NIGHT Information Security News Podcast, April 26, 2012

Hello, I'm Roger Safian. Today is Thursday, April 26, and you're listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

Our first story today is about WordPress. If you're running a blog, or a system that's got blogs, you probably have WordPress out there. WordPress seems to be one of these pieces of software that the bad guys just have in their sights so it's attacked pretty regularly. We see problems here on campus occasionally with it and it's the kind of thing that when an update comes out you definitely need to make sure you take care of that. So if you are running WordPress they just came out with the new version 3.3.2 so please make sure that you grab it. There's actually a beta version out there too if you want to grab that, if you're one of those people, you can try the latest and greatest as well. The new version of WordPress is out there, I'll put a link in the show notes so that you can grab this if you're not aware about where to do it.

And then naturally we still have a lot to talk about with Mac Flashback. And last week we reported that the numbers were actually going down for the Mac Flashback infection which was great news. Apple had put out the update and they had also put out a special update that would remove the software from an infected Mac, if you are running 10.6 or 10.7. It looks like according to several reports right now that in fact the number of computers that are infected is not going down, they're just staying the same and that's certainly not good. This kind of mirrors what we're seeing over here. There are a fair number of computers on campus we find them that are affected and those computers—all of them, every single one of the people that I've spoken to—they have not done the updates, they're just not doing updates anymore. And they don't have antiviral software; they're just kind of ignoring the problem. And I am really beginning to think this is going to be a serious issue in the Macintosh community because the users just haven't had to deal with this here and in some ways it was always a selling point. in fact when we talked to Macintosh users that are affected—whether it's this infection or other infections that we've had in the past—almost universally they all say the same thing: "I can't have this problem, I have a Macintosh" and that's definitely not the case. so right now they're still talking basically the .5 to 1 million machines are still infected and the numbers just don't seem to be changing at all, which is certainly not good and I don't know what Apple is going to do about this but I'm really at this point I think it's going to be incumbent upon Apple to step up to the plate and try to change the culture that they've created where their users are expecting not to have to do anything. And I don't think that's gonna be a very viable solution especially since there are two new versions of software that are trying to attack the same vulnerability. These are called malJava and that's probably a pretty good description for it, you know malevolent Java applications here. So you know it's gonna be a continuing problem and I really hope that Apple finds way to deal with this here.
I did find another interesting story about the Apple and this had to do with Windows malware. And basically what they're saying is the Macintosh is—don't ask me where they got this number from—but they're saying one in five of the Macs out there contains some sort of Windows malware whereas with the Windows computers, only one in 36. I would not be a bit surprised to find out that this is a very similar situation as to what we just reported the Macintosh users aren't updating their machines. which you know that's one issue but they're not running antiviral software and that means that they can have this malware just kind of hanging around on their machines. Now what they're saying is this kind of malware can be passed to a Windows machine, say via USB key and infected USB token, and that's certainly not a good thing. I encourage Macintosh users out there, install updates as soon as you can and please get antiviral software. Here at the University you can get free antiviral software from the NU IT website. If you're outside the University or you just don't want to use our free software, go grab something that you like, I'm sure you can find lots of great reviews or maybe your friends have software that they really liked. What software you're running is not necessarily as important as the fact that you're running some software and you're keeping it up-to-date.

then I found a pretty interesting article about keeping mobile banking safe and you know this is certainly been a bugaboo of mine for quite a while in this podcast, you've heard me talking about mobile banking apps and not doing mobile banking on your smartphones and things of this nature. It's nice to see that I'm not the only person who thinks this way, although I hope it's more than just a handful. and it's also interesting to see that apparently the banks are starting to recognize that they really need to keep this stuff safe or eventually it just won't become a viable business option for them. I think that really is the point, the banks want to be able to use this stuff for business and rightly so, it's a lot of other people and it's safe, why shouldn't you? But at the moment I don't think that it's safe.

And you might have heard this week Google announced that they would have been making a Google Drive available to everybody. And I believe it's going to start with 5 GB, everybody can get 5 GB of storage on Google. And that's pretty good, I like that, you know it's basically free. But almost immediately come the stories: you know what the privacy concerns about this here, who owns the files on your Google Drive for example was a story that I read on CNET. And that's an interesting question right? And so what I would say, not just for Google but for any of these kind of public services that are out there where you can store your files, Dropbox or any of these things, I don't think you want to be storing anything that's of a really sensitive nature. If you need a place where you can store your vacation pictures or something like that, something that if they get lost or someone else sees them, it's not that big a deal, you know that's fine, go ahead. but when you need to store and make copies and retain things like say your tax records or something that you need to keep private, make those backups
yourself, store them yourself, keep them safe, and I just don't trust any of these services—not necessarily Google, but any of these services—because who knows what's gonna happen. At the very least who knows what happens when it's time for them to get new drives to store them on, what happens to the old drives, could somebody take those and get the information off of it? I dunno. I just don't want to have to worry about it. So I'm not gonna store any sensitive information out in the cloud, at least unless I am absolutely certain that I have separately encrypted that information and I am the only one with the key, in which case that it doesn't matter as long as they don’t rubber hose the key outta me they’re safe. So again, go ahead and use these kinds of services but please be careful about the information that you store out there and take reasonable precautions if you're doing so.

And the last story I wanna follow-up on is where we've had several times stories about Facebook and security. People use Facebook and awful lot—I do too. People store a lot of information there, that might not be the best idea. Do you want to have for example your home phone number, your home address, or maybe your cell phone number, maybe even your e-mail address readily available to a lot of people. I don't think that's necessarily a good idea, you have to make those choices for yourself. Facebook does have some new stuff out there about security and I thought it was pretty good. I especially liked the information that they had about passwords—and how to choose a good, safe password and some examples of that—in easy-to-understand terms. So I really like that. Again I'll have a link to this in the show notes for today's show so please if you're a Facebook user give it a whirl and keep your Facebook account safe. And if you've got kids who are using Facebook make sure that they know about this stuff too because I would hate to see anything happen to them because you’re not letting them know this information.

Anyway thanks for listening if you have any comments suggestions please feel free to send them to security@northwestern.edu and as always you'll find additional security information as well some notes to contain the links for today’s podcast at our Website www.it.northwestern.edu/security