
# Listener Feedback #203

**Description:** Leo 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-486.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-486-lq.mp3

---

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. More on the Sony hack, plus we'll answer questions from you, our audience. Stay tuned, the last Security Now! before Christmas is coming up next.

**Leo Laporte:** This is Security Now! with Steve Gibson, Episode 486, recorded December 16th, 2014: Your questions, Steve's answers, #203.

Time for Security Now!, the show that protects you and your loved ones online with the Explainer in Chief his self, Steven Gibson of the Gibson Research Corporation. Well, I should say "Happy Holidays," Steven. Christmas is upon us.

**Steve Gibson:** Thank you, Leo. I guess we are at this point. We're on the 16th of December, so we're halfway into or through December. And, yeah. Anyway, we all have the spirit and lights, and we're whistling Christmas tunes. Oh.

**Leo:** I was drinking eggnog this morning.

**Steve:** Before I forget, I think I had mentioned to you before, but I have been in a live theater where Patrick Stewart was doing his one-man show...

**Leo:** Oh.

**Steve:** ...of "A Christmas Carol."

**Leo:** Because you heard Andy Ihnatko talking about that on MacBreak Weekly earlier today.

**Steve:** Yes.

**Leo:** That's his pick. He loves the Audible book of that.

**Steve:** And I didn't know there was an Audible book of it.

**Leo:** Yeah.

**Steve:** So I wanted to tell our listeners. I waited until the camera was rolling or you were recording this or whatever it is you do.

**Leo:** What is it I do? I don't know.

**Steve:** Push buttons.

**Leo:** Yes.

**Steve:** And magic happens. To tell our listeners that, if you're fans of Patrick Stewart from, of course, "Star Trek: Next Generation," it really is, I mean, Andy is absolutely right. Andy told the story during MacBreak Weekly that annually he gets his - wait. He did say cassettes. So he can't still have a cassette player. But...

**Leo:** With Andy, it's possible.

**Steve:** Or maybe he's been doing it since the era of cassettes, when it was first made available on Audible. Anyway, so Patrick Stewart, "A Christmas Carol," on Audible, and wow. I mean, it was just him, sitting on a stool, and occasionally walking around a little bit. It was fabulous. And I'm probably going to get it myself, which means I'll finally have to get an Audible account.

**Leo:** Wow.

**Steve:** Yeah. Because it was a...

**Leo:** Wow.

**Steve:** It'd be fun to have that. It was spectacular. So just a heads-up for our listeners who like Patrick.

We had a relatively slow week. Got some news, of course. There are new upcoming changes in Chrome being bandied about, we want to talk about, with Google continuing to push security. News of a previously unknown, devastating cyber attack surfaced that had been kept quiet for 10 months, but was massive. And then I wanted to talk a little bit, because there's been a lot of discussion, I mean, one of the things that happened, of course our show last week, we've talked about it, it was titled "Expensive Lessons." And one of the things I did was enumerate the nature of the documents that were leaked or stolen by the hackers of Sony Entertainment.

Well, since then, of course, we're starting to see all the salacious details of the content of the email. And so there's been a lot of interesting discussion. I know that you guys, you had a great coverage of that whole issue on TWiT on Sunday. And so I want to talk a little bit about the ethics of disclosing illegally obtained content, and then Sony's new questionable strategy with the press about that. Verizon has what I would consider a ridiculous Cypher phone app that they have just...

**Leo:** I knew you'd laugh when you read about that.

**Steve:** Oh, my lord. And we've got some miscellaneous fun stuff, and of course questions from our listeners to put us on to other topics that we will be talking about.

**Leo:** Oh, I'm glad.

**Steve:** So a great show.

**Leo:** I'm glad you're going to - yeah. This is all good stuff. We'll talk about this. All right, Steve. The news of the week.

**Steve:** So some dialogue surfaced over in the Chromium Chrome developer team area, suggesting that they want to push further with sort of the overall thrust that Google has been making to secure the Internet. They're planning - I know you're sitting down on your ball, so it's safe to tell you this, Leo.

**Leo:** Uh-oh.

**Steve:** They're planning to explicitly mark non-HTTPS connections as non-secure in some new fashion in the user's experience.

**Leo:** This isn't - weren't they doing this, I mean, this isn't new, is it?

**Steve:** Yeah, no.

**Leo:** No.

**Steve:** So the idea was, what we've had so far has been an indication, if you are using HTTPS, that is, like the key is not broken or the lock is closed, sort of a subtle clue. Then we went with the extended validation certificates. We added the green glow if you were using an EV cert. But if you were not secure, it was just kind of normal. What they're intending to do is like a skull-and-crossbones if you're not using TLS. So that they're going to further, I mean, they're basically going to start warning people when you're not using a secure connection.

**Leo:** Well, but that's - it isn't a lie, I mean, it is less secure. I hope it's not a skull-and-crossbones, though. This site is poison. I mean, if it's kind of a non-loaded thing, I mean, isn't that what the open padlock was?

**Steve:** Yeah. But clearly their intention, though, their intent - well, okay. What they said was: "We, the Chrome Security Team, propose that user agents gradually [that means browsers] gradually change their UX [the user experience] to display non-secure origins as affirmatively non-secure. We intend to devise and begin deploying a transition plan for Chrome in 2015. The goal of this proposal is to more clearly display to users that HTTP provides no data security. We'd like to hear everyone's thoughts on this proposal and to discuss with the web community about how different transition plans might serve users."

And then they finish, saying: "We all need data communication on the web to be secure, private, authenticated, untampered. When there is no data security, the UA should explicitly display that, so users can make informed decisions about how to interact with an origin." So they're clearly saying that they intend to display a signal of some sort that causes users to be anxious or aware in a way that they're not currently, when they're not on a secure connection or secured connection. I mean, I noticed they were careful to say "non-secure" rather than "insecure" because the two are not synonymous.

**Leo:** It's not encrypted. I don't - I think the proof will be in the implementation.

**Steve:** Yes.

**Leo:** I mean, this could be completely innocuous. Or, if they put a big banner up that said "Don't go here," well, that wouldn't be so good.

**Steve:** Or [emulating buzzer]. That would be a bit of problem.

**Leo:** They don't tell us how they're going to do this, what it's going to look like?

**Steve:** No. And at this point this is just sort of a, this is something we think we should do. Now, I don't participate over there. I'm sure that some of our listeners do. And they're inviting comments. What I would like to see, and I would love it if someone would get this into the discussion, is something we talked about recently, and that is, while

we're going to be creating additional distinctions, I think it's important to distinguish a domain validation certificate, a DV certificate, from anything higher class, like an OV, the Organization Validation cert. Remember that the DV, with the EFF's effort, which is going to be hitting around the same timeframe, like second quarter of 2015, where that all becomes free and automated.

At the same time, it's important to understand that the assertion being made is not that you're at the company whose site you are, but only that the domain name validates against the certificate. And that's a subtle but important distinction. So, I mean, if there's some way to, without confusing people, to say we do have EV certs special, it would be nice to have organization validation somehow showing stronger than domain, like then the free automated certs that we're going to start having around the middle of 2015. And then of course they're going to want to do something, who knows what, maybe a yellow triangle or an exclamation point. But, I mean, what they're going to try to do is to affirmatively say to people, your data is not secure on this connection.

**Leo:** Yeah. I mean, we'll see.

**Steve:** Yeah.

**Leo:** Depends how they do it.

**Steve:** Yeah.

**Leo:** Unlocked, you know, an unlocked padlock was there for years. That's how Netscape did it. Remember?

**Steve:** Yeah, but you had to go looking for it.

**Leo:** Yeah, it was like the bottom of the...

**Steve:** Right. And so the idea will be this will be in the URL bar. It'll be in your face so that you're not, you know, so that you're being, I mean, their idea is to put pressure on those websites that will display that in order to induce them to go get themselves the free cert through the EFF's system. And, I mean, I'm not saying it's a bad thing. It's just it could be nice.

