Listener Feedback #80

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world 'application notes' for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-224.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-224-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 224 for November 26, 2009: Your questions, Steve's answers #80.

It's time for Security Now!, the show that covers everything you need to know about security with Steve Gibson, as always - the man behind GRC.com; the discoverer of spyware, the man who coined the term spyware; author of SpinRite, the great hard drive maintenance utility, and a lot of security utilities like ShieldsUP! and more. Hey, Steve, it's good to see you.

Steve Gibson: Hey, Leo. It's great to be with you again, as always.

Leo: Happy Thanksgiving week.

Steve: And thank you. And you know, I think you're right. I think if someone listened to this podcast constantly and thought about it, they probably do over time get everything they need to know about security. We really do cover the bases. And it doesn't happen over a short period of time. But, I mean, I keep hearing from people who write, that go to GRC.com/feedback and send me their thoughts. And they're saying, wow, I'm like my whole group's security guru now, thanks to listening to you guys...

Leo: That's fantastic.

Steve: ...a couple years. So, yeah.

Leo: Yeah, I mean, I think you get - we added security news a couple of years ago. And I think so that way at least you know what's breaking security news. We've been doing Q&As now, this is our 80th, so that's a couple years we've been doing that. And so that covers a lot of bases. And then of course you get these great lectures where you understand, like last week, where you really understand SSL. Those are very valuable. And I think you're right. Cumulatively, I don't know, I think there's nothing we haven't covered at this point, from crypto to SSL to hacks to buffer overflows.

Steve: Social exploits.

Leo: Yeah, you bet. So what's been going on in the world of security since we talked last?

Steve: Well, we've got our regular cast of characters. Actually sort of pretty much the same sort of stuff. A number of listeners wrote about a story which I had run across also, so I thought I would bring it up. This was where some people from the NSA were testifying in Congress about security things and happened to mention that they had worked with Microsoft on hardening of the security of Windows 7. Well, of course this upset some people who are mistrustful of government and specifically the NSA. You may remember that there was a coincidental acronym collision in part of Windows where there was something that, if you looked at the binary code of Windows some years ago you could see _NSAKEY was the - I mean, and it stood for something completely different from National Security - is it Association?

Leo: No, no. That would be a professional group. The National Security Agency.

Steve: Agency, yeah. And so anyway, it turns out that the NSA has been helping Microsoft, but also Apple and Sun and Red Hat.

Leo: Oh, that's interesting, huh.

Steve: And what they've been doing mostly is just sort of working with them on best practices, the idea of making sure that things are bolted down and turned off. I think that probably the companies are saying, hey, is there anything you guys know about that hasn't occurred to us that would help us make our operating systems safer? So it's not like the NSA is creating code or writing blobs of these operating systems that they're then secretly handing to the companies to install.

Leo: Let's hope not.

Steve: Well, yes. And the concern is that, you know, this mistrust, the conspiracy theories that people have...

Leo: Well, it's not just a theory. They were spying on us through the phone company, so...

Steve: That's true. There have been some things...

Leo: We know they have some interest in our activities.

Steve: Yeah. Again, my sense is, though, that with the kind of scrutiny our operating systems get, where we've got packet captures going on, I mean, we have such a community now of security concern surrounding these, it's not like any of this is being done without anyone watching. I mean, everyone is watching. So I'd be really skeptical whether any packets could be playing games without being seen.

Leo: It'd be hard to do these days, yeah.

Steve: But I did want to acknowledge the people that wrote in saying, hey, Steve, did you see this article or this news? What do you think of it? I mean, to me it looks very benign. I mean, I'm probably less prone to conspiracy theorizing than most, so maybe I'm being nave. But to me it looks completely benign.

Leo: Microsoft says there's no backdoor.

Steve: Right. Also the continuing saga of the iPhone jailbroken worms. It's very plural now. I don't know whether you saw this, Leo. But there's - now we're seeing the rapid emergence of very bad worms, which are taking advantage of this default password in the SSH server that the jailbreaking installs in iPhones. There is now one which is actively stealing banking data and enlisting the iPhones into a botnet.

Leo: Wow.

Steve: It's a worm targeting jailbroken phones which steals online - it's designed to steal online banking login credentials, so it's looking for those. It changes the iPhone's password after it gets in so nothing else can get in; connects to a command-and-control server in Lithuania to download additional files and data and to send back the information it has stolen from the phone; and ties the iPhone into a botnet. So this quickly went from some fun and games in Australia a couple weeks ago, where as you remember some random photo was changed on people's backgrounds, the desktop of their iPhone, into now something which is seriously bad.

Leo: Not good.

Steve: So this is a problem with anything that is as intimately connected into a network. I mean, we've certainly seen, I mean, this is why we have the security problems we have

with Windows and all PCs now to varying degrees is that they're part of a big network. Well, phones are computers that are becoming increasingly powerful and open and part of a big network. So that creates this opportunity.

We've got all versions of IE have various types of problems. Starting with the most recent IE, IE8 has a strange problem that's been found in Microsoft's own attempt to prevent the problem.

Leo: Oh, boy.

Steve: There's something called - and we've talked about cross-site scripting. In order to prevent cross-site scripting, one of the things you do is so-called "output encoding." That is, for example, in sites where you allow users to submit their own content, for example, you don't want to allow a user to submit a less-than sign or a greater-than sign because that allows you to bracket some keywords like an href, a link reference, or to invoke scripting or play other games. The idea being that when - what you submit is then presented to a different user by the browser, the browser that's outputting this will see those brackets, the angle brackets, and say oh, this is some html. And it will render that text that somebody else, a malicious user put up as html, interpreting it on the fly. So to prevent that it's possible to do so-called output encoding so that dangerous things that are submitted will not be presented back to the browser in their same dangerous form.

So Microsoft has a cross-site scripting filter in IE8. Apparently they did it wrong. And what's happened is there are now proofs of concept. And it's been shown, and Microsoft has acknowledged, that it is possible to trick their filter so that the filter which is trying to prevent the problem actually creates the problem. So some clever hackers figured out a way to give the filter something to filter which would cause it to do what it was designed to prevent.

Now, what's interesting is that there's a way to turn this off. If a web page is presented with a header from the server which is serving the page, which is x-xss-protection:0, that is, cross-site protection zero, that disables IE8's filter. Well, interestingly, Google knows about this, is aware that there are problems, and in a formal statement from a spokesman said we're aware - well, when asked why their servers were serving this cross-site scripting protection colon zero header to turn this off in IE8, their spokesmen said, "We're aware of a significant flaw affecting the cross-site scripting filter in IE8, and we've taken steps to help protect our users..."

