Listener Feedback Q&A #22

Description: Steve and Leo discuss questions asked by listeners of their 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 they have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-104.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-104-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 104 for August 9, 2007: Your questions, Steve's answers.

Hard to believe it's been two years, 104 episodes. And since Steve Gibson is an engineer and never misses an episode, that means exactly two years, Steve Gibson, we've been doing Security Now!. Hello, Steve.

Steve Gibson: Unbelievable, Leo. It's funny because people who know me have said, okay, how is Leo getting Steve to do this? Like...

Leo: Really?

Steve: Oh, yeah. I mean...

Leo: Well, what do they know that I don't know?

Steve: Just how busy I am and, you know, that it's - it is a - it pulls me away from other stuff. But I really do enjoy it, and...

Leo: Well, now I'm feeling guilty, Steve. I had no idea.

Steve: Nah, no, and it's been great for spreading the word about SpinRite. I mean, nothing has been so good for, you know, as allowing our listeners to tell us their stories. I mean, that's just - that rocks.

Leo: Well, and I know you're committed to security. You have been ever since you first discovered spyware on your system. And so this really is kind of the pro bono work that you've been doing all along with ShieldsUP! and Securable and all that stuff. This is just an extension of that.

Steve: Oh, and I haven't told anybody yet, not even you, Leo, but I'm working on, or getting ready to start working on, my first commercial security thing.

Leo: Really.

Steve: Oh, yup. The first - if we discount ChromaZone that was sort of a wacky screensaver that I did, the first thing seriously I've done since SpinRite.

Leo: Wow.

Steve: I mean, like a commercial security thing that GRC will be publishing. So, yeah.

Leo: When you first discovered spyware, you had started using ZoneAlarm, which had just come out at the time, and you noticed something was phoning home. And you wrote an antispyware application, didn't you?

Steve: Yes. It was related to that. It was, you know, ZoneAlarm discovered. And of course we talked about this last week when we were talking about leak testing stuff because that was sort of the genesis of all that. ZoneAlarm awoke me to a little piece of junk which the Windows version of WinZip had put into my machine. And then a couple weeks later there was sort of an erroneous report of something that sounded much worse. Well, it wasn't as bad as it sounded, but it was really bad. And, you know, for that of course I wrote OptOut. But that was free also because it was just like, okay, get this off your computer, folks.

Leo: That's right, OptOut, I remember that now, yeah.

Steve: And actually that was the genesis of the term "spyware." As far as I know, it was when Gregor Freund, one of the founders of ZoneAlarm, and I were on the phone, we said, you know, this is spyware. So. What a concept.

Leo: And you then, because it became such a big area, a bigger area than you wanted to get into, you kind of ceded the concept to Ad-Aware - to Lavasoft, and they started doing Ad-Aware.

Steve: Exactly, exactly. I said, as long as you guys will agree to keep it free, like just keep a free version, then I'd really not want - this is, I mean, it's like being in the antivirus business where every day it's something else. And it's like, I mean, that just doesn't fit my approach to

things, so.

Leo: No. And in fact now especially you're probably thinking, thank god I didn't get into that business.

Steve: Yeah.

Leo: Hey, let's - this is going to be a Q&A segment because it's mod 4. Or to correct our formula...

Steve: Mod 4 equals - or episode mod 4 equals 0.

Leo: So let's do a little - well, actually, I'll tell you what, let's do the errata because I know you have a tiny little fix and...

Steve: Yes, I've got two things. One thing, now, people can check XP, but I was watching the security updates go into XP. You know how with Windows Update you're able to choose if you want to do an express update or the custom. Well, I always click Custom just because, you know, I'm me. I want to see what Microsoft is giving my machine. Not that I really have any choice in the matter because, you know, it's like, okay, fine, whatever you want to do. Otherwise it keeps bugging you about, oh, you missed this important - it's like, okay, fine. But I saw something go by on an XP system about CardSpace. And I said, what? Wait a minute. That's Vista. No no no, my friend. Somewhere along the way Microsoft has slipped CardSpace into XP, and we all have it now.

Leo: Oh, wow. Now, we talked a little bit about CardSpace, but refresh my memory.

Steve: CardSpace is Microsoft's single sign-on solution, sort of the Microsoft does OpenID sort of deal. And they've promised to be able to use OpenID as a back end. So CardSpace is sort of - you can think of it as the UI for OpenID, and a very nice one. And sure enough, on all of my XP machines, I've looked around, trying to find one that hasn't been updated for a while because I'm trying to think, when did this appear? When did they slip this in? But on your Control Panel of Windows XP there is now a CardSpace item. And you can go in and create your own information cards. Remember it was originally called InfoCard, but we're thinking that there was some sort of a trademark collision or something, or who knows.

Leo: Oh, right, right, right, right.

Steve: Anyway, it's in XP, which makes it very exciting because now of course everybody has it. Either if you've got XP or Vista, then CardSpace is there. And...

Leo: How does it relate to Passport, the old single sign-on?

Steve: It's hopefully something that won't die.

Leo: Because I use Passport still for Expedia, of all things.

Steve: Well, exactly. Some of Microsoft's sites do require it. And Microsoft's goal, of course, was...

Leo: And Hotmail actually, yeah.

Steve: Well, exactly. Microsoft's things do. And their goal was for it to be like the ubiquitous solution. But nobody else wanted it. And so we're hoping with something as open as OpenID behind it, this could be a very nice UI. And what excites me is it's like, okay, well, if Vista has it, I'll care in a few years. But XP has it now, which means that we all have it, essentially.

Leo: Now, how do you get to it, I mean, how do you use it?

Steve: I don't know. No...

Leo: No idea. It was just there.

Steve: Yes, no, all I know so far is, if you go into your Control Panel, you'll find CardSpace. And you can open it up...

Leo: But it's the funniest thing, they just snuck that in there.

Steve: They just slipped it in, yeah. And I only happened to notice it because I, in auditing the things they were going to put in, I think they've already been fixing a few CardSpace glitches. I don't think I saw the actual install. I think I saw an update to it. So it's like, wait a minute, XP doesn't have it. Oh, yes it does. So they just gave it to us.

Leo: I'll be danged.

Steve: And if you run it, you're able to create cards. Now, I don't know anybody who uses them yet. But certainly the hope is that, if OpenID can be a back end, then that makes it completely open and documented and no charge, no one's paying anything, and potentially we'll be able to begin using a single sign-on solution.

