Listener Feedback #202

Description: Mike and I discuss the week's major security events and discuss questions and comments from listeners of previous episodes. We 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-484.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-484-lq.mp3

SHOW TEASE: It's time for Security Now! with Steve Gibson. Steve updates us on the latest Firefox, plus the trouble with iOS v8, and Steve answers your questions. It's Q&A #202. Stick around. Security Now! is next.

MIKE ELGAN: This is Security Now! with Steve Gibson, Episode 484, recorded December 2nd, 2014: Your questions, Steve's answers, #202.

It's time for Security Now! with Steve Gibson, the show where we cover privacy, security, and so much more, including coffee. And we'll be totally talking about coffee here today at some point. How you doing, Steve?

Steve Gibson: Hey, well, everybody knows you are not the voice of Leo.

MIKE: You're kidding.

Steve: So, Mike, it's great to be with you this week. We'll do a Q&A, and everything'll be just fine.

MIKE: I'll believe it when I see it. I hope I don't wreck the show. Leo's off today, and I'm stepping in. I always listen to this show, so it's really great to actually host the show with you, and this is just going to be awesome. So why don't we just launch into the show.

Steve: Well, so we have a Q&A this week. We don't have a ton of news. I want to talk about some new features in the just-released v34 of Firefox. And to sort of tease next week's "deep dive" episode, I thought I was going to talk about the research into de-anonymizing Tor. And I've decided we'll call that one "De-Tor." But it ended up being so interesting and cool that I thought, okay, this is worth a whole podcast. So that'll be next week. Then we have a bunch of, I mean, nothing really happened in the last week, although we've had a couple of very busy weeks before that. So we have a bunch of interesting miscellaneous stuff, and it's a Q&A episode, #202. So we've got 10 interesting and some thought-provoking questions from our listeners that we're going to cover.

MIKE: Fantastic. I can't wait to hear it.

Steve: And it's sort of odd in our - I try to put some sort of a picture on the front page of the show notes every week. And Jenny sent me a picture of the Newf sisters, the twins that she has. She and her daughter each have one, named Paris and Beluga. And I didn't realize it until she commented that they both have their front paws crossed, which was the impetus for taking the picture. Apparently this is something that Newfoundlands do. Jenny is a serial Newfoundland owner. And so they took the picture because both dogs, both pups were sitting there with their right paws crossed over their left. I mean, this wasn't staged, this was just candid.

But we have a sponsor, who we don't have this week, but Leo introduced them last week, BarkBox. And one was sent to me, which I then dropped off with Jen, and the pups got a big kick out of it. So we will talk, I will share Jenny's reaction and theirs, actually, when we next have BarkBox as a sponsor. But that explains why there's a couple dogs on the front page of the show notes, whereas normally we have schematics of networking diagrams and boxes interconnected to stuff, or bar charts showing scary infection rates across the globe. Now we've got Newfs staring at the camera saying, "Can we eat that?" Anyway, so...

MIKE: And crossing their paws. It's amazing.

Steve: And crossing their paws, as apparently Newfs are wont to do. So we're going to talk, next week's topic will

be De-Tor. And I'll just say that the reason it's worth talking about is that stats have been generated by a researcher who believes that anyone who sufficiently wanted to could deanonymize more than 80%, I think the number that I remember was 84%, of supposedly anonymized Tor traffic, using some features of Cisco routers. And that's a high enough number. It's not like maybe they could get lucky. But that's a big number. And we do know, if nothing else, post-Snowden revelations, that organizations like the NSA really do, really would want to be able to provide deanonymizing service for Tor. So definitely worth talking about next week. And we'll do one of our wind-up-your-propeller-cap episodes.

MIKE: Nice.

Steve: Yeah. So we just got a new drop of Firefox, v34. The biggest thing you see, which had been covered, I think it was mentioned maybe a couple weeks ago, is that Firefox for the first time is no longer using Google as their default search engine. If you're upgrading from Firefox, it doesn't boot you out, but it introduces and sort of suggests that let's all switch to Yahoo!. Well, okay. Now, I have no experience with Yahoo!. But I'm not switching. I'm staying with Google. So as I understand it, Google has been a sponsor of Mozilla for, like, for a long time. Do you know what's behind this, Mike? Is this the ascendance of Chrome as, like, competition? Has Google pulled their sponsorship of Firefox? Do you know any more?

MIKE: Well, I have a feeling that Yahoo! paid dearly for this. And the other thing that's interesting about it is the length of the contract. I think this was a five-year contract, where I think the old Google contract was a three-year contract. I think it's pretty standard for money to change hands for these things. But I just think that Yahoo! is desperate and hungry.

Steve: Well, and we do see more Yahoo! stuff in the news, so I think you're right, I think they're clearly pushing wherever they can to make some inroads. And so the default search engine changes. But if you're already at Google, you're not kicked out. They've expanded search features. Oh, I ought to mention also that for Belarusian, Kazakhstan, and Russian locales the search engine is changed to Yandex, Y-A-N-D-E-X, as opposed to Yahoo!. So it's not a global change. They have improved the search bar. They've also got now a real-time chat client called "Hello" is built into Firefox. So that's part of the standard build now. It's also possible in 34 to easily switch themes and personas directly in the customizing mode. Oh, and they're now noticing that, if you're using Wikipedia search, it defaults to HTTPS. So it sort of upgrades your search privacy for you when you are searching in the U.S. Wikipedia.

They have an early implementation of HTTP/2, which is based on SPDY, that we talked about a long time ago. SPDY was the sort of experimental, next-generation HTTP alternative that Google was experimenting with, has been for years. And also ALPN support is there. That's the Application Layer Protocol Negotiation that allows application layer security to be negotiated by connection. So anyway, so this is just sort of early standards stuff moving forward that Mozilla is staying right up with. And they also said that you can now recover from a locked Firefox process in the, quote, "Firefox is already running" dialogue under Windows. Firefox is my browser, I live in it, and I've never encountered that. So I don't know when that happens. But if it does, you can now recover from it.

Oh, and interestingly, they have disabled SSLv3 in the Firefox client. So Firefox will no longer support v3 of SSL. It will be at formally TLS now, 1.0, 1.1, and 1.2. And that's of course because we've had recent problems with the security of SSLv3. So, neat that they're doing that. And I imagine, Mike, that Windows will ultimately - Microsoft with IE will get around to that at some point, which is a good thing to do.

MIKE: Probably take them a while, though.

Steve: Exactly. Precisely. It won't be anytime soon. And just sort of on the developer side, lots of motion forward on the HTML5 standard, mostly in the web crypto area. I saw just a ton of new web crypto APIs that have support. And I think that's good, overall.

