Hello, I’m Roger Safian. Today is Thursday, October 6, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

We’ll start with updates. First of all, I want to talk about Chrome. There’s a new version of Chrome out that fixes several security bugs, so good idea to get it updated. My version of Chrome would not update for some reason; I had to try several times and I was looking around to see if there was a button that would make it update, and finally I went to the Help box or the About box, I don’t remember which one, and finally it started doing the update. I’m not sure what the problem was there, but you might want to double check and make sure that your version of Chrome is updating. I don’t know if this was just something that was a problem with me or more of a general problem, but what I would say is when you’re done, don’t forget to relaunch Chrome so that you’re sure that the updates are actually applied. And then there’s a new version of Firefox and SeaMonkey that’s out. And basically what this is causing problems with is a program by McAfee called ScriptScan. And I don’t know how many people are using this here, I don’t personally use this combination myself, so I do know that according to this article that I read, it’s a problem that’s been known since September. McAfee is working on a new version of ScriptScan that will address this problem, but right now it’s still an issue. So if you happen to be running this combination, you might want to be aware that likely you’re going to need a new version of ScriptScan and the Firefox folks are telling you right now the best solution is to disable that utility. And I hope McAfee, McAfee’s a good company, my guess is that they’re probably going to have this out before you even get a chance to listen to it, this podcast. Then there’s Firefox 7, and, again, new versions of that, they’re always coming out with new versions, but what they’re saying is, what I thought was actually interesting about this here was that they’re trying to put it on a “diet”, is what they called it. There’s just a lot of bugs in Firefox, there’s a lot of updates, and I guess the program is just getting kind of hoggish. And I’m glad that they’re trying to fix the problems - hey, that’s very important - but at the same time you want to make sure that these programs don’t get out of control, whether it’s taking up disk space, taking up memory, whatever - resources aren’t unlimited. I think sometimes the folks who put together these packages don’t realize that, so I wanted to give kudos to the folks at Firefox for actually taking the opportunity to not only fix their product but also to make sure that it’s being done in a way that’s respectful of the resources that their users have. And then last for the updates was Skype, specifically Skype for iOS. This fixes cross-site scripting vulnerability, so - Skype’s really popular - if you haven’t grabbed it already, go and grab the new version of Skype, and make sure that you apply that update so that you’re good.
And then I just sort of want to talk about some other stories that kind of caught me. One was, the title was called “The Future of Malware”. And I kind of like these stories; I don’t know why. I don’t actually “like” them in the sense that like, “Oh great, I want to hear what they have to say”, but I think it’s kind of humorous, especially when you look back at what people have said over the years. But in this particular case, I think this story’s probably pretty close to being right on, mainly because when this guy’s talking about the future of malware, he’s talking about stuff that’s happening right this moment, so his future is apparently our reality. And I think his future is, there’s going to be a lot of social media, a lot of social networking, a lot of social engineering, all of these types of things causing problems for people. And we’re seeing that already, we’ve been seeing that for a long time. And then also, he’s, you know, people going for the money, I know that he mentions in here the things like the smart wallets and stuff like that where you have online shopping and credits and, yeah, absolutely true. My one sort of gripe about this is, this is an article that’s filled with jargon, and it’s filled with jargon that’s, you know, is it really even necessary? I don’t necessarily want to pick on this guy. I think it’s the security community has some sick compulsion where they have to, every new thing that comes along, they have to give it a new term, and I don’t know why. The one that caught me here was “whaling”, where you’re going after the CEO or big corporate executives and stuff like that. Why do you have to give it a new big term? Why is that important? It’s not important, and I think it makes it confusing for users: our message gets confused, people don’t understand all this stuff, and I wish we would just quit doing this. But I encourage you to read the article just to get your taste of what he has to say.

And then an article about Chrome. Remember we just talked about updating Chrome, but basically they tested some of the Chrome extensions, and about 25 percent of them had issues. What I thought was interesting was not in the numbers of extensions that had issues, but also that they tested 51, and of the 51 they said 49 of these things could have been resolved by adapting some extensions to content security policies, and I thought, “Well that’s pretty interesting”, because the number of people who probably have these on their machines, reasonably great would be my guess, and probably most people could solve their problems with just a couple of fixes. So what I’d like to know is, why aren’t these fixes just sort of in your face? If they’re going to solve the problem, why doesn’t Chrome or why doesn’t the company or person who put out the extension make these fixes just pop up and say, “Hey, there’s a security risk here. Would you like us to address it, yes or no?” Why do we have to rely on the users in order to do this? Because I think that’s a mistake. People want to be able to use the computer as a tool; they don’t necessarily want to become the computer security genius.

And then last, but not least, Facebook partnered with a company called Websense, and basically what they’re going to try to do is go through all the stuff that’s on Facebook, and these malicious links that are out there, they’re going to get rid of them. And in the future, hopefully
Websense will prevent these malicious links from showing up, or at least if they do show up, when you click on them, you’ll be notified that there’s something going on that you need to be concerned about. And that’s great; I’m glad to see that Facebook is taking this stuff seriously. I mean, I think we’ve talked about this before, but it’s nice to see when a company makes this sort of a change that it’s a real positive here, and I think this change to Facebook has made, this one particular change, is going to be a real positive. And one of the reasons I think it’s going to be a real positive is it’s not requiring any real intervention on the part of their users. You don’t have to go and change some setting in Facebook, you don’t have to do anything, it’s just going to be there. And I think that’s what we need to rely on. We can’t constantly rely on users going in and making some change, click this box, do that, because that’s just too confusing, there’s too many of those things going on.

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/.

- Information Security News Podcasts Archive
- NUIT Home