**Leo:** Be ready, yeah.

**Steve:** Yeah, exactly.

**Leo:** Yeah. We'll see what they do.

**Steve:** Turns out that there was a major unreported cyber attack against - that went unreported from February 10th, when it occurred, until just a few days ago, against Sheldon Adelson and his Sands properties, the Venetian and the Palazzo. This was on February 10th that they got hit by something that is reminiscent of the Sony attack, but different because this didn't appear to be about exfiltrating incredible amounts of information, as did happen with the Sony attack, but rather deliberately attacking to hurt Sheldon and his properties.

It's believed that this is a direct consequence of him making some very inflammatory statements a few months before that, like I think it was October of 2013. He was on a panel in Manhattan where he came down very, like, essentially ruthlessly against Iran. And they were able to verify that these were hackers that were traced back to Iran. And the point was made in the analysis that independent entities don't do anything without the Iranian government knowing what they're doing. So the sense being this had to have backing of the government.

People, our listeners and my Twitter followers, have commented that it's annoying we don't know more about the technology of the Sony attack and hack. What's fun is a lot is known and is now available about this attack that happened on February 10th. In fact, I wanted to aim people at the story, which was covered in BusinessWeek. So I created a bit.ly shortcut to help people do it - bit.ly/sands-attack, all lowercase - because there's lots of information.

They found, for example, a very small script that was written in Visual Basic, of all things, was installed in the system and was implicated in this destruction. This thing wiped out servers. It wiped out hard drives. It flew through the network and caused what essentially was, they're estimating, about $40 million worth of damage to the network infrastructure that the Las Vegas casinos run on. And it also demonstrates the kind of - sort of the nature of the attack. And when we were talking about the Sony attack last week, I talked about how what normally happens with these advanced persistent threats is that bad guys get a foothold somewhere. They get a toe in the door. Somewhere, in a sprawling network, there is some little mistake made.

This report explains that. And I don't remember now the details. It was in a completely different, geographically remote casino because Sheldon has a bunch spread all over Asia and not only Las Vegas but also around the world. There was one casino where a small mistake was made that - oh, I remember what it was. A brute-force attack on their VPN was detected. And because that's relatively common, they thought, okay, well, yeah, people are trying to crack our VPN. And so this was a VPN into the internal network at that facility. And somehow the bad guys found a way in, and then that was their foothold, and then they were able to use that in order to jump over to the main Las Vegas properties network and set up their major devastating attack. So anyway, the article was interesting because it had a lot more detail about the way this was done. And so I thought our listeners would find it interesting.

**Leo:** Actually, a couple of people want to know who Shelly is. And one of the reasons we're all very interested in this is because we all know Shelly.

**Steve:** Ah, okay, yes.

**Leo:** Because he was the founder of COMDEX.

**Steve:** So Shelly is - he is the, what is it, 43rd, 44th most, like, richest person in the world. Or maybe it's that he has $43 billion.

**Leo:** He has 43 billion. Most of that - so the story of Shelly is fascinating. He created COMDEX.

**Steve:** Yes.

**Leo:** And got out just in the nick of time. And as far as I know, that's where he got his first billion. He sold the trade show. And then he built casinos in Macao. That's where his big money came from. But he does also on the Sands.

**Steve:** But isn't that relatively recent? I thought those were newer than his Sands properties.

**Leo:** They're pretty new.

**Steve:** Yeah.

**Leo:** And that's when he really started to cash in.

**Steve:** Right. Well, because, in fact, those are generating massive revenues for him.

**Leo:** Right. The other thing I think is salient in this, what we were talking about when we talked about the Sony thing last week, you could say, well, Sony Pictures Entertainment, they didn't really worry about security. You can bet - these are the computers that operate the slots. They operate the security in the casinos. These are big, big targets for money. So you can bet they were state-of-the-art secured, I would guess. Wouldn't you?

**Steve:** Yes. Well, yeah. For example, they knew when somebody was pursuing a brute-force attack on their VPN. So that demonstrates they were looking at bandwidth.

**Leo:** They're watching it, yeah.

**Steve:** And they were looking at logs. And the fact that they've been able to recreate the - and that's why this article is so interesting. They were able to recreate the footprints of these attackers. They know where they got in, when they got in, what they did, how they moved across networks. And you only can do that if you've got really good logging in place.

**Leo:** Right.

**Steve:** They obviously didn't stop them. But they were at least able to retrospectively...

**Leo:** Well, partly that's because these guys had no incentive to cover their tracks. They aren't going to get arrested for this; right?

**Steve:** Right. And that was another interesting point is that this article talked about the fact that what we're seeing now are cyber attacks against small pieces of U.S. infrastructure, in the case of the U.S., that don't motivate the government to respond. That is, well, it's too bad Sony got blasted. And it's, oh, well, too bad Shelly got hit. But that doesn't merit a military response from the U.S. government. And so the article drew an interesting distinction, that this was sort of - these attacks were maybe what we're going to be seeing in the future was things that sort of slipped under the radar, but were still doing substantial damage to small pieces of U.S. domestic infrastructure.

**Leo:** Yeah, I mean, this was clearly targeted at Shelly. He's very pro Israel. He's very active, gives a lot of money. In fact, he supported the Newt Gingrich campaign well beyond its stay fresh date. But the interesting thing is, to me, is that here you have something that's highly secured.

**Steve:** Yes.

**Leo:** And they still got in. And that was our point last week, which is you can say all you want about what a crap job Sony did. But I think a determined attacker with some skills and maybe a government behind them, it's going to be hard. We are, along with this news, is news that the United States is very actively going into the grid and trying to protect all those systems on the grid, many of which are run by independent third parties who have not great practices.

**Steve:** Yup.

**Leo:** That's, I mean, if you really want a cyber war, you go after infrastructure.

**Steve:** Yeah. And I think maybe that's the point is that that's the kind of thing that could rally a military response from the U.S., if a foreign country was affirmatively found to be responsible for producing damage to the public infrastructure, as opposed to pieces of much smaller private infrastructure.

**Leo:** Right. Easier. Easier.

**Steve:** We'll see, yeah.

**Leo:** Although I've got to think there's nothing more secure than a casino. I mean, this is the back office operation of the Sands casino.

**Steve:** You raise a really good point, and a lot of the questions that we have today are people following up from last week's discussion about the Sony breach. But, no, your point is a hundred percent. I mean, their security had to be topnotch. And yet, and this was the point that I made last week because, from a standpoint of the things that interest our audience, the question is, how do you prevent what happened to Sony?

**Leo:** Exactly.

**Steve:** And I rather gloomily said, "I don't think you can."

**Leo:** Don't know. I don't know.

**Steve:** And so the point is that, again, their network, despite all of the focus, as you rightly point out, that they brought to bear on security in these casinos, they still got hit really hard. I mean, they were - the story explains they were running around pulling the network cables out of machines that hadn't yet come down because this thing was just rifling...

**Leo:** Get off the 'Net. Air gap it.

**Steve:** Yes, yeah, exactly, because drives were being wiped by this thing.

**Leo:** Yeah.

**Steve:** Yikes.

**Leo:** Pretty amazing.

**Steve:** So the ethics of disclosure.

**Leo:** Ooh, I want to talk about this, yeah.

**Steve:** Yeah. Bloomberg View did a really nice article yesterday, that the headline was "Keep Publishing the Sony Emails." And from all the conversation that I've seen over the last week, and there's also been some interesting legal opinion, one of the determiners of what the press might use to decide what they say and what they deliberately withhold out of respect for the privacy rights of somebody whose information was stolen - and, for example, we were talking about comparing email content to nude photos of Hollywood

people - is whether the disclosure is in the public interest. That is, does it serve a valid public interest?

**Leo:** Boy, I want to hear this logic.

**Steve:** Okay.

**Leo:** Because, I mean, you can make the argument the Pentagon Papers, which were illegally obtained classified documents, it absolutely served the public interest for The New York Times to publish those.

**Steve:** And I was...

**Leo:** I don't know if we can make the same argument about Amy Pascal's emails about the negotiations over "The Interview."