So that's really all the news we have. I hear Leo and Sarah talking about iOS v8. And I've been meaning to say for a while that the iOS 8 bugs are just driving me crazy. I mean, it's sad that - I don't know, are you an iOS or an Android person?

MIKE: I'm on iOS now. I moved from Android to the iPhone 6 Plus, and so I'm back on iOS. And, yeah, it's kind of surprising, isn't it.

Steve: It really is. I mean, Jobs would just be, well, I mean, heads would be rolling, if this was going on at Apple with Steve still at the helm. All kinds of obscure things. A lot of them seem to be keyboard related. I'm a big fan of Swype and SwiftKey. That's just a win on those touchscreens. But I'm seeing, like, new, creative ways that they are finding to fail. Just this morning I could see, like, just the upper maybe 25% of the keyboard skewed off to the side. It was like, okay, what the heck? And but even non-keyboard things. The calendar app had the December month, like, ghosted three times in some sort of a rendering error. And just all kinds of obscure things. It is not only surprising, but it's disappointing because we depend upon this, and we'd like to have a reliable appliance. So anyway, I listen to Leo and Sarah sometimes saying, "What is going on?" And I just want to say, yeah, believe me, you guys are not alone. Everybody is seeing it.

MIKE: Yup.

Steve: And there was an interesting article in The Washington Post. I'm also hearing Leo, and as it was, Leo and Sarah were talking yesterday. You know, Leo is no fan of Twitter. You probably have heard him, Mike, talking about just what a catastrophe he feels it is. Anne Applebaum wrote a nice piece that I'm linking to in the show notes, that I wanted to just point our listeners to, just the first couple paragraphs to give our listeners a sense for it. Anne writes: "If you are reading this article on the Internet, stop afterward and think about it." Okay, so she's saying read the article. Think about it. "Then scroll to the bottom and read the commentary. If there isn't any, try a website that allows comments, preferably one that is political. Then recheck your views." And so what she's saying is read what's posted and wait, assess it, make up your own mind. Then read the comments and see what you now think.

She says: "Chances are your thinking will have changed, especially if you have read a series of insulting, negative, or mocking remarks, as so often you will. Once upon a time, it seemed as if the Internet would be a place of civilized and open debate; now, unedited forums often deteriorate to insult exchanges. Like it or not, this matters. Multiple experiments have shown that perceptions of an article, its writer, or its subject can be profoundly shaped by anonymous online commentary, especially if it is harsh. One group of researchers found that rude comments" - quote, and this is from the research - "'not only polarized readers, but they often changed a participant's interpretation of the news story itself.' A digital analyst at Atlantic Media also discovered that people who read negative comments were more likely to judge that an article was of low quality and, regardless of the content, to doubt the truth of what it stated."

Anyway, I just think this is a fascinating aspect of what's going on with the Internet now that absolutely relates to Leo's current angst with Twitter. And I've experienced it. There are, for example, about SQRL, there are some people who didn't understand what I had created and put up some early blog postings that are critical of it, which are fine, if people would understand the context for that. And one of the problems is that I guess people who don't have a firm sense of their own ability to make up their mind sort of inherently defer to others. And so people will read, as Anne notes, criticism and get hugely swayed. And I end up finding myself having to defend against somebody with no credentials at all who's raised some concerns that actually aren't problems at all, I mean, the person is completely wrong, but it scares people. And we see this happening all over the Internet, in all kinds of instances.

So anyway, that's just the front of a really thought-provoking piece that, if people are interested in the subject, I really would commend them to take a look at. And she wonders toward the end whether anonymity is, for all of its benefits and the power and enabling that it creates on the Internet, if that's not part of the problem. And I wonder - and certainly I would never suggest that people lose the right to be anonymous if they choose. But sort of in the same way that Twitter, to use the example, has the option to verify the identity of Twitter accounts - you know, Leo has the little checkmark. He's a verified identity. People have told me I should do that. I just haven't gotten around to it. But maybe that's the solution is to allow people to have an authenticated identity if they choose, or to be anonymous, oddly named creatures if they don't. But anyway, I thought that this was just an interesting piece that came across. What do you think about the whole thing?

MIKE: It is, yeah, it is interesting. And I've had multiple conversations with Leo about this. And my own view is that I think that anonymity is okay as long as the communications medium you're using enables the person who starts the conversation to delete any comment below that conversation and then block that person from being able to come in later on. There are some social networks that allow that and others that don't. Twitter is where a lot of the problems exist, simply because on Twitter you have no such power. Any tweet, whether it's a response to an initial tweet or not, is equal to every other tweet, for the most part. So, for example, let's say you posted something on Twitter about SQRL, and then a bunch of people commented on it. And let's say somebody was saying all kinds of things that weren't true, and they were being just deliberately malicious or whatever the case may be. And on Twitter there's literally nothing you can do about it. Everyone involved in that conversation who's paying attention will see their comments and your rebuttals as equal, and you can block them if you want. But if you block them, you're simply putting your own head in the sand, and those comments are going on without any control on your part.

Steve: Right, right.

MIKE: Whereas on other social networks, you can go in there and literally delete the comments. And so the conversation that you started, you have sort of stewardship of that conversation, and...

Steve: You're still able to curate it, yeah.

MIKE: Exactly. And I think that's one part of the solution. I don't mean to be super anti-Twitter because Twitter is great in so many ways. And of course we tech journalists love Twitter almost universally. But there's a structural issue about Twitter that leads to this kind of misinformation. It's probably the worst place there is online to have a conversation.

Steve: It's funny, I was speaking of, you know, you were talking about journalists. I heard, or I was watching some interviews of some young, hip, Internet-enabled journalists a couple days ago. And these were, like, on the East Coast, but they were involved in the financial markets. And these were like the people who sleep with their iPhone, like, holding it so they'll be awakened by it vibrating. I mean, they're just so connected to the 'Net. And I'm thinking, okay, that's a little too much.

But they both said that the first thing they do when they wake up is check Twitter and, like, specific feeds because they need, they're literally - they're anxious about the fact that they've been unconscious for six hours, god help them, and as fast as possible they need to come up to speed, due to the nature of their jobs, on what happened during the six hours that their body forced them to be unconscious. And I just thought, okay, well, yeah, I don't want your job. But so, yeah, it's irreplaceable, as you said. But the absolute nature of the fact that it's just such a wild zone also creates a problem.

MIKE: Yup. It's a troll's paradise.

Steve: Yeah. I like the idea of being able to curate a conversation you start. Of course, the flipside is you really need to be a mature curator because you're also able to go too far and curate a dialogue so that it looks like you're walking on water. If people are raising issues which are good ones, if you don't have the strength to allow useful debate, rather than just trolling, then this notion of you having control of the dialogue can be taken too far. I did note, and Anne talks about this, there are confirmed reports of paid organizations deliberately spamming competitors' blogs and feeds, like each political party, for example, in an environment where there are multiple parties, hiring organizations to plant negative information in their competitors' or their opponents' social environment for exactly this fact. Unfortunately, negative stuff has a strong, a high level of traction.

