Hello, I’m Roger Safian. Today is Wednesday, December 14, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

I want to start out with the updates that are available, and there’s a bunch of things that got updated this week. Microsoft had their patch Tuesday yesterday, so there are lots of updates for Windows. You should definitely plan to spend a little extra time when those updates come out because it’ll take a little while to install all the various things that are being updated, lots of their not only Windows but some of their layered products, Internet Explorer and Office and things like that all have updates as well, so it’s going to take a little time. It’s interesting that it looks like Microsoft had to pull one of their updates. They were going to have a fix for the SSL vulnerability that came out, oh, a couple months ago I think that we might’ve talked about that, and it looks like they had to pull that because it was causing some problems, so that’s unfortunate, but hopefully they’ll fix whatever the problem is and it’ll be available for next time. In addition to updating Windows, there’s Chrome. If you’re a Chrome user, there’s for Windows, Mac, Linux, who knows, maybe there’s even a new version for your Android, but Chrome, I think it says here, 15 vulnerabilities? Wow, that’s an awful lot that it’s taken care of. So if you’re a Chrome user, go ahead and grab the latest version of Chrome. And Adobe has released some updates, ColdFusion updates, but it’s interesting they have not yet released the updates for Acrobat and Reader. There are vulnerabilities there that still haven’t been fixed, and I was under the impression they were supposed to be out. Maybe they’re going to be out by the time you hear this podcast, but keep an eye out for that, because the Adobe stuff gets attacked quite often, and I know there’s active exploits going on right now, so you’re going to want to keep an eye out. As I said though, I really thought they were going to have this fixed, so it may very well be patched by the time that you hear this. Speaking of Adobe, if I’m not mistaken, there are also vulnerabilities in Flash, so keep an eye out for an update to Flash Player as well.

And then I want to follow up on a story, a couple stories that I read, that have kind of a relationship, and that is, one was a story I read in Wired called “Think You Can Hide, Anonymous Blogger?” And basically it talks about tracking down an anonymous blogger, and it’s kind of interesting. If you never have really thought about the stuff that is available about you online, even if you think that you’re anonymous, you might not be. So this is kind of an interesting story, and the fact that it kind of goes through the steps of how you figure out who a
person might or might not be, but it also gives you some suggestions about how you might, if you needed to be anonymous, how you might in fact take additional steps to protect yourself. Along these very same lines was, basically I guess it’s a service that I found, and it was from an article that I read from Brian Krebs on Krebs on Security, and basically the service is called “Youhavedownloaded.com”. You plug in your IP address into this, and basically if you connect to it it’ll grab the IP address that you’re using, and then it’ll tell you if you’re in any of the downloading databases that it’s compiled over some number of months. And, you know, this is not by any means a perfect solution, the youhavedownloaded thing. You know, I mean, there’s people who are downloading from behind their wireless router and so, and so then you would have a NATed address or an RC1918 address anyway, and there’s obviously some issues, but once again, if you thought that what you were doing you were completely anonymous while you were doing it, think again, and what I would say to you here is that, more and more, you can expect that the information that is available about you online is going to be more easily available, is going to be in databases and search engines that are going to be geared towards finding this stuff out. You should pretty much expect that if you do anything online at this point, anything, that it’s going to come back to you. So just sort of keep that in mind. I’m not saying that you should or shouldn’t do something. I’m just saying, be prepared that if you are doing something, that you know it’s about you, it’s going to come back some day and you’re going to have to be able to defend your position.

Then I want to close up here with a story about a message that was sent out. It looks like Verizon, somebody did something wrong and sent out a text alert message to residents in New Jersey. There’s a picture on a CNN iReport of what this might look like on your smartphone, and basically it was kind of like “Danger, Will Robinson, take shelter immediately”, that kind of a message from a national Emergency Alert System, and I can imagine how getting something like this would be pretty frightening, especially middle-of-the-night sort of thing and everything. What I would say is, look, these types of things are going to happen, and lots of different corporations, companies, schools, our University for example has got a text messaging system. It doesn’t hurt to double-check these things. Perhaps you can’t check it for your, say your University, your school, your place of business, but you can definitely check this stuff out when it says it’s from the national Emergency Alert System, that stuff is going to be online, and you should definitely, before you run to the air raid shelter, take a moment to just find out what’s going on. And then if something like this is happening, take a moment to make sure that you do things that are going to help you. Hopefully by now you’ve got a grab-and-go bag or something that has you ready to go in case of an emergency so that you can grab this stuff and go. If you’re not familiar with that sort of stuff, just Google it, and you’ll find all sorts of information. I think the Department of Homeland Security even has a web page up about things that should be included in it.
And then I do want to close with a little reminder about holiday shopping scams. Please, be careful out there. There are lots of scams going on. There are lots of bogus e-mails being sent around. Just take a little extra time online during the holiday season. There’s an awful lot of Grinches out there, and you don’t want them to ruin your holiday. 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/.

- Information Security News Podcasts Archive
- NUIT Home