# SECURITY NOW!

**Transcript of Episode #232**

## Listener Feedback #84

**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-232.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-232-lq.mp3

**Leo Laporte:** This is Security Now! with Steve Gibson, Episode 232 for January 21, 2010: Your questions, Steve's answers #84.

It's time for Security Now!. Get ready, fasten your seatbelts, you're about to learn about all the dangers, the hazards, the problems, the issues on the Internet. But here's the good news. Steve Gibson will also tell you what to do about it. Steve Gibson is the man in charge around here. He is a security wizard, the guy who created SpinRite, the world's best hard drive recovery and maintenance utility. He also discovered the first spyware, coined the term "spyware," wrote the first antispyware program, has written a great many security tools for free for people, and has been doing this show, well, I guess if it's 232 episodes - 232, Steve - we must have - and we've never missed one.

**Steve Gibson:** Never missed one. 232 weeks and counting.

**Leo:** Wow. Fourth year. Fifth year of this show.

**Steve:** Into our fifth year, yeah.

**Leo:** Hey, Steve.

**Steve:** Leo, it's great to be with you again, as always. I had a thought yesterday, and then again this morning a little bit, when you were talking about all the security utilities that I create, that it would be maybe useful to create one for this most recent zero-day

IE flaw.

**Leo:** Ooh, yeah.

**Steve:** But then I figured, eh, you know, the half-life of the thing is going to be very short because Microsoft is scampering apparently, maybe even considering an out-of-cycle fix because - not that this is so bad. We've seen these before. But mostly because it's gotten so much attention. And so the PR is really bad for Microsoft.

**Leo:** This is the flaw that was used to hack people's Google accounts; right?

**Steve:** Well, it's - okay. So this first came on the map when Google informed Microsoft that it wasn't, as was initially sort of just conjectured, it wasn't an Adobe flaw. It was an at-that-time unknown, that is to say zero-day vulnerability in Internet Explorer, yet another one, that was in this case being used to penetrate IE6 running on XP.

**Leo:** And of course the first thing that, what was it, the German government said is stop using IE6, and then everywhere people are saying do not use IE6 anymore.

**Steve:** Germany and France both said stop - well, actually I think they said stop using IE in general because the vulnerability exists in all versions of IE.

**Leo:** Right.

**Steve:** But due to the incrementally increasing security that Microsoft has been bringing into play, you know, we've talked about this many times, how unfortunately Microsoft's install base and their previously lax security prevents them from just turning up the security all at once. So very much like how in XP they introduced a firewall, but it wasn't turned on by default. Then in Vista they introduced, or actually at some point in XP also DEP, the Data Execution Prevention technology, but it wasn't really turned on very strong. Then with Service Pack 2 of XP they started turning on the firewall by default. So they've sort of been creeping along, tightening things down as they go. And I've, of course, for years been railing against the idea that scripting was on in email by default. Well, of course that finally got turned off along the way because no one ever did use it. But Microsoft just has to be sort of, you know, to very slowly move forward.

So many of these things that they've done incrementally over time have improved the security of IE: 7 is better than 6; 8 is better than 7. In IE8 its use of data execution protection or prevention is enabled by default, so DEP does prevent this problem. So even though all versions of IE have had the flaw, which someone presumably in China discovered, and what Google did was they found the command-and-control servers, that is, they were able to, once they realized they'd been penetrated, they found some penetrated machines, saw them communicating back to the mothership, tracked those down, found 33 other companies including Adobe, interestingly enough, that had been also penetrated. So this wasn't just an attack against Google. This was an attack against 34 companies using an at-the-time unknown vulnerability in Internet Explorer.

So there's many takeaways from this. One, of course, is to all of our listeners, I'm hoping that nobody is even vulnerable or at risk because you're no longer using IE. That is, everyone within the sound of our voices should have switched to Firefox. And I'm seeing Chrome mentioned sort of as an also option, although Firefox seems to be the one people would be moving to. I'm hoping that everyone has moved there already. Now, of course, Windows users don't have a choice about IE. We have to have IE around to some degree because Microsoft's Windows updating system, if you want to go there and check it out, it wants to be IE.

**Leo:** Yeah. But you can't even uninstall IE if you wanted to, I don't think. I mean...

**Steve:** Right.

**Leo:** ...[indiscernible] stuck with it. So I just - I don't even put an icon on the desktop. I just run Windows Update, I don't even run IE, and leave it at that.

**Steve:** Right. However, things like, for example, Outlook will still be using the IE browsing component in order to display email.

**Leo:** It's really intimately part of Windows, isn't it. You just can't get away from it.

**Steve:** You really can't. So the other - but the other point is you can lock it down. And so I wanted just to take a minute to remind our users how that's done. Because it's not difficult. You start up your copy of Internet Explorer. Just launch if it's in the tray, or you use Windows Update, however it is you get IE going. And then under the Internet Options icon, which generally most recently has looked like a little gear, you open that, go to the bottom line on the menu, which is Internet Options, and then choose the Security tab. That's where it shows you those zones.

And so IE has this notion of different security behavior depending upon whether you're on your local Intranet, on the Internet outside of your own local network, and whether the domain you're going to is trusted or not. So there's all, I mean, it ends up being a confusing and complicated thing because you could, for example, put people in the untrusted zone, which means apply presumably more rigorous security to them.

Anyway, the point of all this is, what I would recommend people do, that is, people who are already switched away from IE - IE, as you say, Leo, is intrinsic to Windows. It's there. We can't get away from it. Various apps are going to bring it up. It still can be exploited even though it's not the browser that you're normally using, although certainly your risk profile is far lower if you're surfing the 'Net with Firefox than with IE.

So you want to set the trusted sites - I'm sorry. You want to set both the Internet zone for outside and the local Intranet zone, both, even your local Intranet zone because that's the zone used, for example, that Outlook uses when it's doing things. You set the security for both those zones to high. And I made sure again that everything is set correctly when you do that. When you set your security to high, basically it just shuts it down. It can barely even bring up a web page because the security is bolted down. And this exploit does require, naturally, scripting. So scripting is shut down, both for the Internet and the Intranet. Then you can set your trusted sites zone to the default level.

Now, in doing this, though, you will completely block Windows Update from running through the browser. So you then need to, on the trusted zone, add *.windowsupdate.com and *.microsoft.com. So essentially what we've done is we've turned IE into a browser only useful for going to Microsoft and using Windows Update. We've also locked it down so that in Outlook there's no scripting and no permissions to run ActiveX controls and none of these things that are dangerous. So if you're going to view email, it's as safe as it could be using Outlook by having IE locked down.

If you for some reason need to use IE for other sites that you trust, you can certainly add those domains to the trusted sites list, and then IE will work the way it normally would. But both for reaching out onto the Internet and your own local use, if you set the security to high for those zones, then you're as secure as you can be while you're using Internet Explorer. And given that it's locked down that much, I would say you're probably as secure as when you've got scripting disabled under Firefox. But as we know, it's difficult to run during the day-to-day use of the 'Net with no scripting. So of course NoScript allows you to do that conditionally. Sort of it's doing a little bit like what IE was doing with its multiple zones.

**Leo:** One of the things, it has a checkbox that says HTTPS, require HTTPS.

**Steve:** Yes.

**Leo:** Should you leave that checked, or should you uncheck that?

**Steve:** I don't think it's that important. I put TWiT in because I also use TWiT...

**Leo:** Right, I have to uncheck it for TWiT because we aren't HTTPS. You can't require it.

**Steve:** Yes. And so I did uncheck it and do have it unchecked, that is to say, not requiring an SSL connection for all of those trusted sites. Well, because they're trusted.

**Leo:** So just to recap, you open the Internet Options control panel. You set security to the max, which breaks every site, basically.

**Steve:** Set it to high for...

**Leo:** To high, all the way up.

**Steve:** For two zones - for the Internet zone and the local Intranet zone.

**Leo:** Oh, important, that's a good point because you want local sites that way, too;

right.

**Steve:** Well, you want your local use of the IE control, which gets sort of mapped into other applications like Outlook. You want it to be locked down because, again, you don't need scripting in email.

**Leo:** All right. So we're going to go to Security. We're going to turn it up all the way to high for local zones and for...

**Steve:** Internet.

**Leo:** Okay. So let me just do that. Okay. So custom level, actually not custom level, I guess default level, and then turn it all the way up. So now it's all the way up for Internet, and it's all the way up for local Intranet.

**Steve:** Correct.

**Leo:** And then I click Trusted Sites, press the default button once again. You have to press default for some reason to have the slider. And the default here is medium.

**Steve:** Yes. And that's fine for trusted sites. That allows the normal sort of scripting things, ActiveX controls. Sites will work the way you expect them to, except that the other thing you need to do then is, while you've clicked that Trusted Sites, then there's a button that says Sites. So you click that, and that will open the list of sites that you have deliberately chosen to trust.