MIKE: Yeah, it certainly does. And it's for exactly the reason they're talking about in this article. This sort of astroturfing works, and that's why political parties do it. And also China does it, and Russia does it, too. In fact, there was a story in the news over the weekend, The New York Times Book Review Podcast was talking, interviewing the author of a book about Putin and the Putin kleptocracy, I don't recall the name of the book ["Putin's Kleptocracy" by Karen Dawisha], but it was a new book that was coming out. And she was saying that she was shocked that the so-called "50-Ruble Army," which is what they call it, it's basically named after the "50-Cent Army" of China, which is where they pay commenters to promote the Kremlin and oppose its critics on message boards all over the world, they were silent. She was saying that they didn't jump in and talk about this.

I posted a little thing on Google Plus about the fact that she mentioned that the 50-Ruble Army wasn't there. And guess what, the 50-Ruble Army came rushing in and just polluted the comments with just crazy talk, exactly as she described it. She was asked to describe what sorts of things, what sort of techniques the 50-Ruble Army uses to sort of block out rational conversation, and that's exactly what happened on my own message board. So that was kind of funny. But, yeah, this is the tragic thing. It works. And over time, more and more organizations, governments, parties, companies are discovering that they can influence public opinion through this kind of fake grassroots commentary.

Steve: Wow. Well, yeah, GRC maintains a bunch of old-school NNTP newsgroups. And it's just - it's an amazingly valuable resource. And years ago you could post to the newsgroups through a web interface. And during the time when I was stirring up some controversy over my railing against Microsoft for having the raw socket interface left in, which was going from Windows 2000 Server, it was going to then become Windows XP. And I begged Microsoft not to leave the raw sockets API in a consumer operating system. Fine to have it in a server. Don't put it into a consumer operating system because raw sockets on the application level gives too much attack power. And it wasn't until Service Pack 2 that they finally understood what I was saying. Actually, the MS Blast Worm that attacked them used XP's raw sockets to blast them with an attack that they couldn't defend against. Fortunately, it was aimed at the wrong URL, so they were able to duck that.

But the point is my taking that position was controversial; and the newsgroups, GRC's newsgroups were just overwhelmed with just junk, I mean, just garbage posts, people who weren't informed, who were just on the bandwagon, enjoying making noise. And it was somebody else who'd been a longstanding participant who noticed from the headers that it was the web interface that was the source of all of this, not people who had taken the time to set up a formal NNTP newsreader.

And so I shut down, I made the web interface read-only, and the problem just went away. Because people were happy to just sort of drive by and drop junk into the forums, but nobody took the time to actually set up a newsreader, and that's been the way it's been ever since. And we just, as a consequence, through that little bit of a bar, little bit of a barrier to entry, we have a paradise of, like, really useful technical discussion on an ongoing basis. So I think part of the problem is it's just so easy to put this stuff up. And you have the advantage of anonymity. Which, again, I wouldn't want to take from anybody. But as we've been saying, it does, it can get, unfortunately, abused.

We talked, oh, I don't know when it was, maybe six months ago about an interesting movie that a friend of the podcast, Jonathan Schiefer, had produced called "Algorithm." And I wanted to let our listeners know, and I will remind everyone next week also, that on Sunday, this coming Sunday morning, well, midnight, so like 12:01 a.m. Pacific time, Jonathan is going to take the movie on YouTube public. The URL is in the show notes for anyone who wants it. I'll tweet it on Sunday after it is public because I've already confused some people who tried to go there, and it says "This is private" at the moment. But it's a - yeah, right, you get the little unhappy confused face if you go to the link. But it's a really interesting, technically accurate, sort of privately produced movie that Jon crowdfunded in order to produce. So as soon as it is public, I will tweet it, and I'll remind everybody next Tuesday. But if you're anxious to get it before then, you could do so by grabbing the URL from the show notes and checking it out on Sunday [https://t.co/ks1gOLZTu0].

Okay, now, this is completely off topic. And I was anticipating that I'd be talking to Leo about this. I don't know if -

do you know anything about Abe and Oddworld?

MIKE: No, I don't.

Steve: Okay. Well, Leo and I have spoken about Abe and Abe's Oddworld and Oddworld Inhabitants for a decade or more. It was a really unique videogame project which launched in 1994, a group of computer animation and special effects people up in San Luis Obispo, led by a guy named Lorne Lanning and Sherry McKenna. They were considering - they were sort of an offshoot of Hollywood, doing projects for Hollywood. And Lorne and Sherry were seeing each other socially. Lorne wasn't around when Sherry was hanging out in his living room, and on his coffee table she saw a sheaf of papers, sort of looked like a screenplay, that Lorne had put together, that he'd never mentioned to her. So she starts reading this. And when he came back she said, "What's this?" And he said, "Oh, it was just sort of some ideas I was working on, maybe for a movie." And she looked at him, and she said, "No, this is our videogame."

And I'm talking about this because it's coming back. It was on the early consoles. And every time another installment would come out - there was Abe's Oddworld, Oddworld Exoddus, or Abe's Exoddus, I think. Then the idea was there was going to be a quintology. I think they did only three or four titles. And I'm not a videogame guy. I mean, I've really no interest in the whole first-person shooter genre, except from a video technology standpoint. I've been fascinated by looking at the way the technology has evolved.

What was unique about this, and the reason they did something, was that it was sort of green. This little character, who was literally a floor polisher, worked in - this is all on an alien planet - worked at Rupture Farms, which was a meatpacking facility. And this sort of takes you through his attempt to free all of his coworkers. It is a puzzle mode game as opposed to a fast reflex, fast action sort of game. And I'm just a sucker for puzzle mode stuff.

And even though I remember the reviews just were wild about it, they called it a - it came out in a time when we were sort of done with what's called the "horizontal scrollers," where you just sort of scroll horizontally and stuff happens. And this was one, except that it was so well done, the graphics and animation, I mean, and the background music, you just felt like you were in this environment. Leo was completely enthralled. He and his son used to play it all the time. I would lose a couple weeks of my life every time a new title came out from these guys because that's all I would do was just sit down and say, okay, I have to just take a timeout. I don't ever go on vacation, so this is my vacation.

