Hello, I’m Roger Safian. Today is Thursday, October 20, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology. It’s gonna be a short show today, just a handful of stories.

I’m gonna start with a story that, I have a little bit of a negative bent on, from Microsoft. And basically, Microsoft, according to a report, says that users are responsible for half of all infections. And so, when I read this, I’m like, “Really? I mean, isn’t that kind of like Anheuser-Busch releasing a report about how beer is good for you?” I mean, this is, Microsoft is saying that the users are responsible for half of the infections - yeah, but they’re doing it with your operating system. You know, you should be taking precautions, as many as possible, in order to make sure that users can’t infect themselves because, let’s face it, most people want to use the computer as a tool to get some work done, to perform some task, to have some fun. They don’t want to become a computer security expert in order to do it. And I think that the fact that Microsoft could put some report out that basically shows how users are infecting themselves, it just doesn’t send a good message. So, I’m not saying the information isn’t true. I’m sure that it is in many cases; users are getting messages and ignoring them or, you know, clicking on links that they shouldn’t have, but you should be expecting that, and Microsoft should be taking as many precautions as they possibly can. And I know that they are, but still, I’ll put a link up to this report, and you guys can take a look at it. There is some interesting data there; one thing that, personally, I thought was interesting is that USB sticks amounted for a quarter of all the infections on Microsoft systems. That’s actually a much higher number than I thought it would be, I didn’t realize that sneakernet played such a big role. So take a look at this report, but let’s not blame the users for getting infections here.

And then, a good thing for Microsoft as well: they came out with something they’re calling the Safety Scanner. Basically, what this looks like is a - it’s an on-demand tool that you download, and then you run it, and it looks to see if there’s anything wrong with your machine. And it looks like it does a pretty thorough check. I ran it, and it takes an awful long time to run. Looks like it’s doing more than just Microsoft Security Essentials. So, my thought is, this could be useful if you’ve got a machine that’s acting up. Maybe you should download this and give it a whirl and see if it helps. It does take an awful long time, I was really surprised at how long it took, and then I didn’t think it had a lot of good reporting. It’s supposed to give you a report at the end, and it does give you some information, but it’s not very detailed. On the other hand, it’s the first time that it’s out, they’re going to hopefully keep this up to date, and it’s free! It’s
hard to really complain about that, so I just bashed Microsoft a little bit in the previous story, and now I want to thank them for taking the time to do this in this story.

And then I want to talk about Google here. There was a story that I saw in Wired that basically said that Google is going to start offering by default, all their connections are going to be https, which is the secure version of http. In other words, what does that mean? So let’s say that you’re in the coffee shop, and you use just a regular old http connection, it’s possible that somebody else could be sniffing your traffic, and they could basically see what you’re typing in, maybe get your results back, things of that nature. That’s why you’ll note that banks and credit card processing, all that stuff, almost always you’ll see the URL is https. If you ever come to a point where you’re seeing it’s not, that should send up a red flag for you. So anyway, Google is going to change all of their connections to be https, which means that data will be encrypted from your machine to them, and that’ll be good. It’ll give a little more security, people won’t be able to sniff your traffic. I’m kind of hoping that this catches on and that other people do it as well. I guess it’ll depend on just how much of an impact - obviously there’s a cost, maybe not an actual dollar cost in order to do this, but there’s an actual cost in having machines that have enough power to encrypt all of this traffic, and my assumption is that Google has got all that. Hopefully it’s not as much as maybe they thought it would be, and maybe other people will take advantage of this as well. I wouldn’t mind if http just went the way of the dodo and all the traffic was encrypted. It just seems like a good safe thing to do, but again I recognize that there’s a cost there and that may not be possible.

And then the last story I wanted to talk about was a story I saw on CNET. And this is pretty much, I just thought was kind of fun. It has to do with Siri on the iPhone 4S, and basically what it turns out is that by default, Siri is set so that even if you have the phone locked, Siri will still answer requests. So you can, you know - somebody else, for example, could tell your iPhone to send an e-mail message to somebody or a text message or make a phone call or send a photograph or something like that to somebody else. Now you can turn this off, and I don’t think this is really that big of a deal, but I would recommend that you turn it off just to prevent mischief. To me, this seems like a great way to play a practical joke on somebody, is to, without them realizing it, have their phone send some sort of a message off to their husband, wife, girlfriend, whoever, and maybe cause some trouble there and then laugh about it. Anyway, it’s easy to turn off. There’s a simple setting, and I’ll put this article to this newsletter on CNET and you’ll be able to turn this off on your iPhone. Siri’s getting a lot of press; seems like the iPhone 4S maybe isn’t getting as much, but, boy, people just seem to love Siri. There’s all sorts of websites created for it, and, kinda cool. It’d be interesting to see how that technology plays out.

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