Hello I'm Rogers a few days Thursday, March 21 in your listing to the information security news podcast brought to you by Northwestern University information technology start with updates and the only dimension one on the try to start limiting the amount of update sites mentioned because pretty much every podcast is an update out there some disco trident mention the updates of their something really important so this particular case there's a new update for OS X and one of things that it fixes a flaw that allowed Java apps to run even if he had the Java plug-in disabled which is obviously not very nice at all so this done new version of OS X out there go and grab it and downloaded make sure it's on your machine than a minute checking that make sure you check your other updates and stuff as well you know reader and you know Jehovah you know that the usual sort of suspects out there that psychic disorder news there was a story I read about the Justice Department quotable bending is kind of caught my eye on some e-mail privacy issues and the you know the Justice Department has been in old advocating for a while that they should have the ability to ask for without a court order somebody's e-mail and the in I obviously think that's that's not a good idea and it looks like they're starting to back off on that but they're still asking for release they've renewed their asking for things like information about twitter messages or Facebook messages and things like that and I really am and understand the problem that the Justice Department has it does not take very long you know when there's something really big going on in summary from the Justice Department could get a judge to look at something and agreed that they need to to be able to do this relatively quickly I can't imagine that having a judge look at this stuff would be that much of a hindrance now again I'm not in the business but I really just think the Justice Department needs to give this stuff up start looking at their business practices and just assume you know what whatever we ask for somebody's personal information we need to make sure without a court order in place to make sure we can actually use that that information down the road then does a story about the former Tribune staffer and why so some of the Tribune that's my local paper and it turns out it's a Tribune staffer who worked at the Fox in California had over exactly where but what this guy did was he gave access to his account to anonymous and an anonymous use that account to you the Tribune system and the and hacking into it when you have all used you should not be doing this stuff you know if you fear employer trust you with information then that's your employer's information and it's not yours and you should not be given the stuff out you know so that's their the snow? That's on the other hand though it'll I don't have a whole lot of sympathy for the Tribune company here they let this guy go and then a couple months later he gave away the account they did not deactivate the account in I don't understand how that can happen right they should have a system in place that as soon as somebody steps out the door their account is already deactivated you have to do this stuff if you don't you're going to end up in a position where things like this are going to happen and this doesn't just apply the Tribune and placed everybody you know if you're in a business environment and somebody leaves their privileges their accounts should be disabled then there's a article I read about Google Chrome and I cool chrome and this is about best security tips for saving safer browsing and its things you know Licata disabled job are hot at ratchet up the privacy settings things like that it's really pretty good and in chrome's got some pretty decent settings and by default it's not too bad but you can make it even more secure just with a couple of clicks so take a look at this article I'll put a link in the show notes in a true find
it interesting that I saw something on Ars Technica about two guys there were indicted in
the plot to sell Subway gift cards worth $40,000 and the more I read this article dwells
just like stun it will boil down to is you know these guys were selling these point-of-sale
computers in what they had done is the one guy actually owned a Subway franchise that
had pretty good idea of how these point-of-sale computers worked in subway and they
were selling into separate business where they were selling these point-of-sale computers
and they just put a backdoor on this stuff than they would go on craigslist and stuff and
sell these gift cards and you know what is up with this stuff I mean it is just don't
understand I mean I I understand that there's crooks everywhere but the amount of
damage that you can do in crime like this here in nobody's getting hurt a mean it's one
thing when you've got a glum bop somebody on the head and take the wallet in old that's
one sort of crime in all but in this kind of crime when it is sitting behind a desk in your
you noticed the money quote unquote roles in that's it you you who read the the credit
card industries the banking industries all of these things really have to get a handle on this
cyber crime issue because in the end if you can get control of the money that's going
around because that's the motivation a lot of this stuff didn't get control of the money you
stop a lot of the cyber crime in another story about the the government this had to do with
national security letters and the of this was an interesting story here and basically what
happened is guy a telecommunications company got a national security letter that said
you know look we need this kind of information and you're not allowed to tell anybody
about it and they said you know this doesn't sound right so they took the Justice
Department to court and they sued them the Justice Department over this national
security letter in this this clause in the decision not allowed to tell anybody about it so
when they did this the Justice Department turned around and countersued them for
violating the national security letter by taking them to court and suing them over the
national security letter which seems somewhere in here there's a joke about a chicken and
egg right and I just you know once again that I understand the issue write about it these
things they need this stuff would not keep secrets tough but you know a little bit of
judicial oversight is not necessarily a bad thing I speaking of a little bit of judicial
oversight is a researcher's been a lot of news about this and I think the only people cares
about is the security guys researcher goes out there he gets a hold of a bond that any
basically scans the entire network billions of addresses right he spends months he's got
the information I think is got 9 TB worth of data that's available now it is a turns out he's
probably violated laws in a lot of different countries across the planet so that's probably
not cool on the other hand eight in oh. This stuff is happening all the time the band guys
are doing it all the time does it he knocked it down on sort of torn on this thing of me
don't get me wrong I don't think you are to be going around rattling the door knobs of
your neighbors to see if there locks are unlocked right that's not cool which is essentially
what this guy was doing he was just doing it electronically but the same time if what
you're really trying to do is in a rally in the beard neighbors locks and then you know
reminder made your doors unlocked and Oki. Doorlock potentially there some good that
can come out of it maybe would've been better for you to publicize this stuff and a lot of
people dropped out and you know he could've made the process a lot more complicated
but I hope that we don't necessarily throw the baby out with the bathwater here he's got 9
TB where the data here and ensure there's lots of information about lots of home devices
and what users could be doing in order to make their devices more secure and I'd like to
really see somebody go through this stuff and really tell us what's in this stuff and it's not back to me because this is a crazy and amount of data but somebody out there will perhaps one of the antiviral companies that I want to close here with the story about the that really I think makes a lot of sense and the title is toned down the rhetoric in cyber warfare and basically what happened is they united will always got his testimony before Congress and you had the manager from the RAND Corporation go before Congress and testify you know look with all this rhetoric about cyber warfare is it doesn't really help us and it's potentially putting the sin of Nuno very dangerous situation world to be trigger happy you know I mean it's-I think you know there's a lot of thought that's going into you know the finger on the button right Juno numbers could launch missiles without a lot of discussion and thought stuff like that but that the owner necessarily sure that that same sort of thought has gone into all this cyber warfare stuff in I mean I might even sure what cyber warfare means you know is is there is is there another country that were given go after mean the fee if an attack comes from you know Great Britain are we to turn around and just assume it's Great Britain that did this one of our strong allies and not assume the possibility that maybe there's somebody else who's using computers and networks in Great Britain that's doing it that has nothing and I mean it just seems like very troublesome here and the press just loves the whole cyber warfare thing that constantly talking about it and a much or they know what they're talking about anyway but Deb I just wish they would give this thing a rest let some people really spend some time in and thoughtfully you know discuss what this means what we need to be able to do under what circumstances will respond and just sort of this you know Tracy cyber warfare talk this needs to end anyway thanks for listening if you have a comments or suggestions please feel free to send them to our – safe in the northwestern.edu and is always defined additional security information as Wilson notes that contain the links for today's podcast at her website www.IT.northwestern.edu/security