Hello I'm Roger safety in today's Thursday, April 25 and you're listening to the information security news podcast brought to you by Northwestern University information technology, start by having couple stores that deal with the bombing in Boston and I certainly want to express my gratitude and thanks to the various law enforcement agencies both in Boston and nationally who helped put the put an end to this thread and all first responders that were involved this bird pretty interesting pretty amazing sort of week that took place while everybody investigated this and glad they were able to get the suspects and you know you could put then dumped of sure everybody was I know I was pretty nervous just sort of watching this unfold it was pretty amazing stuff anyway the Boston bombing spurred a bunch of people to try to find out who did this and us ate a lot of people on the Internet so they looking at different pictures and cameras and you know I took this picture and the it it turns out that some of these folks sent mail and messages around in and set up webpages essentially accusing people of being you know the perpetrator of this crime and it turns out that that wasn't true that some of his people at work used a fact his ears I know all the people that were accused by these Internet folks were not the perpetrators and you really need to take a step back and mean it's it's very dangerous to accuse somebody of a crime like this without having it more than sufficient proof and especially the Internet in a what if you know of something it happened one of these people you love somebody had taken an information and seen him and you know attacked them you know it did innocent person because of something on the Internet that's that's just not good so I don't want to tell people who you out there who are might be investigating something like this to stop doing that and it is a role for everybody to plan and time like that but the same time when you find something we should be reporting that to your local law enforcement you should not just be you know become vigilantes innovative the days of vigilante justice are clearly gone and it's unfortunate that some innocent people had their lives disrupted lease for some period of time because they were accused of this crime than the other thing is another Psalm is everybody wants so much information even myself I want to tons of information when I when this happened and so than the news agencies are reporting stuff without having time to check all their fax either so there perhaps no better and in some cases they're probably worse than just these P&O regular old Joe's on the Internet so we were told that facial recognition software that played a role in catching these folks and I thought that was that was pretty interesting because it essentially what it's saying is that facial recognition software has is advanced enough so that it can pull faces out of crowds and in you know I and a friend stuff about this here but the a lot of the times it's saying it's not is is not quite ready for prime time and here it sounds of it was what turns out facial recognition software did not play a role in ID and the suspects either I still hope facial recognition software is can come in handy because I think there's a lot of roles for especially in these sort of situations we've got crowds of people whether it's of the Boston Marathon or you know of is the Super Bowl are going to Cubs game or somebody at the airport and we got a lot of people you know it is facial recognition software could come in really handy looking for these these kinds of folks so I was disappointed that it wasn't used in to to track down these particular sub suspects them there was a tweak that went out that said the White House had been bombed and when this happened the stock market just took a dive and realistically it turned out moments later people realize that – this was just bogus and that hadn't happen but people put a lot of faith in something like a tweet and you
know you'd listen I understand most of time to get that tweet it's it's legitimate right but when it's something big like this here and you haven't heard it anywhere else you might want to take a step back before you take any action because tweets are clearly not the way that you should be you know basing your for your first information on if anything that should be an indication for you to go to another new site and verify this now you know Lotta new sites carried this to so that would've been dangerous at same time but you know it's it I a boy it's unfortunate in the world that we live in today because everything happened so fast that it when mistakes like this do happen in and I don't think this was a mistake I think this was deliver it but it will mistakes like this do happen its evil repercussions happen really quickly as well so maybe everybody needs just relax a little bit when it comes to news like this here just take a couple moments and let's verify that the stuff that we're reading your reporting is all accurate than others a report out from Verizon about data breaches and it's kind of interesting it's got a lot of sort of of different information statistics and stuff like that and I like that so for example on things this report talks about is the insider threat not being is large is we've been told about in the past and the picture finished it there so many different types of data breaches that take place in a bit one small ones who noted that they seem to be concentrated that I believe in most popular place anyway concentrated these two strong words but the most popular data breach happened of financial institutions so it's of interest to report a public to this the show notes you might want to take a look at it I that I don't know that I necessarily agree with everything that's in it so for example it talks about the state-sponsored attacks and you don't number of attacks from China and stuff like that again these are all based on IP addresses and just because an IP address says that the attackers in China doesn't necessarily mean that attackers in China but still a lot of good information this report and I encourage you to read it and it was a really interesting story essentially a guy gets of I call it home and he claimed that caller claims to be from Microsoft tech support now this is a scam that we've talked about before now the person that answered the phone knew that this was a scam and so he kind of went along with the little ways just to find out what was can happen took some screenshots you took careful notes I believe there's even a video up about it so if you're interested in seeing how this scam works in a pretty detailed fashion again go to the show notes here and take a look at this here it's pretty fast and what's really fascinating about it is once they scammers realized that this guy was onto them they took the opportunity to trash the case machine so you know something else to keep in mind here I mentioned twitter earlier with the AP story it looks like there's also malware out there that's not trying to hijack Twitter accounts for financial fraud and again the idea is people really trust trust these tweets so that when they get one you just react on it and again need to step back this is same thing with e-mail it's it's it's a lot of different things out there it's in the bad guys know that they can it's relatively cheap to send this stuff out and if you send it out to millions of people and you only get a handful of folks the response you can probably get a pretty good return on your investment there and that's what it's all about to them so be cautious you don't make sure that your twitter account is well protected and be very very cautious when you're giving out any of your financial information and the last time I talked about is an android app called fighter and it's available for smart phones it allows you to this is a social networking sort of app that allows you to exchange files and pictures and messages and stuff like that and you can use this app to basically bypass the lock screen on somebody's smart phone and it is
against good story very detailed but at its Tibetan facility in the world could you do need to get a hold of somebody smart phone in order to make this happen so I still think this needs to be fixed on glad there are people out there who are looking into these kinds of situations and reporting and I hope that this app gets updated right away because there's you know something like you I think if you look over the App Store ill-suited as 100 million people downloaded this app so that's a lot of folks so let's make sure the sap gets fixed anyway thanks for listing if you have any comments or suggestions please feel free to send them to our data safe in a northwestern.edu and is always shall find additional security information as well some notes contained a link for today's podcast@herwebsiteWWW.IT.northwestern.edu/security