Leo: Very, very cool. Let's see.

Steve: Okay. So that was my first goodie. And the second one was I had a really short, fun note from a Security Now! listener who wanted to chime in that SpinRite didn't take long for him, either. And remember, after...

Leo: What was that, the three-month SpinRite...

Steve: Kind of knocked you out of your chair, yeah.

Leo: Yeah, when it really sunk in that you meant three months, I was like, what?

Steve: Yeah. His name is Dan Morales. And he sent a note through our GRC support email. And he said, his subject was, "I just purchased SpinRite 6.0, and my desktop was working in an hour." And he says: Hello. I purchased a copy of SpinRite 6.0 this morning, 7/28/2007 - so that was just, you know, a couple weeks ago - one day after my Dell Dimension 8400's Western Digital 160-gig hard drive crashed during a summer rainstorm. So maybe the power went out briefly or something. But whatever happened, he says it only took an hour for SpinRite to blast through the hard drive and clean it up. After an auto reboot, my main XP desktop came up again. I was so relieved. It saved me almost 100 gig in music files, and the first three months of pictures of my nephew. I looked at your testimonial page, and there haven't been any new messages put up in a while. Actually he's right. I've been discussing them here rather than posting them online, and haven't been duplicating them.

Leo: You're talking about SpinRite.info.

Steve: Exactly, the SpinRite.info page. And he says, I would love to see my positive story placed on your site. I already sent an email to friends and family to spread the word and keep SpinRite in mind in case they have any hard drive problems. Thanks so much.

Leo: You're starting a SpinRite cult. It's the cult of SpinRite. Spread the word. Tell everyone you know. SpinRite. That's great.

Steve: Absolutely.

Leo: But, you know, when something works like that, and other things do not, I can understand why people would get kind of excited and say everybody needs to know this.

Steve: And you know, the thing that troubles me is I look at how much benefit our listeners are receiving from learning about SpinRite through the podcast, sort of as a side effect of their listening to Security Now!. And I think of, like, what a small percentage of all PC users you and I are talking to. And so think of all the systems that are, like, oh, well, sorry, reformat your drive, you just lost all of your photos from your whole life. It's just...

Leo: Well, I mention it all the time on the radio show, too. In fact, I think there's a drinking game involved. You know how they have drinking games? When did the drinking games start? I can't remember. But if somebody says a word - I think it was the Bob Newhart show. Whenever anybody said, "Hi, Bob," which apparently they said a lot in that show, you would take a drink. It's a college kid thing.

Steve: Okay.

Leo: So there's a drinking game for the radio show. Apparently every time I recommend SpinRite they have a root beer.

Steve: Well, okay. I think that sounds great.

Leo: All right. So are you ready for some questions, Mr. G.?

Steve: Let's do it.

Leo: All right.

Steve: You were really funny when we were planning this issue. You said, okay, now, this is the one where I get to read, right?

Leo: Well, it's important to me.

Steve: Because of course two weeks ago we had - I know, I think we're going to have you read from now on. You can do the Mailbag, too, Leo.

Leo: I'm a trained professional, Steve. I don't want to say anything, but that's what I do for a living.

Steve: And it shows. I have to have a pop filter in front of my microphone. But you somehow manage to enunciate without blowing any wind into the microphone, so.

Leo: You were fine. And I think it's kind of a good way to distinguish the two. But we'll worry about that offline. Question 1 from listener David Lauery, an interesting issue, actually, he says there are open source Free SSL Certs available from CAcert.org. And I think Thawte for a long time, till VeriSign bought them, was doing the same thing.

Steve: Yes.

Leo: And he wanted to know what you think of these free certs versus the very expensive certs offered by companies like VeriSign.

Steve: Well, it's an interesting issue because, okay, first of all, let's see, there's about nine things I want to say about this.

Leo: You want me to count off? One.

Steve: First of all, it doesn't actually work to have a certificate issued from somebody that your web browser doesn't trust because, as we've talked before, the whole idea is that when you're going to a remote website, and you want to establish a secure encrypted SSL connection, there are basically two things you're getting from that. You're first of all getting your traffic encrypted, which is a really good thing. But you're also getting a verification that they are who they say you are, which - that is, they are who they say they are.

For example, you go to https://grc.com because I have a certificate which I got from VeriSign. And actually he brings up the point because I grumble about how much VeriSign charges me every couple years. But when I'm doing this, the certificate that the browser receives from my server is checked against the list of certificate authorities that the browser already trusts. And it checks to see whether my certificate was signed by one of them, the idea being that they're standing behind some process they went through for verifying that GRC.com really is, that is, the person asking for a certificate every couple years - and paying for it - claiming to be GRC.com really is GRC.com. So first of all, the problem is that these guys are giving certificates away for free. And it's funny, on their web page they say, and we're trying to or hoping to get our certificate authority installed in universal browsers.

Leo: They're nowhere in the chain of trust.

Steve: Exactly. So their certs would not be trusted. But Leo, I wanted to verify that. Now, if you've got IE around, do you have it there...

Leo: Yeah, of course.

Steve: If you go to, and our listeners, too, go to with IE - or you can do it with other browsers if you know where. Go to the Tools, then Internet Options, then click the Content button, and then - or the Content tab.

Leo: Oh, certificates.

Steve: And then Certificates. And then choose - slide over, I think it's the fourth tab is Trusted Root Certification Authorities.

Leo: Yes, you're right, yeah.

Steve: What I was stunned by is look at, I mean, how many there are. A few years ago that little scroll thumb wasn't nearly so small. Now you can hardly grab it, it's so, I mean, there are so many of them. And okay, now, I just - I wrote some of these down because, for example, there's Direccion General de la Policia is a trusted certificate authority. The Japan local government PKI application. ChamberSign, chambers of commerce. TW government root certification. I don't know if that's Taiwan. The Hong Kong Post Office has a certificate in there. Post.Trust Root. Public Notary Root. And even the Turk Trust Electronic Islam [Hizmet Lari ph].

Leo: So these internationally, I mean, they make sense, they've got to support international certification; right? Now, by the way, if you want to see this in Firefox, go to the, again, Tools, Advanced, click the Encryption button, and then View Certificate. No, that's not it. I wonder what - oh, authorities, there it is, yeah. View the Certificate Manager, and the last tab is Authorities. And it's, by the way, Steve, it's actually similar. They've actually organized it, which is nice, into subdirectories. But same one. Chamber of Commerce Root, AOL Time Warner, they even have the Turkish one.

