Hello, I'm Roger Safian. Today is Thursday August 23 and you're listening to the information security news podcast brought to you by Northwestern University Information Technology.

We'll start today the same way we started the last few weeks with updates and it's Adobe again so Flash Player has got a new version, it's for pretty much everything: Windows, Mac, Linux, Android, I guess they don't want to miss anything here, that's good. So please if you haven't had the update recently make sure that you go and grab it for your machine from the Adobe website directly so that you got the safest and most secure version that's out there. And then there's a new version of Apache out there. This is version 2.4.3 and this fixes a lot of bugs but it does have a couple of security fixes in it as well so that's important to do now. Now, Adobe if you're running a Web server then it is a pretty good chance that you might have Adobe on your machine, if it's just running you know you got your Mac or your PC or something like this, you're not running a Web server than this probably doesn't apply to you, but please if you are running a Web server make sure that you keep that up to date and not just while you're updating Adobe, take a look at the other products that are out there that you might be using in your Web server make sure that you get those updated as well. because it's pretty easy to miss these kinds of things and they're not as advanced in some regards as say your local computer is, where as your local computer will often tell you that there's updates available, very often server-type software that's not the case and probably for pretty good reason. For example you wouldn't necessarily want that patch to be applied without somebody had a chance to test it in a test environment and make sure it doesn't break anything of yours or something like that. So again, if you're running Adobe on your web server go and grab the latest version.

Then I read a real interesting blog from Bruce Schneier. Bruce Schneier is one of these people that's just an absolute genius about security. And why thought was interesting about this blog entry was he was talking about an article that was written by Simpson Garfinkel who is another absolute genius about computer security and yet they were both kind of saying the same thing but had little different takes and it concerns the iPhone and security. and you know it's just not often that you see something like this here so I encourage you, I won't even I want to spoil it for you here, so I urge to go take a look at Schneier's blog and if you don't read it regularly you know you might want to bookmark this he's got a lot of great information and he's a great writer himself so please take a look at it, I'm sure you'll enjoy it.

and then I saw an article that said seems like they just took it right from the podcast that we been giving recently and basically what it is—they didn't, I'm only joking there—the title of the article is “Own the Email, Own the Person.”
Absolutely. It showed just how easy it was to take over somebody’s e-mail account using just some simple information that is often generally available on things like Facebook and using the password reset functions and things like that which all of these things we talked about. so I know that all of my regular listeners are going to be safe and not surprised about this but here’s a perfect article for you to send to all of your friends who aren’t believing you when you talk to them about how important it is to be secure online.

and then there was a compromise at Symantec this has to do with their Roadrunner Safe Storage and I'm not sure, I've never heard of this product before so I'm not sure, is this something that's offered by Road Runner the ISP or is this some product that Symantec sells and that I'm just not aware of? anyway it looks like their database got hacked, and what I think is odd is they tell people “look you don't have to worry about this here, there were no credit card numbers or Social Security numbers in this here” but they did say that the attackers may have stolen names, addresses, email addresses, usernames, passwords, secret questions and their answers, and the billing address. You know everything but the password in other words. so this is one more opportunity we’ve talked about the secret questions and answers before which allow people access, you really want to make sure that you control these things well because if you don't and somebody could simply read the secret questions from this compromise and possibly gain access to say your Gmail account because you used the same questions and answers there in order to reestablish your identity. I have to tell you that I just recently had to set this up for some website that I was going to, they want you to answer a couple secret questions and I hate the secret question things. and I use them occasionally but pretty rarely and so I didn't answer them, I just banged my fist on the keyboard and put that in as the response because I figured the odds are pretty good somebody's not gonna be able to bang their fist on the keyboard and come up with the same response. So you may or may not want to do the same thing considering how big your budget is for keyboards but you definitely don't just want to give away answers to some secret questions because some website that you really care very little about wants you to establish them. Just to say no to some of the stuff.