Leo: This is amazing.

Steve: "...by disabling the mechanism on our properties until a fix has been released."

Leo: Wow. Wow.

Steve: Yeah. This is just getting crazy.

Leo: So when I surf to a website on Google, where...

Steve: Well, where they've got active content and they're trying to protect themselves, what they're doing is they've added that header to their otherwise endangered pages so that IE8 won't perform this protection.

Leo: I see.

Steve: And, see, essentially, IE8 is trying to do this on behalf of webmasters who haven't properly output-encoded their pages. So this allows IE8 to protect the website on behalf of the website owners. Well, Google is smart enough to be - they feel - to be doing the output encoding properly, the output encoding protection themselves. So this is really not providing Google with any benefit. And in fact it turns out, due to a flaw in the way Microsoft did this, it's creating a danger where one doesn't exist in the case of Google sites.

Leo: This is wild.

Steve: So it's intended to do good. It does bad. So Google says, uh...

Leo: We'll do no evil.

Steve: ...we'll turn that off till you get it fixed.

Leo: So other webmasters might do the same, could consider doing the same thing, then.

Steve: Well, they could, as long as they're very sure that they've prevented these problems themselves.

Leo: In the first place, right.

Steve: In general it's probably, because this is a specific way of tripping it up, and because it only works under IE8, it's like, well, you know, it's probably doing more good than harm for most webmasters by helping them to eliminate cross-site scripting problems. But in the case of a webmaster who really knows what they're doing, they'd probably want to turn this off just to prevent their site from being abused in this way.

Leo: Can I point out something?

Steve: Oh, yeah.

Leo: If I were a hacker, and I had a cross-site scripting exploit on my web page, I'd

make sure to turn off cross-site scripting protection when I came to my page. So if it's known how to disable this protection, what kind of protection is that?

Steve: Yeah.

Leo: Am I missing something?

Steve: Well, it's that the bad guy who has the server...

Leo: Ah, because of the nature of cross-site scripting, I have to take advantage of somebody else.

Steve: Exactly.

Leo: I see. So it doesn't matter if I issue it from my page.

Steve: Exactly, because you have complete control of your page.

Leo: Got it, got it, got it.

Steve: You can present your visitors with any kind of malicious content you want to. The idea is tricking other sites, like Facebook or MySpace and so forth, to present text that they weren't designed - that they were designed to disallow presenting.

Leo: And I should underscore that, which you've said before, that NoScript prevents cross-site scripting. So if you're using - first of all, you're not vulnerable if you're using Firefox in the first place. But NoScript is a very good, even if you don't use - don't tell Steve. When you turn off the JavaScript stuff, it still prevents cross-site scripting.

Steve: Well, we also have exactly that advice recommended for a new zero-day flaw that is in both IE6 and IE7. Some raw code was posted to a security blog to demo this under an alias, so no one really knows who posted it. But a number of security firms tried running this code, and it immediately crashes IE6 and 7. And it has been shown that it can also be used to run explicit code remotely. It's an abuse of the getElementsByTagName JavaScript method. So it's a method in JavaScript in Microsoft's HTML DLL. It's mshtml.dll. Microsoft has no patch for it. They've acknowledged it. And their recommendation is [clearing throat] disable JavaScript. Not surprisingly. So once again, yes, NoScript would prevent that from being exploited. I would imagine the second Tuesday of December we'll probably be talking to our listeners about a fix for this problem in mshtml, the getElementsByTagName JavaScript exploit, which probably by then will be in active use. So selectively enabling JavaScript I think is still the best policy.

And finally, Opera is a little bit late to the game, but better late than never. Several weeks ago we talked about this buffer overflow in a commonly used C language numeric conversion, the D to A conversion function. Opera has finally updated their browser to v10.10. So any Opera users out there, make sure that you're running 10.10, and you'll get the benefit of that fix.

Leo: 10.10, okay.

Steve: And lastly - that takes care of security stuff. I wanted to mention in errata, for all of our listeners that really appreciated the extra-special, and some thought bizarre, Vitamin D episode we did, I'm getting a flood of questions from people who have wanted to know, they wanted an update, they want to know what's going on. They're sending me articles and links and all kinds of things. I've been deliberately mute on the topic because I have really wanted to respect the Security Now! nature of this podcast and not confuse the two.

So, Leo, you've agreed to do with me a special podcast from time to time on my findings in my own little sort of hobby of health. And so I wanted to tell our listeners that before long we're going to do another one which will follow up some on Vitamin D, but also talk about my next breakthrough for myself. The reason I'm delaying it is that I'm waiting still on some results that will take longer to happen. But I have some exciting news on a different front that I want to share that I think a lot of people will find very interesting. I'll say more when that is in the can and we can point people at it.

Leo: Okay. And I'll get the lawyers working on the disclaimer.

Steve: [Laughing] Yes, we're not doctors. We're not trained medical professionals. I'm just a health hobbyist. But I have some interesting additional news and something else I think people will really find very interesting.

Leo: Excellent.

Steve: And a short note on something that's near and dear to me personally, and that is of course SpinRite. The subject, from a Darren Wigley, was "Thank you times a thousand." And he just said very briefly, he said, "Please know that this software totally bailed me out of a bad situation. At least it was not life-threatening." He said, "Until recently I kept a lot of priceless homemade videos on an external drive. As bad luck would have it, that drive died; and all my movies, I thought, were gone. I purchased and downloaded SpinRite 6 and didn't have much hope. But then out of the blue all my data came home to me. Thank you so much for creating this wonderful software. Crappy software is certainly out there, but it is not this by a long shot. I only hope that others find this great software. I know I will be recommending it. Much success to you in the future, and keep up the good work. DMW." So thanks, Darren, for sharing your testimonial about SpinRite. I really appreciate it

Leo: Very good. Very good. Question 1, Drew in Virginia Beach, VA. He wonders about old code: Steve, I love the show. Insert normal kudos, hooahs, et cetera. You

and Leo are as great as SpinRite is awesome. I'll refer you back to Episode 221, my friend, where you were saying that old code is better code. But if you recall, several episodes earlier you went into detail about how a voting machine, secure in its day, could now be hacked due to improvements over time. Seems to me this is a case where a new security hole was created by its age, since I think you said the ability to find the hole was due to 20 years of advances. Because code, finally able to be stress tested, showed flaws not initially known, doesn't this say old code isn't better, just more abandoned? Just a thought. Hope to hear your response. Drew.