Steve: Well, okay, now, here's what upsets me to some degree is remember that all these things, essentially they've been installed in Windows, and for our browsers to access. And it

means that we will trust without any warning messages, without any exclamation points, without any pop-up dialogues, nothing, we will trust anybody who is signed by any of these people. So inherently the more of these people you're trusting, the lower your security is.

Leo: Well, presumably they validate this somehow; right?

Steve: Well, yes. But, you know...

Leo: But who is Autoridad de Certificacion Firmaprofesional CIF? I mean, who is this person?

Steve: And certainly it's the case that if somebody were caught doing something shady or underhanded, then their CA root certificate would be and could be removed from Windows and from our browsers. But, you know, just sort of that's one of the things that I'm noticing also as I'm looking every time Windows is updating itself. I'm seeing root certificate updates are, like, being sent all the time now, meaning more random bizarre trust is being spread around.

Leo: Well, also they expire. So, in fact, I've had this happen where the root certificate has expired, and they have to be updated regularly.

Steve: Yeah, but in 2029. I mean, it's still a problem.

Leo: Right. Well, the thing that bothers me a little bit more is that somewhere like CAcert, which doesn't want to charge, can't set this up, that they're not in there. It's people who have, apparently, who charge.

Steve: Well, and again, remember that, along with a certificate - and this really speaks against my arguing and grumbling about how much I have to pay, I mean, I'm glad VeriSign jumps through hoops to verify me because I want them to verify everybody else. I mean, I want the idea that an SSL certificate is signed by someone to mean something, to mean that I have some reason to put my faith in them being who they are. And so the reason it's sort of a concern that there's just this bizarre list and growing list of strange authorities which have the full trust of my browser, essentially, is do they have my full trust? I mean, me the user.

Leo: Well, you put your trust in a certifying authority. I don't know who that is. Is that Microsoft? Is that VeriSign? Who is the ultimate authority?

Steve: Well, actually that's the problem.

Leo: Is it Microsoft?

Steve: Microsoft gives the certificates to Windows. So hopefully Microsoft has decided this is a certificate they're willing to have Windows trust. And clearly, I mean, this is an explosion of certification authorities in the last five years. I remember looking...

Leo: Oh, yeah, it was just a handful, yeah.

Steve: Oh, you had VeriSign and Thawte and a few other well-known companies. Now you've got Hong Kong Post Office.

Leo: Well, of course you do. You're sounding provincial now, Steve.

Steve: I don't mean to sound that way. But again, it's just so much.

Leo: And who looks at these? Nobody. And we presume. We just trust Microsoft. And Firefox does the same thing. I want to point out you're trusting Firefox when you use their certificates. By the way, they have at CAcert, they have a process where you could add their certificate to Internet Explorer. But you would have to kind of trust them on your own. And of course since most people don't do that, then, and you use CAcert on your website, you're not going to be a trusted site to them.

Steve: That's exactly right. You are - exactly. And, see, the reason Firefox is showing the same things is that it's actually not the browser.

Leo: Oh, it's the operating system.

Steve: Yes. These are OS-level things. And then there's an API that allows the browser to sort of show them to you and interface to them because of course...

Leo: I didn't get that. Okay. So it's all the same on Windows. I was looking at the MAC list. And so presumably Apple does the same thing.

Steve: Right.

Leo: Okay. Security Now! listener Wes Trexler has a note about LogMeIn's two-factor authentication. We were talking about that on a previous episode. He says: During the multifactor authentication episode, and then again in Episode 101 with the PayPal dongle, I thought I'd write you about what LogMeIn.com has been doing for a few months now that I really like. Instead of having to carry around another dongle, LogMeIn allows you to use your cell phone as a second factor. Oh, that's clever. When you log in, you can have it send a code to your cell phone by text message as further security. Do you see any issues with this method?

Steve: No, and in fact that's one of the things that we talked about in our multifactor authentication episode was that there were already some people who were doing this. And I think it's a very clever and a nice way of operating. It means that, again, something you have, meaning your phone, is being used as an authentication technique. And the value of that, the benefit is that you don't have to have - not only do you not need another dongle, or as we were saying before also multiple dongles for multiple people, but you're using not only something you have, but something you already have, meaning a cell phone - given, of course, that you do have a cell phone.

Leo: Well, and there's some verification, too, with your number. I mean, they can - I don't know if they can, but it is - that's your number.

Steve: Yes, and I don't know whether they look it up. I would imagine they don't. But certainly when you're creating your account with them...

Leo: That's when they get it, yeah.

Steve: You say, yes, I have a cell phone. I want added security. Here's my cell phone number. And so that's the number their server automatically dials and sends a text message to, which you then have to read from the screen and type it into the browser, very much sort of like an email loop, but using a cell phone. So, yeah, I think it's a tremendous solution.

Leo: It is possible to spoof cell phone numbers, but I don't think you can spoof incoming, only outgoing calls. So it seems like that would work. It would be secure. A lot of cell phone-based services like ShoZu use this as a way of verifying.

Steve: Yeah. The hacker would need to somehow - who didn't have your call, would need to somehow intercept a call going to you. And, you know, that's certainly beyond the means of most script kiddie sort of...

Leo: Tom Cruise could do it in "Mission Impossible," but nobody else.

Steve: There you go.

Leo: Alexander Wood writing from Google Mail asks: I reformat the hard drive on my main system every eight to nine months in order to eliminate bit rot. Wow.

Steve: That's what he called it, yeah.

Leo: Wow. When I do, I do a full NTFS format, usually takes over an hour on my 240-gig RAID 0 array. It's two 120-gigabyte Seagate drives. System's almost four years old now. Does this reformat force the drive to check every sector and ensure that my hard drives will last longer? Interesting question. Does it help the drives in any other way, or does it in general hurt them because of the heavy-duty writing and work the drive has to do during a reformat? The drives, as he said, are four years old. They seem fine. Probably mostly because they're well cooled, mounted, on an Alphonos suspension from Silentpcreview.com, and because the computer never gets moved and is in a location with good ventilation. I do back up to an external drive whenever I create important data. Which is of course a very good idea.

Steve: Well, this is an interesting idea. Certainly this guy is being very careful.

Leo: He just formats every few months, basically.

