Hello, I’m Roger Safian. Today is Thursday, May 24, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

We’ll start today’s news with the Facebook. And Facebook has obviously been in the news all week long, they just had their IPO last week on Friday or Thursday, I don’t remember the exact dates, there were some problems on NASDAQ when the IPO went in, and the IPO didn’t do as good as I think people are were expecting it to do, at least a stock price didn’t accelerate the way people thought, and now there's already a lawsuit—welcome to the to the world Facebook, boy what a bad way to come in. You know, you just come in and problems, problems, problems, it's kind of a shame. Anyway what we're talking about with Facebook is a story that I read that came out actually just before they went public and it was essentially, how do criminals make money? And how criminals use Facebook? And this is nine ways that criminals use Facebook. And it's not Facebook like you or I might use to keep in touch with each other and stuff, but some of the scams and things that they do on Facebook. So it's kind of interesting to read at least from my point of view because it gives you the opportunity to see what is the other side doing and what can you do to protect yourself. So as I always do, I'll post a link in the show notes so that you can take a look at this here and read it, I thought it was pretty interesting and hope you do as well.

And then I read an article here about spam with malicious attachments is rising again. And I haven't really seen this myself, I guess I'll believe the report here but you know it used to be, years ago, malicious attachments and spam and these would be like zip files or .exe's, things of those natures, all the time I would see it, just all the time. And it pretty much went away. Links and things like that would show up. Certainly there have been a handful of malicious attachments and I think part of the problem may be why I don't see this as much is we do have, here at the University, filters and antiviral technology that's looking for this kind of stuff. So if it does come in e-mail message there's a pretty good chance of it'll get filtered off. That's probably true also for Google and Yahoo, places like that, so I don't think it's a very effective way to deliver malware. But I guess it's on the rise, who knows why. It's according to some of the statistics here 1.14% carry the attachments and if you talking about 300 million malicious attachments just 1.14% —why am I having so much trouble with that anyway—that's really something. Anyway take a look at this here, it's kind of interesting to see how this stuff works, especially how this the spammers are evolving. For every new technology or countermeasure that you put in place, they'll come up with some new technique or way to get around it. And you know that's just the way that life is, it keeps us busy all the time.
Speaking of changes, Android. Sophos, a traditional antiviral company, has got a antiviral app for your Android. It's in beta, I would not encourage you to run right down download this app. What I would encourage you though is to take a look at it to see what they're doing. to me it seemed kind of interesting, I'm a little reluctant to tell you to put a beta app for antiviral software on your Android, just because if something goes wrong you know it's going be a pain to not have that device, and I'm sure that it won't—I'm not saying against Sophos—it's just the nature of beta software is it’s still in development, there’s probably still some bugs there, they need to get a wider test. Now if you happen to be one of those people who likes living on the edge, then this is definitely for you: grab and install it and knock yourself out. But if you're conservative, this is your phone, this is your tablet, and you wanna make sure it's available, I might wait until the actual product is available before I installed the software.

Now something that I've talked about an awful lot is financial websites’ online banking, especially using mobile devices. There was a story that caught my eye right away “Unseen dangers of financial websites.” and basically what they're suggesting is that the financial websites are not paying enough attention to some of the stuff that surrounds their websites. In other words they might try very hard to protect your account information and your login information things of that nature, but it looks like the financial websites are not devoting enough energy then to the other aspects of their websites: “click here for help" or something like that, and that's a bad thing. So this is kind of an interesting article, a new twist on it, at least it was for me, and I thought it was a good read, the author spent a lot of time talking about stuff, it was pretty lengthy so give it a whirl.

And then you probably have heard us talk about DNS changer over the past year or so I guess since that first came out. Google is going to start notifying people who have this software. Now there’s reports that 1 million people could still be infected with this malware. And what Google is going to do is, when you do a search from an infected machine, Google’s going to put up a warning across the top of your machine or the search results page that your machine’s infected with this software. So you definitely want to take and pay attention to this here. It’s bad software, it needs to be cleaned up, there's a lot of ways to do it too. So please if you see this result come up when you do a Google search definitely you want to take action to make sure that you get your machine clean.

And then something that we just talked about, and in fact we just had a Tech Talk here on campus, was about trips with your computers. And here's another story about the business trips and common precautions that you might want to take when you're traveling in order to make sure that you're safe. And some of the stuff is things that we've talked about here many times: updating your software and keeping backups and things of that nature. So I’m gonna place the link again in the show notes, there’s a lot of great information here. Please, if you're going to travel and you have to take your machine with you, make sure that it's secure.
And then the last thing I wanna talk about was one of these infographics that I found. And this infographic is about free Wi-Fi: friend or foe? And I love this sort of infographic technology and wish I was creative enough to do something like this myself where you essentially briefly put some information but you put it in a graphical format that think a lot of people can relate to and easily understand. My only gripe about this is I wish the infographic was small enough or formatted so that I could put it on a poster or and 8 ½ x 11 sheet of paper and put it up in the break room or something. It’s not unfortunately, but there’s a lot of really great information here and it’s really well done. So please I hope if you take nothing else in the podcast today, take a look at this one link and look at this infographic because I think you’ll find the information there very useful.

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.