Steve: Well, I wanted to put this question in, also as a proxy for all the people who wrote. It's interesting. I guess this is sort of a little bit of a religious issue, religious in the sense of what one believes that...

Leo: It's a matter of faith.

Steve: It's a matter of faith. And I wanted to say I don't know that there's really a right answer. It's certainly the case that code can be written to be incredibly bulletproof, but to do so is incredibly expensive. I look at the code that is used to run the shuttle, the NASA shuttle project. And the amount of reviewing and testing and debugging that they do makes that the most expensive code per byte that, I mean, it's orders of magnitude more expensive. But it has to be correct. So it is possible to create correct code. It's just excruciatingly expensive. I mean, it's uneconomical unless the cost of a mistake is people dying in outer space. So we don't have code typically that is written that well because it's too expensive.

I mean, I'm reminded, remember the horrible story with the Pinto with the bad gas tank where it was found that if you rear-ended a Pinto, that the gas tank had a high likelihood of exploding? And it turned out that the manufacturer knew about that. But they made the decision that, well, a certain number of them are going to have that problem, and we'll make restitution for those problems. But that makes more sense than recalling all the Pintos that have been sold. I mean, it was an economic calculation that was hard to understand, but that's the one they made.

And similarly, everyone wants code to be bug free, but it's so difficult to make that happen. It's just it's not economical. So in practice what happens, and this is what we spend so much time on this show looking at in detail, dicing and parsing, is that code is launched with problems. And in fact I remember, I haven't seen this for a long time so I don't know if Microsoft is still doing it - and I'm sure you'll remember, Leo. Remember those days when we could see, we would see, there were public bug lists of known problems in newly released versions of Windows. And, I mean, it was like 50,000 problems. But it was like, you'd read them, and you'd just kind of, oh my goodness, this is what they've released? It's like, yes, but this is only going to affect people whose first name begins with F and live in Tampa on odd Thursdays of a full moon. I mean, it was just unlikely things to happen. They know it's there, but oh, well, we didn't get around to fixing it because we promised everyone we were going to ship this thing in the same year as the operating system was named, and it was getting near Christmas so we really had no choice.

So what Microsoft does is, well, I'm sorry, what everybody does is pretty much do the best job they can and figure that, well, as problems arise we'll fix them incrementally. Well, what that means is that, as long as you stop adding new things, if all you do is fix

problems, and you fix them carefully so that your fixes don't induce new problems - and that's one thing we do see also, we often see fixes creating new problems. But if you're really careful, then in theory older code is allowed to become more bulletproof over time. And if you can then stop messing with it, if you can stop adding things to it, it has a chance to get better. But it's also the case that people can make more problems than they're fixing, or they can stop messing around with it and cause more problems.

So again, I completely recognize that there are many ways to look at this. Maybe there isn't an answer. Maybe it's not possible to say old code is better than new code. I like to think that systems which have been around a while, that have been maintained well and carefully, are - if nothing else, they're a known quantity from a security standpoint. Whereas anything new is, I think, fundamentally more dangerous. I think that I can state with some reason to have some authority.

Leo: Okay. I think there's problems on both sides. That sounds perfect.

Steve: Yes. There are problems with both sides. But if nothing else, something which has been around is a known quantity.

Leo: Right.

Steve: And I guess that's really - I guess that's...

Leo: Better the devil you know than the devil you don't know.

Steve: From a security standpoint I think that's absolutely true, yes. So, you know, I can stand behind that representation.

Leo: Yeah. And following along the same lines we've got one from an anonymous listener who says: Is old code really better than new code? After four-plus years of listening, it's apparent you favor old over new because you think the problems are discovered, known, and perhaps even fixed. Being a software guy myself, who started programming on the original PC in assembler, then spending the rest of the '80s and '90s at Lotus working on 1-2-3 and others, I can understand your favoritism. Yet the thought occurs to me that, given the last five years of concentration on secure code creating by Microsoft - ah. This is a good point actually.

Steve: Yes.

Leo: Perhaps the favoritism might be misplaced. I have the advantage, as you do, from MSDN to play with the new O/S and apps. And I'm suggesting a case can be made that newer software coming from Microsoft is more secure than old stuff. For example, I find IE8 much more - well, we [chuckling]. I find IE8 much more secure than Firefox or Safari or the previous IEs. Well...

Steve: Oops.

Leo: Maybe not. Windows 7 seems more - "seems" is a big word - more secure than Windows XP. It's a thought I'd like you to mull over because I'm interested in what you think. He's saying essentially that improved techniques in writing software and improved coding tools make it more reliable.

Steve: Yes. And I thought, because this was a different question than the first one, this was also worth looking at. One of the things that I have been - that I try to be very careful about is to separate insecurity from mistakes from insecurity from policy. I've really never argued strongly about Microsoft's security mistakes. I mean, we point them out. We're sorry for them. We hope they're going to fix them soon. My argument with Microsoft traditionally has been that they were insecure by policy. They had a firewall in XP that was turned off when you installed it. And they said, oh, well - I remember this so well. Yeah, but the path most users will arrive at as they're installing XP, they'll come to a dialogue box, they'll be offered to have it turned on or something. I never bought that, and that was never the case. Which is why XP's firewall initially was off all the time, and they were having all these problems with - the other problem, by policy, is services that were running by default, by policy, in Windows.

So my traditional argument with Microsoft is that these were not mistakes they were making. These were policies. I mean, this wasn't some coder who had a wrong check for the end of a buffer in code. This was Microsoft saying, well, it'll be easier for users if these things are turned on by default. It's like, yes. And it will be easier for hackers to get into those users' computers if those things are turned on by default.

Leo: Right.

Steve: So the good news is, slowly, I mean like glacially slowly, Microsoft's security policies have matured, at a speed that's so slow I can't and I will never understand why. But it has happened, and we're here today rather than where we were years ago, where the firewall is on by default. Services are not on, or at least not exposed. And they finally offered this notion of local services, where they understand things make sense to have on the local area network but not published out over the Internet, so the notion of a service scope, where it's a local scope as opposed to a global scope of access. So that's very much the case.