Steve: Yeah, about every eight to nine months he does a format. Now, RAID 0 is the spanning RAID. So he takes two 120-gig drives, and they're merged by his RAID controller into a virtual 240-gig array. Now, if you do a quick NTFS format, which is an option offered when you know your drives are good, basically all that does is it just builds the file structure onto a drive which it assumes is empty and all sectors are perfect, which all contemporary drives, of course, as we've talked about before, because they've got on-the-fly sector relocation, they look perfect from the outside. But when you do a painful, as he said, multi-hour format, what's going on is - and this, you know...

Leo: As opposed to the quick format which you can do.

Steve: Exactly, as opposed to the quick format. And this hails from the original days when drives were not known to present a perfect surface, that is, where they actually had defects. Original drives, old RLL and MFM drives, had bit flags in the headers of their sectors that said the following sector is defective, don't use it. So when you did a so-called "high-level" format, as opposed to a low-level format which is actually a physical format of the surface, the high-level format is the thing that builds the file structure on the disk. When you do that, the system would go out and read every single sector to check for bad flags in the sector headers, and also just to make sure that it is able to read the sector without any errors. So that's what's going on for the two hours is his drive is just sitting there going tick tick tick tick tick tick tick tick tick, you know, cylinder by cylinder, reading all the sectors, looking for any bad flag bits, which it will almost certainly not find. But it is doing a read. And as we talked about several weeks ago, if the drive has some correction which it is applying to the sectors, which grows beyond a certain point, that will flag the sector as needing to be replaced before it gets bad enough that it's no longer correctable.

So the answer to his question is, yes, when he refers to "bit rot," this is what he's talking about. And doing a full format, a full high-level format will force the system to read every sector and allow your drive, very much like running SpinRite on it does. And it's why SpinRite takes hours, too, is that it just, you know, it takes that long to read that much data, suck it through the bus, even if you're not doing anything with it. It just takes that long to read all that data. In the process, the drive is given the opportunity of noticing that there's a problem on a sector that it wouldn't otherwise have been able to notice by itself, and that allows it to spare the sector out, removing it from service. So it's, yeah, it's a useful thing to do, for sure.

Leo: In the old days of pre-IDE drives, we'd be able to do a low-level format on these RLLs and MFM drives. You can't do a low-level format anymore.

Steve: Correct. The command is still there. And it's supported. But all it does is zero the sector in most cases. It doesn't actually rewrite the headers, which is what real low-level formats used to do.

Leo: So the OS format is the best you can do.

Steve: Oh, well, actually running SpinRite is even...

Leo: That would be even better.

Steve: Yeah, it's made for that. And it can then handle - the problem is, if you were doing a format, and you ran across a sector that you couldn't read, now, presumably he's backed up all

his data, he's doing a format, and then he has to restore it. So that's why SpinRite is a superior solution if what you want to do...

Leo: You don't have to do all the backup and restore thing.

Steve: Exactly. Remember, a format says I'm wiping out my entire file system, and then I'm reestablishing it. So he's got to do a backup. Hopefully he wants to ver- I mean, you would want to verify the backup to make sure that you really got it because you're about to reformat the drive that that backup came from, deliberately erasing everything. Then you are restoring in order to put everything back. So, you know, SpinRite essentially folds all that into a single operation and certainly makes it a lot easier to do.

Leo: Mark Schreiber in San Francisco has a common problem. He uses a form on his website for email. And he says lately spammers have figured out how to send spam via this email form. He says: I guess that's why people use CAPTCHAs. My hosting service won't allow me to use a CAPTCHA. He does have antispam, but a lot of it gets through. He says: Is there any way to outwit the spammers? Is form mail dead?

Steve: Unfortunately, I've got to say that it's a problem now. Although I haven't yet implemented myself reCAPTCHA, although I want to find a reason to.

Leo: I have to tell you, just from my own experience, that spammers are not machines, that CAPTCHA doesn't stop them. Maybe they are using robotics. I have spammers on TWiT.tv, it's one of the reasons I've turned off comments, who would not only fill out the form, but wait for the email to come back to them, they actually have email accounts, for the - I was doing email validation, and they'd still spam.

Steve: And so, and this is like spam spam, or just like annoying people?

Leo: And this is the thing. I think I know what's happening to Mark because we have a form for asking questions on the lab. And what's happening is, these spammers are hiring very cheap labor in third world nations to just look for every form and fill it out. They're really trying to do comment spam. I bet you anything what he's getting is a bunch of links. And it's not spam to him. They're hoping that it'll get on a page somewhere. Our form, for instance, on the lab, is an email form. It doesn't go on a page. But we still get that kind of spam. The kind of spam they'd like to have show up on a web page is a comment. It's called "comment spam."

Steve: Yes. And of course you know why, it's because you've got a highly ranked site.

Leo: Right. They want our Google juice.

Steve: Exactly. So if their links appear on your site, the search engines assume that you're explicitly linking to them because you think they're good people.

Leo: Right. And I can tell you right now, CAPTCHA doesn't stop them. Even email

validation doesn't stop them. And I've talked to many other people who say the same thing. You know, to leave a comment on TWiT in the old days you had to register with a real email address, which I would then send a code to you, then you click the link and validate it. They would do that. Not only would they create these accounts, they'd sit on them for months, sleeper accounts, and then ladle the spam out. It's a very big problem. So CAPTCHA's not going to fix it. Delayed email validation doesn't fix - nothing fixes it. These people are very determined. And the truth is they don't really care if it works or not. They just do it everywhere. You know, we use no-follow links, which means that they get no Google juice out of it. Doesn't matter. They still do it. They're not smart, they're just...

Steve: Just persistent.

Leo: Just persistent.

Steve: And they're just shotgunning everything.

Leo: That's the thing, that's the point. And I suspect that's what Mark's getting. They see a form, they don't care, they don't pay attention enough to see whether it's comment spam or going to you personally. Going to you personally is worthless to them. They don't want that.

Steve: Right.

Leo: Let's talk about Chad in Charlotte, North Carolina. Great place for barbecue, I can tell you. He says he wants to increase his anonymity online. He's heard about using public proxy servers. In fact, he's been to those sites we've mentioned before where they have lists all over the world where you can use public proxy servers. He says: Is it dangerous to use these? Plus is there an advantage to using different types? There are anonymous; high anonymity, I guess that'd be like TOR; transparent. Could you talk a little more about these proxy servers, public proxy servers?

