Hello, I'm Roger Safian. Today is Thursday, January 19, and you're listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

We're going to start off by talking about vulnerabilities with Apache. There's a new version of the Apache Tomcat server out there and if you're running a web server—a lot of web servers run Apache and we don't often talk about web servers, or servers in general, very often this is geared towards your personal machine, your laptop, your desktop, whatever—but a lot of folks are running servers as well and with this Apache vulnerability out there it looks like it's bad enough where somebody could use it to effectively DOS your machine. So if you are running a web server, you are running Apache, Tomcat, go out and grab the latest version. And if you've been running it for a while and you've got one of the older versions of Tomcat on your machine, give some thought to upgrading straight to the 7.x tree of Tomcat, don't just keep running 6 or 5 or whatever it is that you're running out there.

Then there's been a leak, a hack of T-Mobile, and it looks like some of the accounts and passwords—I don't know if it's all of them but at least some of them—have been put available online. And what's interesting about this particular thing is the accounts are—and my suspicion is maybe this is just because what was first released—but really poor choices of passwords—121212 and things like that. If you're going to put a password on an account—and I realize that for a lot of these cellphone type accounts, you're gonna be using basically the PIN, the 10 digits so you don't have a lot of choices—but at least put a little bit of effort into it. If you're using a password like 1234 or something like that, people are just going to guess it easy. What's the point of even choosing a password that's that poor? So please, two things: if you are using T-Mobile, check to see if your account is on this list and if it is, you definitely want to change your PIN. And then if you are using a PIN to protect your services, regardless of who it is that you're using it with, please choose a PIN that at least makes some sort of sense, anything but the common ones that you can Google any number of lists out there and you'll find plenty of common passwords that are used, make sure that you're not choosing one of those.

Then when we're talking about break-ins, Zappos, which is an online shoes, I believe is what they primarily sell, they got broken into and they released—what was exposed was customer information: names, e-mail addresses, billing, stuff like that information—but not actual credit card information. The only thing that they had was the last four digits of your credit cards. Now, just the last four digits is scary enough, but it's not a complete problem. Where I think this again is the sort of thing where if you're using Zappos and your Zappos password was the same as say your Gmail account where you're receiving information about your purchases, then you're gonna want to go to change those passwords everywhere. And again, what I would recommend that you do with these kinds of things is always make sure—it's not practical in this day and age to have a unique password, I think, for everything—but what you want to do is protect things
based on what’s the risk to you. Your primary email accounts, that’s a pretty risky password to allow someone else to get, so you want to make sure that that’s unique. Financial institutions, you want to make sure those are unique. Other things, maybe you want to share a little bit, but keep an eye on ‘em, come up with some system that is not going to be too painful for you but at the same time is going to provide you with some decent protection.

One thing to keep in mind about the Zappos case is they were bought by Amazon a couple three years ago, I don’t remember when that happened, but the Amazon accounts and passwords are not part of this problem, this would have been only if you were a Zappos customer I believe prior to the Amazon purchase. But regardless, it wouldn’t hurt to change your password if you’re using Zappos and you’re doing it via Amazon anyway.

And then the last thing that I want to talk about here is a guide for travelers with digital devices and this is from the EFF and it’s kind of interesting. What I would say here is it’s geared towards people crossing the border and what sort of searches can be done on your machine and things of that nature and what I would say is don’t use it for that—just use it. There’s a lot of really great information in here and if you lose your laptop you’ll know that information is protected if you’re using some of the techniques and tips that are in this document. So there’s a lot of really good information here regardless of whether or not you’re using it for its intended purpose traveling—go ahead and check it out, I’m sure you’ll find some tips and techniques here that you’ll find useful and I would certainly encourage you to take and use them.

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/.