And certainly also the focus that Microsoft has had is having an effect. I do agree that Microsoft is clearly concerned about security. This anonymous listener mentions the MSDN, which is the so-called Microsoft Developers Network, which I subscribe to every year. And now when I look at the online help for Windows functions, many of them have new stuff in red where it says, warning, this function is deprecated in favor of the following function, which will perform end-of-buffer overrun checks for you. It is strongly recommended you not use this function, you use the new one. And so they're creating an awareness which is really important. I mean, just doing that, just saying, uh, wait a minute, smoking is bad for your health is on the carton. So it's like, oh, it's going to affect somebody. And just warning developers, this function could be bad for your code security. Make sure you want to use it, and why not go check out this one. I mean, that kind of thing makes a lot of sense. And so, yes, I do agree that Microsoft's new stuff is certainly better than when their old stuff was new.

Leo: It's not merely that, though. I mean, for instance, buffer overflows come from using, you know, not checking bounds and things like that. If policies are in place for programmers to do the right thing, or even maybe compilers are smart enough to prevent that kind of thing, doesn't that make them less likely?

Steve: You know, the problem is programmers don't want a compiler to be that smart because then they're not fun to program.

Leo: Right.

Steve: Programmers want macho. They want horsepower. They want access. They want C pointers where you're able to play games at a low level. The reason C is such a popular language from the beginning is that it is so dangerous. And programmers want the danger. There are certainly languages which could be created that absolutely will not let you make a mistake. They just don't have the capability of those kinds of errors. And those languages exist. They're well understood and well known, and not well used. No one wants to use them.

Leo: Like Ada.

Steve: Yeah, well, I mean, I don't know specifically if Ada doesn't allow you to do that. But it's certainly the case that, you know, heavily interpreted languages just don't give you the flexibility. They're absolutely safe, but they're just not - they're not macho.

Leo: Yeah, yeah. Not macho. I like that. Programmers, stop being so macho. You're causing problems. Let's talk about the Web of Trust. Brandon in Indianapolis wonders about such things. He says: Back in Episode 214 you guys highlighted the Google.com/safebrowsing page. It's very cool. However, why wouldn't someone just install Web of Trust? It's over at www.mywot.com. This is new to me. It's an add-on for Firefox and Internet Explorer that will rank sites based on reported malware and phishing and so on. It ranks sites three ways: Green is trusted; yellow is proceed with caution; red, don't ever go there. On sites that have malicious ads or pop-ups on them, the add-on will warn you before loading in the pop-up, asking you if you're sure and informing you the site is known as a malicious one. Best part is it will rank search results. So you can go to Google and type in "free," and it will give you red, yellow, and green rankings on each site. I use this in a couple of ways. One is to stay protected, the other to infect virtual machines with malware and then try to clean them later. What?

Steve: I think he's saying that this will help you find bad sites so you can go to them and get yourself infected. It's like, okay.

Leo: I've installed - okay is right. I've installed it on my mom's PC as I'm always the one she calls when she has issues. You guys do a wonderful show. Been listening since Episode 1. Keep up the good work. Well, did you try this little plug-in?

Steve: I didn't. But I wanted to address the idea, the concept of webs of trust. It's not something we've ever talked about in all of our episodes, all 224 of them. Well, I guess now we have, so this is Episode 224. So not in the previous 223 episodes. You know, the concept is an interesting one. It sort of evolved out of the frustration, I think, of 4K trust assertion. We've often talked about how annoying it is that people have to purchase certificates from a certificate authority, that these people who are really doing nothing other than issuing some bits are needing to be paid because what they're doing is some research. They're performing research. Every couple of years I've got to go jump through hoops. They've got to do telephone calls, and they check my D&B numbers and things in order for me to get SSL certificates for GRC.com. I have to prove, you know, who I am, and that I'm the webmaster for that domain, and we're a real corporation, and we've been around, and here's our address. And, you know, this information is current. So in return for all that, they make an assertion that they stand behind. They get some money to run their infrastructure. I get my certificate, which then has to be renewed every few years, and we go through all this again.

There are, you know, people in the Richard Stallman sort of world who just hate all that idea. And so they've said, wait a minute, rather than have a single central authority that everyone trusts and that that authority then makes assertions, why not create a web of non-authority, but by having the web be big enough and people sort of vouching for each other, then that sort of creates sort of this floating set of assertions where a whole bunch of people have all agreed that this person is who they say they are, and they've made similar assertions. I'm sure you've heard of these Web of Trust parties where people will get together and show each other their IDs, sort of verify them informally, and then...

Leo: Yeah, it's for PGP key signing, yeah.

Steve: That's a perfect example, where it creates, I mean, and that's an instance of a web of trust. In this case, for example, where we've got this Web of Trust server, it's relying on people to report malicious conduct and sites that they run across as they run across them. And then it uses these add-ons in the browsers to alert people so the browsers are, whenever you're trying to go somewhere, the browser's add-on is going to ping back to this mywot.com server with the URL; ask that server to represent whether it knows anything good, bad, or indifferent about the site; and then present the user with green, yellow, or red based on that. The alternative that he mentions is Google, which is out there spidering the world, literally the entire Internet, and using its own analysis of what sites do to determine whether they are doing known bad things or not.

Leo: And actually OpenDNS is similar. It will flag a phishing site. It's not as effective as Google or MyWot, probably, but...

Steve: Yeah. And anyway, so...

Leo: There are other people doing this.

Steve: Yeah. I guess, I mean, if you had a large enough community, if you had people actively feeding back their experiences, then I think the notion of a web of trust for this can function. I guess if there's a way to have both, I'd just as soon have both. That is, use the web of trust plug-in and also use Google as my search engine, and let Google

make sure that it's looked at these links before I have the opportunity to click on them, so I have a chance to protect myself. So anyway, I wanted to highlight it as an alternative and also to sort of talk about something we never have before, which is this notion of sort of a non-central authority sort of cross-representation of trust as an alternative.

Leo: Yeah. I'll have to take a - I mean, I'm looking at it. They have a decent pedigree. They're funded by Open Ocean and Finnish - they're from Finland. It looks like they do tools. I'm not sure exactly where their system is a community-based system, even though Web of Trust implies it is.

Steve: Yeah, and it does sound like from the description that maybe you use the add-on in order to send the feedback back. So you probably have the add-on as the interactive agent.