Steve: Yeah. Essentially, my sense is this problem has been solved, that is, this need has been addressed by, as you just mentioned a second ago, Leo, by TOR, The Onion Router system. We've done an entire episode on TOR, Chad. So if you're listening to this, as I hope you are, check out our episode on TOR. It's a beautiful technology which is specifically for allowing people to be anonymous. And it's an open source effort. The system is such that even malicious TOR servers aren't able to really take too much advantage, although if you're on - the server at the very edge of the network where you emerge from the onion router, it'll be decrypting your traffic and, you know, and could be seeing what you're doing. But again, anonymity to third parties is generally what your goal is. The reason I think this is superior to these lists of public proxy servers is there's no way to know what the motivations are for those, and they could be bad guys who have gotten their proxy servers on these lists specifically because they hope people will use them, and they're going to in one way or another abuse the trust of the proxy. So...

Leo: They may be watching the traffic that's going through them, for instance.

Steve: Sure, they could be, absolutely. I mean, literally, if you're logging into your - they may

be seeing your log-in passwords going by and have, you know, and grab your account and use it to spam. So I would say, since there is a solution as good as TOR and no real strong reason not to use it because it's configurable and it's designed for this, and it does take measures to prevent any single bad TOR server from being able to abuse the user - again, we cover all this in our TOR episode. I would suggest, Chad, that you listen to that and give TOR a try.

Leo: Now, he was - and he does say he's doing it for anonymity. There is, I should point out, another reason why people use these. And it's not anonymity, it's because they want - it happens a lot in Canada. This is how I know about it. They want to appear to be coming from another country. In the case of Canadians, they can't use - some software they can't download or whatever because they're not in the U.S. So they'll use a public proxy server that gives them an endpoint in the U.S., and then that way they can be an American. But that's a whole different purpose.

Steve: Well, and that's a very good point, too, about TOR. TOR has servers all over the world, and you are...

Leo: But you couldn't use it for that because you don't know where you're going to end up.

Steve: No, remember, we took a question in the Mailbag two weeks ago where the guy mentioned that you're able to ask for a specific server to be your endpoint. And he was talking about it from a standpoint of creating a static IP, that is, it was static and never changing and not his.

Leo: Clever. I think that's what transparent would be, and then there's anonymous and high anonymity. Patrick wants to know more about this PayPal authentication process. He's worried if it's vulnerable to a man-in-the-middle attack. He's writing from Sartell, Minnesota. You know how, when you go to a website and pay with PayPal, it'll bounce you to the PayPal site, where you enter your password, and then bounce you back to the originating site. He says: Could this transaction be hijacked, or could a malicious site in the first place act as a man in the middle between you and PayPal and steal your password info? For example, he says, you go to badguydiamonds.com, try to buy a stone, a false PayPal screen, saying https, by the way, is shown and captures your info as it's relayed to PayPal in the background. Then you complete your transaction, and they've got your PayPal log-in. He says: Is https going to always show the true website in the URL?

Steve: Well, this is a great question because it involves a couple things. First of all, we'll mention, as we have, the very popular PayPal Security Key. An advantage of that is that that number that you append to your log-in password is only valid for 30 seconds.

Leo: So even if they get it they can't re-use it.

Steve: Exactly. That's what's so nice about this. And I've got to say, though, I mean, he brings up a very good point.

Leo: I do this all the time. Every time I buy from PayPal this is what happens.

Steve: Well, yes. And when I'm using some third-party website, and they say would you like to

use PayPal, I say, well, yeah, I want to. I click on that option because I love the idea of not giving these people my PayPal information and using PayPal. But then I'm redirected to PayPal. And, I mean, I'm freaked out at that point because it just seems to me exactly as it seems to Patrick, that, you know, how do I know I really went to PayPal? So this is where...

Leo: Well, he's saying can you look at the address bar and trust it.

Steve: No. I would say that the problem is that, for example, if something got into your local hosts file, or it was filtering your Internet traffic, that is, if something bad is on your computer, for example used a script exploit to get into your machine, your hosts file, as we've talked about before, is the first place that your system looks for the equivalent of DNS. So if there was PayPal.com entering your hosts file, referring to a bogus IP, your browser could show PayPal.com and not be at PayPal, not have gone to one of PayPal's IP addresses. So, but again, it would have a difficult time...

Leo: They'd have to get to your system, I mean, this is a complicated hack.

Steve: Well, but again, if they also put in a Trusted Root Certificate, which is available on your system, then they could sign the certificate of the bogus website pretending to be PayPal, and your browser wouldn't even notice. And as far as I know, nothing would notice. So, I mean, again, you're right, Leo, that it involves a client-side attack. It involves doing things on your machine. But you just do want to be careful about this. I'm glad Patrick brings it up because, I mean, I always right-click on the page, make sure that I've got a certificate that is valid from PayPal and is signed by, you know, the Hong Kong Post Office.

Leo: Now, if you get that certificate, and you look at it, then you feel pretty confident; right?

Steve: Yes. Then I'm, you know, and I use a different email address always when I'm logging into these guys. PayPal has, like, my main personal address, not the one I normally use. So the fact that I've been redirected to PayPal and PayPal has found, knows my real email address, which they got from my PayPal cookie on my machine, I mean, it's not in the cookie, but it allows PayPal to associate me with them. It's like, okay, this must be PayPal because they know things I didn't tell this third-party site.

Leo: You've got me scared now.

Steve: Well, it's a little freaky.

Leo: Got a letter from Yorkshire in the U.K. Paul Elliott is wondering about what he calls "native hard drive encryption." We're talking about TPM. We did that on Episode 99, which is the hardware chip that does encryption. He asks how it's used to encrypt the entire hard drive. For instance, he says, in a standard encrypted file, if a single bit becomes corrupted, the whole file is lost just because the encryption breaks. Is that true for hard drive encryption? It's quite scary to think about losing an entire hard drive from a single bad bit. Or am I missing something?

Steve: Well, there were a couple things that are sort of confused here that I wanted to clarify.

First of all, I did talk about hard drive encryption, referring to I believe it was Hitachi, who in rummaging around I had noticed they were announcing the very first native drive encryption technology, so that more than just locking the hard drive, this thing would actually require to be given a password at power-up from the BIOS, presumably, otherwise you wouldn't be able to boot. And then it would use actually a pass phrase of some sort. It would use that as the cryptographic key to perform on-the-fly decryption as sectors come off the drive and as sectors go onto the drive. So that no non-encrypted data is ever stored on the drive. Now, that does require BIOS support. And again, this is just leading-edge stuff. None of this exists as far as I know.

