Hello, I'm Roger. Safe in today's Thursday, May 2nd and you're listening to the information security news podcast brought to you by Northwestern University information technology. The first story today is about the free virus protection guide and the UI love stuff like this and would find it on the net and I'm always putting these things up there but this one is takes a bunch of different antiviral packages that are out there and counter views him and talks about being of the pluses and minuses there advantages of installing them naturally all a big fan of antivirus software I don't think the antivirus software is the silver bullet solution by think it's a great thing to have on your machine doesn't usually consume that many resources and if it stops ill problems coming through that's great I don't necessarily think you want more than one sometimes I stab second package on the machine just in case but usually only will actively run one at a time so put a link to this in the show notes and you can take a look at it yourself if you're pain-free antiviral software you don't depending him particular feature using if I'm usually the free stuff just it just does just as good a job especially for a home user and then last week we talked about the you know these these Internet investigators who impressed in the Boston bombing of how they falsely accuse some people of being involved in it and the below that sounds in a good thing this week there's a story that the code looks at the opposite end of it you know where it is the title is the Internet does is actually surprisingly good at crime-fighting and what they're talking about is his various cold cases that have been put forward on the Internet and people have come together investigated found and an basically solve crimes so it's it's a good counter story to the story that I posted last week and the I would still say that we need to be deafening to be careful when you have civilians out there conducting these kinds of investigations and making their allegations in public they're not subject to the same rules and restrictions that government agencies law enforcement agencies are and to me that's a real area for concern that is a story that normally would just ignore it so the U.S. Army's working on new technology replaced a GPS system and the recess in gnome I would just ignore dislike while you know whatever the Army's working on let them do their thing but the GPS man I love that GPS in a semi-phone so my carts everywhere I love the GPS it so I don't like it asked for directions and to have it GPS gets me around so I really enjoy it now my guess is that the current GPS system which if you don't know was developed by the military current GPS system that we use I suspect is likely to stay around anyway just because it's so popular no doubt it's expensive to Rhonda with although satellites everything like this but the military has completely different needs for example: this article anyway submarines can't use GPS because you are underwater in the signal doesn't get down to where their act and you know that's an issue am sure there's a lot of other issues when you're talking about the military stroke I find this particularly interesting I I really do hope though that in the end we end up with a civilian GPS system because I have really really become very dependent on my GPS and I would hate to see it go down with talked about the Internet cameras before his illegal web cameras and lots of people have computers these days special laptops come built-in with them smart phones that got a camera that's seeking to face time or whatever with your friends great technology a lot of folks have bought little USB cameras then they can put on their computer you got an older computer and income with 11 the companies that makes this is D-Link and D-Link and they make a lot of stuff routers network cards all sorts of things and the days if there's a security flaw in this Internet cameras out there basically it could allow anybody to hijack the stream of
what's on your camera so that anybody could see it that's probably something you don't want and you know the worst thing about this flaws it looks like what D-Link did this on their cameras they essentially put a backdoor password you know this is the kind of thing that causes the Internet crash in the and one cent 1984 was said that only remember it's been a long time now write 1983 perhaps but though the great Internet warm worm the Morris worm that's one of things it did was was overthrown on the the mail servers if you're running SMTP and didn't put the password to the no wizened toboggan and let everybody and give you root access folio that's obviously a problem and spend this is a known problem for a long time the fact that they're still doing this in all these years later that's a real problem anyway they do have an upgrade available so if you're running a D-Link camera please go grab us or you would want somebody to do compromise your privacy of that way of them speak of privacy Facebook I've had several of these guides over the last few years about how you can secure Facebook this one is a Facebook security for young adults parents and educators Straley written for a well of me knows I have I find it actually pretty good read so if you fear using Facebook especially if you've got enough your parenting you've got children be in a you really want to read this and see what you can do in order to make their Facebook experience both pleasing for them but give you the peace of mind to know that there than not can you get in any serious trouble in things that you can discuss with them I really love these sorts of guides I think they're very useful then I saw a great story on Ars Technica and irises got a lot of great stories anyway but this one just played out like to pick a show on television and basically what it is what they're calling sex torsion plot which I think is kind of a cool word anyway and basically what somebody did is this was an online poker player in the broken other, this happens a lot they filed some pictures you know new pictures of the person or compromising pictures the person and basically said look if you don't if you don't pay me a certain amount of money I'm just before these pictures to everybody to me this else typical extortion but the it that what's great about this story is it really goes through the whole thing from the FBI showing up at the guys house how the FBI found him you know that the questioning of him and it's really fascinating reading it's pretty long story to it's like 33 pages long on and on ours which is a fairly long story it was just it was a great read him and I really encourage you to give this a read it if you're interested in how this sort of stuff works not that you want to be interested now extortion works which is sort of like that you know the criminal mind and this is fascinating so go ahead and the and give this a read and then there's a story that I saw about a Utah health breach could cross the $406 million and basically what they're saying here is 780,000 Utah residents run a computer that were hacked in order to secure this computer therefore he spent $9 million on audits and upgrades and credit monitoring and other saying that the total costs could be $406 million now here's where have concerns that there's a kind of extrapolating stuff here right that we party spent $9 million that's a real expense rates with weave and would and probably should've been spent before right but then there assuming that this could be these other expenses and they come up with these giant numbers now the one thing that I took of the story 780,000 Utah residents right that's what the story says but right now they're saying so far at least 10 victims so 780,000 in the event tenant an immediate title. That story doesn't even say that these 10 victims have been absolutely tied to this breach this breach happened in 2012 that means even if it happened on the last day of 2012 which you probably didn't you know it's had a good
four months into the good four months they've only had 10 victims that they could tie to
this thing no innovators there's a lot of FUD here and and and I don't like it when they
throw around these these exceedingly high numbers like $406 million in oh and in 10
people of 780,000, or something wrong here so so minis to really look at this and hope
that they do now maybe this breach could've been prevented if they did seen this next
story in that set at the NIST has got all their checklists available reorganized it looks like
and if you've got an a machine that looks like that got checklist for just about everything
a look this 210 of them out there they cover it things like Internet Explorer Apple Panther
you know I mean there's there's checklist for just any anything in oh really I do love these
things because it's a great opportunity for you to grab something all in one place in oh
here's how to step you need to take in order to secure this particular operating system or
this particular product and its outstanding and this does such a great job on these things if
you've never gone to this website before to see these checklists deftly want to go do that
and somebody you should be doing this is the people this next story which is came from
Consumer Reports and basically what Consumer Reports is saying is only 39% of
smartphone users secure their phone and you know that's not the that's not good at all so
you deftly want to make sure if you got a smartphone we've talked about some of the
things are out there but you want to make sure that you use secure the phone you want to
at least use a pen if you can set your phone so that will automatically erase after certain of
the number of failed attempts that's probably good to make sure that the pin that you
choose isn't easily guessable things at 123456123411111 overall really terrible pins and
the unit was smart it's very easy to lose us the device or smart phone it's it's not that big
people are leaving him in and slipping out pockets in your cabin leaving them in the
airport leaving them in restaurants amid their they're smaller and there's in other
relatively convenient for criminals to steal you know you're walking down the street
talking on your phone that we have criminal runs up and grabs and takes off you know
you can build around him attaching probably not you know you want to make sure that
the date of Japan on the phone to secure the way that you do addition make sure that you
get a good strong plan on there and if you can remotely wipe the phone even better so of
family thanks for listening Kevin, suggestions please feel free to seminar – safe in a
northwestern.edu and as always you find additional security information as well's notes to
contain the links for today's podcast at her website www.IT.northwestern.edu/security