Leo: Of course then you have to trust them because you're - so it's more than web of trust. It's a leap of faith. I'm going to have MyLOF.com. Number 4, John Edwards from Edinburgh, Scotland. He's in password hell: Dear Steve. On SN-222 you spoke of an overheard discussion at your local Starbucks - other coffee outlets are available. The discussion was a company's policy of making their employees change their password on a regular basis. You said this policy makes sense. But it seemed the people in the discussion thought otherwise. They were trying to find all sorts of ways to circumvent it, kind of ridiculously extreme ways to circumvent it.

What do you say to the whole big wide world of Joe Public who have to use passwords and usernames for most all of their everyday life, be it paying bills to numerous firms, banking, email, general shopping, eBay, PayPal, Amazon, even tax and yes, TWiT forums. The list, as we all know, is endless. The last count I had 65 different sets of passwords and usernames, of which 21 were essential. Now, try and keep all those in your brain, never mind having to periodically change them, voluntarily or under pressure. I can sympathize, he says, with the people in that overheard conversation. These people no doubt have the same problem we all do. And day by day it just gets worse out there. Where is it going to end up?

Steve, I often joke to my friends at the bank. I say, "Guys, if you give me anymore passwords, I'll have to start a wee black book to keep them in." I'm sorry, I didn't say "book" right. Book. A wee black book. All joking aside, Steve, I guess many people do just that. I have a half a dozen bank accounts. Each one needs a telephone inquiry password or an Internet banking password and username. And they're all starting to move toward three-part passwords, that is to say, three individual passwords and a username. It's a security nightmare. Help! P.S.: I now find I can't live without Security Now!. As each week passes by, I become more educated and terrified. Keep up the terror, guys. Well, that's what I do. I use Evernote, and I keep all my passwords in there, and I encrypt them.

Steve: Yup. And Leo, I'm still using - we've talked about this a couple times - an offline Palm Pilot, sitting off to the side here. It's by my right hand. Anytime I need it I can put in a few characters, because the little notepad has a very nice search, and it instantly finds, like I remember that I wanted to know what my Chase - I have, like, Chase online access to my main credit cards. And I'd forgotten what my Chase password was.

Leo: Oh, yeah, all the time.

Steve: And it was something that I wanted to make sure was going to be very, very safe. So I put in CHA and hit find, and bang, there it finds it. And I look at it, go okay, and transcribe it onto the web browser, and then I'm logged in.

Leo: Now, do you sync that to anything? Or is it just on that Palm?

Steve: I do not sync it to anything because I don't...

Leo: So if anything should happen to that Palm, what are you going to do?

Steve: [Laughing] That's a problem.

Leo: Yeah.

Steve: Yeah. It will sync itself to an SD card because it's got an SD card reader. And so I'm able to copy it to an SD card.

Leo: Oh, all right.

Steve: But I don't want to sync it to a PC because then all that stuff is in the PC, where it's then no longer offline.

Leo: Well, and that's the problem I have with Evernote because it's, you know, the convenience of it is it's on my iPhone, it's on all my computers, and it's in the cloud. But it's risky. Of course I do encrypt. But you have to trust their encryption. And, by the way, my encryption password, it's just the same, it's one password. So in effect there's one password to get all that data.

Steve: Yeah. And if I were to start again I would probably do something like that. At this point, since this sort of has been my incremental solution for many years, and it works, and it's as secure as I can, I mean, it's not universal. I don't have it on my portable phone and other things. I will not stick it in my phone because we were just talking about problems with iPhones. So, I mean, this is a dilemma. And I liked John's note because he just sort of says, you know, this is really a problem.

And part of me thinks that, one way or another, eventually this will be solved. It's hard to guess what the solution will be. I mean, it's hard to know what the solution will be. Maybe it'll just be solved incrementally. It may be that we'll, you know, we've talked about solutions. Like things like VeriSign, where they offer a one-time password based on a credit card with a battery in it, or the football that is based on time. And so you loop through third parties. It may be that ultimately these sorts of things, which are still

nascent, which are still not universally adopted, will begin to see some convergence around a solution. Or our favorite little gizmo...

Leo: The Kindle?

Steve: The USB gizmo. I can't believe I've forgotten what it is now.

Leo: I've forgotten it, too. I know what you're talking about. Stina's thing.

Steve: Yeah, Stina's thing.

Leo: YubiKey.

Steve: YubiKey, yes. It might be that something like that makes absolute sense. So I just sort of wanted to say yes, John, I feel your pain, and I feel the pain of this poor guy that we talked about two weeks ago who was deliberately jumping through hoops so as not to be forced to change his password because he so much didn't want to. And the bad thing is we know most people, most non-listeners of this podcast are using one password for everything.

Leo: Oh, yeah.

Steve: Or just a couple. And they're vulnerable to that being - losing control of it, to it getting away from them. But...

Leo: And there are choices. There's, like, KeePass. There's RoboForm and 1Password on the Windows and Mac, respectively. I mean, there are tools to do this.

Steve: Yeah.

Leo: But the people who use them are more sophisticated, frankly. My mom doesn't use a password manager.

Steve: No. And we talk a little bit - there are some interesting questions this week. We're going to be talking briefly about this notion of Internet access as a human right and how we feel about that. And there's this notion that, as a consequence of pressure on us, we're being pushed onto the Internet. I mean, it's necessary almost for more and more things that we want to do during the day. Unfortunately, authentication comes hand in hand with that. We need to be able to identify ourselves in a secure way. And, I mean, I really see this as a huge disconnect, a huge problem which is burdening people, for which there isn't a unified solution. There isn't one solution that works for everybody because it's not all pulled together yet. And somehow it needs to be. This is the kind of thing that Stina and YubiKey and VeriSign and these kinds of companies are saying -

they're out there waving their arms around saying we solved the problem, we solved the problem. Except they haven't until everyone uses them.

Leo: Right.

Steve: So, and we've talked about also the problem of having like a keychain full of dongles of non-unified solutions. That's not a solution, either.

Leo: No. And so I'm glad he wrote because I certainly hope we didn't come off as unsympathetic to these guys. I didn't really like the way they were solving it; but, I mean, I share their pain. Doug Smith, Albany, New York worries when human rights become inhuman rights: Hi, Steve and Leo. A couple episodes ago, I'm not sure exactly when, I recall you and Leo discussing a move afoot in some places to establish Internet access as a basic human right. My take on your comments was that you both were leaning in favor of that idea, basically pointing out there is much that people miss out on if they don't have access.