**Leo:** Right. And if you don't use IE, just do *.microsoft.com and *.windowsupdate.com.

**Steve:** Exactly.

**Leo:** Uncheck https, and you're done.

**Steve:** Yes.

**Leo:** And basically IE will now only work properly for those two sites, but that's all you want.

**Steve:** Exactly.

**Leo:** Does this fix the problem then for Outlook email? I mean, will Outlook email work okay?

**Steve:** It does fix the problem for Outlook email.

**Leo:** Scripts won't work in Outlook email, but that's what you want.

**Steve:** Exactly. Because scripts are the big problem. And it shuts down ActiveX controls. It just bolts it down so that essentially you've said, okay, we're not going to use IE for much. We can't get away from it completely. But, you know, where it does need to get used, at least it won't be able to do, you know, won't do any harm.

**Leo:** Now, IE7 and 8 have protected mode browsing.

**Steve:** Yes, and basically that's bringing these same things along by default. This is Microsoft again sort of very slowly, I mean, we've had the tools since IE5 to do this. But it wasn't default. And as we know - I call it the tyranny of the default is, you know, unfortunately the default is what the vast majority of people use. Microsoft I remember was saying, oh, yeah, but XP has a firewall. It's like, yes, but it's off by default. Oh, yeah, but, I mean, this mumbo-jumbo about, well, but most people will run across the dialogue that suggests they turn it on. Well, if that was true, then we wouldn't have had the Code Red and the Nimda worms, which both occurred on XP because the firewall was not on by default. So that just wasn't the case.

**Leo:** You know, it's funny, these - you've been talking about doing this because you used IE for a long time. We only recently got you to move over to Firefox, like in the last couple of years. But I know you've come on the TV shows and told us about this process. But it's really important, even if you don't use IE, to do this now because you just want to lock this sucker down.

**Steve:** Yes.

**Leo:** It's still used so often.

**Steve:** Yes. IE is built into Windows. You can't get rid of it. It's used in places you don't expect it to be used. There are other places like in the Help system or other applications that will invoke the IE control. You've probably seen like some strange software that says "Requires Internet Explorer 6 or later." And you're thinking, well, why does my MP3 player need a certain version of IE? It's because it's assuming the presence of the IE control, that is, the IE surface which it's using to render things. And there are - I don't talk about all the really obscure security exploits that occur in applications that are low instance. But there's a lot more going on that people are aware of that use a common control like this. So just, as you said, locking this down now, it's very much like turning scripting off in Acrobat. Just turn scripting off in Acrobat because you don't need it, and it will make your PDFs a lot safer.

**Leo:** I love security tips like this because they have very little consequence. Unlike, say, running NoScript in Firefox, which really kind of becomes an issue. This is easy. Everybody could do it. I'm going to do it. I'm going to remind people to do this on the radio show. In fact, why don't you come on the radio show this weekend.

**Steve:** Love to.

**Leo:** And just tell people, do this in light of what we're learning now. And then you don't have to think about it.

**Steve:** Right.

**Leo:** I like it. All right.

**Steve:** A number of our listeners wrote to tell me something that I had run across, actually I think I had a note for it last week, and I forgot to mention it. And that is that Gmail - this is unrelated to the Google attacks. But Gmail now enforces HTTPS connections by default. We've talked for years about how to get Google Mail to be secure for the entire duration of the connection. If you went to Gmail using a secure connection, HTTPS for logging in, then it left you there for your entire use of Gmail. But if you went there with an unsecure connection initially, it switched you into security for the process of logging on and then back out of security otherwise. Interestingly, and not surprisingly, Google is citing the increased use of open WiFi hotspots...

**Leo:** Oh, boy.

**Steve:** ...as the motivation, their motivation for doing this. And notably, the other free popular email, web-based email, Yahoo! and Microsoft, that is, Microsoft with Hotmail, neither use HTTPS except briefly during logon. So this really does give Gmail a leg up in security. Now, because they are concerned maybe somebody would have a problem with this, I don't really know who could, but there is an option to turn that off in the configuration settings. But the default is secure, which is really nice. That's a great move forward for them.

**Leo:** Yeah. Well, we've been telling people for a long time to just turn it on. But now you don't have to. Just it is.

**Steve:** Right. And while we're on the topic of Google, there's been so much buzz in the last couple weeks about the presumed Chinese attack on Google. One security researcher claims to have recognized code in the exploit that is known to be used in China. The problem is it's very difficult to have absolute accountability. I don't really have any particular feeling one way or the other about these claims that this was backed by the Chinese government. I mean, my sense is, well, okay, we really don't know. I dislike making accusations like that, that can't be really soundly confirmed. And frankly, there's no way to confirm this. I don't think there ever will be a way, unless somebody with direct knowledge says, yes, I know from first-hand, not from reverse-engineering something and recognizing a byte pattern that I saw once. Or these other sort of gray comments of, like, well, this is much too sophisticated to have come from hackers. We don't see this in normal hacking stuff. This must have come from state-sponsored accomplices. It's like, eh, okay. I just don't put any credence behind that. I don't see that that makes any sense. So...

**Leo:** By the way, I don't know if you mentioned this. Microsoft announced this morning that they're going to patch this zero-day exploit on the 21st.

**Steve:** Oh, I did not see that.

**Leo:** They're going to do an out-of-cycle Thursday update on the 21st.

**Steve:** Good.

**Leo:** That's tomorrow.

**Steve:** I'm not surprised.

**Leo:** Actually that's when this show comes out, so today.

**Steve:** Fantastic. Well, that's - isn't it interesting how quickly they're able to move when they want to.

**Leo:** Yeah.

**Steve:** Because they didn't find out about this, I mean, we know when they found out about it. They found out about it, like, you know, last week. And because it's generated so much fury and, as you said, governments are recommending that people not use IE, but use instead - in fact Germany said use Firefox or Google's Chrome browser. Do not use Internet Explorer until it gets fixed.

**Leo:** Although we do know that any Internet access is risky, and I'm sure Chrome and Firefox have all sorts of unpublished exploits. I mean...

**Steve:** Sure. We know for a fact that they're providing security updates to fix their security problems, as well.

**Leo:** I'm sure both Google and Mozilla are saying, there but for the grace of god go we. I mean...

**Steve:** Yeah.

**Leo:** Microsoft doesn't have the greatest track record. But I don't think they're particularly worse than anybody else.

**Steve:** No. I agree. The IETF has ratified the fix for the SSL renegotiation vulnerability. Remember that many weeks ago we did a podcast specifically explaining what the flaw was that had been found in the SSL protocol, which essentially it allowed somebody who was able to intercept traffic to inject their own content into an SSL connection in a way that was not detectable by either end. And the way they were able to do this was to take advantage of the fact that what's called the renegotiation hadn't been exactly designed correctly. The idea was that the designers assumed that when you were renegotiating, you would be renegotiating from within the SSL tunnel. That is, within an existing established security construct, you would be sending renegotiation back and forth. They failed to see that there was a way that a hacker could use renegotiation in order to sort of splice their own data in.

So what was required to fix this was an explicit use of the previous security context, that is, information that would only be known to each endpoint, explicitly connected to and added to the renegotiation process. So that strengthens the protocol. The problem is that we've ended up moving towards a kludge, unfortunately, because the specification states that this extension information, this renegotiation extension information should be able to be appended to the end of the existing handshake without upsetting either end. It turns out there are implementations of SSL and TLS which this breaks. So they have been unable to extend the protocol the way it was designed to be extended without breaking existing implementations, which is really a shame.

So what they've had to do, and this is the kludge part, is we talked about the way the SSL protocol works in detail. There is something called a cipher suite which essentially each end sends back and forth. The client initiating the connection says here's the collection of ciphers I know about. The server from that set looks at those that it understands and chooses one in an order of most desirable to least desirable, and then says this is the one we'll use. That's how they agree on a cipher for their encryption that they both know.

Well, by design, any that are not known are ignored. And that is done correctly. So the bad news is this fix for the SSL/TLS protocol requires, in order not to break poorly implemented but widely distributed existing SSL requires that the extra information for securing renegotiation be stuck in as a fake cipher. Which is really annoying. I mean, it's the definition of a kludge.

**Leo:** Kludge, yeah.

**Steve:** But it's the only way they were able to get it to work and not break things. Now, maybe in the fullness of time, like a decade from now, these existing broken implementations will go away, and then it'll be possible to say, okay, we no longer need to overload the cipher suite definition with this kludge-y renegotiation information because all of those old, poorly implemented endpoints have died off. So we can just do it the way we always intended to. We can hope that that ends up happening. So who knows. But I did want to let people know that we're moving forward.

Now, nobody's implemented this yet. The spec is done. The RFC exists. We know how to do it. So now what'll happen is these will be implemented and put into test. And it'll be a while before we start actually seeing this rev. But I'm sure that our listeners will know right here on this podcast because I'll know, and I'll let everyone know, as these fixes begin to migrate into downloadable updates. I'm sure Windows and Mac and the Linuxes will get new distros that have this thing fixed. So anyway, we're moving towards getting SSL cleaned up.