**Steve:** I have one.

**Leo:** Okay. I'd like to hear it. Because I disagree. We have intentionally stayed away from the content.

**Steve:** You haven't heard it.

**Leo:** Let me hear it.

**Steve:** You haven't heard it yet.

**Leo:** Let me hear it.

**Steve:** So you can't dis- okay.

**Leo:** No, I didn't say I disagree with that. But I have said up to now - and my problem is that Bloomberg and all these people have a vested interest in publishing this stuff. It's great for business.

**Steve:** It's also good for something else.

**Leo:** Okay, good. I want to hear the public weal.

**Steve:** Okay. So the next step from the Pentagon Papers is of course the Snowden leaks.

**Leo:** Absolutely.

**Steve:** And I, again, absolutely feel, as I said the day we first reported this, that while I could never do it because oaths are oaths, I thought this was a good thing. And a year later I remember saying, when we were sort of testing that again, can we imagine having - standing here today, not knowing what we know? That is, hasn't that been valuable? And of course the NSA and law enforcement would adamantly disagree that this was in the public interest. And of course that's the point.

The direct upshot of what Snowden did, of those leaks, has been a year that we've chronicled here on the podcast of radical change in the industry's security posture. We've suddenly seen Google go crazy, if not overboard, in pushing security. We've got Apple advertising as a marketing feature the fact that they can no longer decrypt people's phones, where in the past they were able to respond to the letters requiring them to do so. Google has announced that Android will be following. We've got third-party communication apps coming out constantly. And whereas previously our acronym on the podcast, TNO, Trust No One, was something that we and our listeners understood and cared about, suddenly now everyone cares about it. So it really - there has been a massive benefit of public security that is a direct consequence of what Snowden showed us was going on.

So, Sony. Sony's also certainly not happy that these details are being published. And I have no interest in the underwear of executives. I mean, I don't care about that. But I'm not sure that the message would have gotten through to the degree it has were it not for these details. That is, last week I took the time to enumerate much more clearly the kind of content. I mean, the least disclosure is to say, oh, 12-plus terabytes. Okay. That doesn't mean anything to anybody. So I understood that it was important to say, yes, but that's salary ledgers and financial reports and income projections and blah blah blah blah. And so that I thought helped, by further enumerating and making more clear the nature of what this loss meant, helped it to hit home.

And while I have no interest, and I haven't looked at or gone seeking any of the details of the email, it's been all the buzz in the press. And it's evoked apologies and all kinds of additional pain. And while I wouldn't wish that pain on anyone, the sad thing is I think it's human nature that that's what it takes for people who really need to be pushed to increase the level of their security to do so. That is, there are certainly executives now, and actually I've received email from people saying - I mean, like, prominent people - how do we get ourselves secure? Because the nature of this, the details are unfortunately necessary in order to get people to understand what it really means.

And so I would argue that that's in the public interest. It's in the public interest, I mean, in corporate interest, if it finally penetrates the thick skulls of the CEO and the COO that they're going to have to spend the money that the CIO has been begging for in order to implement better security because security is hard. It's painful. It's difficult. And increasing it is a good thing. So that's my argument.

**Leo:** I totally disagree.

**Steve:** Okay.

**Leo:** So it would be like saying, hey, you just got robbed of $100,000 by leaving your door unlocked. So, but we're going to keep the money so that you learn the lesson that you ought to lock the door. This is stolen material. There's no excuse for telling people what somebody made to make a movie. The list you gave, I have no problem with the list you gave, or I would have stopped you. The list you gave is completely appropriate and fine.

**Steve:** Right.

**Leo:** I don't think that the contents of those emails should be disclosed. I think they're stolen goods. I think it's as bad as showing the naked pictures. The press would have shown the naked pictures if they thought they could have gotten away with it. The only reason they didn't is because they were naked pictures. This is just as good, as far as they're concerned, is going to generate just as many clicks. And I think every argument I hear for releasing the salacious details of the Sony leak is an argument from somebody who says, "I'm going to make money on this because we're going to get lots of clicks." I think there's - I don't see how that improves - look. Sony knows what got stolen. I don't think this improves their attitude. And what you listed, I like what you listed. I think there's nothing wrong with saying here's what they got.

**Steve:** Right.

**Leo:** Without revealing the details. And I don't think that's what we're talking about. I think what Sony's saying is stop publishing our private emails. Those are private. I don't think they should be published by journalistic entities who are equating it with Snowden's revelations. These are not Snowden's revelations. Anyway. You stand firm.

**Steve:** Well, yeah. I mean, I see your point. It's not Sony we're trying to teach a lesson to, though. That horse has left the barn. It's the other companies whose behavior could improve, but only if they understand what's...

**Leo:** I don't think it's The Verge's job to make these other companies improve their security. I don't think it improves the public - there's no public benefit from us knowing how much James Franco got for being in "The Interview." I just - I don't get it. I don't get the value. I agree, believe me, I'm a firm defender of the fourth estate and the right of the press and the people's right to know, if it affects the people. You can't make that argument.

**Steve:** Right.

**Leo:** That any of this salacious stuff affects the people. This is publishing it because we love reading it. And I confess, until I really kind of thought about this, I was reading all those articles, and I even reported one tidbit, which was what James

Franco got paid for driving himself to work because that's, wow, what a story. But as I started to see more and more, I started to really feel for these people. And these people are not the people who were responsible for the poor, lax security.

**Steve:** Correct.

**Leo:** Why should, I mean, I don't understand why Seth Rogen and James Franco should have to suffer because some CIO didn't do his job. And I don't see how it benefits any of us for them to have that information revealed.

**Steve:** Right. Well, and Brian Krebs reported, he said: "Over the weekend I received a nice holiday letter from lawyers representing Sony Pictures Entertainment, demanding that I cease publishing detailed stories about the company's recent hacking and delete any company data collected in the process of reporting on the breach. While I have not been the most prolific writer about this incident to date, rest assured such threats will not deter this reporter from covering important news and facts related to the breach."

**Leo:** Nor should they.

**Steve:** Right.

**Leo:** I'm with him on that.

**Steve:** Right. And so the letter that he received said SPE - and this of course is from our friend David Boies, who is the attorney who stepped into this.

**Leo:** Boies, yes, yeah.

**Steve:** Yeah, Boies, said: "SPE [Sony Pictures Entertainment] does not consent to your possession, review, copying, dissemination, publication, uploading, downloading, or making any use of the stolen information, and to request your cooperation in destroying the stolen information," said SPE lawyers. And that's what Brian wrote.

**Leo:** I wouldn't want my private emails to be revealed to benefit - who, I don't know - to make people be more secure. I'm sure you wouldn't, either. I've had my private emails revealed, and I don't like it.

**Steve:** No, no, it's, again, it's not - no.

**Leo:** I'm against it.

**Steve:** There's no question that the degree to which this is bad for Sony affects other companies' security.

**Leo:** Right.

**Steve:** That's my belief.

**Leo:** But I also agree with you and Brian that a free press does not get deterred by this kind of thing. But I would guess that Brian is not, I mean, his audience doesn't care...

**Steve:** No.

**Leo:** ...about the details of what was leaked.

**Steve:** He's like our audience. It's like ours, where we were talking about the broad...

**Leo:** The security implications, yeah.

**Steve:** Security implications and a broad-stroke appreciation for what this meant from a security standpoint.

**Leo:** Right. I would also say, hey, be careful what you defend in case it comes back to haunt you. I wonder how the editors at some of these publications would feel if the same thing happened to them.

**Steve:** Yeah. Yeah. Well, and that's, I mean, my point is nobody would think this is good. But security is hard. And it needs respect. It needs attention. It needs money.

**Leo:** Right. Well, I agree with you on that. But I, gosh, if you just say all the stuff that they got, isn't that sufficient? They have to be - you have to embarrass people for them, for others to take security seriously? That's sad.