While I don't dispute the idea, I must say my gut reaction was more of fear rather than comfort because I believe that it should be a basic human right to be off the grid, as well. There's a different between a right and a requirement. But all right. We'll go on. I don't think anyone should be obligated to have Internet connectivity to fulfill their civic duties. They should not be required to have an email address. They should not be required to have a cell phone. I'm with you on all of this. They should not be required to vote electronically over a network. They should not be required to submit their taxes electronically, and they should not be required to have Internet access at home in order for their children to attend public schools.

I'm much more afraid of the ways government would abuse Internet connectivity when it is deemed to be available to everyone than I am of the consequences of people not having access. The fact that not everyone has access means that government is still responsible for communicating with us even if we don't own a computer or have an ISP contract. Just another perspective I'd like to hear represented. As always, thanks for the great podcast. You guys are the best. Doug Smith. What do you think?

Steve: I really do see his point. I've been, as a non-parent, I hear stories from other parents of, like, the way papers are submitted now. Even at the high school level you can't submit papers handwritten. They have to be printed from a computer. And one of the reasons is that they're put through a central clearinghouse, an online database, to look for forgery or for...

Leo: Plagiarism, yeah.

Steve: For plagiarism. And when my sister told me that my niece and nephew were doing this, it's like, huh? I mean, that was news to me. And so seems to me that that's a good example of you have to be using a computer. You have to have access to a computer. And I think that's what he means by they should not be required to have Internet access at home in order for their children to attend public schools. I mean, it's the way things are done now. And I know that one of the gals that I hang out with at

Starbucks in the morning is a schoolteacher, and she sort of - she's a science teacher for her elementary school and sort of has taken up the responsibility of educating the other teachers in using the web services that are available. And it's not possible now not to use that sort of technology as a teacher. And she posts things on her site which she assumes students and parents will have access to. And the sense is you have to be online now in order to be functional in a public school.

And I completely agree with him. I heard you chiming in when he talks about email and cell phones. I'm annoyed now when I'm filling out a form, and some random form line wants my email address. I protect my email address. I don't want spam. I want control over that. And the idea that this is the way I'm going to be contacted, I would like the choice. And so I really understand what he says. I'm not sure that I intended us to sound, like, positive or encouraging of the notion that Internet access was being defined as a human right. I just thought it was interesting in the sort of, like, wow, that strikes me as a big deal, as a significant thing, not something small.

Leo: I'm of the opinion it absolutely is a human right. And the point being that everybody should have it available, not required. Although what if we take what he just wrote, and we put in "telephone" or "snail mail" or "television"? I mean, part of what he's saying makes sense to us because these are new technologies. But you wouldn't really be puzzled by somebody who said what's your phone number and then had difficulty dealing with you because you didn't have a phone. We've accepted that as being kind of ubiquitous.

Steve: Yeah, that's true. If someone actually had no cell phone and no home phone...

Leo: No way of reaching them by phone.

Steve: No phone.

Leo: That's their right. It's their privilege. But as a result there are going to be some consequences in the modern world.

Steve: Yeah.

Leo: And because that's an older technology we kind of accept that. We understand that. And there are some hermits who don't want a phone, and that's fine. You can do that. But expect to have a little more difficulty in your life. And I think that's all that's going to happen here.

But what's very important is - and I think it's akin to electricity. I often liken it to the rural electrification programs of the Great Depression, where there were people in this country in rural areas who had no access to electricity. And it was deemed a priority by the government, and it happened to help in the Depression employ people with programs like the Tennessee Valley Authority to electrify these rural areas because - you know, "right" is a strong word. We can argue about what's a right. But it's certainly something everybody ought to have access to is electricity. And I think

the Internet is very similar to that now. You don't have to have electricity. You don't have to have a phone. You don't have to have the Internet. But you should have it if you want it. You know? You should have the right to have it if you want it.

Steve: Yes. You should be able to get it, and it should be affordable.

Leo: Yes. It's not free. Nobody's saying it's free.

Steve: Reasonably affordable.

Leo: But there's lifeline phone service that's subsidized by all of us who have phones so that people who can't afford a phone, can't afford a full price phone, can at least get lifeline service because it's recognized that a telephone is a vital important lifeline, at least for 911 if nothing else. So I think it's like that.

Steve: There are public utility or public service opportunities for web connection also, like public libraries, where you're able to use a computer. And thanks to web-based technologies you can have an email address on Google Mail or Hotmail that gives you an email address even though you don't have your own Internet connection and computers and things. So there are ways to solve the problem.

Leo: They do that, in fact, at least here in California, for homeless people. They have programs to give them phone numbers and email because it's hard to apply for a job if you don't have somewhere you can be reached.

Steve: Right.

Leo: And the idea being, if you provide this for these people, maybe they can get work, and they can get off the streets. But, you know, it's very hard to get off the streets, when you're living on the streets, if you've got nothing.

Steve: Right.

Leo: So I don't think anybody's saying that there's an equivalent between a right and a requirement. I'm just saying that I think it's very important that we recognize Internet access is increasingly important to participation in our modern world.

Steve: Yeah, and I do like your analogy with the notion of telephone, for example, or even electricity. I mean, it's, yeah, I think that's a good one.

Leo: It's easy for us with new technologies because, I mean, well, we lived without a

computer, you and I, when we were young men. We lived without email. We survived. But times have changed. I wouldn't expect my kids to do so. Although I'm reading Jerry Pournelle's book right now, "Lucifer's Hammer," about a comet hitting the earth and losing, you know, basically civilization is gone. And you really realize how dependent we are on technology. And, I mean, there's not - there's only, I don't know how much, 30 days of food in the U.S. We all live pretty - almost hand-to-mouth, really.

Steve: Wow.

Leo: So should something horrible happen - and by the way, he also raises the issue in the book, very few of us actually know how any of this works. You get in your car, and you drive around, but we have no idea how it works.

Steve: It's a really good point, too, how much of the detailed knowledge required to recreate the technology is gone.

Leo: It's gone.

Steve: Yeah.

