Hello, I’m Roger Safian. Today is Thursday, October 13, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology. This podcast is going to have a lot of stuff about Facebook, so if you’re not a big Facebook user or a fan of Facebook, when I start talking about it, you might want to just end it right there.

But we’ll start with updates. Both Apple and Windows, there are updates out for both of those operating systems. The Windows updates are pretty much typical, what you’d expect, you know, it’s patch Tuesday just happened. There’s a moderate number, I think 8 or 9 updates happened on my computer, and it’s important to make sure that you get your machine up to date as we’ve talked about many times. With Apple it looks like they updated just about everything too, and so don’t forget that after you’re done updating your machine, make sure if you’ve got other Apple devices that you’ve updated those as well. Maybe it’s iTunes on your PC, maybe it’s Apple TV, maybe it’s your iPod, there’s updates for all of these things, so make sure that you go and grab them, because you don’t want to be behind when these things are out there.

And then another story, and the only other story that I’m going to have that doesn’t deal with Facebook, is about protecting your kids while they’re online. Now this is something that I think parents really do have to pay more attention to. I mean I think there’s sort of an inclination to assume that your child is at home, so they have to be safe. And that’s not necessarily the case when you’re talking about a computer that’s networked. If you’ve got a child, and the child has a computer in their room or in a space where you’re not available a lot of time, and that computer is online, you want to take some precautions to make sure that your child is safe because there’s all kinds of people in the world, and a lot of those people are on the Internet, and it doesn’t just have to be your child is out there in danger, now they can be at home and in danger. So I saw this article here, it’s from a report on Fox News actually, on protecting your kids, and they suggest some applications that you can - in some cases you have to purchase these things - that you can use in order to make sure that your children are safe. But what I would say is the best thing that you can do is just make sure that you know what your kids are doing when they’re online. That way - I’m not suggesting that your child is going to try to do something that they shouldn’t be doing, but they might not realize - you know, they’re kids, and they don’t have the body of experience that you do - so, if you’re just around and you know what they’re doing online, your child is going to be much more safe than if you just let the child do whatever they want on the computer and you just ignore it.

Alright, so now it’s Facebook time. Pretty interesting article from PCWorld about privacy settings, and they list 11 settings that you want to check on right now. I don’t know if you want
to check on them right this moment, but they seem like a good thing to do, to check on these privacy settings, and the reason that I say that is Facebook has been making so many changes lately that it’s pretty getting difficult. You know, one moment you check something and things are working that you want it to, and then they change something. Maybe they get rid of that feature altogether or they add some new feature to something that you don’t have. I applaud the fact that Facebook is trying to change and trying to evolve, and also it seems like they’re trying to take privacy a little more seriously, although these other stories I’m going to tell you might suggest otherwise. So, great, but you do have to go and set a lot of these things. I guess if I had to ding Facebook or many other services, a lot of times they make things available to you, but they’re off by default, and you have to go and set those things up. So, this is an interesting article; take a look at it, I’ll have a link in the show notes so that you can do that.

And then there’s a story that came out of Stanford Law School, and it’s a paper, and it’s gotten a lot of publicity. The student that did this, I gotta really give a lot of props to; the person really put a lot of effort into this, and I think it’s good to get to people talking about this, and basically it’s tracking the trackers. And what he’s saying is, “Look, it’s pretty easy to find people if you know their username”, and lots of people are tracking you. I mean, you go to, you know, Panera - I get my lunch at Panera and Panera I’m in their little Panera club and they know my username and they send me e-mail about specials and things like that, and hey there’s nothing wrong with that, but that - one more thing that Panera knows about me. And if Panera is sharing that information - and a lot of these places do - and what this person does is kind of puts together a matrix of who’s sharing what and what sort of information do they have, and it gives some real plausible scenarios how just relatively simple pieces of information, like a username, can be pretty easy to track somebody down. So, again, real props to this person, and I would really encourage you to take a look at this article and read it. And if you do read the article, go down to the bottom and read some of the comments too because I thought the comments were every bit as enlightening as the article, and I like the fact that the author has gone through and changed a few things and added a few updates and made a few more explanations; I like to see that sort of feedback from the community, and then that improves things, so that’s great.

And then the other thing was a story that I read, and basically what this guy did, he’s a European, and my understanding, I guess the way this works in Europe, you can contact a company and say, “Look, I’d like to know all the information that you have about me”. So what this person did, I guess he’s done it a couple times because he’s got at least a couple documents there, he contacted Facebook and said, “I’d like to know all the information that you have on me”. And so Facebook sent him basically a dump of all the information that they’ve got. And what he’s saying, I guess in at least in one case, is it was 800 pages of personal data. Now, some of this stuff is what you would expect, you know, who your friends are. But some of the other stuff, you know, where you’re logging in from, lots of different information
like that, IP addresses that you’ve used, names that you’ve used, when you’ve changed different settings, all of these sorts of things. And I don’t necessarily think that there’s anything wrong with this, but I guess what I do think is sort of really opens up your eyes when you see all of this data all in one place. It really gives you an idea of just how much a company like Facebook, or probably any other place where you do regular business, knows about you. And so I think that’s what I found really unique about this particular article was just put it all right out there and let you take a look, and it can be pretty shocking to see 800 pages - or maybe in your case, it’s less, maybe it’s only 20 pages - but I’ll bet most people never thought that Facebook had some double-digit number of pages of data about them. I never really gave it a lot of thought, and I try to keep track of these things, but I probably wouldn’t have guessed that, so thanks for this guy for putting this together.

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