**Steve:** Yeah, it is sad.

**Leo:** But maybe that's the state we're in.

**Steve:** So Verizon last Thursday introduced, to some fanfare, Voice Cypher, along with the encryption company who created it called Cellcrypt. And they said this "offers business and government customers end-to-end encryption for voice calls on iOS, Android, or Blackberry devices equipped with their special app. The encryption software

provides secure communications for people speaking on devices with the app" - now, this is not me speaking, this is them, because otherwise I'd be putting air quotes around all this - "regardless of their wireless carrier, and it can also connect to an organization's secure phone system."

And then they said: "Cellcrypt and Verizon both say that law enforcement agencies will be able to access communications that take place over Voice Cypher, so long as they're able to prove that there's a legitimate law enforcement reason for doing so." And the vice president, the North American vice president of Cellcrypt, a guy named Seth Polansky, disputed the idea that building technology to allow wiretapping is a security risk. He said: "It's only creating a weakness when it's a legitimate government agency request. Just because a government access option exists doesn't mean other companies can access it."

And then, as if that wasn't all just crazy enough, I love their slogan. They doubled down with the slogan: "Security when it matters most." Which of course is exactly what it isn't because, when it matters most, the government is able to wiretap it. So anyway, I just got a kick out of this, that they're - I think it's also not cheap. The app is free to download, but in the announcement I remember seeing, like, $45 a month you pay for the privilege of this Verizon-backed, point-to-point voice encryption. We already have free solutions that do this, that we've talked about on the podcast. So it's like, well, I'm sure there will be users of it. And it's okay.

I did forget to mention last week, and I intended to, that there was just, in miscellaneous sci-fi notes, that there was a three-night miniseries that would be airing on the Syfy channel. The first chapter was last night. I did tweet it yesterday beforehand, and I know that a bunch of my followers had intended to DVR it and then did. So I was glad I remembered at least then. I'm sure that Syfy will be reairing it. If they're not reairing last night's tonight, you know, they tend to reair this a lot.

So it's yesterday the 15th, today the 16th, and tomorrow the 17th, called "Ascension." And I watched the first hour of it before it got to be my bedtime, and I decided, okay, well, I maybe will finish the rest of last night's and then see. I got a lot of feedback from people who thought it was great. It's okay, you know, we're sort of in a sci-fi desert at the moment, or drought. So it's sort of typical of what you get from them. And Leo, do you know what this site, gog.com, is?

**Leo:** G-O-G?

**Steve:** Gog.com.

**Leo:** No.

**Steve:** A listener, Isaac Johns in Louisiana, sent us a note about Abe. He said Abe's Oddworld has been out for PC...

**Leo:** Oh, Good Old Games. I do know about Good Old Games. Yeah, love Good Old Games, yeah.

**Steve:** Oh, good. So they're legitimate?

**Leo:** Oh, yeah. These are all licensed. These are licensed.

**Steve:** Oh, good, good, good, because the Oddworld series for the PC is, like, $5 or $6. So if you search for Oddworld, you'll find three of them - Abe's Oddysee, Abe's Exoddus, and Stranger's Wrath - downloadable for the PC. So I did want, because we've been talking about it the last couple weeks, due to its sort of rebirth on the PS4 and on the iPad, I'm glad to know these guys are legit. And if anyone is interested, I really, again, for six bucks, if you've got a PC, certainly I remember running it on a PC 20 years ago. So you don't need some fancy state-of-the-art...

**Leo:** It's probably a DOS game.

**Steve:** Yeah. You don't need a fancy gaming box. Anything will run this.

**Leo:** Actually, no, it's Windows XP or better, it says.

**Steve:** Yeah, so XP, yeah.

**Leo:** Yeah, yeah. That is great. I'm happy to hear it.

**Steve:** I wanted to give our listeners a heads-up that that was there. And, boy, just looking at those screenshots, Leo, just kind of like - I feel nostalgic.

**Leo:** Brings back the memories. What a great game this was, yeah.

**Steve:** So well done.

**Leo:** And, you know, the whole plan, as we mentioned, was to have a whole Oddworld Universe that would go on and on.

**Steve:** Yeah. A quintology was what was originally targeted. What they ended up doing, Abe was the first character. Then Munch was the second.

**Leo:** Right.

**Steve:** And so they introduced Munch, who was like a weird little guy who kind of waddled around. And then they sort of went off plan and did a second, like a sequel to Abe, because the first one was - and so, right, there's Munch's Oddysee. And that was the second one. Then they did Abe's Exoddus to follow Abe's Oddysee, to create the first three.

**Leo:** So there are - they've kind of kept going in ways that I didn't really realize. There's a few more of them here.

**Steve:** Yeah.

**Leo:** So Munch's Oddysee HD came out for the PS3 a couple years ago. New 'n' Tasty.

**Steve:** And that's the very new one, which is now...

**Leo:** That's the one you were talking about, yeah.

**Steve:** Yup. And that's on the PS4, and it'll be coming out with other platforms. But basically it's a remake of the original Abe's Oddysee, which you can get for six bucks for the PC. And especially if you've got kids, I can't think of anything, I mean, it is like, you know, PG rated. I mean, okay, there's a grinder. But...

**Leo:** It's perfect because it's a little bit gory.

**Steve:** It's a little edgy.

**Leo:** Right.

**Steve:** So your kids aren't going to think you're a wimp. They're going to think, okay, Dad's cool, he knew about this.

**Leo:** Yeah, yeah. Like I said, I played this with Henry when he was probably nine or 10. And he and I both have very fond memories of playing this game. This is the last one, Stranger's Wrath, yeah.

**Steve:** Yeah, it'll run on the machine you've got in the garage.

**Leo:** Yeah, but now I have to get a Windows machine. I wonder if those HP Streams - it'd be worth buying a $200 HP Stream just to play this game. Maybe.

**Steve:** It would.

**Leo:** Maybe.

**Steve:** It would, yeah. And while I was going through the mailbag for today's Q&A, I ran across a nice note. I don't seem to have the guy's name here. Normally I - oh, I think it actually was, he sent it to be anonymously. But so it was Friday, December 12th. The subject was SpinRite saved a server RAID array. And this caught my attention because he came very close to the point of no return, but also is clearly operating some major facility. He said: "Steve, every weekday morning I do a visual" - so every weekday morning, probably when he goes in - "I do a visual inspection of our servers for any issues," he says in parens, "(scanning the server status screens and hard drive LEDs). I'm also responsible for backups.

"One morning I was checking the previous evening's backups on one of our NAS servers," you know, network-attached storage. "I noticed a major read/write error in the backup log, causing the backup job to fail completely. Checking if the backup volume was mounted correctly, I immediately noticed that the volume had disappeared. I then began scouring the system logs; and, sure enough, we had a drive failure in our RAID 5 array. Come to find out we had another drive failure at a prior time, which makes two drive failures at this point, causing the entire array to be lost." Because remember that a RAID 5 has - it can tolerate one drive failure because essentially it sort of runs like a checksum drive. And so any of the remaining can reconstruct the entire RAID content. But you only get one. That's why I'm running RAID 6.

He said: "These two failures slipped by me since the visual inspection on this one custom-built server fails to indicate a problem for any of the drives. It only shows a green LED for power." And that's a little scary because typical drive back planes now will show you like a red or sometimes yellow error light if the drive is having a problem, separate from drive activity, or in this case, drive power. So he just - his visual scan wasn't showing that one drive had died some time ago, and now finally a second one followed it.

He said: "Figuring out the problem took only minutes. And looking at what the logs were telling me, my mind immediately went to a previous episode of Security Now!. In that episode, you were discussing how a SpinRite customer was able to save his/her RAID array by removing the drive and booting it as a standalone drive connected via a separate interface. I thought, I can do this.

So he says: "I removed the first failed drive, connected to a laptop via a SATA to USB interface, and booted SpinRite. I immediately heard some truly awful sounds coming from the drive. Well, that sounds bad; and, sure enough, I could not get SpinRite or the laptop to recognize that drive at all. Trying the second bad drive, it booted, and SpinRite saw it. Running Level 2, I noticed that at times the drive would seem to have a hard time reading a sector. After a few seconds, it would work through it and go on to the next sector." Which of course is exactly the behavior that SpinRite users through the last couple decades have seen. And that's what SpinRite does is it sits there and fixes that sector, and then we get to move on.

