Hello I'm Roger safety in today's Thursday, April 4 and your listing to the information security news podcast brought to you by Northwestern University information technology will start with a story about the spammers and using Google translate to bypass filters this is kind of an interesting technique and basically what it boils down to is they send you a message that's got the foreign language in it and then it's automatically translated by Google translate and then that redirects you to another site and at this other site is where the actual fishing takes place and the foreign language and translate sort of combination there is what's throwing things off and another was talked in the past about kind of like that an escalation you know there's you know bad guy comes up with an attack good guy comes up with a way to stop the attack bad guy finds a way to modify it good guy modifies that you know it's always this constant back-and-forth thing but you know the reason I think it's important to bring this up is not just to mention the sort of back and forth again but you know it's one more thing to think about when you're getting a hold of your e-mail messages and stuff like that in order to make sure that you're secure in all of the translate button which no play in I would use that pretty freely I think you know if there was if I got something a foreign text that I didn't I do very often but occasionally I write I got stuff that only Cuomo wonder what this really is sometimes it looks conference related and so I can want to see what's going on there and the yard for a likely click on the translate button anyway I'll put a link to in the show notes need to read how this does kind of interesting another store that they'll put a link to it involves you might've heard there was it we purported on for couple weeks as attack against spam house than that in Europe I think they're in the Netherlands and the it it turns out that there's a lot of other devices besides you know the quote a quote typical computer you know like my laptop here in your desk or something like that it that is involved in is kind of tax and it turns out that things like cable cable boxes and you know TiVos and you know maybe TVs them it is just all sorts of devices and really when you think about it in on a mistaken about my own home network here in oh my TVs are on the Internet or online should say you know the TiVos there of the videogame systems to you that there's just a lot of stuff that's all plugged in and for one reason or another has Internet access and think what's important that you make sure that your all of this stuff you want to make sure is behind your router that provides you a little bit of practice are little bit of security inside and the other thing that you want to make sure that you do is to keep these devices up-to-date and don't forget about keeping that router your home router and stuff up-to-date every now and then there's an update for that you don't if you could turn on logging go ahead and do it in only if if your TV is only expected to be connecting to port 80 443 maybe maybe can get out look forth as a connecting on other sites or on other ports going to other sites and they wanted it is kind of one of notes: noninvasive very often the logging funk Chanel Elian home routers is turned off which means a lot of stuff could be happening on your home network and you wouldn't necessarily know about that should tell you from somebody who's turned on logging you get an awful lot of information sometimes it's about things that you just don't need to know about but if you're willing to kind of weed through that stuff little bit or at least recognize that for what it is and be able to spot anomaly I think you're a vegan to do okay here so Robert keep your stuff up-to-date and make sure that all of your home devices are behind your router don't plug things straight into your cable modem and use it that way you're talking about securing of first technologies I got sent a securing web applications technologies checklists and this is a
pretty interesting little listener covers ways for handling you no errors for example or you know cleaning up your input and output in O'Connor making sure that feels irks only getting data that they should be and things of that nature but I love these checklist because it's a convenient way to make sure that you doing all the things that need to be done and it's their release. The link to this the show notes hopefully you find it useful and somebody also sent me an article it was an older article but the work get ready come up to the summer here in so this was 10 travel tips for protecting your privacy and you don't get stuck you either so many different things I just got back from vacation last month and I went into an Internet café and when I sat down at the machine the person that was there before they're all their stuff was still logged in so for example one of the tips that some listing is logout of public computers and you know I think it's nice to be able to review the sorts of things especially as your get ready to plan your vacation there's so many things these days that are involved in Internet access and say your private information so for example think about digital cameras lana digital cameras these days especially the newer newer ones come with Wi-Fi built into it so that it's easy for you to transfer those pictures you know that a lot of the digital cameras do since it got Wi-Fi built in the bottom have GPS built in Latimer tagging pictures so you know when and where was taken in others a lot of personal information again just focusing on the cameras a lot of personal information that's in there so you are think about these things when you're traveling because you know nothings Garuda vacation more release our the memories more than when you get home and you find out that you know something really bad is happened but she didn't take some cautions that speaking of not taking cautions here's a story about the woman's laptop was stolen from woman's health enterprise and units Personal information under for I don't know how many thousands of patients and it's just not good and in this day and age I do not understand how a health organization any health organization just doesn't have those laptops encrypted that if you've got even if you don't think there's any data on it better safe than sorry your health organization just encrypt all your laptops you this this should not be happening and I don't know sickly what the story is serious all the details but somebody in this organization needs to beat needs to payday need to really like trauma mouth like you know the French Revolution guillotined the crowds cheering is that as tax comes downright mean this is just should not be happening anymore this day and age and maybe we need to make an example out of somebody and I want to close with a story about cyber attacks and losses now everybody has seen headlines were you know they fail you new your city's relatively large figures talking about you know how much money is being lost a cyber attacks and cyber crime and you know you pick the sort of in a word of the day and put it in there I know from our own experiences here you know there are or losses but the losses of you know are mainly in time and you know things like that is sold so they've got companies have come forward now and said look were suffering no major financial losses couple little exceptions here you can read the article to find out which company said what but for the most part it turns out companies are saying look we are not having any losses to cyber attacks now I don't believe that either why believe is the companies have a vested interest in this keeping their shareholders happy by saying we don't have any losses to cyber attacks the big companies who sell these cyber protection software in oh antiviral Sweetser and intrusion prevention device whatever it happens to be right they have an interest in making sure that these numbers are huge and you know this is a lot of fun out
there in oh there's there's we really need to have a good way to express this stuff. In a way that can be expressed with not necessarily you know when you finger at somebody holding them to task things need to be fixed soon off your big corporation X and there's a problem unique to fix that problem but you shouldn't necessarily be penalized because you reported to know we've got this problem because if more and more companies were reporting a we saw this and this is how we fixed it it's likely that more more companies would start fixing those problems instead of each one having to discover the problem on their own and then address it on their own and kind of keeping things secret you know may visit you run into somebody you know at a conference and you tell him a little bit about what happened but for the most part companies are very hush-hush about these kind of things anyway thanks for listing if you have any comments or suggestions please feel free to send them to our – safe in a northwestern.edu is always show find additional security information is posted notes that contain the links for today's podcast at her website www.IT.northwestern.edu/security