Hello, I’m Roger Safian. Today is Thursday, September 8, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

Going to start with the updates for Microsoft which are going to be coming out next Tuesday, that’s September 13. There are a lot of them. Looks like it’s going to be a big bunch of updates. Looks like it covered most of the Microsoft products. So make sure that you probably give yourself a little more time on Tuesday afternoon or maybe Wednesday when your machine is installing the patches. You know, if you’re used to, I know sometimes I’m in kind of a rush to leave the office and I like taking my laptop with me, and when it starts installing those patches it can take a little while, so it looks like it’s going to be a big bunch this week, so make sure you leave yourself a little more time so you can get those patches installed.

And then I wanted to talk about phishing. We had a relatively small outbreak of phishing on campus, and by “phishing”, I mean, this is where - you’ve probably all seen this - you get an e-mail message that purports to be, say, from your bank, and they want you to, you know, “Look, we’ve noticed some sort of activity, and we want you to log in here and change your password or do whatever”. And basically what they’re trying to do is get your credentials, whether it’s your bank, or the university, or your e-mail account, these things exist all over the place. And it’s very very difficult, I think, more and more, for people to tell, you know, is this link in this message legitimate, and is it not? And I think that’s one problem. Now there’s techniques that you can do, hovering your cursor over it and studying where the link is really sending you and things of that nature, so there are some things you can do there. But I think the problem becomes when you couple that, the difficulty of understanding whether or not that link is legitimate, with a link that sends you to what looks like a legitimate site. So maybe it’s got your logo or your colors or it’s for products that you use; it makes it very difficult for most users to determine if the site they’re on is legitimate or not. And what I’m recommending is, look, just don’t trust these links anymore. If you get a message from a site that’s important, your bank, your employer, in this case the university, don’t trust it. Bookmark the links that are important to you, and if you get a message that says you need to change your password, go to your bookmark and do it. You know, you need to go to your bank, go to your bookmark and do it. Don’t trust any links. It’s just too difficult, it’s too much trouble. Eventually you’re going to be in a rush, or you’ll be on a mobile device, and it’ll be small and hard to, and you’ll click on something that you don’t want to, so just don’t trust the links in messages, especially in messages that involve these sort of sensitive sites where there’s a lot of risk to you financially or your employer, things like that.
Then I want to talk about TrueCrypt. TrueCrypt is a public domain encryption program that’s out there, and it’s, we recommend it, it’s a pretty good program, and they’ve got a brand new version out, 7.1, which supports Mac OS Lion, so the latest version of the Mac OS is supported. So that’s pretty cool. It’s got both 32 and 64 bits, so if you’re looking to encrypt your machine and you have been delaying doing it because you’ve got a Mac, and maybe you don’t want to use the built-in Mac encryption for whatever reason, that’s cool, there’s another alternative, TrueCrypt, and I encourage you to give it a whirl. I’ll put a link in the show notes so you can check that out.

And while we’re talking about the Mac, the Defense Information System Agency as released a draft STIG for Mac OS X. Now it’s for the 10.6 Mac OS, so not the Lion, but likely it applies to everything prior to that. I haven’t looked it over very carefully because I just haven’t had a chance, this just came out today. If you haven’t seen one of these STIG’s before from DISA, they’re really great documents. I’m so glad that they release these documents and make them available to the public. And they have them for a variety of different things: they’ve got them for Windows, they’ve got them for the Mac, they’ve probably got it for your router, they probably have it for everything that you really care about. And that’s great, and they really put a lot of thought into these things. A lot of times they have nice checklists that go with them, so I encourage you, if you’re thinking about locking down your Mac, go ahead and take a look at this STIG and see if there’s some information there that you could use.

And then Microsoft came out with a tool that basically helps you identify and remove rootkits, and it does it from offline. Basically, you create a bootable device, whether it’s, you know, CD, DVD, a USB stick, something of that nature, you put this software on it and then you boot up your machine from that device and scan it. And, hey, that’s great. Now, will this work? My guess is, it will work sometimes, and sometimes it won’t. It’s probably like many of the other tools that are out there, but I would encourage you, one more tool in the toolbox is a good thing, so if you got to take care of PC’s, this is probably a good tool that you’re going to want to have around. Caveats: remember, this is beta software, and remember, your system has to pass the Genuine Windows validation in order for you to use it, but, sans those two concerns, I’d say you want to give this a whirl.

And then the last thing I want to talk about is Java 7, brand new version of Java is out. I have not downloaded it and installed it; it just came out through my desk moments before I came by to do this. If I were going to be recommending to my department about what to do here, I think I would recommend don’t run right out and install Java 7. I would wait a week or so before I did this, because it’s brand new, it’s not going to delete the old version even if you decide to install Java 7. Java 6, whatever that you’ve got on your machine will still be there, so you’re going to have to delete that manually. It just seems like a new major release like this is probably always
a good idea to wait just a little while. And then you might want to check some of the things that you’ve got that rely on Java. A lot of things, a lot of applications, rely on Java, and if you put a new release on, it’s entirely possible that they may change something that might stop that application that you need from working. So, kind of be cautious when you’re doing this.

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
- NUIIT Home