He says: "I ran SpinRite until 50% completion and decided to give it a try back in the server. Sure enough, the drive came back up, and the RAID controller gave me the okay, and the RAID volume is back up, but in degraded mode since the complete loss of the other drive. I was able to get all of this done within one workday and had backups running again that evening with no data loss. I've got two new drives on the way and will be replacing them and rebuilding the array as time permits. Thank you for a great product." And whoever you are, thank you for the great testimonial. I really appreciate it.

**Leo:** Steven "Tiberius" Gibson. He is @SGgrc on the Twitter. That's one way you can ask questions. You can also go to his website, GRC.com/feedback, ask questions there. And you have cobbled together some questions from our audience. You ready?

**Steve:** You bet. I was going to say that we've really developed a nice little community over on Twitter.

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

**Steve:** It's really - it's vibrant. And, you know, I get great tips and leads from people who want to make sure that I've seen stuff. And I'm able to answer short questions. And I always like, you know, I get up in the morning, and I scroll back and catch up with what has gone on while I've been unconscious. And so, yeah, it's really been a good thing.

**Leo:** Isn't that nice? And they're global. They're all over the world, like this. The first question comes from Dorset in the United Kingdom. Andrew Stevenson wonders about the POODLE TLS attack. Steve and Leo, Ivan Ristic over - he doesn't talk like that. Ivan Ristic - I'm doing the Dick van Dyke from "Mary Poppins." Ivan Ristic over at SSL Labs has implemented a test for POODLE - oh, of course Ivan has - against TLS. My question, does this attack deserve an F rating? Do you think this attack is more damaging than POODLE against SSL3? Also, have you seen that SSL Labs now demotes sites to a grade B if they support RC4 ciphers? To reacquire your previous - I guess I'm wondering, I'm thinking Andrew might just happen to have a site with a B rating. To recover your previous A+ rating for GRC.com - you mean you don't have one, Steve?

**Steve:** No.

**Leo:** You'd have to remove RC4 ciphers, disable SSL3, upgrade to SHA-2 certs, install TLS_FALLBACK_SCSV downgrade attack prevention, et cetera, et cetera, et cetera. What do you say?

**Steve:** So, okay. So GRC used to be A+ rated at SSL Labs.

**Leo:** Oh, man.

**Steve:** And we are back to a C.

**Leo:** Grading a - C?

**Steve:** A C, as a consequence of a number of things. I'm still opting for compatibility.

And the problem is that GRC is HTTPS, meaning if you even try to connect to me HTTP, the first thing the server does is bounce your browser over to S. There's no way to access, to get in the front door without security. And of course then I also have an HSTS, the simple transport security header with a long life which Ivan gives me good credit for. He likes the fact that I'm doing that. So I'm telling all browsers, remember that we're only secure. The problem is there are still - there's still a big install base of users who I don't want to deny access unless they have the latest and greatest. I mean, we know that they're out there. They're unable to use SHA-256 because they don't have Service Pack 3 of XP. They've got something older than that.

So I'm going to tolerate for, oh, I don't know how long, maybe six months into 2015, a substandard grade from SSL Labs on purpose. There's nothing wrong with GRC's security. I do have prevention against insecurity for eCommerce because I don't even use or require security for, like, cookies, for example, for handling our sessions, so there's nothing for POODLE to get that GRC is doing. That said, we're sort of - there's tension that we've talked about before. And that's my favorite word to describe this because certainly Ivan's whole point of having SSL Labs grading websites is to find problems with them. That's his deal. Mine is to offer a service to as many people as I can. And meanwhile, that against the backdrop of us moving forward with standards.

So I do think it's time that I drop RC4. And at that point I think I get to pop up to a B rating. So I won't have the A+ that I had a few months ago, before we knew that there were these additional, at the time unseen, problems in the protocol. I'm doing everything the same, but now we've decided, okay, this is a problem. And so I am going to drop RC4, and I'll disable SSL. But I'm going to hang back with SHA-1 certificates because there's nothing that anyone knows is wrong with those. And we will see how Chrome moves forward with their push for SHA-256, which I support, and I'll switch over to those. But I'm going to hang back.

The idea will be that, as other sites switch, that will create pain for the people who still don't, still can't do SHA-256. They will be forced to use Chrome or to use Firefox. They will no longer be able to use IE. I want them to still be able to GRC.com. So I'm going to lag on that, and then I will make a switch. And of course, if we do find that, like, something is surprisingly wrong with SHA-1, which nobody at this point expects, then I can easily switch over to 256.

So, yeah, I'm going to tolerate - I'll bring my grade up to a B, I think, by agreeing that RC4, it's time to say goodbye to that, and SSL3. It's now time not to allow a downgrade to SSL3. It would be nice if Microsoft adds this TLS fallback to their offerings. We'll see if they do that because, if they would add that to server platforms that they're still supporting, and they're still supporting my Windows Server 2008 R2, if we could get that feature in an update, then that would be a good thing, too. That would help everybody. But I can get rid of SSL3 without a problem.

**Leo:** I think there's a little bit of...

**Steve:** Yes, there is.

**Leo:** I'm a little dubious about Ivan being the arbiter of what is good and wholesome on the 'Net. And I'm always just a little uncomfortable with recommending SSL Labs tests for that reason. It's just one guy's opinion.

**Steve:** Well, I mean, I guess the problem is that it's hard not to give a grade. I mean, that's just a powerful psychological thing. And I loved having an A+ while I was A+. I only had that for a few months, and then I fell back off of the leading edge of the cipher curve. It would be a little nicer, I mean, he does break it all down. So somebody who cares can look at the things that I'm doing and see, oh, look, Steve's supporting perfect forward secrecy, like with all of the ciphers anyone is using. And way down at the bottom there's a couple RC4s because he doesn't want to lock somebody out who wants to get to his site for the purpose of using the services at GRC. If I were to do that, nobody could ever use GRC. And that bites a little bit. So I'm going to lag on that.

**Leo:** Sometimes the perfect is the enemy of the good. This would be a good example of that. Phil S. in Central New York coins the term "The Gibson Comma." There's a Twitter account called the Oxford Comma that tweeted me, "Leo, do you support or do you not the Oxford comma?" Hi, Steve. Avid listen - I haven't responded yet. Avid listener from Central New York here. During the past few months my team and I have been patching our web servers monthly - monthly - thanks to POODLE and the Microsoft patches and so on. We value and use your cipher suites list for our hardening procedures. Oh, that's great. That's on GRC.com. You can go to bit.ly/grcciphers, with an "i." But I discovered a missing comma - oh, dear, oh, lord - on line 24 which we've dubbed "The Gibson Comma." Oh. A quick fix on your end, but while you're in there can you review and update the suites as SSL Labs is capping grades to B when it sees RC4? Many thanks. Phil. Did you fix the comma?

**Steve:** No.

**Leo:** No.

**Steve:** No, because I wanted you to click on the link first. So when I first saw this...

**Leo:** Ha ha ha, it was a joke. I get it.

**Steve:** No, no, no, it's real. When I first saw this, I thought it said "The Gibson Coma." And I thought, what? That doesn't sound good. I don't want to be inducing a coma in anybody. Anyway, so you can see, like, the fourth from the end, and it happens to be, I think, one of the RC4 lines. So what this is - yup, there. Oh, it's at the end of the MD5. It's missing its comma there. So that's the Gibson Lack of Comma. So what that is...

**Leo:** You've got a new line. I don't think you need a comma and a new line, okay? I'm just saying.

**Steve:** Yeah. So this is for Windows servers. I went through and looked at all the available cipher suites and carefully hand-tuned the list in order of the one we would prefer that a client connected with first. So it's very carefully designed for maximum forward secrecy and maximum security as we go down the list. So it goes from strongest to weakest that are currently offered by Windows server platforms.

**Leo:** I would presume the server would query in that order; right? It would try to connect with the first one, and then the second, and then the third.