And then there was an interesting story about Android Trojans and basically what it said is Kaspersky put out a report that said the number of Android malware tripled in the second quarter of 2012, stands at 15,000. And meanwhile Fsecure put out a report that they said they saw a moderate increase of 40 pieces of new Android malware. Now the reason that they're different is Fsecure is just considering families you know so there might be 1000 different versions of the same piece of malware because it’s twisted around and changed a little bit just to try to make it harder to discover. Whereas Kaspersky would count each one of those is a separate piece of malware. And the point I want to make about this whole thing, and I realize I'm rambling on here, is this is the kind of thing that just bugs me. Why can't they just agree? Kaspersky and Fsecure both the same business, both respected, what they do, why can't they just agree this is what
were going to define as a piece of malware and report it that way instead of putting these numbers out there that are one side is small, one is low. I mean I have to say that in the case of the Kaspersky report, it does sound a bit alarmist and let's face it they're in the businesses selling this stuff, I think they have an economic incentive to be alarmist. I don't think that what they're saying is deliberately not true or anything like that but they could be a little softer and I think it's definitely a problem. so read this here and you'll get an idea of what it is talking about when I talk about these different things about how the companies use these types of terms in order to I think further their agenda which is basically selling more software. I have another story about that right at the end of this podcast which I'm going to get to—don't want to give it away but I know you'll like it.

And then there's a tool that was just released that basically simplifies spoofing of SMS messages on iOS device. So in other words you could get a message from thinking it's from say your brother and it turns out it's not and that's potentially very bad thing. Now this is potentially a networking issue and not necessarily in iOS issue but it's certainly something you should be aware of, much like e-mail messages, much like links in e-mail messages or addresses on websites, you know text messages those things get spoofed as well. don't just rely on those, don't rely on a phone number that you get, you know if you're not sure about something always just use your bookmark and call the person back or go to the website directly, you'll be fine.

and then we're always talking about passwords and there's a great article on Ars Technica about passwords called “Passwords Under Assault” and what's interesting about this is they talk about how quickly you can break passwords and compared to how quickly you could break passwords say just a few years ago, they talked about passwords on different devices and different services. It's really a fascinating article so please, there'll be a link in the show notes, as soon as you're done listing to this podcast, you know go grab that the show notes and there's several great articles you want to read.

And amongst them is an article from our friends over at Purdue about student should take cyber security precautions and I love this. And Jean Spafford who's another true visionary in computer security and has been for a long time talks about some of the very things that we've talked about for a long time but puts it into a nice succinct article that you can easily pass on. If you've got somebody who's heading off to college this year as a freshman or just heading off to college in general, probably a good idea to get them to take a look at this article so that they can review it just to make sure that they're taking these precautions. These are things that we've talked about many times: updating your operating system, picking good passwords, and doing regular backups, things of that nature.

And then I've got two more stories that I figure are kind of interesting and fun at the same time. one is €1 million were swiped from ATMs using bent forks and
basically what the bad guys did is they would make a cash withdrawal and when
the money came out they would cram a fork into the slot where you get the
money from and then they’d make another larger withdrawal but cancel that one
but by now the machine had already bunched up all the money and they would
just use the fork to yank out all the money. And they stole €1 million by using
these little bent shrimp forks stuffed into a cash machine. Now this seems like
something that just should not happen and yet somebody’s picked up €1 million
because of it.

And I want to close with a story about cars and their security, specifically they’re
talking about Bluetooth but there’s other things as well here, and McAfee is
apparently working on some security software or improving the security of cars.
And you know this is good on some level, I mean who’s against trying to improve
the security of cars but at the same time please don’t model the car after your
computer. we can’t have you know your car needs to get regular updates unless
there’s gonna be network there all the time and I don’t think that’s something we
can rely on, where your car’s gonna be able to connect with networking to get
regular updates, and that’s got its own set of problems. Please just make the car
secure so that we don’t have to deal with these things, don’t put another piece of
software on a device that is going to be really difficult for people to operate and
update, that’s just unacceptable. So again I have no idea what’s being planned
here but if you’re listening Mr. McAfee and Mr. S-secure in all of these other
antiviral companies out there, don’t think about antiviral software for the car
because it’s just a bad idea.

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.