So what Leo and Sarah talked about yesterday is there is a new title available using a character which they created toward the end called "The Stranger." This is available on iOS. So they were showing it on iPad Today yesterday, called Oddworld: Stranger's Wrath. And it is coming soon to Android. But anyone who has a PS4, because it's the only platform their remake of the original Abe's Oddworld is available for, if you're interested, check out Abe's Oddworld. The game is called "New 'n' Tasty," currently only on the PS4. They are going to be backporting it to the 3 and the PlayStation, the Mac, the PC, and the Xbox One. But it's not available on those platforms yet. And just to give you a sense for it, Escapist gave it a 5 out of 5, Eurogamer a 9 out of 10, Gadget Show a 5 out of 5, PS Nation a 9 out of 10, Meristation a 9 out of 10, Nowgamer a 9 out of 10, and IGN an 8.5 out of 10. I mean, so I can't wait till they get this thing on additional platforms.

And I know this is not a podcast about games. But for what it's worth, if you are a person who likes sort of the puzzle genre, you can play some of the videos on their site. It's Oddworld Inhabitants is the formal publisher. You'll immediately get a sense for what they've done. It is really charming. And the other thing is that it was always inherently nonviolent. And that's why Leo liked it so much and enjoyed sharing it with Henry is that this was about doing good and sort of ecology and, I mean, it's still interesting.

But they were under pressure to do a first-person shooter because that's what everyone was wanting, even though they were very successful with their puzzle platforms. So this Stranger character shot weird little animals that did the - instead of like a grenade blowing up, it would be some little fur ball that was mostly teeth, and it would buzz around on the bad guys whenever it shot them. So even then they tried to tone it down and keep it from being your typical first-person shooter game. So anyway, I just, for what it's worth, I recommend all of their content without reservation. And I'll have fun talking to Leo about it when he's back with me.

MIKE: Well, it sounds really cool. I'm going to have to check it out. I just am completely unfamiliar. I'm not a gamer, either. I just have maybe one or two games that I play every now and then. But this sounds really great. I love what you're talking about, how it's like sort of the opposite of Grand Theft Auto.

Steve: Yes.

MIKE: You know, it's constructive and interesting rather than just blowing people away. And, yeah, sounds really fascinating.

Steve: Yeah. Well, it has heart. I mean, first of all, these guys are talented graphic artists and designers. So a huge amount of just emotive content in the game. I mean, it's just - I just can't recommend it highly enough. So if I've managed to tease anybody, go check out Oddworld Inhabitants. I was just delighted that they're still around, and they're producing content. It is really unique and really special. In fact, Leo played a video. If anyone's curious, you could get yesterday's, that would be December 1's iPad Today because there is a video at the beginning of the game that Leo played that gives you a great sense for just how good this is. And again, for younger kids and for us

old people, too.

MIKE: Sounds awesome.

Steve: So I encountered, when going through the mailbag today, a note which was - it's one of the kinds of things that we hear about SpinRite from time to time that surprises people. And that's because it's not always clear when a hard drive is having trouble. So this was from a guy - well, I guess a guy. I'm sorry if you're not. All I have for a name is M-A-R-B-L-A, so MarBla or something.

MIKE: MarBla.

Steve: In Poland. Anyway, his email was titled "SpinRite Saved Chromium Browsers." So he wrote: "Hi, Mr. G. Recently I had some serious issues with the browsers that work with the Chromium engine, Google Chrome and Opera." He said: "Pages did not want to load, not possible to load settings page, et cetera. I tried multiple times to uninstall and install the software again, scanned my computer with many antivirus and antimalware software, but nothing I tried helped. I was forced to use Firefox, [and he says] not my favorite, on this particular machine. But finally I received a strange message from Windows operating system that my hard drive needs attention as there are a lot of errors." And he says: "Probably some input from the SMART system? So I launched SpinRite at Level 2. After a few hours it showed three red 'U' marks, and the system restarted. And, yes, Chromium browsers now all work perfectly again. So sometimes you can't expect what can actually help in your software problem. Thanks, and greetings for you and Leo." And MarBla, thank you for sharing your success with SpinRite.

MIKE: Who'd a thought. It fixes Chromium. That's awesome.

Steve: Yeah. Indeed.

MIKE: Well, Steve, we've got some questions here. Why don't we just launch in? I'll ask you the questions; you answer them. Because if you ask the questions and I answer them, people are going to get some bad answers. So let's do this right.

Steve: That sounds like a plan.

MIKE: All right. So let's start with Yves Nadeau. I'm probably messing up the pronunciation there. Hi, Steve Gibson. I got a domain-level SSL for my blog for 98 cents a year on Cyber Monday. It works so far, but how do I prioritize it over regular HTTP?

Steve: Well, I saw this, and I thought this was a really great question because we've been talking recently about the EFF's pending project, due out in the second quarter of 2015, to for the first time ever make domain-level, that is, Domain Validation, DV certificates, available for free by coming up with a clever means of automating the process that allows a server to assert its ownership over a domain name and thus qualify to get certificate protection to basically allow it, in the same way that it would be having an HTTP conversation, to have an HTTPS conversation. When you think about it, I mean, if it's already able to control an HTTP connection, that is, to demonstrate that it's the server there, then why not just allow it to secure essentially the connections to the same domain that it was creating over nonsecure. So I just love the idea.

So in this case he's got a very inexpensive cert, and everyone in the second quarter of 2015 will be able to get them for free. But the problem is, once you get the certificate, then your server can respond to https:// and whatever. But it's doubtless also still going to respond to HTTP. So he's saying, okay, I've got the security now. How do I get it used?

And so there are a couple things you can do. It is definitely possible to, depending upon what server platform you're using - IIS, Apache, Nginx, whatever - to talk to the server administrators. Now, he says he has a blog, so I'm assuming that somebody else is running, who knows where, it might be with WordPress, for example. But taking that as an example, there is a WordPress plugin which you can add to your WordPress installation which will automatically convert the HTTP links to HTTPS. So there's that. You can also, in the config file for the server, you can redirect any browser that attempts to connect to any URL on your blog from HTTP to HTTPS. It's called an HTTP redirect. So those sorts of things you could achieve by contacting the administrator and saying, "Hey, is this a feature that you can offer my blog?"

The alternative way is just to start using HTTPS for everything. If there's, for example, if you're able to edit past blog posts, just go through and change all references to http:// and your domain and blog, change it to HTTPS. You'll want to make sure that all of the explicit HTTP references on the page to your domain are changed. Otherwise you'll start getting those mixed-content warnings, where a secure page also contains unsecured other bits and pieces, pictures and scripts and so forth. So you'll want to make sure you move the whole thing over. And you can easily test it to make sure that you're not having a mixed content problem.

So really the best thing to do is just start using HTTPS ubiquitously. Use it everywhere. When you post links to your blog, post them as HTTPS. When you tweet links, tweet them as HTTPS. Google will pick that up and switch itself over, and so it'll start showing your links preferentially using HTTPS. So you can sort of do it casually, just by using it. Or, if you want to go further, you can enforce it at the server side so that the server turns any nonsecured query,

basically sends back a response to the client saying, oh, this has moved permanently to, and then it gives it the same URL, just adding an "S" after the HTTP, in which case the client reissues the query over on the secure side. And actually, if you do that, Google is very smart about that. It'll notice that links it had are being now redirected permanently, and it'll go back and fix them in its index. So I think a lot of people are going to be wanting to do this about six months from now, which is going to be great.