**Steve:** Well, what happens, yeah, what happens is the client, remember, in the TLS handshake, the client offers all the ones it has. And so the server then uses the sequence that I have created, going down its list, looking for the first match with any of the ones in the client. Thus we get the strongest negotiated security available.

And so I have been needing to go back in because, with that update a couple months ago, I think it was two months ago, I want to say it was 068 was the Microsoft update, that was the one that silently fixed a problem that had not previously been disclosed and treated us to four new cipher suites which were really new and tasty, to borrow Oddworld's title. And so I've been wanting to merge those in. And that would of course push, now I'll push some of the RC4 ciphers off the bottom and then pop my grade up at SSL Labs from an embarrassing C to a, well, somewhat less embarrassing B. At least I could maybe beg my way into a good school.

**Leo:** Well, yeah. Gentleman's C is not going to work here, I think.

**Steve:** No, I don't think so.

**Leo:** You need to step up your game.

**Steve:** So for anyone who's interested, as you said...

**Leo:** And fix the comma.

**Steve:** ...it's bit.ly - yes. Oh, yes, thank you for - yeah. Bit.ly/grcciphers is the list. But that's the old one. If you look at it, and you see that there's a comma missing from the fourth to the last line, and there's still some RC4s, then you know you don't have the new one. I'll be getting to that here pretty quick.

**Leo:** That's why you left the comma out. Now we know. So people could tell if it was...

**Steve:** Yeah, we have a - it's a canary.

**Leo:** A canary.

**Steve:** It's really weird, too, because Microsoft has a character limit on the length that string can be. So I put in new lines to make it visually clear. But to use it you have to remove the new lines and then cut and paste it into the registry. And I think it's 2048. And the problem is there are more useful ciphers that you'd like to have that are

available, except you run out of room because they're too long. And so it's, ugh. And so it really is sort of a balancing act. You've got to, like, you've only got 2,048 characters, I think that's what it was. And so you've got to go through and go, okay, well, we don't have room for this one, but we do have room for that one. And so you have to, like, deliberately withhold some you'd like to have in the interests of, again, of compatibility. That's why I spent some time building this list, and people are using it with their servers. So there.

**Leo:** So there. It's very cool. How did you build the list? Did you pull it from the code or...

**Steve:** In the registry help it gives you a list of all of them. And so I copied that out. And it also says, but warning, the string you provide can only be 2,047 characters long. And it's like, okay, is that going to be a problem? And so then I look, and the list is like 3K long. So it's like, yes, that's going to be a problem. I can't have them all.

**Leo:** I love it.

**Steve:** They've got to fix that. That's ridiculous. I don't know what that's about. Come on.

**Leo:** Ron in Daytona Beach, Florida. He's got a question about VPN usage and spying: I use a VPN most of the time using proXPN, our fine sponsor. Thank you, Ron. Question: When I connect, I have many choices of terminating VPN locations. Yeah, that's one of their features. The U.S. one gave me the best performance. That makes sense. It's geographically proximate. However, I feel that when I connect to one of the U.S. ones, my traffic is still subject to spying. Oh, no. I'm guessing my ISP can't track me directly anymore, but the National Spy Agency is still collecting my packets. Is this true, or am I just being overly paranoid?

**Steve:** So we see this question in various forms, and I know you get it a lot, Leo.

**Leo:** Yeah.

**Steve:** I've heard listeners on your weekend show, The Tech Guy show, asking. The question would be, do you think the NSA is specifically capturing traffic from the proXPN servers more than they're capturing traffic coming into the U.S. through the fiber optic undersea cables. And maybe it's all of the above. But I guarantee you that there are taps on all of the oceanic cables coming into the country because that's where terrorists are, presumably. And their articulated responsibility is to protect us from them. So we know they're tapping traffic coming into the country. We also know that they're sniffing what they can get that's available within the country, unfortunately. There's that room that we know about in L.A., or was it San Francisco, where the fiber optic tap was installed that we originally talked about a year and a half ago.

**Leo:** AT&T WorldNet in San Francisco, yeah.

**Steve:** That's it. So I don't really think that there's a difference. What the VPN certainly does is it protects your ISP from collecting any metadata. Metadata, of course, is even if they can't decrypt what you're doing because you're over SSL or TLS - boy, I wish they hadn't changed the name. That just really annoys me. I guess I just have to support the TLS. Everybody knows what that is now. They can't see what's in there, but they can see the IPs that you're visiting, and they can see the DNS queries that you're making. So running through the VPN does prevent that. It prevents any visibility into your traffic until it gets to that server.

But as for NSA difference, I really don't - can't say that I would imagine it makes a difference. We will soon, eventually, when the world lets us, get to our podcast about the Tor Deanonymizing which is on my very short list of things to talk about, because as I mentioned it looks like it's not quite providing the protection that we were hoping under some circumstances. But short of that, I think that the VPN offers local protection, but probably doesn't matter too much whether the NSA is checking or not. I think they're as likely to be looking at traffic coming into the U.S. if you connect to an extraterritorial VPN server.

**Leo:** Strikes me that, if people took the energy that they spent trying to protect themselves, possibly futilely, against snooping by the spy services, and instead directed that energy towards our members of Congress, saying fix this, there'd be more - that'd be a more useful use of your juice.

**Steve:** Or both. Let's do both.

**Leo:** You could do both. But people spend so much energy on, well, is this safe? Are they going to be able to spy on me here? Just send a couple of messages to your member of Congress, too, as long as you're doing that. Because that's really the only way, and maybe even that's not going to be good enough. But that is the only route to getting this in hand.

**Steve:** Leo, I think we're heading for legislation which mandates a backdoor.

**Leo:** Yeah, we do look - it does look like that. You've got your Ron Wydens on one hand, and then you've got your backdoor guys on the other.

**Steve:** Yeah. And, I mean, the boogieman of protecting us from the bad guys, the whole terrorism argument, and the argument, you know, I mean, we talked last week about Posner saying "I can't believe it's legal for anyone to sell a phone that can't be decrypted." It's like, oh, goodness. I mean, I just think we're losing this. And I predicted a few years ago, which is why I suspended work on CryptoLink, because I thought, well, I don't want the government to come along and say, "Gibson, you've got to build a backdoor into the VPN you just spent all your time making absolutely secure." It's like, uh, no.

**Leo:** Anthony Headley, who must also be from the U.K. because that's a very British name, wondered: Whatever happened to the SmushBox? Hey, Steve. Whatever happened to Mark Thompson and company's SmushBox? In the last episode, Leo remarked the guys from ITPro were sending SMS notifications, and I was reminded of SmushBox. Yeah, we ordered one. I have one. I know you do, too, Steve. From their site I see they had a rocky start due to some faulty microSDs. They offered to fix the issue. That seems to have solved the issue. Where does that stand right now, Steve? I'm just wondering if either of you have received your boxes - yes.

**Steve:** Yup.

**Leo:** Do they work? Can't tell you because I haven't set it up. Thanks, love the blah, blah, blah, Anthony.

**Steve:** So we've talked about it since. And I need to distance Mark Thompson from this. It wasn't his company. It was some guys that he knew of, and I knew of them because I know of him. And he thought it was a cool thing. I mean, he thought it was a neat idea. And you and I agreed, Leo, and we both got them. The problem, or part of the deal was, they had a special deal with T-Mobile so that for $20 a month you could have unlimited number of messages that this SmushBox would send.

**Leo:** Yeah, that was cool.

**Steve:** That was what that was about.

**Leo:** And that ran out.

**Steve:** And, yes, and that's what happened was it turns out that one hand didn't know what the other was doing. They got into some fights with T-Mobile. And so they did send an email out to all the SmushBox owners, apologizing for the fact that they were unable ultimately to honor the original contract.

**Leo:** But this will still work. I just have to pay more. Is that right?

**Steve:** Precisely.

**Leo:** Oh, okay.

**Steve:** So, yes. So it is a beautiful, nice, USB interface to text machine that can send out mass texts. But it's up to the individual to create an account with T-Mobile, rather than all running it through a grandfathered blanket $20 a month forever deal. That's what fell apart.

