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

We're going to start with updates and we have an update for Chrome, this is for Chrome 16, if you're using Chrome 16 which is the latest actual version. There’s a Chrome 17 that's a beta version and then the versions prior to 16 are all outdated. There’s a new version of Chrome out, it fixes some security holes so make sure you grab the latest version when you get a chance if you're a Chrome user and a lot of people are, it’s a pretty popular browser these days.

And then we don’t often talk about Linux issues so I have one here for Linux. There is a bug in Linux right now that looks like it’s in procmem which is for memory and would allow privilege escalation. Obviously that’s a very bad thing. My understanding from reading some of the stuff online is that there’s a patch already in development so maybe by the time you’re gonna hear this, the patch will already be out there. But if you’re a Linux user, definitely you want to keep your eyes open because there should be a new kernel patch coming out relatively soon.

And then we’re always talking about various vulnerabilities and what you can do about it and occasionally they’ve come out with these what are called eye charts. And basically you click on it and it rather quickly tells you if you’ve got a problem or not. Somebody’s come up with one of these for DNS issues and this is a lot of malware these days changes your DNS so that you’re using the DNS server off in who-knows-where-land instead of your real DNS server. And then what they try to do is direct you towards sites that they would want you to go to. For example, a rogue version of your bank instead of your actual bank. So this DNS eye chart is out there and basically if the chart is green you’re ok, it’s really easy to use. I’ll put a link to that in the Show Notes if you go over there you’ll be able to see it or just Google “DNS changer eye chart” and you'll find it.

Then I want to talk about Symantec and pcAnywhere and their source code being out and anonymous. And basically what it turns out is Symantec is saying “Look, pcAnywhere has got some serious problems and we recommend that you disable it until we can fix them.” Now Symantec did come out with some fixes this week but they’re still saying that’s not enough, they’re expecting to do more and they’re going to do more and they just don’t want you to be running pcAnywhere until you get these fixes in place. Now this comes from—my understanding is anyway this comes from the code being discovered from Symantec, an earlier version, and I guess the anonymous group got ahold of it so they published it and there’s lots of vulnerabilities that I guess they knew about but weren’t fixing right away. And now because all of this has gone public and there’s a lot of publicity—a very bad thing here. So I’m not a huge fan of these kind of software anyway, this remote access software, but if you are using pcAnywhere please
really consider taking it down until they get this addressed because the last thing you want to do is install the backdoor for the bad guys on your machine.

Then I want to talk a little bit about Google and their changes to their privacy policies. Basically what Google just sent out—I think I got the notice yesterday—was that they’re going to change their privacy policies, basically collapse all the privacy policies they have into one. Now there’s a part of me who thinks “Now this is pretty good” because there’s one privacy policy for say Gmail and another privacy policy for Google docs and so it’s nice to have one policy that’s available for everything. But there are some things about this policy that maybe I’m not overly thrilled about and basically they’re things like you’re not allowed to opt out of it anymore. Basically what they’re telling you is “Look, we’re gonna be able to look at all of your data.” I don’t necessarily think this is the end of the world, there’s a lot of talk on the internet about how bad this is, and I’m not saying it’s good, but what I would say is it’s free. I’m not foolish enough to believe that Google is creating mail services and all of this stuff for free because, well, they’re just great, generous, and wonderful people—I’m sure they are great, generous, and wonderful people—but they’re a business and businesses in there to make money and if you believe you’re getting something for free, well, you’re wrong. There’s some catch, there’s always a catch. And at least Google is upfront about what their catch is, if they see that you’re shopping for car, they’re gonna try to direct ads your way, if they know you like a particular brand of something, they’re going to try direct advertising your way, that’s just the way things are.

It does concern me a little about what kind of information Google might be collecting and what they might do with it. And it was interesting, a story just came out—I think this was just yesterday, it was before the Google thing broke actually—and what they’re saying is Justice Sonya Sotomayor came out with a part of an opinion she just wrote, she was talking about—and this was, I believe this was for the Supreme Court just came out with about searching with GPS, you know the cops attach a GPS to your car, is that legal or is that not legal?—and basically what she says is “Look, we might need to rethink a lot of things including a part, a doctrine that’s called the third-party doctrine, which basically says ’Look, if you give your information away, then you don’t have any expectation for privacy.’” And what Justice Sotomayor is saying is in today’s environment, that may not make any sense and I’m kind of glad to see that so I’ll post a link to that article as well. Give it a look, if you get a chance. I would love to see the court’s really look at this kind of thing to determine what sort of access, for example, law enforcement might need in order to get Google to give them information. My bet is Google is gonna require a court order before they’ll do anything ’cause that’s the way they’ve operated in the past but who knows.

If you’ve been using DreamHost, the Web-hosting service, be aware that they’ve had a break in, you probably know this already because they’ve contacted you. Make sure you’ve changed those passwords on DreamHost. Make sure you’ve changed the passwords for anything else that was associated with DreamHost too, for example maybe your email account or if you use the same password on Amazon or anything like this here, make that sure you change that.
I found a really interesting graphic, this infographic it’s called, and it’s put out by ZoneAlarm and it’s about online banking and security. And you know this is kind of one of my bugaboos and that we’ve talked about it a lot and I thought “Wow, here in one page, they’ve got a lot of great information, some tips about how you can be secure and whatnot,” so again, as I always do, I’ll make a link available to this on the website.

And then one last thing I want to talk about is best practices for recovery from malicious erasure of files. And this is actually put out by the FBI and this is pretty interesting and I would certainly encourage you to give this a look. Not so much because I think it’s—you need to know how to recover from the erasure of files, but I think it’s going to be pretty important when it comes to “How might I stop this kind of thing from happening?” There’s some interesting tips there that you might like.

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/.