Then last little bit of interesting - this really qualifies more as errata, is I have a couple old email accounts that I've sort of left around because they pick up interesting stuff every so often. And for the last week I've been getting an interesting piece of email that was just sort of a case in point. It reputes to be from, in one case, UPS Manager Bret McCracken, and every couple days...

**Leo:** I'm a crackin' you.

**Steve:** I'm a crackin' you. Every couple days I get one from someone else. But this one, Bret McCracken kind of cracked me up. And the email address of service@ups.com. The subject is, in this one case, "UPS tracking number 55741879." Well, first of all, I know what UPS tracking numbers look like.

**Leo:** That ain't it, yeah.

**Steve:** That's not one.

**Leo:** At least they could fake it well. You know? C'mon, guys.

**Steve:** Don't you wish?

**Leo:** Look one up.

**Steve:** And so then it says, "Dear Customer!" Okay. They're not going to use, you know, UPS is not going to use an exclamation point. And it reads, "The courier company was not able to deliver your parcel by your address." Close, but not quite the way we would speak English. "Cause: Error in shipping address. You may pick up the parcel at our post office personaly," spelled with one "l." Well, of course post office is different from UPS, and we've got a typo, a spelling mistake. Then it says, "Please attention!" Okay.

**Leo:** It's amazing this stuff works.

**Steve:** "The shipping label is attached to this email. Please print this label to get this package at our post office. Please do not reply to this email. It is an unmonitored mailbox. Thank you. United Parcel Service." And then there was an attachment, UPS_invoice_Nr34678 - and that doesn't bear any resemblance to the tracking number - dot zip.

So using my tools, you know, I have things like hex editors which are bulletproof and so forth, I looked inside the ZIP. And sure enough, there's not a DOC or an HTML or something. There's an EXE file. So presumably somebody receiving this would click on the link, would open the ZIP file. Then there would be - it's the same named thing, EXE, which they would run. And of course we know what would happen next. It contains a trojan that would take over their machine.

I don't commonly get these. So I thought this was interesting, and I thought I would just share with our listeners an example of what is being sent. I now get this, this particular piece of email, or this particular account, like daily. And the name changes, and the details change a little bit. But again, a careful read demonstrates this is clearly not from UPS. But unfortunately I'm sure there are people who scan it quickly and think, oh, I didn't get a package? I want my packages. Even though I wasn't expecting one.

**Leo:** They don't read it that carefully. They just say, oh. Now, what's interesting is that could have been a PDF file, right, with the various Adobe exploits. It could have been a...

**Steve:** Could have been a PDF. Could have been an HTML. Could have been a link. Could have been, you know, there are so many ways.

**Leo:** Doesn't have to be an executable nowadays.

**Steve:** Doesn't have to be. In this case they thoughtfully provided me with the trojan in the email. Yes, and so the takeaway is it's never safe to click on a link in email even that looks even more legitimate than this does because this was a bad attempt. So we can't rely on the fact that the English and the UPS tracking number doesn't even look like one. But unfortunately this kind of attack is being successful.

**Leo:** It's amazing.

**Steve:** And that's not good news.

**Leo:** Yeah, it's amazing.

**Steve:** And finally, I had just a fun little holiday SpinRite story to share from Dan Collins, who's a listener, who sent this subject: "Yet Another SpinRite Story." He said, "To Steve and all the wonderful folks at GRC: As is usual over the holidays I found myself at my grandmother's house." And I'm thinking, "To grandmother's house we go." And I got a kick out of him saying, he said, "On arrival I was greeted with, 'Merry Christmas. And by the way, I have a project for you,' says Granny. By her tone I assumed it would be something simple like installing a program or finding a bookmark that she lost.

"Well, I was half right. It was simple, but it was somewhat more serious. Her picture storage computer wouldn't boot. And she hadn't backed it up for several months. I reminded her of 'that spinning program her son had emailed her,' and she fetched it out of her email." Of course he's talking about SpinRite. "First, I tried to put SpinRite on a USB flash drive, but the computer informed me that it couldn't boot because it was 'missing operating system.' I tried again, to no avail. It turns out the issue was resolved when I used a 512MB USB thumb drive instead of the 16GB one I had been using. I know that I've used large USB drives to boot SpinRite in the past. However, with newer computers. Perhaps this older computer can't handle booting from such a large USB drive. I saw no mention of this in the documentation, but it turns out the same thing happens on one of her other computers. It also would boot the smaller drive, but not the larger one.

"I probably don't have to tell you that once I managed to get SpinRite to run, her drive was fixed, and her pictures were quickly copied to her external drive, which she keeps in a fireproof safe."

**Leo:** Good for her.

**Steve:** Good for you, Granny.

**Leo:** Way to go, Granny.

**Steve:** Although you ought to apparently take it out of the fireproof safe a little more often.

**Leo:** And use it.

**Steve:** And use it to back up your computer. And I was wondering, gee, maybe the fact that it's so inaccessible sort of, you know, keeps her from doing it as much as she otherwise would.

**Leo:** Right, right, right.

**Steve:** "After fixing a large number of other issues, including one faulty CD drive, replacing the hard drive, and the other CD drive refusing to boot the Windows XP reinstallation CD whenever I had the new hard drive plugged in" - wow, sounds like Granny's computer...

**Leo:** Yeah.

**Steve:** ...is nearing the end of its life - "but booting correctly whenever I unplugged the hard drive, we had finally reinstalled her OS and once again had this computer in operation." Boy, yeah, Merry Christmas. And he says, "As I write this, SpinRite is chugging away at her other computers." Sounds like Granny's pretty well connected there. "Thanks for a great product. At least three people whose computers I have saved with it have bought their own copy of SpinRite. And I usually carry my own copy everywhere I go, except this one time that I needed it, though I'll probably have to make sure I get a smaller USB drive for it so I don't have this annoying issue again. Thanks so much. Dan." So, neat SpinRite story. Thanks for sharing, Dan.

**Leo:** We have questions, if you have answers, Steve, lots of them. Let's get to our questions. We've got 10 great ones from our audience. As always, you can go to GRC.com/feedback to submit your question. That's what Walt Houser from Potomac, Maryland did. Walt says: In show #231 you said the American Bankers Association recommends businesses use a separate machine for online banking. True story. However, did the ABA recommend this for their non-business customers? Perhaps they figure people like Cormac Herley - see SN-229 - that users won't bother; or, two, the press will use this advice to announce the death of online banking. That's the last thing they want.

He says: Leo quoted somebody in the chatroom suggesting a Live Linux CD because you can't write to it, and you know it's known good every time you boot it. Your listeners are very clever. Is there an ISO from a trusted source? You use one for SpinRite. Prior to being cut, could [image] be tailored so that the browser has one's financial links - banks, stock accounts, credit cards, et cetera, if not cookies, in the image when it boots? This way you would not lose the authentication. Oh, you could do that, actually. It's not a bad idea. Or would that open a hijacking attack vector not worth the risk? Great job on Security Now!. You guys make me look so smart at work. Congratulations on the Top Tech podcast for 2009. That's right, we won that one. And he said: I enjoyed the amazing CES live show with Leo, Kiki, Colleen, and the crew. Good. Thank you, Walt.

**Steve:** Well, so Leo, this was really one for you. I figured you would be in touch with good sources of a Live Linux CD.

**Leo:** You bet.

**Steve:** We did have a bunch of listeners who liked the tip a lot, just as Walt did. So...

**Leo:** Couple of ways to do this. And I love his idea. And I'll tell you actually how you could solve - even do that. But of course a Live Linux CD from one of the distributors is not going to have any customization at all, of course, but you know it's good. One of the things that, for this very reason, that every single reputable distributor of a Linux distribution does, is provide an MD5 or a SHA hash with the download, so that you can verify the download when you get it. So you know there's been no man in the middle. Nothing's been replaced. You're getting the actual download.

So you want to, if you're concerned about that, and probably it's worth doing it for something like this, download it from a reputable source. I'll give you a couple of good choices. And then run the MD5 hash against it. If you don't know how to do that, they'll have explanations on how to do that, to make sure you got the thing that you thought you got.

By the way, most open source companies do this now. So Ubuntu is probably the best place to start. This is the Linux that works best with almost all PC hardware. It's very easy to use. They'll even send you a disk if you want to be sure you got the right one. Unless you think there's a man in the middle at the post office, I think you'll be okay. That's Ubuntu.com. A really great source for Linux. But there is another place you can go that gives you a list of all the different Linux distributions so you can pick one that maybe fits the - if you've got unusual hardware, if you want one that's smaller or bigger or whatever. It's called DistroWatch. There's two, actually. I like DistroWatch. They literally list all the different Linux distributions and reviews thereof. Let me - I can pull that up for you.

**Steve:** Although for this we're not really wanting, like, an installed Linux. We're wanting specifically a live boot...

**Leo:** Yeah, everybody does this. Everybody does this now. It was kind of pioneered by one particular Linux, and then everybody now does it. And so, yeah, you're looking for the Live CD version of any Linux that you get. And when you go to DistroWatch, it points you back to the distributor. You're not - but I think it's good to look at these reviews because then you know it's legit. You can even get FreeBSD, and they will send you CDs and so forth.

