Hello, I’m Roger Safian. Today is Thursday, March 29, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

Our first story today is about Adobe. There’s a new version of Flash Player out there. As you can imagine this version fixes some security vulnerabilities and Flash is one of those things on the Internet that certainly has its share of issues. It’s used a lot so it’s a high-value target so the bad guys attack it regularly. So Adobe’s put a new version out, the one thing about this that I think is really great is they have installed an auto update feature on this version so Adobe will go check for itself and make sure that it's staying current and I really think that that's the kind of feature that every piece of software needs to have. Don’t need to check every day but once a week or something like that just to make sure that things are up to date, I really like that and it helps people keep their machines current and that's the best thing they can do to maintain their security. This is not just for your computer though they've got it for every—I saw it for my Android, there was an update for, you probably got it for your tablet as well. If you're using Flash make sure that you get this update and install it. And as I said with the auto-update, it ought to be a little easier to make sure that you keep your machine up to date.

And then there were updates for Chrome as well: 17 high risk vulnerabilities fixed in this latest release. Google fixes the Chrome browser it seems at least once or twice a month they release a new version where they fix a bunch or errors and it's great, I like the fact that they really do seem to want to make the browser more and more secure and so I would encourage you’re your using Chrome to go grab the latest version of that browser as well.

And then I had a couple stories that want to talk about that are directed more towards folks who are running servers and the first one is about WordPress. And WordPress is something that we find on quite a few services over here and we've had some issues with it in the past and at the moment we haven't had any problems, we've kind of got things under control here, at least I hope we do. but there's a new WordPress compromise out there that's allowing a piece of malware called CRIDEX to spread and what you really want to do is make sure that you go grab the latest version of WordPress. Again it's one of these things that it's high-value so it gets attacked quite a bit, and the malware that's out there is—you've probably already seen stuff coming from it, these e-mails from the Better Business Bureau or something like that where they’re telling you about a problem—and what really there is another lesson here in addition to keeping WordPress up-to-date, just don't click on these links that come in e-mails. I just don't believe that you know an e-mail that you get from stuff—if you're expecting something from the Better Business Bureau maybe it's best to call them and verify it or send them an e-mail message yourself instead of just clicking a link to something that’s out of the blue from them. Anyway, bottom line here, if you're running a server that’s got WordPress on it make sure you grab the latest version.
And then the other thing I wanted to talk about for servers was a tool from McAfee and McAfee's got a plug-in that can check the security features for MySQL databases. And that's pretty useful I think, it's probably not as rich as if you're using a commercial tool but a lot of people aren't using commercial tools and can't afford them and that's why I really like it when companies like McAfee release these tools because they really provide value to the community and I think they really do help get things in a more secure state. It's a good thing, it's is a good way to participate in that in the community. So if you are running MySQL you might want take a look at this tool and see if it can be useful for you. I’ll put a link in the show notes so that you know where to grab it from.

And the last couple stories I wanted to talk about were for just your regular old users and the first one has a great two-minute video from Microsoft about the how a financial botnet infects your computer. And I love these videos when they put things like this out because it really kind of puts things in terms that anybody can understand. I think a lot of times when the computer folks get together they start talking in a language that just loses people right away. And so a video like this quickly and easily, without a lot of jargon, explains what the problem is and how to protect yourself and you know it's only 2 minutes. So if you’re supporting users you might want to make sure that they have an opportunity to see this video because it's probably a great way that they can quickly get themselves a little more aware of what's a pretty serious problem.

Than the last story that we want talk about today is an article I found that’s from Canada actually, the Times Colonist. I don't generally read that paper obviously, but it's a story in there and basically what they're saying is something that we've been saying here for a long time and the title is “cell phones quickly becoming the repository of an owner’s entire identity.” and it's amazing what stuff is on the cell phones these days. I mean certainly you're aware of it, people have their financial data, people have e-mail, people have their calendaring, pictures there's all sorts of personal information out there. Just the amount of data that's on your typical smartphone is just unbelievable these days. And it's a market that's very difficult to control because people have all sorts of stuff on it, it's a small little device that can easily be lost, there's resistance to using things like passwords or pins or gestures. So you know, I like this article, it's an interesting article and I encourage you to read it, there’ll be a link in the show notes. And again if you are using smartphone—my guess is most of us are—make sure that you take steps in order to keep that smartphone secure because you really don’t want take a chance on losing it, there’s an awful lot of data there.

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/.