**Leo:** So somewhere I can put a SIMM in here.

**Steve:** It's got one built in. It's already in there.

**Leo:** Okay. So I would just call T-Mobile and say, hey, activate me, baby.

**Steve:** Yes, exactly. And then you're able to send and receive texts with that. And so one of these days you and I are going to figure out how that's useful. It's a beautiful thing.

**Leo:** Well, I always, you know, and we have been - as you know, we're designing a new TWiT site. And it's kind of one of the things on our wish list, to be able to send out text notifications when a live show begins recording...

**Steve:** Oh, yes.

**Leo:** ...when a show has finished recording and is now in editing, and when a show ships.

**Steve:** Special, yeah, exactly, like allow people to subscribe to a feed of real-time events.

**Leo:** Right.

**Steve:** Yeah, very neat.

**Leo:** Well, that we can do. And we can easily do something that they pull. But this is pushed. So I don't know, I mean, it's easy to do something that's pull, that you would poll us - in fact, that's kind of how RSS works anyway.

**Steve:** Yeah, but I think texting is just so ubiquitous and so simple that - and people are able to send back, like, send back a stop if they don't want to receive that anymore and basically control it through text. I think that's cool. And look, you were even able to find yours. I don't know where - mine's, like, mine's BuriedBox. I don't know where mine...

**Leo:** You know what's bad? I can't find the documentation. Must be on...

**Steve:** Might have been online.

**Leo:** Maybe it's on the website.

**Steve:** Yeah.

**Leo:** There's no documentation at all. It is pretty, though.

**Steve:** Well, they did a beautiful job.

**Leo:** Yeah. My SmushBox. Question 5 from Michael Peters. He hails from Meerbusch, Germany. Meerbusch. He wonders about whitelisting executables: During the recent episode of Security Now!, while you were talking about the Sony case, you mentioned whitelisting of executables as the "only real way to keep the bad guys out." Indeed, I see this as the last chance left to get more security into a larger company network. For our company and our network, no user except the IT people should be able to launch any kind of program that hasn't been approved by the IT staff. Boy, that seems obvious.

**Steve:** Yeah.

**Leo:** Unfortunately, we never took the time to give Windows AppLocker a try, and I'm wondering whether such a scenario could be realistic, or am I missing something? Love your show, although it frightens me more and more. Steve is really great; Leo, too. Besides, it's helping me improve my English. Well, your English is perfect. Kind regards, Michael from Germany. We have an AppLocker license. When we bought the new Dell machines for our editors, six of them, Russell talked me into - he said we should get AppLocker, too. I said, deal. So, but I don't think we've turned it on yet. But we haven't - the machines are just getting implemented now. So what is that?

**Steve:** So AppLocker is a feature that was introduced into Windows 7. And as we know, I will ultimately be moving from XP to 7, kicking and screaming, at some point. I mean, I have 7 everywhere else, just not on my main system because it's such a pain. I mean, I have to, like, start over. I have this incredibly mature, perfect workstation with everything installed. And just the idea of starting over is daunting. And there's never time. I've got to, like, say, okay, well, after SQRL and after SpinRite 6.1, then maybe I'll make the switch. But the point is that it's built into Windows 7, and it's continued to thrive, and it's in Windows 8, as well. And it is a built-in - it's not - there's, like, I think it's in Ultimate and, you know, they've got all these different SKUs now. I don't think it's in Home or even Pro, but it is in Ultimate. And I'm going to deploy it from day one because...

**Leo:** It's a little weird to do it on a home system. I mean, in a business you can say, hey, you can use Office and our line of business stuff, but you can't use any other apps. That's a reasonable thing for a business to do. But at home, don't you want to just do what you want to do?

**Steve:** Well, but it's me; you know? And what I was going to say was...

[Crosstalk]

**Leo:** ...locker?

**Steve:** No. So AppLocker is an application whitelister.

**Leo:** Right.

**Steve:** So only the specific apps which have been whitelisted are allowed to execute.

**Leo:** And a malware can't pose as one of those apps; right?

**Steve:** Precisely.

**Leo:** Is there a hash or something?

**Steve:** Yes, yes.

**Leo:** Okay.

**Steve:** So, and remember back in the day of ZoneAlarm there was the question of whether - because ZoneAlarm was a whitelisting firewall. It would pop up and say, such-and-such wants to access the Internet. And you'd say - you'd look at it and go, okay, yeah. And then the question was whether malware could say that it's Internet Explorer, you know, IExplore.exe, and sneak by. But it wasn't just a filename match, it was a match on the signature of the app itself. So it caught that. So that's what's built into Windows 7 and 8. And I just - I want to try it.

One of the things that I do is I have some sounds associated with different events in Windows. And one of the events in Windows is application execution. And it's just a little snap sound. But every so often I'm, like, working, and I hear a snap. Which means I didn't just start something, but something started. And I sometimes wonder what that was because that would be a quick clue that something's in my system that I'm not aware of. So I'm going to do the experiment. And this is the kind of the thing that's difficult to turn on later because, like, nothing will work. Although you are able to put it in an audit mode, and that could be useful all on its own.

**Leo:** Yeah. You say, hey, audit what I'm doing right now because I know there's nothing bad on here. Please add these things to my whitelist.

**Steve:** Right.

**Leo:** Yeah.

**Steve:** Right. And so you train it during a time when you know that your system is fresh and set up. And then you're able to look at a log of the things it has blocked or that it has permitted and, like, tweak it over time. It's basically, it's like an application firewall. And I would argue maybe that's where we're going to end up. We ended up there with data firewalls, and that may be the way that we ultimately lock our systems down. And it's built into Windows.

**Leo:** Love to get this for Macintosh. So am I correct, because I say this on the radio show all the time - and I probably should run these things by you before I say them. But I have been saying on the radio show, look. To get malware, to get on your system, the bad guy has to have you run a program in some form or fashion. The malware maybe a malformed PDF, and you run Reader, and it's got a bug. But ultimately the way you infect systems is by executing code.

**Steve:** Correct.

**Leo:** And if the bad guy can't get you to execute code, then you're safe. And so the idea being we only can execute these set programs. You should be safe. Now, if one of those programs is Reader, and you get a malformed PDF, and Reader's not up to date, well, you'll still get bit.

**Steve:** Correct. Or if you're lured to a phishing site, and they tell a nave user, oh, we'd love to show you this video that you're interested in, but you have a vulnerable or obsolete version of the video player. Click here to update it.

**Leo:** Right, right.

**Steve:** And so many people who are not podcast listeners...

**Leo:** Easy, easy to fall for that.

**Steve:** Yes.

**Leo:** But, now, AppLocker would stop you because the installer for this...

**Steve:** Correct.

**Leo:** ...malware would be not allowed.

**Steve:** Correct.

**Leo:** Yeah. All right. OS X does something a little similar. But of course, as always with Apple, it's Apple that gets to decide. You can say I'm not going to run unsigned code on this machine, and Apple is the signatory. So if it's not signed code, it won't run.

**Steve:** Right. And of course we did that with Windows with device drivers. Microsoft said we're going to up the ante on device drivers, so you've got to have the device drivers signed. And that is a useful bar to put on applications also, say that we're not going to run applications that don't come from - theirs is, I'm blanking on it, I have a license from Microsoft. All of my apps are signed. Authenticode is their executable technology. And so it's like, don't allow anything that's not Authenticode signed. The problem is it's not impossible for bad guys to get an Authenticode cert. And in fact one thing we did see that happened from the Sony hack is that malware was quickly signed with the Sony certificate.

**Leo:** [Laughing]

**Steve:** Which was stolen from Sony.

**Leo:** Oh, lordy, lordy.

**Steve:** Yup.

**Leo:** So this says "allow apps." This is in the security settings on OS X, Yosemite or later. Allow apps downloaded from, in the most strict form, the App Store only. So Apple has approved Apple's whitelist, in effect. But most people, and the default is, Mac App Store or identified developers. That really means one with a certificate that is an Apple-generated certificate. And then this is the least secure and, by the way, not the default. The default setting is no apps downloaded from anywhere. So current Mac machines, really, you can only run apps, unless you've changed the settings, from the App Store, approved by Apple, or where a developer has a certificate from Apple. I think that's pretty good. That's Gatekeeper.