But I was also talking about my ThinkPad, where I've got my fingerprint reader, and I've enabled the TPM system so that it checks my fingerprint. And, given that it matches, it then uses the associated password as the password to unlock the hard drive. Now, again, that's different than encrypting it. Many laptops support the notion of locking the hard drive. It's something that is unlockable by the manufacturer. But it's, you know, it's go through, get a court order, the FBI or law enforcement would be needed to say, look, we need to get the data...

Leo: Oh, that's interesting. There's a back door.

Steve: Oh, yeah, absolutely. And there are data recovery companies that also have the ability to get past that.

Leo: Oh, I didn't know that.

Steve: So basically it just, I mean, it makes it much more difficult. But it's certainly not as strong as encrypting the entire drive, which is why I really love that idea. And hopefully...

Leo: But how robust is that? I mean, he's worried about a bit corruption.

Steve: Ah, right, exactly. The next point is this is always done on a sector-by-sector basis. The drive doesn't know about files. The file system and the operating system know about files. The drive just knows about sectors. So each run of the 4,096 bits, or 512 bytes, of a sector would be encrypted. And it is the case that, with this, if you had something that was uncorrectable, you would no longer be able to, for example, recover everything in the sector except that little run of bad bits. So, for example, some of the benefit that SpinRite offers would be lost because it'd be no longer possible, basically the entire sector would have to be recovered at once, or at least up to the point - presumably you could be doing encryption until you get to the bad spot. So the further down the sector it is, the more unencrypted data you would get. So, you know, it is the case that there would be some fragility. But it would only be 512 bytes, and only in the case that that sector was uncorrectable prior to doing the decryption.

Leo: So it's really no different than an unencrypted drive, really. Right? That's roughly the same, yeah.

Steve: Right, yup.

Leo: Moving along to question number eight from Leo, I like the name, Leo Sallen in

Australia. He wanted to listen to "On Intelligence," which is the book we've been talking about, the [Jeff] Hawkins book. He says: I love the show. I own SpinRite. I've even used it to save myself. And he's using it all the time, so he hopes he doesn't have to use it again to save himself. He went to look for "On Intelligence" on Audible in Australia. You do get the free book, he said, but he couldn't find the listing for the book or author. And I, you know, we get this from time to time, I understand that - I'll answer this one, Steve.

I understand that - and by the way, Audible doesn't even sponsor this podcast, so it's kind of - this is gratuitous here. But understand that Audible's just a book store. And they are limited by what the publishers want to do. In fact, it's kind of interesting, if you're in Britain and you want to listen to Harry Potter, you have to listen to Stephen Fry read it. If you're in the U.S., you have to listen to Jim Dale read it. And that's just because they're different publishers. So apparently "On Intelligence" either has a different publisher in Australia who doesn't want to support audio books, or whatever. You know, there's some reason. But it comes down to essentially the fact that unfortunately it's not yet an international marketplace when it comes to books. Same reason you can't get the U.K. version of Harry Potter in the states and vice versa.

So Leo, my suggestion is, I guess you can't listen to it, but you certainly could buy it, and I would look for it. Hawkins, Jeff Hawkins is the author. And I don't know what the Sony Connect situation is with that. They may or may not - they have the same restrictions, I'm sure. They may or may not have an eBook version of it. That's where you got it; right, Steve?

Steve: Yeah.

Leo: But you have to have a Sony eBook Reader. Worth reading, however you get it. And he says at the end: Thanks again for the best podcast out there and for SpinRite.

Steve: And I ought to mention, I did mention it before also, that I have Jeff's book on the Palm, not surprisingly.

Leo: Oh, you didn't get it on the Sony Connect Reader, you got it on the Palm.

Steve: Exactly. Well, I have it on both. I've got it on the Reader. Remember I wanted to see whether I could go back to reading on the Palm.

Leo: Right.

Steve: Even though the screen is so high contrast on the Palm, but I just love the size of the screen on the eReader. So...

Leo: Where did you get it for the Palm? What bookstore did you get that from?

Steve: It's the main Palm - just ereader.com, and they definitely have it there.

Leo: Well, they have it there if you're in the U.S.

Steve: Right, exactly.

Leo: That's the problem is that it's all, you know, it's international. You know, it's tough because we're an international podcast. For instance, Vijay Albuquerque in London - or it could be Vijay London in Albuquerque, doesn't matter - now has plenty of room on his drive. He says: Dear Steve and Leo, after hearing about SpaceMonger, which by the way, Steve, I've been recommending everywhere, the original free version...

Steve: Yup, it's so nice.

Leo: I just recommended it on the radio show last weekend. He says: I've reclaimed virtually gigabytes of data from my hard drive. It gives you a visual display of what's wasting space on your hard drive, makes it easier to get rid of it. He says: Is there something for memory, for RAM? He's using the process monitor. You hit Ctrl-Alt-Del to get the Task Manager, and then you can click Processes and see the list of processes. But there must be a simpler, friendlier tool out there, something like SpaceMonger for RAM. I like it.

Steve: RAM Monger or something, yeah. Well, it was an interesting question, so I wanted to explain that, you know, RAM is an entirely different animal than hard drive space because it is inherently dynamic. So applications which are running will use differing amounts of RAM, but there's really no way to tell an application to stop using that much memory unless it's a sloppy application that, for example, you could have a photo editing program where you edit a big photo which takes up a whole bunch of memory, and then when you close that photo it doesn't release the memory, for example. So it's possible that you could have apps which are misbehaving and essentially leaking memory.

But thankfully all Windows versions for the last decade have cleaned up the so-called "resource leaks" when the application terminates and freed up anything, any resources that they had allocated. So really just terminating processes, if you can, that is, if you don't need them around, that are using up a lot of memory, will release their memory. But there isn't anything that you could run to really clean up memory. There are some sort of hokey programs that are supposed to optimize your RAM. But they've really got a bad reputation. And really just, if you have this problem, just restarting Windows and getting things going again is the way to clear everything out.

Leo: In the old days of Windows 95, 98, and ME, the memory manager was pretty pathetic, and so you would have fragmentation of RAM, and you'd have some issues. But XP's memory manager is fine, and there's no point in compacting RAM.

Steve: Right, right.