**Steve:** And so, for example, if we'd used Ubuntu, then you get an ISO, you burn that to a CD, you boot the CD, and it's going to take you to - it's going to switch into graphics mode, put you on a desktop, and there will be a Firefox icon.

**Leo:** Yup. Yup. Ubuntu's a really good choice for that. So, yeah. You're essentially booting from a CD, an unchanged CD every single time. It is easy to slipstream these. That's what it's called, "slipstreaming Linux CDs." If you Google that, you'll find ways to do that. And what it's essentially doing is modifying the Linux CD and then making your own ISO out of it. So you could do that. But it is, as he points out, there's some risk there. You have to make sure you know what you're doing, and you aren't including malware into your slipstream Linux boot disk.

**Steve:** And so then the idea would be you could create, for example, icons on the desktop for the URLs for the sites you visit or shortcuts in the browser, log on in order to install cookies and things in that, and then you would take a snapshot, essentially, of a working, tuned-up version and make that then your boot from then on.

**Leo:** Right. Now, you know, remember Linux doesn't usually have things like Flash installed. So if your bank is using Flash cookies, you're going to have to really customize it to get those to work. I think we agreed, didn't we, on the episode that that was part of the advantage of this was having to fully authenticate each and every time.

**Steve:** You're probably more secure if you just absolutely start with a completely clean system, the idea being that you're already going through some substantial trouble if you care enough to shut down Windows, boot the CD, get into there for doing your banking and things. And Walt did ask if they recommended it for their non-business customers. I mean, this is...

**Leo:** I'm never going to do that.

**Steve:** This is arguably an extreme end caution thing to do. But it's one way to really be safe. And I don't think things are getting any better in the future. We're seeing no end of this podcast where we keep track of...

**Leo:** Yeah, we won't have to stop doing it because, oh, it's safe now. We can go home.

**Steve:** Yeah, no more problems.

**Leo:** I don't think that's going to happen. No, I think a Live CD is a great choice, and I know a lot of security experts actually do that. And then you're just - you're protected. It can't be modified.

**Steve:** Right.

**Leo:** Nathan Howard in Bella Vista, Arkansas notes that GRC and TWiT are his one-stop shop for electronic security and literary needs. Hi, Steve and Leo. I just wanted to thank you both for a fantastic show. I, too, have never missed listening to Security Now!. Not only do I get my computer security needs met, I also get my fix for great science fiction books to read. This Christmas I downloaded the electronic versions of "Gibraltar Earth," "[Gibraltar] Sun," and "[Gibraltar] Stars." That's those great Mike, what is, McCollum?

**Steve:** Mike McCollum.

**Leo:** Yeah. Sci-fi books from Sci-Fi Arizona.

**Steve:** Yeah, Scifi-AZ.com.

**Leo:** I'm halfway through "Gibraltar Sun" and couldn't be happier with the series. After I finish with "Gibraltar Stars," I plan on getting "The Mote in God's Eye," another recommendation of yours. Keep up the good work on both fronts. We won't be hearing from him for about four years.

**Steve:** Well, I just liked this because I wanted to remind people about the Gibraltar series, which I really enjoyed. And I don't remember now when, it might have been during CES you were talking about "The Mote in God's Eye"?

**Leo:** Oh, I've talked about it a number of times, on TWiT, as well. You know, this is

Jerry Pournelle.

**Steve:** And are you reading it?

**Leo:** Yeah, I just finished it. I just read - Audible has two Jerry Pournelle, actually I think they have more, but two of the Jerry Pournelle/Larry Niven collaborations on there. And I first read "Lucifer's Hammer," and we did I think talk a little bit about that. And then I just finished "Mote in God's Eye." And both are really great. They're a little, I have to say, as sometimes happens with sci-fi, Heinlein stuff, too, it's a little dated.

**Steve:** Yeah.

**Leo:** But if you take that into account, just some great writing and really fun books to read. Very long. Very long. That's why I said we aren't going to hear from him for a while.

**Steve:** Yup.

**Leo:** Josh H. in Mississippi wonders, "Encrypting Random Access Memory, is it possible?" Dear Steve, I've been using TrueCrypt to encrypt my hard drive for some time now, and I love it; but I have heard of attacks against the memory that can be used to find the encryption key. If a hacker can get access to the memory, all bets seem to be off. He would also have access to whatever sensitive information was stored there. I was wondering if you know of a way to encrypt the data that's in the computer's memory chips, either through a hardware solution - a chip - or software. If this is possible, it would prevent all attacks on the memory. Thanks for the podcast. I love it. Keep up the good work.

**Steve:** Well, Josh, there's a problem with that. But it's interesting, and it also highlights something that we talk about as sort of a fundamental concept of security and the way you need to use information. Looking, for example, first at TrueCrypt, TrueCrypt inserts itself between the hard drive and the computer so that when you write to the hard drive, the data is encrypted on the fly as it's going to the hard drive, and so that when it's stored on a hard drive, it's encrypted. And then of course the reverse happens. When the data is read from the hard drive into memory for use, it's decrypted.

Now, the computer has to deal with it in an unencrypted form. So I guess in theory you could have encryption on the bus, in between the memory and the computer, so that the actual contents of the memory were being kept encrypted. And literally as the computer was fetching instructions and data from the memory into itself, it was decrypted. But it's just - it wouldn't be practical to do that. There have been some questions about this concern about freezing memory in order to hold the contents, to keep them from being grabbed by bad guys and hackers and so forth. The fact is, and this came from some research that Princeton did where they sprayed freeze-y stuff on memory and unplugged the computer, and a few minutes later the contents of the memory was still intact. They were able to plug it in again and see that most of the data was there and recover, through some tricky approaches, things that had been lost.

But it's really not a practical attack. It's not something that I think most people need to worry about. When we were talking about this in detail, we said, if you were concerned about it, turn the computer off, your own laptop off. Count 1,001, 1,002, 1,003. Normally the memory is running very warm. It's not going to hold its data very long.

The other thing that this touches on that I want to just sort of remind our listeners about is the fundamental problem that any device has of needing to use something that's encrypted, like we've talked about in the case of a consumer HD DVD, where the DVD disk is encrypted, but in order to use it, it has to be decrypted. Just like in order to use the contents of memory it has to be decrypted, or the contents of your hard drive it has to be decrypted. There's a limitation to what is possible. And that represents the vulnerability in any of these systems is you've got to decrypt it to use it, which means...

**Leo:** It's always got to be in the clear at some point.

**Steve:** Exactly. And that's something always to keep in mind. So at some point there just isn't anything more you can do.

**Leo:** Well, and RAM has to be in the clear at some point. I mean, it has to be decrypted to use it. So even if you encrypted it, there's going to be an attack vector because there's some point where it's decrypted.

**Steve:** Exactly. You could have, for example, if a hacker were able to get the computer to jump through their own code, then if the computer can access the memory, then a subroutine that is the hacker's code could access the memory on behalf of the hacker. So again it would be in the clear. There just, exactly as you say, Leo, in order to be used, it's got to be decrypted. And so there's always some way of inserting one's self at that point where it's actually in use. At that point it is not encrypted.

**Leo:** It's a good idea. It's a good idea, but nothing stays encrypted forever, I guess, is...

**Steve:** And so the model is, understand what the dangers are and just plan for safety. For example, turning off your laptop, but making sure you stay with it for a few seconds. I mean, although it would be quite a scene to have someone grab it from you, flip it over, open the door, and spray freeze-y stuff in it. It'd pretty much give away the fact that they were doing that.

**Leo:** Excuse me, why did you do that? Oh, no problem, I'm just checking, we're just checking the bit pump, make sure it's working okay.

**Steve:** Concerned your RAM may be overheating, sir. We're cooling it off for you. It's a new service at Starbucks.

**Leo:** Yes. The deep freeze. Derek Bailey in Ohio needs a bit of info-tech career advice. Actually this is a great one. I'm very interested in your answer here. Hi, Steve. If I'm taking you away - I love this. If I'm taking you away from your busy schedule, I apologize; but I need some advice from the master. I'm currently working my way through college and paying bills through a retail store specializing in electronics. Here's a hint as to which one. Does the TRS-80 bring back any memories?

**Steve:** Boy, that would have to be Radio Shack, wouldn't it.

**Leo:** You know, I just - I was watching on Twitter last night, one of the people I follow mentioned, you know, I always forget how nice and often very helpful the people at Radio Shack are. And it's true because a lot of times it's college kids like Derek who really do know what they're talking about.

**Steve:** Yes.

**Leo:** Before I was left with no other choice than to go back to retail, I was a sysadmin for the school I graduated from. Because I did not have a college degree I was being paid minimum wage to maintain their Windows 98 SE rated machines running XP and their Windows Server 2003 box which managed the network traffic. I was the admin when I was a student there, and I was working only for experience and no compensation. Obviously, if they won't look for grants and pay for new machines, why would they want to pay more than minimum wage for quality IT service when they can get a kid to do it for free?