Leo: We're living in this house of cards. Let's hope it all stays okay here. Hey, Joe Perleberg from Green Bay, Wisconsin has our next question. He has some insights on the fingerprints that we've talked about in the past required for checks at the bank: Steve and Leo, I was listening to the latest episode of Security Now!. I have some more information regarding the taking of fingerprints when cashing checks. I live in Green Bay, Wisconsin. And of the many banks I went to around town, nearly all of them, all of them required a fingerprint to cash a check for a non-account holder. Also, I even noticed some retailers that asked for a fingerprint - whoa - when writing a check over a certain amount to purchase items. Wow. Retailers now have fingerprint devices? I completely agree with your stance on the issue, but I thought you should know that this is by no means an isolated incident. I was told by several banks this is a new measure to protect against check fraud, but that it doesn't necessarily stem from 9/11. Which is what I thought. Thanks for putting out an excellent show.

Steve: You know, I guess I'm sort of out of touch with checks. I'm not a check user.

Leo: Don't use checks.

Steve: Yeah, I use my credit card as cash and then pay the balance every month, so it works for me. The card company's not real happy with me because they don't make any money from me. I guess they get a percentage, though, of all of the money that I run through the card, so they're making it there. But I thought that was interesting feedback. The problem of course is that, you know, you mentioned, whoa, retailers are taking

fingerprints now. The problem is storage is cheap, data transit is virtually free, and the technology for reading fingerprints went from once upon a time getting ink on you that no one would want to do, to sticking your thumb on an optical scanner. Well, the cost of doing that has just dropped to nothing. So...

Leo: I have one on my new Dell computer. And actually I kind of like it. It has a preboot authentication. So it's kind of like the BIOS password. When you open the thing up, before Windows even does anything, you have to scan your password. I kind of like that.

Steve: Yeah, well, I have it on all of my laptops. Not my Macs, but both of my Lenovos. And the drive is encrypted. The fingerprint is down in the TPM, the Trusted Platform Module.

Leo: It's TPM, that's right, yeah.

Steve: Nothing can get to it. And it turns on, and it says, okay, let's see who you are. And so I swipe my finger over the scanner, and it looks for the match and finds it, unlocks the drive, and then it can boot. But until I do that, it's locked up tight. No, it is - see, there I have no problem with it because I'm controlling the information. It's in the TPM. And it's my laptop recognizing me. The idea, though, I mean, it just, oh my god, the idea that retailers are sucking in people's fingerprints, we're in for a fall. This is not going to end well.

Leo: I like it. It's like your mom saying, "This is all going to end in tears."

Steve: This is not going to end well.

Leo: Joe Dorward from Berkshire, England brings us the Head Shaker of the Week report: Steve, I just attempted to log out from my Hotmail account. Here's the error message I got: "Sign out failed. We could not sign you out because your browser seems to be blocking third-party cookies. Close all browser windows to sign out. To prevent this error in the future, you must enable third-party cookies by changing your browser settings." Thank you.

Steve: That's the most backwards thing I have ever heard of.

Leo: Well, I can't even think of why, right, because you're in Hotmail. This is first-party cookies they want to set. Who's setting a third-party cookie?

Steve: And it's to leave. It's not to...

Leo: It's not even...

Steve: It's not to sign in. It's not like they're using some third-party authentication server. I mean, apparently they are. But they're trying to do that to say goodbye somehow. And so they're saying, well, unfortunately we cannot log you out because you're blocking third-party cookies. Which means we're sending your browser something to cause it to get something from another server. And because you're not sending a cookie back, that other server can't recognize who you are, and that's preventing us from accepting your logout. It's like, okay.

So then they're saying close all browser windows. So that at least is good. That means they're using session cookies somewhere rather than persistent cookies. So losing your session cookie is what happens when you close all your browser windows. So that's good. But then they're saying, just so you don't have this problem in the future, turn on third-party cookies so that we can log you out next time. I don't know. It's just I got the biggest kick out of that. It's like, okay, well, who knows what Hotmail is doing.

Leo: You see nowadays a lot of sites that require third-party cookies in a lot of ways. I use a service called Feedly that is kind of a home page service I really like for - it gives me Google Reader and my home page at Firefox. But for obvious reasons it needs third-party cookies because it's on the Feedly site, but it's getting it from Google Reader, I mean, it's just - you're seeing more and more of this. But as we've talked about before, and I encourage people to listen to earlier shows, third-party cookies are a way information can leak from the page that you're on to somebody else and can even leak across site.

Steve: Yes. And so I would say that awareness of them is all that we would really hope people have. And then arrange a solution that works for you.

Leo: Now, you treat all cookies as session cookies; right? You say they're only alive through the session. Or is that you that does that?

Steve: Yes. It's a nice setting in Firefox that allows me to normally discard all cookies. But when I'm at a site where I do want to be remembered, then I use just a simple little tool. And it's simple to the point where you don't even need it. If you went into Firefox's UI you could say "trust this site." But it allows me just - it's a little tiny "c," "c" stands for cookie, and I'm able to click on it and just say, like when I'm on Amazon or eBay or PayPal, a site that I care about where I'm going to be coming back in the future, I'd like them to remember who I am, I just say, yep, remember that cookie. And so it creates an exception to the normal policy of discarding them all the time. And then they're persistent. So it's, again, it's an opt-in rather than an opt-out approach.

Leo: Right. And Euchre [sp] points out in our chatroom that the reason Hotmail would do it is because you're on Hotmail.com, but there are other Microsoft.com and maybe even Live.com sites involved. And so those would show up as third-party cookies. Even though they're all from Microsoft, they're different domain names; right?

Steve: Right.

Leo: So I guess that makes sense. Our last question, Mr. Gibson, comes to us...

Steve: This is so sad.

Leo: I haven't read it yet. But I see the title. I'm intrigued. Steve in Rochester, New York brings us the Sad Biometric Stupidity Story of the Week. I love these. This is of the ilk of the knuckle at Disneyland; right?

Steve: Oh, if only.

Leo: Worse? Hey, Steve and Leo. I just finished listening to Episode 222 with the story about a man who couldn't cash his wife's check without giving up his fingerprint. We were just talking about that. In early September, at a Bank of America in Tampa, the same thing happened. The really sad part is the bank wouldn't make an exception even though the man had no arms and therefore no fingerprints to give. This is the story at ABC local news. Unbelievable. "Man with no arms denied check cashing. A man born without arms is upset that a bank would not allow him to cash a check without having a thumbprint. Steve Valdez said a Bank of America branch in downtown Tampa [Florida] would not allow him to cash a check from his wife last week." He wasn't an account holder, so as usual they asked for a thumbprint. He's got prosthetic arms, but there's no fingerprint. He presented two forms of ID, still was denied.