Leo: I think the memory manager does a pretty good job of getting rid of unused blocks. It can't solve a memory leak, but nothing can solve it. If the operating system won't get rid of that block, you know, release the block, no program's going to come along and do it. So...

Steve: Right.

Leo: Bill Rakosnik of Bishop, Georgia has actually a very interesting question. He says: Can I get a virus by watching video on YouTube? Can video infect you? Is it an executable?

Steve: It's interesting. Unfortunately, and I don't know of any instance of this happening, but yes. Actually there have been old instances. I know that RealMedia years ago was having problems with malware, essentially, or malvideos.

Leo: What's happening is you have an executable program, like the WinAmp player, which had a problem also. And you take advantage of a flaw in the executable program. So the video itself is harmless, it's the fact that it's using a flaw in the video player.

Steve: Or even in some cases in the codecs themselves, that is, the actual decompressor which goes from the compressed format. So essentially it's not the case that any video could give you this kind of problem. It's that the video would be a way of getting code in your machine which is exploitable, that is, where there's some sort of a security flaw in something not even about security, it's about playing music or playing videos. But they've found a way of sort of, for example, giving bogus data in the video to the thing that's trying to play it back, which cause your typical thing like a buffer overrun or a stack overflow or something, that would then allow additional code contained in the movie file to execute. And so, yes, you would essentially be infected by watching that video. And again, it's like anything else. It's something which, as soon as it's found, it'll be patched by the vendor of your OS. And this kind of stuff is going on all the time. So potentially it could be a problem.

Leo: YouTube uses Flash. I don't know of any exploits with Flash right now, but of course there always could be. Somebody could find a flaw in Flash. This reminds me of the

JPEG flaw we've talked about before. Same thing. JPEG itself is harmless because it isn't an executable. But the player, in this case your browser, whatever program is displaying the JPEG, could have a flaw that then the data in the JPEG file could be used to exploit.

Steve: Exactly.

Leo: I think best advice is keep your codecs and your players up to date, you know. But it's harder because, you know, we keep our operating system up to date because it's automatic. You know, if you're using the RealMedia player, I don't know how automatic those updates are. I guess until you run it you don't know.

Steve: Well, it's a very good point. I mean, we've sort of touched on this issue tangentially before when we've talked about websites, for example, using old exploitable wiki code or something, where now we've got Macs updating themselves, Windows is updating itself constantly, I mean, it's now we're all running forward trying to keep our software secure, yet all of this sort of non-primetime code can sit on servers for a long time and be there years after exploits are known. And it is the way people are now exploiting these sorts of systems.

Leo: In fact, you made that point. You made that point really well where you said that, well, now that Windows is in good shape they're going to look for other vectors.

Steve: Yup, other low-hanging fruit, as they say.

Leo: Marcus, I think it's probably Kaczmarek in Kenai, Alaska, is worried, as I am, about U3. That's that new technology in the flash drives that automatically launch applications when you plus in the flash drive. He wonders, if it's insecure, how do I get it off my jump drive? You said you'd cover this, but we haven't covered it yet. We haven't.

Steve: Yeah, in fact, you know, I was going to talk enthusiastically about U3 in the vein of it being a virtual machine sort of technology, the idea being that you could carry this around and plug it into a machine. And so I got some. I mean, I purchased them deliberately to experiment with them. And I'll tell you, Leo, I mean, for a security person, the idea that you plug this into a system, and without asking you it does a bunch of stuff to that machine. I just don't like it. It ought to come neutered so that you have to manually enable features if you want them, rather than the other way around. And so I just - I thought, I'm not helping these people. This just is not right.

Leo: You know, the easy way to do this would be to have an autorun.inf file on there. And then you could disable it by just deleting that. But they don't do that. They mount a disk, a bootable disk, essentially. And there's no way, as far as I can tell, there's no way to disable that functionality in a U3 thumb drive; is there?

Steve: Now, well, the good news is that they provide the option for scrubbing themselves off of the thumb. But of course that's only after it runs the first time. So we can presume there's nothing evil about U3. I didn't mean to assume that there was. I just dislike from a security standpoint the idea that - and I mean then, well, let me finish that thought - the idea that it's enabled by default when all you're doing is buying RAM. I mean, you just want to buy a thumb drive. You buy it from SanDisk, and it has U3. And but all you want is two gigs or four gigs or whatever. And instead, you get this thing that runs the moment, you know, the first time it has contact with your machine. It's like, okay, that seems backwards to me.

Leo: So if you delete the U3 Launchpad, it won't do that anymore.

Steve: No. It turns out it is pernicious. You have to use it to delete itself. And I've experimented with this because I have scraped it off of a couple of these thumb drives. And so you can't get rid of it easily. You have to use it to remove itself because it needs to uninstall the mounted virtual CD which it uses to protect part of itself from accidental erasure. It's got to uninstall that and then delete itself and clean itself off. And it goes through a bunch to remove. So the answer to Marcus's question is, just look at the menu that pops up. There is a way to completely remove it from your system. And I'm glad for that, but I sure wish they did it differently. I wish they had it like, hey, you got a chunk of files there, and you run something to install it on itself rather than having it active when you buy it. Because most people just want the storage space. They don't want this thing to take off and run.

Leo: If you go to U3.com/uninstall, it says, wait, you're about to throw out the part that makes your drive smart. The Launchpad makes your drive more than a data storage device, blah blah blah blah blah. If you're uninstalling due to a problem, check out our troubleshooting page. Removing the U3 Launchpad disables the smart functionality, so think before you click and make the smart choice. Oh my god.

Steve: Yeah, boohoo.

Leo: Boohoo. Finally they have links that say, tell me more, I'll keep the Launchpad for now; or, finally, you can click the last one that says Remove Launchpad. And then you provide the brand of the smart drive. You have to give them a reason, although my suggestion would be give the reason "U3 Sucks," and then submit and continue. You have to go through hoops. And I really think it's inappropriate for them to make this big deal about how cool, you know, don't throw it out. Unbelievable.

Steve: Yeah. I mean, obviously you're there at that page because you've made the decision.

Leo: And what they don't say, and I wish they would, they say all the benefits of U3. At no point on this page do they talk about why you might want to remove it.

Steve: So we won't be - we will not be promoting them as something that we think is wonderful. And...

Leo: And there's use for it, but hackers have a great use for it, too. So we should just point out that you can, there is kind of a generic U3 uninstaller, U3.com/uninstall.