Well, after a year I asked for a raise. Not highway robbery, just enough to get by. Well, they told me they did not believe I had sufficient knowledge of computer networking to be a salaried employee, even though neither the school board nor the principal had ever seen my rsum. So, back to retail.

So my point is to ask you about your rsum. As it's posted on the GRC site, I notice you have had several IT jobs from a young age. I'm a 20-year-old college student with an okay rsum, considering. I know the job market isn't so hot right now. But do you have any advice for a struggling IT guy seeking to work without the degree but plenty of credentials? Maybe how you were able to attain such positions at such a young age. Any advice would be much appreciated.

I didn't mean to write a novel, but I wanted to thank you for SpinRite, the world's best hard disk data recovery tool, and thank you for Security Now!. I've been a faithful listener for almost two years. Looking forward to CryptoLink. And as always, keep up the good work. Thanks, Derek. I have a lot - I have a number of follow-on questions for you, but I'll let you start with your answer here.

**Steve:** Well, this is the first time I've ever chosen a question like this, although I do see them from our listeners a lot.

**Leo:** It's a good topic, I think.

**Steve:** Yeah. I see them from our listeners a lot, young listeners who are in school. They're feeling intimidated; and, boy, I don't blame anyone for feeling that way about just the size of the industry and the size of the world and the idea of having to compete. For me, and hopefully for these people, computers have always been a passion. And my trick was I loved it so much that I was always able, or I was always willing and able at the time, which is one of the reasons that being young helps, I was always able to work for free. That is, I would just volunteer. I would say, hey, you know, I can fix these things. Would you let me? There's - I don't remember now whether it's on my rsum, but there was a stereo chain at the time called Pacific Stereo when I was...

**Leo:** I remember that, yeah.

**Steve:** Yeah. Like I think I was 12. And I had taught myself electronics. And they had this repair department full of stuff that was broken. And I just, I mean, it would have been, to me, so much fun to fix this stuff. So I said to the repair guy, who really it turns out didn't know how to repair anything, I mean, he didn't - he had a whole tech bench of cool equipment, but didn't know how to use it. And I said, "Well, would you mind if I fixed these things?" And he said, "What?" And I said, "Oh, just I want to." And he said, "Okay, fine." So I went through and basically repaired everything. They had, like, shelves full of stuff that was just sitting there. I don't know what the plan was to fix it. But they didn't have the ability to do so.

And invariably what happened was that I would be offered a job after I had demonstrated what I could do. And that basic scenario repeated itself time and time again as I would - I did stuff because I loved to do it. And they didn't want to lose me. And so I proved myself for free just because I wanted to. And then they ended up thinking, hey, you know, we don't want this kid to wander off. What does it take to keep you? So that was the formula that I used. I mean, it doesn't work for everyone. Certainly not if you're...

**Leo:** It might work less now. I mean, this is a different time.

**Steve:** Yes, and I really think, yes, I really do think that it is less applicable today than it was then. What I tell people when they ask me sort of generically, like, what should I do, I explain that I've been really fortunate to be able to make money, support myself, doing what I love. And I can't - I mean, like you do, Leo.

**Leo:** Yes, yes.

**Steve:** You love this. And there's no better way to spend your life, if you can, than spend it doing something that you love. And if you're able to support yourself, that's just, I mean, there's nothing better. What I think the Internet has changed is that in the same way that eBay works because it leverages - this is an extreme example, but I'll call it "perfect knowledge." That is, eBay works because someone can dig something out of their garage that is obscure and, with the breadth of eBay, find a collection of people who value what they are willing to sell, and get a fair price for it. And it's the communication that the Internet provides that makes that so-called "perfect communication" possible.

Well, my feeling is that that's sort of where the job market is headed. And what I mean is that, to turn that into a piece of advice, I would say to people, find something you love and be the best at it. I mean, really, really, really good. There's all kinds of people who can do something a little bit, who are generalists. I mean, especially now with the Internet, you can become sort of a semi-expert in whatever you want to in an afternoon, just by Googling for a while. I mean, much as I did when I was curious about Vitamin D. I'm not a doctor, but all the information is there if you just go to look at it.

So what I advise people is, you know, young people who are trying to start out, is find something and excel. Because once upon a time, when we didn't have the Internet, you couldn't get compensated for being really, really the best at something because there was no way to get the knowledge out. I think of like the Andy and Opie and Mayberry small town example. Well, if somebody was fantastic at something, they didn't have the reach to have their expertise known. So the town happened to have a fantastic plumber, for example. But it's like, oh, well, so what? Other towns have plumbers, too. There was no way to know that this particular guy could, like, really fix anything.

But in this day and age it is possible to know. People talk. People communicate. The Internet is a way of sharing this. We have the whole social networking notion where something like somebody who is the best at something can get known. And so what I tell people is do what you love, if you can. Be, I mean, really, really good at it. And my sense is the Internet allows that skill, that knowledge, to be found by other people who are looking for it, just like eBay allows obscure things in people's garages to be found, and for a fair exchange of value.

**Leo:** What about certifications, that kind of thing? I mean, there are things like the A+ or the MCSC or these certs that you can get. They're very - they tend to be expensive. And a lot of people say they're not worth anything. But they might convince an employer that you have some skills.

**Steve:** Yeah, you know, probably due to my own background, I'm skeptical. The absolute best guy I ever hired...

**Leo:** Yeah, that's right, you were an employer. I should - you know what this is all about.

**Steve:** Yeah. I mean, the best guy I ever hired was a hobbyist. Like me, he had been building things in his garage in elementary school and junior high. And he showed me photos of these projects. He'd built this and that, I mean, you couldn't stop this guy from inventing things and building things. And he had all of this, I mean, and I hired him when he was in high school, before he had a degree, the best engineer I ever had. And...

**Leo:** Well, look at Colleen. I mean, Colleen's degree is in sociology. So some of this - of course you and I have an advantage because we know something about technology. So we can vet somebody and tell if they know what they're doing. Whereas I'm sure the school board has no idea what questions to ask. That's where certs sometimes are useful. I don't think certs are real.

**Steve:** And I think the problem with certifications is that they're trying to do something; but, much like with any other kind of testing, they really only determine whether you're able to answer the questions on the test.

**Leo:** Right. That's not necessarily what you're looking for.

**Steve:** No. You want somebody who can face something they've never seen before and say, oh, I can figure this out. And figuring something out is very different from answering a multiple-choice question correctly.

**Leo:** Exactly. I mean, I don't - I have no idea how Colleen would do on an A+. I'm sure she'd do fine. But those aren't the skills I'm looking for with her. It's creativity, rapid response. You know what? You said it. In some ways passion is important.

**Steve:** I really think it is. I think that's where - I think that's what drives it. And related to this, I'm also asked often, how do I learn a new computer language? I want to learn a language. And there are books that tell you what the syntax is. But I always tell people, find a problem. Think of something that's a problem that you - and force yourself to use that language to solve it. And you'll immediately start learning the language in a useful way that I think is far more valuable than sitting there and studying the text in a sort of a dry, clinical fashion and then saying, okay, I read the book, I know the language. It's like, uh, okay, have you solved any problems with it? Well, no, but I can take a test.

**Leo:** You know, and I did stuff in my life that I didn't - wasn't my, you know, my passion, but always kept in mind what I loved doing and always moved in that direction and always had that as a goal to do what I love, not stuff I had to do. But there were times I was working in - I loved radio, but there were times I was working in radio that this job wasn't great, or there were times when I was working in TV where I wasn't happy. But I always focused on what I loved and what my passion - the thing about following your passion is it'll get you through those times when you're living on rice and beans, and you're not doing the thing that you want to do the most. But the passion keeps you going. It's true with podcasting, too. There's times when nobody's listening, but your passion will keep you going.

**Steve:** Yeah. If there's any way, it's certainly the way to live.

**Leo:** Yeah. It's hard to do that. Takes some courage. I recognize that. It's not - you have to have a little faith in yourself and a faith in the world that it's going to work out. Doesn't always seem obvious.

Here's a - we've got a tome, here, from a listener who did identify himself to you but asked for anonymity on the show and sent greetings from San Miguel de Allende, Guanajuato, Mexico. Beautiful area. He says: I'm a long-time Security Now! listener, as well as a SpinRite owner, and cannot thank you and Leo enough for all the effort you put into both the show and your software. I would love to be able to relate another SpinRite success story, but most of the 200 stories I've heard on the show are more entertaining than any of my own experiences. About the only thing I can say about SpinRite is it works.

Over the last few months I've listened with growing interest to your discussion of different routers and the way in which some of them take over the handling of DNS queries. After listening to your explanation of why this was not a good idea, I realized that my own router was assigning only one DNS, a local address, 192.168.1.254 to all of the computers on my network. That was the number of the router. My router is a Thomson TG587 V7 DSL modem and router provided by his ISP, Telmex, Telefonos Mexicanos, the national phone company here in Mexico. This discovery that my local network was functioning on only one DNS server immediately explained the increase in problems I've been experiencing on the Internet since changing to the new DSL modem not so long ago.