"He said a bank manager told him he could either come back to the bank with his wife or open an account himself. Bank of America spokeswoman Nicole Nastacie said the bank has apologized to Valdez. [She] said the bank should have 'offered alternative requirements if an individual is not able to give a thumbprint.'" I wonder what happens at Disneyland to the guy. That's just, oh, that's...

Steve: Isn't that amazing?

Leo: I think he has a lawsuit under the Americans With Disabilities Act, to be honest.

Steve: I would imagine. I mean, here's a policy which obviously wasn't well thought through. And it's like, okay. And, well, and so here's the problem. As we move forward, and the need for a fingerprint becomes ubiquitous, what does he do? I mean, it's nuts.

Leo: Not everybody has a fingerprint.

Steve: Not everybody has one to give, even if you wanted to give one.

Leo: Sorry.

Steve: Yeah. And believe me, I'm sure our listeners know, resist with your last breath. I mean, again, the idea that retailers have fingerprint scanners, I mean, [verbal shudder]. It's a reason to use a credit card.

Leo: Well, you know what's next: DNA. Everybody can give DNA in some form.

Steve: You're probably right. So here, lick this swab, and we'll...

Leo: Yeah, give me a hair. You know? I mean, seriously. I think that we are ready - and by the way, the implications of that are terrifying.

Steve: Oh, boy. Because after we've got the genome sequence, yes, then it's like, oh, well, don't worry, we're going to check out your health factors in the future and see what problems you're prone to. Oh, no, it gets very Big Brother-y pretty quickly.

Leo: I just got word that I am going to be allowed to participate in a very interesting project that a geneticist named George Church does, or is doing, that you're probably going to say, Leo, stop right now, don't do it. He's at Harvard. And he is doing - let me see what they call this. He's at the Harvard Medical School, and he's a professor of genetics, professor of health sciences and technology. He's got a project called the human, I'm sorry, the Personal Genome Project, in which he asks...

Steve: PGP.

Leo: PGP. He asks people to not only give up their genome - you volunteer for this - but also to answer extensive questionnaires about your phenotype - medical records...

Steve: In order to match them up, yup.

Leo: Reason being, if somebody is willing to do this, if enough people are willing to do this, there's huge value because you can say, well, look, here's a gene site that seems to be correlated to obesity.

Steve: Yes.

Leo: But you can't do that unless you've got the two. So Esther Dyson has volunteered to do this; a number of his colleagues at Harvard. And I said, you know, I'm already a public figure. So I can't be harmed at this point by this kind of stuff. I self-insure because I have my own business. So I don't have to worry about discrimination by employer or an insurer. So I volunteered to do this. And by the way, all data is published including your name because they say we can't guarantee full anonymity.

Steve: Wow.

Leo: So rather than try to guarantee full anonymity, we tell you upfront we're going to publish it.

Steve: I think that's very cool. I mean, if that's - I think - I take my hat off to that. I think that's exactly the right way to do it.

Leo: Yeah. Just don't promise something you can't guarantee.

Steve: Yeah.

Leo: However, you can see the huge societal value to people volunteering to do this. They hope to get 100,000 volunteers.

Steve: Yeah.

Leo: Anyway, I volunteered. We're going to interview him on Futures in Biotech and talk about it. And I realize, I understand the risks. I mean, I understand maybe better than most because of doing this show with you for so long. But I think it's worthwhile.

Steve: Yeah. And, I mean, certainly this kind of information could be used for good. And of course it could also be used for discrimination.

Leo: Yeah.

Steve: Which is, you know, the dark side of that is, well...

Leo: Absolutely. I could be denied insurance. I could be denied employment. But I'm of an age now, and my business is my own. So I feel like relatively protected. I mean, 10 years from now I could be on the street looking for work. But I'm willing to take that chance. And I think there is such a benefit. Anyway, we're going to talk to him. I think it's very interesting.

Steve: Very cool.

Leo: They don't do your whole - they can't do your whole genotype. They do a portion of your genotype. But it is, you know, it's very interesting, I think.

Steve: Well, and it makes sense that it needs to be voluntary because this is

supersensitive information. And...

Leo: They have a very extensive informed consent document, as you might imagine.

Steve: Yeah.

Leo: And you have to pass tests and so forth before you can participate.

Steve: Cool.

Leo: I think it's very, very interesting. People want to know more about it, it's PersonalGenomes.org. And I don't know if they're looking for volunteers from the public yet or not. I know that was the plan. I guess they are. It's a very interesting idea.

Steve, I really appreciate your time, as always, and your insights. And it's so valuable to talk to you. And I thank

you for doing the show, as I know everyone else does. People can go to Steve's website, GRC.com, Gibson Research Corporation. That's where all of the freebies like ShieldsUP!, DCOMbobulator, Shoot The Messenger, some great security stuff, Perfect Paper Passwords, live. Also 16KB versions of this show. Thanks to Steve, by the way, who's taken over the editing of that. Do you do that yourself, or do you get somebody to do it with you, or...

Steve: No, I do it myself. You drop the file in the drop box, I get it in the later afternoon, I edit it down and post it for Elaine to do the transcriptions.

Leo: That's very nice. Steve pays for the transcriptions, too. So this is his commitment to you. So transcriptions, 16KB versions, and of course the full version and all the show notes at GRC.com. And while you're there, help Steve out a little bit. Help a brother out. Pick up a copy of SpinRite - help yourself out - the world's best hard drive maintenance and recovery utility.

Steve: It may come in handy.

Leo: Yes, it may, definitely.

Steve: And this is our Thanksgiving episode. So Happy Thanksgiving to everyone, those who observe Thanksgiving.

Leo: That's right, this will ship on Thanksgiving, that's right.

Steve: Yeah.

Leo: So if the turkey didn't put you to sleep, maybe we did.

Steve: If the tryptophan doesn't get you...

Leo: Security Now! might. Great, Steve. Thanks. Have a great - are you going to Mom's for Thanksgiving or staying home?

Steve: Nope, going to have dinner down here in Southern California with a bunch of friends. And I do Mom's on Christmas.

Leo: That's great. Not a ham sandwich, I hope, on turkey day.

Steve: Nope.

Leo: Okay. Get some actual turkey in you.

Steve: Thanks, Leo.

Leo: See you next time on Security Now!.