Steve: And again, I'm sure we're going to get mail from people saying, hey, I use U3 thumb drives, and I love them. It does blah blah blah blah blah. I've got all - I've got Skype, and I've got my applications, and I've got crypto stuff, and it's so cool because I can go to anyone's computer and plug it in, and it just takes over and runs, and I can do what I want. And then when I unmount it and pull it out, my whole little U3 environment comes with me. And it's like, yes, I know. And that's what it does. So there's the only commercial I'm going to give them. I just think that it is backwards that this thing is running by default and just goes the moment you first touch it to a computer, rather than, hey, if you want U3, have it installed, but have it passive until you explicitly enable it on that device. Then it should come to life. And clearly, the attitude you just displayed, Leo, reading that page shows that these people think differently. So...

Leo: Well, in their defense, you don't have to buy a U3 drive. But the problem is you get them - I got it by accident. You know, you just say, oh, I'll take a thumb drive, and you don't see, oh, it's a U3 drive.

Steve: Right. Well, for example, SanDisk is promoting it as value-added to your four gigs. It's like, yeah, but I don't want it. But it turns out you can't get rid of it until you run it. And that's wrong.

Leo: Well, I'm not sure that's true. I'm looking at - PC Magazine has an article on, it says, "Keeping U3 Under Control." It says, if you insert the drive and hold the shift key down, just like autorun, it won't do the U3.

Steve: Okay, good.

Leo: And at that point you can then go to the device manager...

Steve: And format it.

Leo: No, formatting it does not work, actually. But you can right-click the U3 drive and choose Disable on U3 so that it will not automatically launch. It doesn't release the space, but at least it won't automatically launch. So I think that you - and then I presume you could run the removal tool that you've downloaded by pulling teeth at U3.com. So I think you could actually get rid of it without running it at any one time. It does, now, correct me if I'm wrong, but it does put stuff on your system; right? The first time you run it, does it not copy...

Steve: I don't think so. I don't think...

Leo: It doesn't, okay.

Steve: I think that that's one of the cool things that, you know, that they're promoting. Although you do have to U3-ize the - unless the applications are specifically U3-aware, they may be mucking around making modifications. So you have to, I mean, this is an uphill battle these U3 guys are promoting here. And I did, I downloaded all the information once and read through it. It's like, okay, this seems like a lot to go through.

Leo: Well, I mean, look, if you listen to Security Now!, you know it's a bad idea to let anything install anything at ay time, period. And so if you're that kind of a paranoid person, there you go, that's what you need to know.

Sam Osborne, Bathurst, New South Wales, Australia has been pondering CAPTCHAs. Couldn't CAPTCHA be more like a general knowledge question in an image? See, everybody's trying to think of new ways to have CAPTCHAs work. So he's saying, obviously the whole point is to disable or defeat AI in computers. For example, he says, why don't they just say what is the capital of Australia? Or type in the word "enough" backwards? Or spell out the number 8. Oh, that's an interesting idea. A color that is between red and yellow that is also a fruit. How could a computer - because a computer doesn't understand a question like that and can't get the context of that.

Steve: The problem is, I have a hard time understanding questions like that.

Leo: C'mon, Steve. A color that's between red and yellow that's also a fruit.

Steve: I hope Sydney is the capital of Australia.

Leo: Enough, type the word "enough" backwards you could do.

Steve: Okay. The problem is, first of all, okay, there are two classes of question he asked. Some are knowledge, and some are puzzles.

Leo: Can't do knowledge. I agree with you, you can't do knowledge.

Steve: Yes. The problem with knowledge is that then the people have to know the answer. And it's like, you know, what's Claus's first name? It's like, oh. Well, Santa. Okay, well, that may be knowledge, but it's also sort of a puzzle. Or certainly type in the word "enough" backwards, that's a puzzle, or spell out the number 8 is a puzzle. But in what language? So now we have language problems because these - and some people spell "colour" as actually he did. I spell it c-o-l-o-r. He spelled it in his email c-o-l-o-u-r. So that's a problem. And so I assume that the fruit he's thinking of is orange, which is between red and yellow. But I'm not sure what between red and yellow means. But mostly it's not possible to have a large enough collection of these puzzles that some spammer's not going to sit there failing the CAPTCHA, capturing the puzzles, and then building a solver that just knows all the puzzles that are possible.

And this did also sort of come up in our CAPTCHA episode. By definition, a CAPTCHA has to be a puzzle or a task that is fully automatable, meaning that no one sat down and came up with all of the possible questions and answers, but rather an algorithm randomly generated numbers and letters, turned them into a picture, messed up the picture to make it hard to automate, and then presented it. So anyway, you know, you're right. Lots of people have been trying to come up with solutions. But as he says, a general knowledge question, the problem is we don't all have the same knowledge, and anything that has a limited domain of questions can be brute-forced. And then, you know, goodbye CAPTCHA.

Leo: Right. Steve, it's always a pleasure talking to you. You make this all clear. I love it.

Steve: Well, it's always fun doing this, Leo. I really appreciate here we are at the end of our second year. Not yet into our third year, end of our second year with Episode 104. I just want to thank our listeners for being so great. They send lots of email. They're posting lots of questions to the Security Now! page at GRC.com. I really do appreciate people who are saying, hey, you know, I bought SpinRite knowing that I may need it someday and to support the show. And of course I know that they are signing up for your PayPal donations over on TWiT.tv, Leo. So we've just got, I mean, a ton of really great listeners. And I love doing the show with you.

Leo: You know, well, I love doing it with you. Steve, I would be remiss if I didn't mention GRC.com after all those nice things you said. GRC is a great place to get free stuff like the Security Now! podcast, of course, in 16KB versions for the download impaired. Also great transcriptions, thanks to Elaine. But also all of Steve's free software, like ShieldsUP!, Shoot The Messenger, DCOMbobulator, Wizmo, a ton of, I mean, Steve just writes all this great stuff that's absolutely free. GRC.com. What's not free is SpinRite, his great disk maintenance and recovery utility. Every nerd ought to have one. Actually all the nerds do have one, don't they. They have a...

Steve: They do, yeah.

Leo: ...site license. Well, Steve, thanks so much for a great two years. And here's to many, many more. As long as you want to do Security Now!, as long as people continue to listen, there's no reason not to keep doing it. I just - I love it, too. Thank you, Steve.

Steve: I'm glad, Leo, it's my pleasure. And next week we start into our third year with Episode 105.

Leo: Happy Anniversary. See you later.