Normally it would be a simple matter to log into my router's web interface to change the numbers of the DNS server or maybe disable the router's serving as the DNS server. But here's where the plot thickens. When I tried to access the web interface for my router, I discovered I didn't have the right password. The online documentation for the Thomson states that the default password is the WEP key stamped on the bottom of the router, but it didn't work. I did the reset as described in the documentation. Still no luck. So I did the even longer reset that restores to factory defaults. None of the advertised default passwords worked.

Online I found dozens of mentions from other Telmex users offering many different password options. None of them worked. Several calls to Telmex's Infinitum technical support failed to find anyone who was able or willing to tell me what the correct password was. Wow. That's weird. After a week of frustrating phone calls to tech support, Telmex offered to replace the "defective" router.

Back on the 'Net I dug further into the problem and found the documentation for the Thomson TG587. He gives a long URL which I've put in our show notes on the FriendFeed page. On Page 59 it says "Your system administrator may have disabled the physical reset button of the gateway. In this case, a hardware reset to defaults is not possible." Ah. That explained why the modem did not reset to the default password. I didn't know that it was possible to disable the reset button on a router. Apparently this is what Telmex did in order to prevent end users from changing any of the settings. I can understand them doing that. The effect of this is that users of the new Thomson modems Telmex provides are stuck with using a router they cannot configure. They have to use WEP security with a WEP key they cannot change. And they have to use a single DNS IP address in the local router. So far I have not been able to determine the actual IP address or addresses of the DNS servers used by the router because it's hidden, of course, behind the local IP.

So here are my questions: One, is there any way to reset the modem to the default password, or is the device effectively bricked? Two, is there any way to determine the real IP address or addresses of the DNS server I'm using when the router reports a local address? Three, if I manually configure my preferred DNS servers in Windows, does this take precedence over the DNS entries served up by the router; and, if so, is this the way everyone should deal with routers that are managing DNS queries? If you read this on your show, I'd appreciate your not using my name.

Somebody at Telmex might take offense to my telling everyone all of this, and they probably have it within their power to take away my broadband and relegate me to a dialup connection for the rest of my life here in Mexico. Muchimos gracias again to you and Leo for providing such an invaluable resource as Security Now!. Wow. You know, I think that that's probably not unusual, especially in an area where they don't have sophisticated users who will discover this chicanery.

**Steve:** Well, and yes. You can imagine that this is probably not the way things were originally, that they ran across problems with, especially in a DSL situation, where they may have a bunch of specific ISP-side settings that really should not be changed. So they may have had really bad tech support problems with people who were going in and resetting things and changing settings. And then they'd deploy some service, some field service guy who'd go out there and say, well, who changed all these? Oh, well, my son thought he could make it better, blah blah blah. So anyway, I can see from the corporate side that there was some motivation, or there certainly could have been.

To answer the questions, I'm not an expert on this particular brand of router, so I have no idea whether it's possible to reenable the reset switch. Routers no longer have batteries in them, so it's not like the old days Leo and I remember, where you could take the battery out of the motherboard, and it would cause the BIOS RAM to lose its memory after a few seconds, and then you could always, like - or to reset the BIOS password that way. Now routers use nonvolatile memory. So it sounds to me like there's a bit of data in the nonvolatile memory which is instructing the router to ignore the reset button. That being the case, without the password, there's no way to reset the router.

So I would, given everything that we've heard about this router, probably there's a password which is set by the ISP. And one of the things they do is disable the reset button so that no one and nothing can ever change that in the future. So I would say it's effectively bricked.

Assuming that the router is a hybrid DSL modem router, that is, out of one end is the DSL connections, the copper connections to the ISP, and the other side is LAN, there's no way to see the LAN, I'm sorry, the WAN, the Wide Area Network, the public network side of the router, before it gets to the DSL modem. If they were two separate units, if you had a DSL modem and a router separately, then in theory you could, in order to determine what DNS the router was using, you could sniff that connection between the modem and the router, if you used packet sniffing, in order to determine what DNS servers the router was using. But in an integrated unit there's no way to get there.

The good news is that it is absolutely possible to manually configure Windows' use of DNS. It's in the standard dialogue where you normally have it set for Obtain IP address automatically and Obtain DNS servers automatically. So one of the things that the Windows OS does when it's booting is to use the protocol we talked about last week, DHCP, the Dynamic Host Configuration Protocol, to get that information from the router. And we know that it's getting the router's own gateway as DNS. So all you have to do is choose some alternative DNS servers and put them in instead.

What I would suggest is that, unfortunately, DNS is geographically biased in terms of performance. I don't know, for example, what OpenDNS servers, how they would perform for you. We do have, GRC has the DNS Benchmark utility we talked about before. It's GRC.com/DNS/benchmark.htm. And you can run that in order to see how the set of servers that the benchmark knows about compare. What I would do is ask other people in your area who are not stuck behind this ISP's closed router. See if you can get the IP addresses of some publicly available DNS servers that other people in the same geographic region are using. You could put those into the benchmark utility and see how they perform. Basically you're going to want to find some alternative ones which perform at the top of the scale. And then just put them into Windows, tell Windows use these instead of obtaining it automatically, and see how your Internet experience is improved.

**Leo:** Should be quite a bit.

**Steve:** Yeah.

**Leo:** But who knows. I mean...

**Steve:** Yeah.

**Leo:** Now, we had two interesting comments in chat. One is from a Telmex customer in Mexico City who says his is not locked down. So it might be router specific. It might be that in San Miguel they lock them down, but not in Mexico City. And then we have a UK listener who has a similar modem who says, "Mine is locked down, too." So it could be the model number. It could be, you know, it's one of those things that I would suspect that any modem that's designed for an ISP to distribute has some settings like this, has some capabilities like this.

**Steve:** Yup, exactly.

**Leo:** And then it's up to the ISP whether it's going to use them or not. Question 6 from Giovanni Martinez in Toa Alta, Puerto Rico. He says: I'm 33 years old. I'm making my bachelor's degree in Information Systems, concentration in networks. I have been listening to your show for a while, and it is amazing. That's great. I also listen to other podcasts, but you know how to explain everything, Steve, in a clear and simple way, even though the subject matter is very complicated. I use all the resources you mention in the show.

By the way, I visited Shadowserver.org, and it is great. But when I wanted to subscribe to the mailing list, it took me to mail.shadowserver.org/mailman/listinfo/shadowserver, et cetera, and then got a certificate error. I'm getting one, too, actually. I just went to the site, and it says "Safari can't verify the identity of the website."

**Steve:** I noticed it's https.

**Leo:** Yes.

**Steve:** So it's trying to establish a secure connection to that server.

**Leo:** I get this a lot, actually. So I'm glad he wrote and asked about it. This may mean the server has generated its own security credentials, which Google Chrome - oh, he's using Chrome - cannot rely on for identify information. Or an attacker may be trying to intercept your communications. You should not proceed, says Chrome, especially if you've never seen this warning before for this site. So, Giovanni asks, is this website reliable? Thanks for your help, and keep up the great job you're doing. Just in case, English is not my first language, so if I said something weird, please forgive me. But I think it was all fine.

Yeah, I'm getting exactly the same thing. Safari, which is also giving me a certificate error, says the certificate for this website was signed by an unknown certifying authority. You might be connecting to a website that is pretending to be mail.shadowserver.org, which could put your confidential information at risk. It's not quite so draconian as Chrome. It just says, would you like to connect anyway? And then I can show the certificate. I can even check a box on Safari that says always trust the certificate or not.

**Steve:** Well, in my case, on Firefox, I get an intercept that says "This connection is untrusted. You have asked Firefox to connect securely to mail.shadowserver.org. But we can't confirm that your connection is secure." Now, if in Firefox I open the technical details, it says, "Mail.shadowserver.org uses an invalid security certificate. The certificate is not trusted because it is self-signed."

**Leo:** Self-signed. That's what I'm seeing, as well.

**Steve:** Yes. And so now that's the key. And we've never talked about that before. So this was a great question for that reason. This is something which some organizations do because they object to the idea of - mostly because they object to the idea of paying some third-party site for the privilege of signing their certificate for them. So we understand how this works. If we pay VeriSign to sign our server certificate, then our browser that trusts VeriSign is able to trust the certificate that VeriSign signed. So...

**Leo:** The web of trust.

**Steve:** Well, yeah. In this case the certificate chain...

**Leo:** Chain, yeah.

**Steve:** ...that is anchored by a known and trusted certificate authority. But a group like the Shadowserver guys, they're saying, wait a minute.

**Leo:** We don't want to do that.

**Steve:** We don't want to do it. We don't want to pay a third party. What we care about is an SSL connection. That is, the thing we want is to have security. But remember that the other thing that SSL affords us is authentication. And so a self-signed certificate gives you security, but not authentication. And so I would say it's fine. You want to go in with your head up. It is the case that you're not getting authentication from the connection, but you're getting an SSL secure connection. So for something like this you could say either trust it always, or trust it this time. I would say just trust it this time. And then your SSL connection will work, you'll have safety while you're signing up to this mailing list, and then you can go from there.

