Hello Roger safely and today is Thursday, June 27 and you're listening to the information security news podcast brought to you by Northwestern University information technology.

want to type up some updates to WordPress there's a new version of 3.5.2 which correct fixes quite a few security vulnerabilities and the ISO to want to make sure is enough using blogging software you. Odds are pretty good WordPress is really popular and so it's a pretty popular thing to attack an on campus we've seen them compromised here quite often and will work tracking down these phishing sites seems very often that those are also compromised WordPress sites so if you are blogging even if you're not running the software yourself you know but you're just honest service that allows you to do blogging check to see what version of WordPress is running there and if it's not at least 3.5.21 to drop a note to your ministry at her and remind them that there's a new version of WordPress out and they should update it will put a note to the in the show notes so that you can send the link along about what the update fixes and how to get it them what talk about this Facebook bug there was the came out at the end of last week Facebook admitted that they had exposed the contact information of perhaps 6 million users it turns out that this was because will bog that they had with the there's the serves the Facebook says Rick and download your information and you've probably seen this if you've connected to it worry you cannot you give it your Gmail address and it downloads all your contacts from Gmail or from your union whatever other accounts to God and the trust finals people on Facebook and you connect to up with him and stuff that can be kind of useful so it turns out that one was doing this here it looks like it might have also been making other people's information available at the same time and the obviously that's not a good thing that Facebook has said that they have fixed this problem it in and I believe them but but it turns out that it looks like the problem may have been larger at least people are discussing on the net that the that the Dean of the number people 6 million was the number that Facebook gave remember the number may have been larger NIH probably also fair to put out the for Facebook 6 million years West explain yourselves a, people write good number for six Main dollar man but not a good number Facebook but that's all like one half of one percent of Facebook's users now that this sort of talk is that right now maybe that number is much higher maybe it's doubled maybe it's a triple to know but still you don't talk and maybe one or 2% of Facebook's users being impacted by this thing what I think is perhaps a little more disturbing though is it appears that when you uploaded information so you major your contact list available on Facebook it looks like it All of that stuff and you know I don't know why Sophie couldn't find you know Joe with Yahoo.com it Joe's information and that's that to me I think that's a more disturbing aspect of this Facebook thing Facebook is usually I don't think they're very up front about how they do things their they really need to get a lesson transparency but a you know I think we'll probably talk about this next week to it is an excellent chance that given a little more time or probably didn't have more information available but what I would say is if you did upload this information seems like there's a pretty good chance of that information was made available how widely probably not too widely but you don't not up not a perfect situation anyway I enough about Facebook is about ATM card hacking and we've mentioned before about scammers in essentially these are little device is very often that are put in front of the slot where you slide your card into the ATM so when you slide your card into the ATM this little device reads your card and then it's in opposite continues forward and is read by the ATM signature cash everything looks fine
right little device collects your information and so that they can use that in order to get money out of your accounts they usually need to have something else somebody's shoulder surfing your password or New Year's camera that's nearby collecting in which are typing on the keypad there's a Wi-Fi phone website that has some pictures of furnace skimming skimmers that were at ATMs I think Stephen got something for up one at a gas station so it's kind of adjusting its and I think it's been a become more and more and important the kind of recognize the ATM house should look if there something unusual about it what untidy what I do I used I use the ATM just like everybody else right and what I always do is always shake the ATM (it were on putting my card and I shaken a little bit more the keypad is sites in a room but you are rubbed just to see if everything is solid like animal that helps or not but I kind of feel that like you know maybe somebody put something on there it can't be attached that good to me maybe I would notice and shake it loose or something and I'll anyway that's what I do but I do deftly play very close attention and I think you should as well because nobody wants to get the right temp ATM card act store here from Stanford and the Mozilla foundation and essentially what they're trying to do is tackle cookie privacy issues that cookies these a little files that are written on your machine when you go to website information could be written in the form of a cookie and then that information is available to certain other websites is so what they're trying to do is restrict us how widely shared information cookies could be in a solidify visit Amazon and Amazon's got a cookie on my machine that says I looked at the you know what ever up Kleenex out you might notice to them when you go to maybe CNN you might see an ad on the site of CNN for Kleenex and the way that they're doing that is a big thing I was looking for Kleenex on Amazon right and try searching for car sometime unit new-car ads all over the place and there do they do that with cookie so they want to try to restrict these things and the it is a vacant they're trying to use her restricts and heuristics you know they can work the innovator work maybe not 100% maybe not even 90% they can get you a lot of the stuff done but they're not going to be perfect and you know the problem is when you're talking about big numbers and you're off by 10% that's a lot that you're missing or a lot that you're doing that you shouldn't be doing rights so they really need to get these things as close as possible now Safari has been doing this for a while were essentially they of it. The algorithm that I believe they use is if you visit the domain directly they can set cookies first party cookies on your machine if you've never visited the domain directly they can't in a something very basic like that so I yanked it him. Stacy how this plays out enough to get people extent for the Mozilla working on a problem I got a pretty good feeling that were going to find some some interesting information there and in the last store they want talk about was you may remember a few years ago there was a movie out there called supersize me essentially what this was is you know this guy from month he ate nothing but McDonald's he had to try to eat everything that was on the menu and any time they asked him would you like me to supersize that he had to say yes and that might've been some other rules I don't remember at all and you know basically it was what happened him of the eating amounts with the goggles and that somebody on Ars Technica has essentially taken this here inputted into download me and basically what they're doing is they they had a Windows machine I don't remember what version was a might've been XP and they they installed they got it up to date and they they started doing searches for your common search terms things that were listed in the top 50 in all over the place so free game cheats are free
games you know things like this are screensavers music things of that nature and how much malware with a get it turns out why to bid it's really an interesting article again Ars Technica has really done an excellent job here and encourage you to read it it's it's kind of it by midnight I was at Apsley fascinated by the story was best thing I think around all week and I I encourage you to give it a read yourself I think you'll enjoy it thanks for listening if you have any comments suggestions please feel free to send them to our – safe in a northwestern.edu and is always to find additional security information as well so notes that contain the links for today's podcast at her website www.IT.northwestern.edu/security