MIKE: Wow. Cool. All right.

Steve: Yeah.

MIKE: Question #2: Jim in Philadelphia is suffering under corporate SSL interception: Hi, Steve and Leo. I'm a longtime listener, and I look forward to hearing the show each and every week. Recently, with the help of Steve's HTTPS Fingerprints service, I discovered that my company is doing SSL interception of both our HTTP and HTTPS traffic. While I wasn't completely surprised to discover this, I was surprised that it was effective across the board. My banking information, my credit card data, my medical claims were all being decrypted, scanned, and analyzed before leaving our network. I understand the reasons for a company to put this process in place, but surely there must be boundaries? I feel like this is a lawsuit waiting to happen.

If my understanding is correct, setting up a VPN would not help because they would just play man in the middle with that connection, as well. Is there a way around this, or should I just resign myself to never visiting these sites from my work computer? Thanks, and keep up the great work. Jim.

Steve: Okay. So I'm seeing more and more people, I don't know if people are - I think it's probably the awareness that we've created by talking about this problem on the podcast and then giving people a quick means to check using the HTTPS fingerprinting service at GRC. What that does is GRC shows you the serial numbers of certificates out on the Internet that the GRC server sees, and then a user inside of a corporate network compares those to the certificates they're seeing, and they should be the same. If they're not, then there's a very strong chance that essentially a sanctioned man-in-the-middle attack or - like I don't really want to use the word "attack" because it's not an attack. But still, a man-in-the-middle interception is happening.

Okay. So a VPN, if it worked, would almost certainly solve the problem, Jim. This is the firewall that your corporation is using is intercepting HTTP traffic and generating certificates for the sites you visit on the fly. Doubtless your machine accepted in the past a certificate from the firewall which essentially gives it permission to sign on behalf of, well, of anyone it wants to, essentially, which is what makes this a little concerning and frightening. But it's not able to do this with a VPN connection. The problem is that it may - that same technology is very likely, unless it's explicitly permitted, blocking VPN connections. The good news is many VPN services have like a free trial offer, so you could certainly easily experiment with running a VPN connection.

The way VPNs work is that, all of the commercial ones, you receive a certificate which your VPN client has, and that certificate has been signed by the server. But it is not using the regular public, public key crypto system. It's using it, I mean, it's using public key technology, but not the infrastructure, not the whole certificate authority hierarchy. So you get the benefit of very good end-to-end authentication because you're using essentially private certificates. But that means that it cannot be intercepted by regular SSL traffic interception. So it may be that the corporation is blocking VPNs as part of their overall security architecture. But if they're not, then you could absolutely use a VPN in order to essentially create your own tunnel through their firewall, bypassing all of this interception and getting out onto the Internet, where then you would be - you'd then be able to use HTTPS through the VPN tunnel and get really good security that nobody was intercepting.

MIKE: All right. Question #3. Rob Blair in Toronto noticed that Mozilla removed the force OCSP mode. And he says: Hi, Steve and Leo. I'm running Firefox 33.1.1, and I just noticed that in my security settings I no longer have an option for how I want to use OCSP. It used to offer don't check, optional, and force. Now there's only a checkbox for whether to use it or not. Yikes. Any idea when or why this change was made? Thanks.

Steve: Okay. So I looked, and I was already up to v34 that I was just talking about at the top of the show. And sure enough, it's gone from the UI. He was using 33.1.1, which was the last prior version. I didn't notice when it went away. And we saw this happening with Chrome. Now we're seeing something similar. Essentially, I think that they're trying to simplify the user's experience. The good news is the feature itself is not gone. When we spent all of this time a few months back talking about the whole OCSP certificate revocation issue, many people who are Firefox users turned that on and reported - okay. And so what that was doing is that was enforcing OCSP so that Firefox would only function if it affirmatively was able to verify that the certificate was still valid. Nobody - okay, I can't say nobody. But, like, .01, to make up a number, like almost nobody ever had a problem. I'm running it. I've got, I mean, as I said, I live in Firefox. No problem at all.

So the thing to do is go to the famous smorgasbord settings page in Firefox. In the URL bar you put about:config. Instead of https:, you put about:, and then config, C-O-N-F-I-G. You'll end up with more settings than you have ever seen or imagined anything could have. So the good news is there's a search bar. Put in "OCSP," and that reduces it, I'm looking at mine, to one, two, three, four, five, six items. And the last one there is "ocsp.required," and I see that it's still set for "true." So because mine, in my UI, was - really, you're going to want to put in at the top there, in the search bar, put in "OCSP," and it'll just whittle that craziness down. There it is. Bang. So I had left my Firefox with that enabled. Even though they removed it from the UI, they did not turn it off. So good for them. So there's "enabled," and there's "required" is the last two items there. And I've got mine still set for "true" in both

cases.

So they are honoring it. And anybody who still wants to enforce it, if it was enforced by the UI checkbox before, then it has continued to be. And if you never got around to doing that, but you want to, unfortunately they've no longer made it easy. It's not in the UI, but it is in this crazy about:config page, where you're easily able to set that to true, and it'll be sticky. So, Rob, it's still there. And you're still protected; and I am, too. So thanks for bringing that up. I'm glad to know that Mozilla didn't turn it off for people who had it on when they removed it from the user interface.

MIKE: Fantastic. All right, Steve. We have Question #4 from Chris Haas in La Crosse, Wisconsin, who's wondering about the far future of CA expiration dates. He writes: Hi, Steve and Leo. I really love watching the show and listening to Steve going into deep dives on subjects most people don't talk about until it's too late. I recently opened up my local Windows certificate manager - that's certmgr.msc - and was surprised to see how many trusted root CAs that have what I consider to be insanely far future expiration dates. GoDaddy and AOL - AOL! - for instance, expire in 2037, and AOL's was created in 2002. I get the "if it works today it should also work tomorrow" principle, but this is excessive. I know that they can be revoked, but still someone had to consciously say, "Hey, don't worry. Unless you hear something otherwise, just blindly trust us for the next quarter of a century." And someone at Microsoft said, "Yeah, we'll only patch Windows 8 for the next seven years, but that sounds like a good idea." Is this not much of an issue?