**Leo:** I can, you know, especially given Shadowserver and what they do, I completely understand why they would say, well, we're going to use self-signed. You get SSL.

**Steve:** Yes.

**Leo:** This is not about - we're not using the SSL for validation of who we are, we're using the SSL for a secure connection.

**Steve:** Right. And so anyway, I wanted to specifically address it because it's a great question. And I would say there's nothing wrong with a self-signed certificate. The biggest problem is everybody is going to get this warning. And you're probably - you may wonder why you don't have many people signing up for your mailing list. It's because they're freaked out by it. They don't know what that means.

**Leo:** I get it a lot for some reason. But I always look, and usually it's self-signed. It's either self-signed or it's expired. That's not likely to happen with you.

**Steve:** Right.

**Leo:** In both cases I go, yeah, yeah, whatever.

**Steve:** Exactly. And that's what I would recommend.

**Leo:** Neil Ellis in the U.K. asks for our audio books, our picks for audio books. He says: Hello, guys. I hope you both had a great festive period. But really I need your help. I have an Audible Platinum subscription. That's the two books a month. And I've really enjoyed the Peter Hamilton books, the Dune books, the Hyperion series. These are all things we've recommended. But I've finished them all. I don't know where to go from here. And as you both have similar tastes, I would love to get a few recommendations. I have about 25 hours a week at work. No wonder he got through so many. He says 25 hours a week to listen. He says: After listening to TWiT and my audio books, I'm done, I'm out. Thanks, and keep up the podcasts. Yeah, we only produce about, I don't know, 20 hours a week of podcasts. So he needs to supplement.

**Steve:** He's got some great job, though.

**Leo:** No kidding.

**Steve:** If he's able to listen to audio books while he's working.

**Leo:** Well, I'm thinking there are a lot of jobs, if you're like a night watchman or whatever, where you could have one ear, you could have an ear bud in, and that would really kind of take some of the sting out of the boredom; you know?

**Steve:** Yeah. So I just posted this because I imagine that Neil is not alone, and I wondered if you had any other suggestions, Leo.

**Leo:** Oh, do I. I have some great ones. And this might be a good opportunity for us to do a little ad. How about that? Do you mind?

**Steve:** Oh, what a concept.

**Leo:** This is not a setup, ladies and gentlemen. It just so happens that Audible...

**Steve:** It's a real question. He really did ask the question.

**Leo:** It's a real question. And Audible is a sponsor of the show, and we love Audible. In fact, if you go to Audible.com - I'm sorry, I always get this one wrong - AudiblePodcast.com/securitynow, they have a little bit of a different URL for you. AudiblePodcast, because they want to be different, .com/securitynow. You can sign up for the Gold account. Now he has a Platinum account, which means he gets two books a month. Actually that's what I have, too. And I don't go through two books a month, but I just love collecting them.

The thing about Audible, when you get those Audible books, they kind of are yours forever, unlike, say, iTunes, where if you delete it accidentally you can't get it again. Audible keeps your library online forever. And you can go back. I have now 300 books. It's just like a little library. And so I guess with books you often do want to listen again. So you can go back and listen to anything that you ever have purchased. In fact, if you take advantage of this deal, you get to keep this book forever. You can cancel Audible at any time, or decide to go a la carte, which Audible does sell books a la carte. So you're not kind of stuck with the subscription. But you do get to keep the book forever.

I'm just looking at my list here. I think I have - how many purchased. All my books, I can only show 200 a page. I think I have two pages. I have, like, 400 items on my list of books that I have purchased and listened to. But I can tell you, the book I'm going to recommend, the two books I'm going to recommend this week, given that he's interested clearly in science fiction, are books I am not listening to yet. They're on my next listen list. You can set up a wish list of books that you want to listen to the next time. They're cued up for purchase for me in a couple of days. Actually tomorrow. And these are books that Tom Merritt and Veronica Belmont recommended. They do a science fiction podcast called Sword and Laser. And Molly Wood, too. They said, "Have you ever listened to 'Daemon' by Daniel Suarez?" I said, "No, I haven't heard of that." They said, "You haven't listened to it? You've got to listen to it." And then they said, "And the new one just came out, "Freedom."

So here's two books by Daniel Suarez. "Daemon," you'll like this story, Steve, it's "Daemon," actually, D-a-e-m-o-n. Matthew Sobol was a legendary computer game designer, the architect behind half a dozen popular online games. His premature death depressed both gamers and his company's stock price. But Sobol's fans aren't the only ones to note his passing. When his obituary is posted online, a previously dormant daemon, that's a background computer process, activates, initiating a chain of events intended to unravel the fabric of our hyper-efficient, interconnected world. Ooh. Doesn't that sound great? Daniel Suarez is a computer wiz himself. So this is Michael Creighton-style or maybe Neal Stephenson-style sci-fi, written by somebody who's not making it up. He knows what he's talking about. Comes very highly recommended.

So to answer your question, Neil - now, he's in the U.K. And I have to tell you, not all books available on the U.S. Audible site are available on the U.K. site because you have to make deals with publishers everywhere. But it's published by Penguin, which is a U.K. company, so I bet you you can get this in the U.K. D-a-e-m-o-n. Look up Daniel Suarez. And these two books, I mean, it's only 30 hours, so it's only going to get you through the next week and a half. I'm so jealous.

**Steve:** Isn't that a rough job.

**Leo:** I would love to spend 25 hours a week listening to audio books. I did actually when I used to commute. That's how I got my list so long. I love audio books from Audible. 70,000 titles. You'll never run out. And one thing you'll note about Audible listeners is they love trading back and forth. Oh, have you heard this? Have you heard that? So there's our Audible recommendation. You can get that first one free by going to AudiblePodcast.com/securitynow. "Daemon" by Daniel Suarez. It's my next listen. I'll give you a review, Steve, when I've listened to it. Doesn't it sound great?

**Steve:** It does sound good, yes.

**Leo:** Sounds like my kind of book. I can't wait. And it comes highly recommended from two people whose taste in sci-fi I really, really trust. AudiblePodcast.com/securitynow. We thank them for their support for the Security Now! show. And I shall move on now to Question 8, if you don't mind. But thank you for that one, Neil.

Rick Lim, Surrey, British Columbia, wonders about SSL certificate verification. It's kind of along the same lines of our last one. Steve and Leo, thanks for the great show. I've been listening to the episodes on SSL certificates and heard you mention that there are inexpensive and expensive non-EV certs, the difference being the amount of verification done by the Certifying Authority, or CA.

I had received an email that a subscription of mine had expired, and it looked like a valid email. Because I knew the subscription was due, I followed the embedded link. Oh. Oh. Always type in your links; right? I followed the embedded link, and it took me to a website that turned the URL bar green, a major vendor in Redmond, Washington. Curiosity got the better of me, and I looked at the cert. The company's physical address looked good. The certifying authority, VeriSign, looked good. The rest of the flotsam and jetsam, et cetera. Well, suddenly I realized that I'm just as informed as the next web shopper. I don't know what fields to pay attention to in the cert - which are significant, which should I ignore. My questions are, how do we tell a cheap non-EV cert from a trustworthy non-EV cert? What cert fields are significant? And by the way, he says, I love the SpinRite stories. Keep those up. Thanks. So, first of all, what's an EV cert, and what's a non-EV cert?

**Steve:** EV stands for Extended Validation. And so that's the extra color that we're seeing increasingly in some web browsers where...

**Leo:** That's that green bar.

**Steve:** Exactly. The implication is that in order to issue an extended validation cert, more work was done to verify the identity of the site whose certificate was signed. So the point being, because there are, and we talked about it the other day, like even some free SSL certificate signing companies that'll just sign a certificate for a year for free. They acknowledge that they're doing very little verification.

**Leo:** Most of the time it's just verifying the email address.

**Steve:** Exactly. Or like looking up the web record to see that if it looks like you're in charge of the domain.

**Leo:** How reliable is that? Because when I get an email cert, the way that VeriSign even validates it is merely to send me an email to that email address to see if I respond. Is that reliable?

**Steve:** Well, in my case, I do use VeriSign also. And there's a - we have a phone number in the domain registrar logs. And I think Dun & Bradstreet has a number for us.

**Leo:** That's for the EV thing, though; right?

**Steve:** No, no, just for...

**Leo:** That's just the regular one.

**Steve:** Yeah, for VeriSign...

**Leo:** That's - and the self-cert. But I'm talking about an email signature, an encryption cert, an S/MIME cert.

**Steve:** Oh, never applied for one.

**Leo:** Yeah, I think all they do, I mean, this is all they've ever done with me is validate the address. And you see this all the time. Anytime you sign up for a site they'll send you an email saying click this to make sure this is you.

**Steve:** Yes.

**Leo:** Can that be faked? I mean, I guess somebody would have to be able to get your email to fake that.

**Steve:** They would have - exactly. And the idea would be, well, it's just like when you're signing up for a mailing list. They send you an email confirmation loop to verify that you're at the other end of the address that you just manually gave.

