. Anyway it’s interesting reading nonetheless, so if you’re interested in this kind of thing, go ahead, there’ll be a link, grab it.

And then the last thing was, it’s an old article but somebody put it up on something that I read. And it was from 2003 and it’s from the Harvard School of Law and it’s interpreting access and authorization and computer misuse statutes. And I love this kind of stuff. It was really pretty fascinating, it’s really well written too. So if you’re interested in the law, and as I said it’s a few years old already, but again it will be in the show notes, give it a whirl.

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.