Steve: Okay. So really that's a great point. The way to think about this, I think, is sort of as a hierarchy of levels of protection of certificates. So the root CAs are assumed to have extremely good security. We've covered instances where they have unfortunately failed to demonstrate that. But the presumption is they're like security anchors. They've got really good security. They've got the keys to the kingdom really well protected. And for that reason they're willing to - essentially they issued themselves certificates with this far expiration date. You can understand the motivation for doing so because it's somewhat burdensome to get their certificate into every platform that needs to trust the certificates they sign.

Now, probably we're seeing more of an historical, sort of an historical bias because, in this day and age, OS versions are changing. We've got on-the-fly updates. The whole connectivity means that in fact it would be not a huge deal for CAs to have shorter-lived certificates that they themselves were replacing in all of the systems that need to trust them. But that's not the way the world is. The world still has really long-life certificates. The danger is that their private key would get compromised. And, I mean, that's really the secret that they're keeping is the private key associated with the public key, which is part of the signature of their certificate.

So what's happened is, and this is maybe about 10 years ago, it used to be that the CAs were signing certificates with their root, and everyone got a little concerned because essentially that meant that their private key, that thing that is there, they absolutely have to keep secret because, if they don't keep it secret, every browser will remove their certificate, and every certificate, every customer certificate they've signed with that would be invalidated, creating a disaster.

So the danger was that that master secret that absolutely cannot be allowed to escape, that is being used every time they sign a certificate, meaning it has to come out to play. So the philosophy of, like, how to protect themselves changed, and they created intermediate certificates. So that today, for example, you don't see the end certificate of the server signed directly with the root. Instead, you'll see it signed with an intermediate certificate, and that will have a much shorter expiration.

When I saw the question I thought, I wonder what Mozilla is doing? So I went over, I did https://www.mozilla.org. Up came an EV certificate. I clicked the link. I saw that Mozilla gets their certificate from my favorite provider, DigiCert. And sure enough, the root certificate is 2037, and there is an intermediate that expires 10 years sooner than that, the idea being that, now that the root has signed the intermediate, and that intermediate has certificate signing authority, then the root can be literally stuck in a vault so that it never, they never are endangering their root, the root's private key from escaping. It only has to sign the intermediate certificate once, where that certificate has itself certificate signing privileges. Then they lock the root away, never to need it until they need to renew their intermediate certificate. So that gives them much more safety. The only thing that then could escape would be the intermediate certificate. And while that would not be good, it's way better because then none of the browsers would need to disavow the root certificate. They would just need to get another server certificate signed with a new intermediate certificate.

So anyway, that's the story. The roots do have long life, under the presumption that the security of the CA is going to be extremely good. And the incentive is for it to be extremely good because literally the entire business model of the CA is banking on it. We discussed, I think it was DigiNotar, years ago. They were found to be signing fraudulent certificates. They're now bankrupt. They were bankrupt instantly because of their conduct in the handling of that leak. So no certificate authority wants to allow that to happen. The use of this sort of three-stage chain allows them the ability both to have an anchor which lives effectively forever, but at the same time not put it at risk by sort of moving to an intermediate certificate that they are able to - that has a shorter life because they only need to resign that with the master every decade or so.

MIKE: Hmm. All right.

Steve: Really cool system.

MIKE: Very, yeah. All right. Question #5, Joshua in Michigan wonders how a student should safely report a vulnerability. He writes: Hello, Steve. I'm a huge fan of the show. I started taking classes in computer science when I was in the eighth grade, and I can say you've been a big part of my inspiration and interest in computer science and security.

I'm contacting you because I found a security flaw in an online class that I am taking. I'm still a high school student, but I'm taking an online Spanish class, so I have time to dual enroll and take computer science classes at my local university. In my computer science class we've been working with web development, and I was curious as to what software my class was built on. So as I was inspecting the source, I saw a CSV file. It was named a random number, so I was curious and downloaded the file. It was under the overview directory, so I thought it might be an outline of my assignments for the semester. But the file actually contains the grades for every student in my class. Wow.

Obviously, this is a security flaw, and I know I should report it. The biggest concern is how I should go about reporting it. I've read about too many white hats who've gotten in trouble for responsibly reporting vulnerabilities. I'm still in the class right now, and I don't want it to affect my enrollment. If they dropped me from the class, I don't know how it would affect my grades, and I don't know how I'd be able to make it up.

What do you think is the best way for me to go about reporting this? I looked on their website, and I couldn't find a logical place to report it, either. I want to make sure the issue is dealt with, so I don't just want to send it to their general sales query email. I really appreciate you looking into this. I know you're very busy, but I'm both conflicted and concerned about how to approach this, and I need some help. Thank you. Joshua.

Steve: I thought that was really interesting.

MIKE: Yeah.

Steve: And, first of all, Joshua's completely correct. I should mention that he used his full first and last name, and I removed his last name because there's a lot of Joshuas in Michigan, and there's no need to narrow him down.

Okay. So he's found a problem, and he's completely right that, unfortunately, as he knows from this podcast, we're often reporting on unfortunately misinformed or poorly informed bureaucrats who blame the messenger, shoot the messenger, when they absolutely should not do so. Here's what I would recommend, and I spent a little time thinking about this. First of all, I think you have to go old-school. You don't want to do anything in email or PDF or electronic because it's just - it leaves a trail. So I would create a short note that explains the problem, with enough technical detail that whoever is in charge of this will understand what it was you found and how to fix it. I would also print a copy of the CSV file. That is to say, part of this note wants to get their attention. And if they see a printout of all the grades of the students in the class, that'll get their attention.

However, do not print it on any printer that you own, especially a laser printer, because unfortunately we know that printers are - the term is "watermarking." They actually don't use water, they use yellow dots if they're color laser printers. And they actually salt pages with yellow dots to identify the printer that has printed it. So I would say maybe create a PDF or just a Word doc or whatever, whatever format you're comfortable with, and take it to a printing facility and pay cash, just to have, you know, like a Jiffy Quick or a FedEx printer or I can't think of the really famous one. We've always had one on the West Coast. Kinko's is the name I was trying to think of.

Anyway, so get this printed on paper, fold it up, stick it in an envelope, and old-school address it to somebody who is in authority, and send it to them. I think that's the best thing you can do. It will be anonymous. There will be no electronic trail that can be traced back to you. They will get the information. They will believe what you've told them because right there will be a printout of the CSV. And I think that stands the greatest chance for getting this thing fixed and for keeping you completely free of any ridiculous claims of being a bad guy.

MIKE: And it's kind of a sad fact that an honest person trying to do the right thing has to be very careful and cover their tracks, as if they were doing something wrong, when in fact quite the opposite is the case.

Steve: Yeah, it really is. And, I mean, we see this over and over. People really get themselves in trouble, just from trying to say, look, I'm just trying to help you.