**Leo:** That's reasonably secure.

**Steve:** So to answer Rick's question, I would say what you can tell from the certificate is who signed it. So you follow the certificate chain back to the root and see who that is. If it's Free Certs R Us, then I would say, well, maybe you need to wonder how much to trust that. If it's VeriSign or Thawte or GoDaddy, some reputable company who you've heard of before, I would say, okay, it's more trustworthy. But the point is, it ends up sort of coming down to a social engineering issue. There's really no way, one way or the other, to know for sure. But you can see who signed it and then just use your own judgment. If you've never heard of them, go to their website. Look around. See what they charge. Are they free? Are they expensive? Do they look like they're doing a good job? Maybe they'll have an FAQ on their site where they'll talk about what steps they go through prior to issuing a certificate.

So unfortunately all of our trust in authentication through SSL is about - it ultimately comes down to trusting the people who sign the certificate. And we know from my comments a long time ago when I scrolled down through the incredibly long list of trusted certificate authorities, that my concern was the more there are, the less we know about each one. So ultimately we're relying on the integrity of whoever it was who signed a specific certificate. So all you can do is track that back and see what you think of those people. Make just sort of a value, a judgment call. There is no further authority. No one else to ask.

**Leo:** Andy Goldbaum, Warwick, New York offers us the Private Browsing Tip of the Week [fanfare]. I'm using the latest version of Firefox with NoScript fully enabled. Just as you recommend, Steve. It took a few months for me to get used to the NoScript mode, but now I don't even notice myself "allowing" various sites and web pages. I guess I should do that. I discovered that when using Firefox in Private Browsing Mode or when you clear recent history, NoScript retains the website address of any site you said okay to in the whitelist tab. Adobe Flash also continues to store Flash cookies in Private Browsing Mode, as well. So if you want to browse the web privately, at least as far as your own computer is concerned, you also need to delete the NoScript whitelist entry and Flash cookies. A little tip. Thanks for the show.

**Steve:** This was a really good point because it reminds us that, when Firefox is told to implement private browsing, it's handling those aspects of the browsing session that it's responsible for. But it's not responsible for policing Flash cookies or NoScript's actions during that time. That is, there's no way for it to know what it was that any of the add-ons that it might have or the embedded objects that might be on the page, there's no way for it to know what they did.

So I just thought this was a really good point, that when you go into private browsing, it's not like suddenly somehow everything else is taken care of. Andy noted that NoScript was remembering the permissions that it was given, and that if it was important, somebody could come along and look at your NoScript permissions and see sites that you had given permission to while in private browsing mode because that's outside of Firefox's jurisdiction, essentially, for enforcing privacy, just as Flash cookies would be. Whereas browser cookies are within Firefox's purview.

So the notion of using a Live Linux boot CD would enforce an absolute version of privacy because nothing is being written to the hard drive or stored permanently. But private browsing is convenient. But it's, again, this is a great tip because it reminds us that there are things that Firefox or, for example, IE offers the same sort of feature now in IE8. There are things that can be stored that are outside of their control.

**Leo:** Yeah. Private browsing is not as private as you think, I guess is the subtitle of that one.

**Steve:** Or not absolutely private because the things that you invite into the browser page can also remember that you were there.

**Leo:** But if your wife is that sophisticated, she's looking at the whitelist tab or your Flash cookies, maybe you should just stop browsing porn anyway. I'm sorry, that was mean. Lasse "Laslo" Huhtala in Sweden - I can't read the diacritical remarks, it just didn't come out right - Somewhere, Sweden, offers his keyboard cleaning tip. I probably would read it wrong anyway, so sorry, Laslo. Steve, greetings from Sweden. I was just - we have so many Swedish listeners. By the way, I've got to learn Swedish, and then this would be solved. I was just watching the Security Now! show where you and Leo were talking about cleaning keyboards in various ways. This is our Keyboard Cleaning Tip of the Week. Here's my five cents.

Okay, so pry the key caps off. Stick the key caps in one of those bags people use for cleaning their delicates. You know, they're like the - anyway. If you're married you'll know what I'm talking about. And throw the bag in the washer. The washing bag keeps everything together. It's actually fairly important. It's like netted. And the loose bits don't get lost that way. Of course you want to avoid aggressive cleaning agents and high heat. Your ordinary liquid washing agent is fine. He uses the hand wash temperature setting up to regular temperatures, but not over 40 Celsius. You can actually also stick cables, for example, detachable keyboard cables, in the same bag and wash those. Works like a charm.

I've got to say something right here, though. Make darn sure you've fully dried that before you plug that cable back in. No wet cables. Okay? Just really, you know, it takes longer than you think. I learned this trick back in the '80s when working for the Swedish phone company who often recycled cables for phone receivers and then stuck them on phones as new. But that's, you know what, that's - I think that's smart. Why throw it out? Wash it.

**Steve:** Yup.

**Leo:** Also you might want to thank Jeri Ellsworth, who by being on Leo and Kiki's show introduced me to TWiT, which in turn introduced me to your show, which ultimately led me to SpinRite. I registered my SpinRite just a few weeks ago, and I'm very impressed with it. Happy 2010. Your cyber-pal Laslo of Sweden.

**Steve:** Well, there's another tip. I like it. The idea of putting the key tops, I mean, I look at mine, and I'm going to have to spend some time. The good news is we all have digital cameras now on our phones or standalone. You take a picture of the keyboard first because, as you commented, Leo...

**Leo:** You have to, yeah.

**Steve:** ...it's important to be able to get the caps back in the right order. Otherwise you'll be typing strange things, going what the heck...

**Leo:** When we first did this tip, which we started - it was on the pilot for The Screen Savers in 1997 or 1998. Kate Botello and I did this tip, cleaning your keyboard. And we used a Polaroid camera. Just shows you how long ago that was.

**Steve:** Yeah. I look at mine, and they're just grungy. I mean, you know?

**Leo:** Oh, disgusting, yeah.

**Steve:** And of course the ones I use more often, the keyboard originally had sort of a matte surface on the keys. So there are still some that have retained their matte surface. But the ones that I really use have just been polished shiny by my fingers.

**Leo:** Yeah, you can tell.

**Steve:** So I really do need to take this off and give it some cleaning. So I just - I liked - I thought that was a great tip from a listener.

**Leo:** Good idea. Thank you, Laslo. Nice to have you listening in Sweden. And thank you, Steve. We have gone through 10 great questions, your great answers.

**Steve:** Lots of security news and tidbits for the week.

**Leo:** Yeah, good show this week, yeah.

**Steve:** Yeah.

**Leo:** Make sure you get that Microsoft zero-day exploit update. It comes out today.

**Steve:** Yes, good, very, very good point. That's out of cycle and important. I do think, though, that following the suggestions I had for just in general bolting down IE, for those people who are not using it all the time during the day, that is, who have switched to Firefox but still have IE sort of there as a looming threat, it makes a lot of sense to just lock it down.

**Leo:** Really, really. I love that. And I just did it on this machine. And when I get home I'm going to do it on all my Windows machines at home. I think that's great thinking.

**Steve:** And we'll set me up to repeat it to your listeners on the weekend.

**Leo:** Yeah. We will do that.

**Steve:** Cool.

**Leo:** Thank you, Steve. And we'll be back next week, as always. You can watch this show live. We do it every Wednesday at 11:00 a.m. Pacific.

**Steve:** Oh, except not next week.

**Leo:** Oh, next week we're moving it. Because Apple's got some verkakte announcement they're going to make.

**Steve:** Wonder what that could be.

**Leo:** You know, it's funny, before the show began Steve and I were talking, and he said he's excited about this. I guess because it might be a book reader; right?

**Steve:** It just might be wonderful. I want, you know, every time the doorbell rings and UPS brings something, I think, oh, maybe it'll be wonderful. Normally I'm disappointed. But, you know, Jobs has a way of not disappointing us.

**Leo:** He has a track record. And I think the way that Apple has already kind of seeded the press with stories, they believe that this is as revolutionary a product as the iPod was, as the iPhone. Maybe even as the Apple II.

**Steve:** Ah. I want one. I don't know, I don't care what it is. I want one.

**Leo:** I think it's a new category. I think it's going - as you said, it's going to be a crossover category of some - hardware category of some kind. And I think it could be very good. We're going to do all-day coverage of it from 9:00 a.m. to 4:00 p.m. Pacific.

**Steve:** Next Wednesday.

**Leo:** Next Wednesday.

**Steve:** When we would normally be recording.

**Leo:** Exactly.

**Steve:** So we're going to be recording on Tuesday instead.

**Leo:** So Tuesday, January 26, at 11:00 a.m. Pacific, 2:00 p.m. Eastern, you can watch the show at live.twit.tv. The following day we'll be there all day, live.twit.tv, just obsessively talking about the tablet.

**Steve:** Yay.

**Leo:** Yay. And then we're back to our normal time every Wednesday.

**Steve:** Yup.

**Leo:** The following week. Steve, have a great week. We'll talk to you next time...

**Steve:** Talk to you then, Leo, thanks.

**Leo:** ...on Security Now!. Bye bye.