Hello, I'm Roger Safia. Today is Thursday, February 9, and you're listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

We'll start today with updates to PHP. There's a new version of PHP 5.310 and PHP is used in Web servers and frequently when we do see Web servers attacked, PHP is one of the methods that the bad guys use. In fact almost exclusively we see Web server attacks involve PHP. So if you are running a Web server make sure you grab the latest version of PHP because it is something that's attacked quite often.

And then I wanted to tell you about a tool that I found—and there's other tools out there but I've found this tool and decide to give a try and it works pretty good so I'll let you try it as well—it's called Do Not Track Plus. And basically this is kind of like an ad blocker and what it does is it looks for software built in to Web servers that is trying to track you. So you might've noticed if you go to a website and you search for “buying a new car” for example that a lot of the ads that show up on other webpages will all relate to buying a new car or special offers for the car that you are searching for, things of that nature. this Do Not Track eliminates all that stuff so when you run it you'll note that the ads that you get are not tailored towards you in the same fashion as they were before and in fact ads just disappear, very often they're not on the websites, so that's great. I happen to like it. Now I do have one concern about this particular piece of software and that is the licensing agreement—the licensing agreement is basically nonexistent, it looks like somebody took a template that said “put your licensing agreement here” and they just typed in “hey is my licensing agreement” and that's all it says. So it worries me that at some point they'll maybe change that and who knows but that's my only concern. Other than that I'll put a link to this in the show notes you'd give it a whirl if you like, looks like it's available for most of the major browsers right now so you can feel free to use that.

And then last week we talked about a privacy guide for Twitter, this week we've got one for LinkedIn. And the LinkedIn one is actually, I have to say, is pretty good. It's not written by LinkedIn, it's written by a vendor and it's really well done, I mean a lot of pictures, it makes it really easy to explain what's going on. I would really encourage you to give, if you are a LinkedIn user, definitely give this a try because I think you'll find it very useful. And then while we're talking about social networking there's more of these scams going on on Facebook. And you've probably even seen this here, I know I have, it's a message something along the lines of “The United States declares war on Saudi Arabia” and you know when you get the sensationalistic headlines on Facebook, just don't click on that link. It
almost always, it's going to be bad and in this particular case it's rogue antivirus is being installed on your machine. so just don't trust Facebook, I mean that there's things that it does, and there's things that it does well, and there's things it does not so well. This is one of things I just don't—it's not it's not made for this. If you're if you're worried about whether or not something took place, go to your favorite news site and likely it will be the very first article that's there. I'm not seeing Facebook scooping all of the major news players when it comes to things like this here.

There is an update to the Android market. Google has apparently been testing this for some while some while but now it's pretty much there can use all the time. And basically what this is is they've got a tool in place that's going to scan the software, the apps, before they're available. And this is pretty—this is a good idea and I my assumption is that Apple has similar sort of tools available on there's. It's called Bouncer, basically it's looking for known problems whether it be malware or privacy issues, things of this nature. I think it's a good sign, it's something that needs to be done. and as you know from listening this to podcast there's definitely—the way that apps are handled in the Android Market and the way that apps are handled in the iTunes Apple market are definitely different. and it basically boils down to this: Apple has a lot of control over what goes into their market, they're very controlling about that, that's got good sides and it's got bad sides. Google takes the opposite approach, anything can go in on it, so it's got good sizes and it's got bad sides. They're trying to address malware concerns here and I'm sure this will help some, but I think that what's shown is that a large chunk of bad apps come, not from the Google market, but from these other markets that are out there—you don't just have to you download your apps from the Google market, you could get it from lots of places. so I encourage this, I don't think it's going to be a silver bullet because there's lots of places where people are getting these bad apps and this only addresses the one market.

We've talked a bit about the DNS changer, the Operation Ghosts Click malware bust, that happened a few months ago and it looks like there's still a lot of people still infected with this here. Now I put up an eye chart, a DNS changer eye chart, a few weeks ago, you might want to go back to the show notes on that and take a look as that'll tell you if you're infected or not with basically just one click, so that's pretty useful. But it looks like, surprisingly, half of the Fortune 500 companies might still be infected with this as well. Now it's one thing to assume that it's difficult for me, the home user, to keep my machine safe but when you think about Fortune 500 companies you're thinking an IT staff and rules and regulations and you'd think they'd be able address this—kinda surprised and I hope they do get to this here because this type of malware just, it should be gone by now, there's no reason why it should be sitting on their machine.

Quick story about Apple—if you are an Apple user there's a tool out there that will crack the encryption on FileVault. And basically what it does is the key for FileVault is stored in RAM, so you boot up the machine, you type in the password
and it what happens is this tool is able to going to RAM, grab that key, and then brute force it. And that's not a good thing and I hope that Apple is able to address this because FileVault is really a pretty useful tool if you want to keep your stuff safe. I should tell you though it's probably not the end of the world because it's, again the key's got to be in RAM. So as long as you're not saving your FileVault password so that it's automatically in there every time you start up your machine, if somebody was to steal your machine the password would not be in RAM when they restarted. This is probably a good reason for you to want to shut your machine down when you're moving it and not to sleep it and open it up all the time. I know that's a hassle but you definitely want to think about doing that.

And then I want to end with a story that I can't believe this here, and it's Motorola, they had some Xoom tablets refurbished and they sold them on Woot. And apparently they had a lot of them, the article here says 6200 of them, but about 100 of them they sold on Woot that did not erase the previous user's data. they basically—I don't know what happened some sort of slip up or something like this and Motorola is working with customers in order to make this right by giving them protection and stuff, and I hope they're doing it on both ends: not just for people bought these but people that had a return of Xoom to Motorola. This type of thing should not happen. I just don't see in this day and age how a drive can leave a shop, a factory, whatever with data on it and I would encourage you to think about this for your own personal use as well. When you're getting rid of the device—be at your old laptop, your desktop computer, your smartphone, whatever happens to be—make sure that all of that data is gone. Take the drive part of the computer before you donate it to somebody and just destroy the drive. Make sure you remove that RAM chip and delete all of your contacts and stuff from your phones. There’s no reason in this day and age why data should just be walking out the door like this here.

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/.