MIKE: Yeah. All right, well, Question #6. An anonymous listener in Sweden shares his chilling true story: Hi, Steve and Leo. Blah blah blah, loving and using my SpinRite corporate license every week at work. A small story reminding why you should backup every day: When I got to work this Monday, a support request came from my boss that had noted that he did not have any folders left in Outlook, only the standard folders, and all mail had moved to the inbox and marked as unread. After some investigation I noted, for a change, the trouble was not with his hard drive, so I couldn't just use SpinRite to save us again. The reason that all mail had moved was that someone had broken in through the RDP, the Remote Desktop Protocol, and encrypted every Office document and all Outlook files during the weekend, then left a ransom note - over 600 of them, one in every folder.

So when Outlook started and did not find its standard PSD database file, it created a new one and re-downloaded all mail from the POP server. Thus, they are all "unread." And wouldn't you know it, the backup of my boss's machine had stopped silently a long time ago, and no one noticed. So we have saved the encrypted files in case a time

comes when the encryption can be broken, but we don't have much hope for that. The moral of the story is have SpinRite for recovery, and verify your backups for when it's NOT the hard drive that crashes.

Steve: Yeah, I thought this was interesting. I just wanted to give our listeners a heads-up about this form of attack. If this was in 600 different folders, it sounds like this is some sort of an automated tool which is cracking through RDP. If I'd had more time this morning, I would have dug into RDP protocol because I do remember not long ago, in the last few months, there was a patch that fixed that, that fixed a problem. It must then be that someone got into their network or that RDP was exposed. It runs on a well-known port, and it's not something you really want to have available out on the public Internet.

So, I mean, it's like the old days when servers used to have services running and all their ports exposed, just by default, and people were blocking the ones they didn't want to have access to, or they didn't want to have anyone outside on the Internet to have access to. And we inverted that so that we're only allowing access to the ones we do want people to have. For someone to be able to get from the outside to his boss's remote desktop protocol port is frightening in itself. So for what it's worth, I'm sure there was a patch in the not too distant past that probably fixed what this attacker found, was probably scanning for on the Internet, found and then leveraged. So make sure you don't have RDP exposed. It's too dangerous.

And, yeah, and do verify that backups are actually happening. You know, we do hear stories about this from time to time where a backup system silently stops doing its work, you know, who knows why? The medium fills up, or it's generating errors to an email address that has changed, and no one told the backup server to update its reporting email. One reason or another, it doesn't happen. And then something collapses that absolutely was depending on there being a backup. So, yikes.

MIKE: Well, Steve, here comes the Wild One: Jim M. in Northern Virginia provides us with the source of the name "Regin." Am I saying that right, Steve? Is it Regin?

Steve: You know, we didn't know. I was assuming it was because I was guessing it stood for Registry Installer because that's the technology. Now we know what it stands for. You're about to tell us.

MIKE: Okay.

Steve: And technically, I guess, if we were Norse, we would know how to pronounce it.

MIKE: And we are not, and so don't. Let's go with Regin. And so, Steve, in case you haven't seen, in Norse mythology Regin is a cunning dwarf who raises the hero Sigurd as his own son - I'm going to get all this wrong, I guarantee it - as his own son in order to use him as an instrument of revenge against Regin's deceitful brother, Fafnir. Having become a dragon after stealing the family's hoard of gold, Fafnir is killed by Sigurd, who then goes on to kill Regin when he learns that his adopted father used him to avenge his brother's crime. Now the old Norse dwarf has a second life as a newly discovered, highly advanced piece of malware, techspeak for software used to damage or infiltrate computers.

Steve: So anyway, Jim provides a link to a blog at ForeignPolicy.com where it explains this. And so, yeah, we were fumbling around with the name last week, not knowing what to use. Now, if anyone knows, at least we know where it came from.

[blog.foreignpolicy.com/posts/2014/11/24/this_malware_may_have_gotten_the_nsa_caught_with_its_hand_in_the_cookie_jar]

I did want to mention that there's still no confirmation, but there's very, very strong rumor which has not been confirmed that, as we suspected, that the NSA and also the U.K. intelligence services were probably using this. More disturbing is - and again, no firm confirmation - but that the AV companies have been aware of this for years and assumed it was Western state espionage malware and kept quiet about it. Which, if true, would be disturbing because it would say that they understood that this malware existed, that nobody wanted it in their machine, but they were essentially being complicit with the spooks who had developed and deployed this and weren't pointing at it because that would of course render it useless. So again, no confirmation of any of that, so we just have to call that gossip. And I don't like to do gossip, but I think it's necessary to share what the rumor mill is churning.

MIKE: Yes. And again, if you know the pronunciation, please help us out. We need it on Tech News Today, as well. We don't know what to call this thing. It's a Norse dwarf. We've got to call it something.

Joseph Laba in West Bloomfield, Michigan wondered about CryptoLink: Hi Steve. Just wondering, with the cessation of TrueCrypt support, is there any chance that CryptoLink might be revived? I'm somewhat familiar with its history and why it was shelved, but haven't the successes of TrueCrypt, LastPass, and other TNO systems demonstrated that it's feasible to do it without sacrificing any principles or convictions? Thanks. Long-time listener and SpinRite owner, Joe.

Steve: Okay. So just to recap, CryptoLink is a project I spent a good deal of time, actually, a couple years ago, spec'ing out and designing. The idea behind CryptoLink was that it was Trust No One and had a whole bunch of features which to me seemed like any VPN ought to have them, but none of them do, which would ultimately mean that you would always be able to succeed in establishing a connection. And there were just a whole bunch of other neat things about it. The plan at the time was that I would invest a huge amount of time creating another commercial product for GRC to go along with SpinRite.

Then I saw the handwriting on the wall of what's happening with our intelligence agencies. And it felt to me like we were approaching a time when Trust No One irreversible encryption solutions could actually become illegal. And in fact there was a story just today, and I can't remember the context of it. It was there's an old 18th-century law, something about writs, which courts have just started to use, that is, the federal government is starting to use a writ or to have judges issue them as a new way of forcing companies to decrypt phones, like forcing Apple to decrypt their iPhone and so forth.

Clearly, we're reaching a tipping point where we're going to find out what individual privacy rights are. Apple famously with iOS 8 has deliberately designed a system that they are asserting they are unable to decrypt. And the NSA lead, the new head of the NSA has unfortunately said that Apple is marketing their technology to pedophiles and organized crime and so forth. I mean, way over the top rhetoric, but that's what this has come to.

