Hello, I’m Roger Safian. Today is Thursday, March 22, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

We’re gonna start this week with the, what is the big story about Microsoft and their patches and that is there was a critical update that they had in that bundle from last week and that was for their remote desktop service. And this is a vulnerability that looks like it could be wormed that we mentioned this in last week's podcast. Well it turns out that it looks like Microsoft made a mistake and may have released information concerning this bug to a wider community than they expected and in they may have sort of accelerated the process of the bad guys releasing one of these worms that's going to affect the service. So it's really critical at this point, if you haven't done it already make sure that you've got the patches applied. Certainly make sure that you got this patch applied for RDP. And then you also might want to make sure that if you are using RDP that you’ve got it well protected, turn it on when you need it, turn it off when you don't. If you were using RDP and you haven't used it recently, might be a good time to turn it off. This is the kind of service that can be really handy at certain times but it's probably a service that you don't need all the time. So if you're in an environment where you can enable and disable when you need to, I would certainly encourage you to do that.

And I did read a report this week that said that there were something like 5 million machines—somebody did a scan, an online scan of the Internet, I don't know how much of it—but they said it was 5 million machines that they found running RDP. So it's a pretty popular service, I don't know how popular it is here at the University but I definitely know a lot of people are running it. so really it's the kind of thing you want to make sure: RDP, get that patch, apply it; if you don't need to use it, then don’t—just turn it off, turn it on when you do.

Speaking of patches, we’ve mentioned this story I think now for several years and it came up again, always comes up around tax season. And that is that the IRS is just not getting their security services done as quickly as they need to. They’re behind on patching, policies and procedures, just all sorts of things the government accounting office released a report. I’ll put a link up to this story. But you know if any agency at in the United States government has got issues, you don't want it to be the IRS. If you’ve got information about virtually everyone in the United States, you really want to make sure that that information is secure, very secure especially when it's your own identifier, the Social Security number, that often is the root cause of problems such as identity theft. You know it's really disappointing when I read something that says the IRS is just not as secure as they need to be.

Got a couple of checklist here as well—and I love these checklists, I always do, and hope that you guys use them and like them. Sometimes their stuff in the checklist that I don't like, but you know often there's a lot of good information there. I encourage you just try these things out. First one is for smartphones and again, a lot of good information, some
stuff that that you're probably already doing—at least I hope you are—using a gesture or a good PIN for your smartphone. Maybe there's other things that you're not, like using antiviral software and there is a debate about whether or not you need antiviral software. But certainly I encourage you to look over this checklist and see if there are things on it that you could be doing in order to make yourself more secure. Especially as we start getting closer and closer to summer when people to be traveling, you want to make sure that those smart phones are locked down because if you lose it, you don't want to have all the information that you got on your smartphone to come back to haunt you.

And then there was a great article about controlling your privacy on Google. and with Google releasing more and more stuff—everything that is tied to Google—when I think about it, every single day I'm using Google in one way or another whether it's with Android on my smartphone or its Gmail or maybe it's Google docs, they have so much stuff. So you know take a look at this here because it's really well done kind of walks you through some of the stuff that you need to do on Google in order to protect your privacy. And some of the stuff you may not necessarily be concerned—personally I don't mind if Google has a service that they give me for free that I like and it's supported by ads, I don't necessarily mind that they're using my information to generate those ads. You may feel differently about it but this is a great source of information and I encourage you to give it a whirl.

And the last thing that I want to talk about is its report out of the UK and that the headline, it essentially says it all: “Indian call centers selling your credit card details and medical records for just 2P,” which is nothing, selling your information for nickel. and it's absolutely, this is a concern that I really have, as you farm this information out to people that are making less and less money, I think the odds increase that people are gonna take that information and they’re gonna sell it. You know, if you can't make money one way and it seems like easy money another way, they're going to do it. And I'm not sure that these, when they farm your information out to these various company—and this is your credit card information, your banking information, maybe it’s information on purchases, a lot of big support companies farm their information out to these call centers—they don't pay these people what I would consider living wage and I think that encourages this kind of activity. So it’s an interesting story, I’ll put up a link to it in the notes for this podcast.

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/.