Hello, I’m Roger Safian. Today is Thursday, November 17, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

We’ve got the usual updates from Apple and Microsoft even though they just released stuff recently. There’s always a little fix; it seems like Apple’s put out a new version of iTunes and Microsoft made a couple of modifications, so double-check to make sure that you’ve got those things. And then in addition, you’ll find you happen to be using Google’s Chrome browser, they’ve put out a new version that fixes a bunch of security holes. I just actually read a report recently that said Google has overtaken Microsoft and Oracle for the number of bugs that are out there. I don’t know how people compile these lists; it seems a little unlikely that Google with just a handful of products could compete with Microsoft in this category, where it’s just got many many products. But there’s definitely some holes in Chrome, and those have been patched, so go out and grab that new version of Chrome if you’re a Chrome user. And then if you’re using Adobe Flash, which if you’re using a Microsoft-based browser the odds are pretty good that you’ve got that, there’s a new version of Flash as well, so it should update itself if you’ve got a recent version, but if you don’t see that update go ahead to the Adobe website and you can download straight from them so that you can get the latest version of Flash. That’s a product that seems to get hit quite often when there is a vulnerability; the bad guys really like to work it because they know a lot of people don’t update their browsers, and you know that’s a serious issue.

Speaking of updates, there’s a new worm going around, and basically you might get this as a pop-up. What it looks like is the Windows Genuine Advantage checker. You might have seen this; you don’t get it very often, but usually the first time you go to the Windows update site you’ll get a message that says, you know, “Verifying Genuine Advantage”, and then you need to click there and it’s a pretty painless process. Well there’s a worm that kind of looks like this. Now you should not see this Genuine Advantage thing unless you’re going to the Microsoft Update site. So if you see this and you’re not doing that, automatically just close it down. That’s a bug. You’re just not gonna see this unless you’re going to the Microsoft Update site, which for most people is something that you’re probably not doing anymore. Even the updates that happen on the computers, they happen automatically, or you go to your computer and you click on, you know, do the Windows update, you just shouldn’t see this Genuine Advantage
thing very often, so if you’re seeing it the odds are pretty good that it’s some sort of piece of malware.

Then there’s been some issues on Facebook. They started a few days ago and you might have seen it: your friends might have pictures of Justin Bieber in kind of sexually-charged positions, or even there was some reports of animal cruelty pictures and stuff like this. Anyway, you’ll see on one of your friend’s wall, these weird pictures, and what it is is a piece of malware that’s going around. And Facebook of course says “Hey look, it’s not us! We didn’t do this! It’s not our problem”. And maybe there’s some truth to that. They’re still investigating it. It looks like there’s certainly, perhaps, users with outdated browsers, maybe users are clicking on something and it’s making this happen. I’m sure that Facebook is not strictly to blame here, but what I would say is that it’s just too easy for this kind of stuff to happen on Facebook, and Facebook needs to - I understand there’s a trade-off between security and usability, but Facebook has really gone towards the usability end of things, and I think it would serve them well to start paying a little more attention to the security end of things and sacrifice some usability. The easier you make it for people to post pictures and make updates and things like that, the easier you make it for this type of nonsense to take place. Now hopefully they’ll get it under control. I would say, though, if you’re a Facebook user, you know, hey, it’s important just like we’ve talked about many times during these podcasts, you have to keep things up to date, you have to keep your browsers up to date, you have to keep your patches on, you have to do all of these things, so you have a role to play in this as well. Facebook does have security settings; make sure you take advantage of those things when you get the opportunity to.

And then there was a data breach for Steam. If you’re not familiar with it, Steam is a site that allows online downloading of games. It’s used in a whole bunch of different things, so, personally I don’t have anything that uses it, but I know it’s very popular because my son used to use it all the time. Anyway, there’s a breach there, and these types of things happen, and what Steam is saying - at least what they said initially - is, you know, “look, there’s no credit card data was exposed”, but that might not be the case anymore. There’s some new reports coming out that suggest maybe credit card data has been exposed. And what it might be is there’s actually two different things that happens here, is there’s the forums, you know, people discuss whatever game that they’re playing on Steam, and then there’s Steam itself. And apparently you can have two different passwords for this service; you can have a forum password, you can have a Steam password. What it turns out is that most people have the same password for both, and it looks like that might be related to it, so that the forum break-in may have allowed the Steam break-in. What’s important for you to know is if you are a user of Steam, you definitely want to let your credit card company know that there could be some problems there, and it’s probably a good idea to change your password on Steam and Valve and all their other services that they’ve got over there.
And then speaking of passwords, there’s a list that somebody put together which I kind of like: “The 25 Worst Passwords of 2011”. These are passwords that we’ve talked about before, you know, “123456” and things of that nature, “password”. You know, I just can’t believe that people are still using these passwords, but they are popular, and I can tell you when we see attacks that take place here at the university, it’s not unusual at all to see somebody log-in with a password of “master” or something like that, which is a very common password and has been for a long time. You know, please, take a look at this list. It’ll give you some ideas of the passwords that you just absolutely should not choose. If you happen to have one of those passwords, why don’t you go and change it now and save yourself some grief.

And then speaking of passwords and changing them, somebody’s put together a site, “Should I Change my Password?” And what this is, is, it tries to consolidate all the data from these different break-ins that take place, sees if your e-mail account is listed amongst those that have been exposed, and then tells you, should you change your password, yes or no, based on whether or not they think the password to your e-mail account might have been exposed. Now I’m kind of leery of these kinds of sites, they’ve been around for a while, just because it seems like - I dunno, I just feel uncomfortable about people clicking on this “Should I Change my Password”. But it’s gotten to the point now where, I just recognized, it probably is a good idea; these breaches are happening so often, it probably makes sense to have some sites out there that are legitimate and vetted and that will keep track of this stuff and let you know when it happens, because it’s clear that the vendors are not doing a very good job in this particular area. So I’m going to put a link to one of these sites out there, and go give it a whirl. It’s pretty easy to use; you just plop your e-mail address in, and you’ll get back a yes or no. It’s simple.

Then I want to close with “12 Scams of Christmas”. You know, it’s the holiday season, right? Next week is Thursday, Friday’s going to be Black Friday and Cyber Monday’s coming up and online shopping and everybody’s going to be going crazy. There’s no doubt about, and the bad guys, they are aware of this. It’s a moneymaking time for them. So take a look at some of these scams. A lot of them are things we’ve talked about: phony Facebook promotions and contests, phishing scams and online coupon scams. All of these things are going to be in full swing for the holiday season and you don’t want your holiday to be ruined or at least tainted because you get taken by one of these things. So take a look at this stuff, and hopefully it’ll help you have a good safe holiday shopping experience.

And then I want to remind folks that with the Thanksgiving holiday in the US being next Thursday, I’m gonna try to get the podcast out a little earlier next week. Hopefully that’ll all work out well. 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