So here's where I stand. I'm busy finishing SQRL. Then I am busy finishing SpinRite 6.1 and 6.2, which will add support for USB features and push SpinRite a little bit further. I want to get 6.1 out without delaying it for the work I want to do for 6.2. At that point we'll see where we stand. I don't think I will ever do CryptoLink as a commercial product. But if I always plan for it to be freeware, then I won't mind if I just have to, I mean, I don't know where I would stand. I guess, if I'm not selling it, if I just put it out into the world, then it's freeware, and people can use it, and we'll just have to see. Maybe we will have something definitive by then where we decide that it is going to be safe for companies to create encryption which is unbreakable. Right now, I think that's still up in the air. And so where I am with CryptoLink is up in the air because the only way I would do it, if it was unbreakable. There'd just be no point in doing a brand new VPN - well, I just wouldn't do it if I had to make it - if I had to put a backdoor in for anyone.

MIKE: All right. Well, Question #9, Russell Gadd in the U.K. offers a terrific tip about determining what computer or tablet to buy: Steve, one of the lurkers in your newsgroups, Neil Hutton, is a techie who fixes people's PCs. He has created an excellent website advising ordinary folks what to buy to avoid malware - PCs, tablets, et cetera - mainly avoiding Windows. It would merit a mention on Security Now!.

Steve: Okay. So I went there, and I am very impressed. The URL is HowToReplaceYourPC.com. And I want to commend this, maybe not to our listeners because they probably already know, but to their family members. Unfortunately, we just missed Thanksgiving, because this would have been a perfect time for you to print this on everyone's napkins when your family convened. But we do have Christmas coming up: HowToReplaceYourPC.com. I am very impressed. I like the style. I like the design. It's funny because it's organized correctly. There's as much there for digging as deeply as you want. He says he's going to - his job is dealing with people's PCs of all makes and models that are broken. And he says, okay, if you absolutely don't have any time to spend, get a MacBook Air. Period. But if you don't - and so if you're unwilling to go any further for advice, do that. But you may not find that it fits as well as what you could learn about if you dig a little deeper at this site.

So anyway, as I said, I'm very impressed: HowToReplaceYourPC.com. This is for all of the relatives and friends and family who ask us these questions. Just tell them, go here, and you'll be able to help yourself, because I think this guy, Neil Hutton, has done just a beautiful job.

MIKE: Wonderful. Now, a quick bit of advice. He mentioned that, if you don't know what else to say, just go for the MacBook Air. Wouldn't you think that, for avoiding problems, a Chromebook would even be better than a MacBook Air?

Steve: Yeah, I didn't have enough time to spend on his site because I just, again, encountered this during my read through my mailbag this morning, preparing the notes for the podcast. I agree with you, and I'll bet you he even says that. The question would be that people would probably maybe run into things it won't do. And so the advantage of the MacBook Air is, of course, you're - okay. First, nothing does everything to the degree that Windows does. But at the same time, nothing is more dangerous than Windows. For example, the malware, Regin or whatever it's called that we were just talking about. That's Windows-only malware. So if you have a Mac, Regin can't get you. And most of the malware that is out in the world is Windows.

So I think there's like a set of stages where you back away from being able to do absolutely everything you could ever want, but also having absolutely maximum exposure to malware. You step back a notch to the Mac. There are going to be some things that you'll run across that are Windows-only. The good news is much more things now are also available on the Mac, or probably a version or a solution that does the same thing for the Mac. And the level of danger you have is backed off.

But, for example, and I'll bet you he covers this, if, as you certainly know this, Mike, if all your grandmother is doing is baking cookies and surfing the 'Net and doing email, and she uses Gmail, yeah, a Chromebook would be absolutely, first of all, much less expensive, and sufficient. So, and I think that's what this site does. The idea is it carefully matches your needs so you're not spending more money than you need to, you're not buying capability that is going to be unused and will only end up getting you in trouble.

MIKE: All right. Sounds like a great, great site. Can't wait to check it out myself. Last question. Bryce Klippenstein in Calgary, Alberta, Canada wonders about the Security Now! show notes. He writes: I have noticed that the links to the show notes almost always seem to go to a blank wiki page. Are the show notes only posted for some episodes, or is there somewhere else I should be looking for the show notes? Thanks.

Steve: Okay. So I don't know what, well, okay, I do know what it is. It's that I've been referring much more heavily during the podcast to links in the show notes. The show notes are what I'm looking at right now; and, Mike, what you're looking at; what Leo is always looking at. They're always at GRC. However, the podcast that TWiT publishes has up until now just linked to a blank wiki page, which hasn't been what we should have been doing. I just sent email because I must have encountered, like, one out of every two pieces of email in the mailbag were people saying "Where are the show notes? You keep talking about the show notes, but I click on it, and it's a blank wiki page." So I've just asked the producers to start using the GRC URL in the podcast feed. So from this podcast, 484 on, hopefully they will do that.

If it turns out that you still get the TWiT.tv link, GRC always has them. I tweet them at the beginning of the show. They always exist because it's what we run this podcast from. And the entire history of them is on GRC. So if you go to GRC.com/sn, that's the Security Now! page. So the first icon is the high-bandwidth audio. Second icon is the audio I recompress for Elaine at quarter the bitrate, at 16Kb. The third icon is the show notes. That's a PDF with all of the stuff and clickable links. So you can always find them there. But I bet you now that having finally thought to bring this to the attention of the fabulous producers over there in TWiT Land, the link to GRC's notes will now be in the podcast feed. So Bryce, thanks for mentioning it. Everybody else who asked the same question, I saw you all, and it finally got me to ask TWiT to fix this. So I think we're going to be okay now.

MIKE: Fantastic. Well, Steve, how do you end the show? Do we have any final comments? Any other sort of...

Steve: We just tell people that you can find the podcast in their podcast feeds, that they're at TWiT.tv/sn, that I have - oh, that also Elaine transcribes them, so text versions for those who want to read along are at GRC.com/sn. And the 16Kb quarter-size ones for those who are, as Leo puts it, bandwidth impaired, are also available at GRC.com. And that next week we're going to be doing a deep dive, unless, I mean, the world could - the sky could fall. Hopefully the bad guys are taking the holidays off, so maybe nothing bad will happen in the meantime. Assuming that nothing comes in to intervene, we're going to do a deep dive next week into the technology that has been developed and confirmed for deanonymizing Tor users who are specifically using Tor because it's an anonymizing service. And we're probably going to call the podcast "De-Tor."

MIKE: That's fantastic. And of course Steve and Leo do Security Now! at 1:00 p.m. Pacific, 4:00 p.m. Eastern, 2000 UTC, every Tuesday, right here on the TWiT network. Don't miss it. Steve, thank you for tolerating my amateurish hosting, co-hosting of the show. It's been a real...

Steve: Yeah, you did a great job. And thank you for filling in.

MIKE: Well, thank you so much, Steve. And again, I can't wait for that next week's issue. I'm really, really curious about that. It's really one of the most fascinating stories of the year, in my opinion. So I'm looking forward to that. So thanks again, everyone, for tuning in. And you can tune in for Security Now! again next week on Tuesday.