**Steve:** Well, yes. So, yeah, so what I would do, and I know our listeners, you want to go to that middle option. Switch it now.

**Leo:** Well, that's the default, yeah.

**Steve:** That is, take it off - oh, it is, oh.

**Leo:** That's the default, yes.

**Steve:** That is the default.

**Leo:** That's the default. If you say "anywhere," they give you this big warning.

**Steve:** Oh, good.

**Leo:** And furthermore, they say, in 30 days we're going to go back to the default.

**Steve:** Now, good. Apple really has learned a lot of lessons in the last couple years. We've seen them really tightening things up that way. And that's fabulous. I mean, it's like allowing Flash and then, like, disabling it again automatically.

**Leo:** I know, I love it.

**Steve:** It's like, yes, that's exactly what we want.

**Leo:** You can have Flash, but only for a few days.

**Steve:** Yeah. So I was going to say, if you had that default setting, and you did run an app that was not from a well-known developer, that just gives you a chance. You're going to get a dialogue that's going to scare you, and then you can say, oh, how much do I trust where I got this from?

**Leo:** You actually have to - you have to kind of override it. It'll say I'm not going to open this because it's not from a certified developer. And then, if you wish to open it, you need to right-click on this app and select "Open," and then we will open it for you. But you cannot just, you know, you don't click a button that says "Okay." You have to kind of do something else.

**Steve:** Right.

**Leo:** I think that's the right way to do it.

**Steve:** Yeah.

**Leo:** Yeah. Moving on, Question 6. Dave Held, Redondo Beach, California. He was floored: I was floored by your "Oh, well, nothing can be done" response to the Sony hack. If it's true, as you say, that computer systems simply cannot be secured against attack - and that isn't exactly what we said, but...

**Steve:** No.

**Leo:** Well, don't you realize that implies the end of electronic methods in business and a massive return to paper documents and locked file cabinets? What movie star will discuss her future roles and earnings via email? What corporations will store their contract negotiation proposals on servers, or even use anything more complex than a typewriter to prepare them? By the way, that's one of the upshots of this Sony hack is Sony is in fact stymied. They are having a lot of difficulty making deals. They are no longer using email. They're only making phone calls. I mean, that is how Sony's responded to this, going back to the Stone Age.

**Steve:** And I think, didn't we hear that Russia had switched to typewriters?

**Leo:** Yeah.

**Steve:** For the same reason?

**Leo:** Yeah.

**Steve:** Yeah. Okay...

**Leo:** So, but I don't think you were saying it's impossible.

**Steve:** No.

**Leo:** Just not practical.

**Steve:** The response is a little more nuanced than that. But, yes, exactly. It was, in reality, could I actually claim, could I design a system that would meet Sony's requirements and be secure? No. You just can't. There are...

**Leo:** Could you do better than Sony? Yes.

**Steve:** Yes. And I talked about a number of things that could be done. I've been, like, challenging myself in the week since I said that, kind of thinking, well, what would I do? And something like whitelisting apps so that only IT-approved things will run on your machine.

**Leo:** I like that.

**Steve:** Yes. And then set up a virtual machine which does not have privileges on the network, but is like, you know, uses a VLAN out to the Internet so that, if somebody wants to do anything else, they can do it in this container without IT permission, but they

can't access any resources within Sony. All they can do is get to the Internet. So if they want to run QuickBooks or whatever, or run an unapproved browser or some network-connected software, they can. But it won't run on their machine, it'll only run in the virtual machine. And the only thing the virtual machine can see is the Internet. It cannot see the rest of their machine or anything else.

So that's the kind of thing that, once you implement it, people kind of grumble. It's like, well, they didn't have this at my old job. And it's like, well, no. We've got security at this place. So, I mean, there are things you could do. Also, it really does seem like their network was just one mass of interconnectivity. And siloing networks, which is some lack of convenience, but it does mean that one entry point doesn't get you to the entire corporate crown jewels everywhere. So anyway, I did want to clarify in case anyone else felt that. And I did see some tweets to that effect. It was like, "What, Gibson can't do it?"

It's like, it's not possible because you have, first of all, a huge number of systems in which we are actually finding vulnerabilities constantly. And you've got the human factor. The human factor is why you have a company, I mean, of people. And they're going to do dumb things. There just isn't any way to prevent that. There is a way to lock them down. And something like whitelisting apps on their machine that is connected and then giving them freedom in a virtual machine that is not part of the Sony network, that would be an interesting thing to explore.

**Leo:** Well, and we've talked about AppLocker. I mean, that's something you can do. There are things you can do.

**Steve:** Yup. Yup.

**Leo:** But I think that that was kind of my point with the hack of the Sands casino, where presumably they did everything anybody knew how to do. I can't imagine they weren't following best practices.

**Steve:** You know, I'll bet that after that they're doing more.

**Leo:** Yes. Yeah.

**Steve:** So doesn't...

**Leo:** There's always more.

**Steve:** Yeah. So doesn't that tell us that they weren't doing everything that they could do? Because there's no question that they're doing more now. And if Sony ever does recover, we know there will be changes there.

**Leo:** Yeah. You hear it pouring rain here? I don't know if you can...

**Steve:** I do. I was thinking, where is the - who left the faucet on?

**Leo:** Yeah. Somebody's popping corn or something.

**Steve:** Wow.

**Leo:** Mark Jones, Midland, Michigan. He encountered some unsettling verification questions: Steve and Leo, love the show, look forward to it every week. When trying to schedule a FedEx delivery, I was asked to create an account. I've seen this, and I can explain what's going on. But I was shocked when a verification page confronted me with multiple choice questions about past addresses, last digits of my driver's license, names of others at my address, type of car registered to me. I was then even more shocked when it said that I had the answers wrong. It then asked me a different set of equally curious questions.

At first I was shocked that FedEx could know any of these things. Next, I felt like I was providing data about myself that otherwise would be unknown. Others on the web have indicated FedEx is relying on credit reports. I decided I don't need a FedEx account. No question here, just an alert at another unsettling turn of events. Leo might be right, the privacy battle is lost. No. There's good news. This isn't as bad as it looks.

**Steve:** Just I love the idea of encountering a security question, and it's like, what was the name of your first childhood sweetheart, and you type in "Julie."

**Leo:** Nope. No.

**Steve:** And it says, "No. Have you forgot about Sarah?"

**Leo:** That would be scary. This isn't quite that bad. He's right. It comes from credit bureau information. I don't even think FedEx ever sees this. I've seen this, I've been exposed to this many times.

**Steve:** So it's trying to, without knowing anything about you, trying to verify your identity...

**Leo:** You are who you say you are.

**Steve:** ...and who you are claiming to be.

**Leo:** Right.

**Steve:** Ah, interesting.

**Leo:** So it's an interesting puzzle; right? You want to authenticate somebody, but you don't have any previous conversation with them.

**Steve:** Right.

**Leo:** So there's no password. There's no secret questions. It's like secret questions, but you don't - so the only thing you can do is you go to one of the three reporting credit bureaus, and they provide you with these questions based on information that's in your credit report.

**Steve:** Ah.

**Leo:** I don't know what FedEx is doing, but the ones I have used, I'm pretty sure the way it works, these guys aren't seeing it. The intermediary's not seeing it. This is directly coming from as an interaction with Experian or TransUnion.

**Steve:** Come to think of it, I've seen...

**Leo:** You've seen this.

**Steve:** Yeah, I've encountered that, too.

**Leo:** You have.

**Steve:** And there have been, like, some strange addresses for me. It's like, wait a minute.

**Leo:** Yeah, they'll give you four - so what they'll do is they'll give you four addresses.

**Steve:** Right, right.

**Leo:** Three of which are bogus, one of which - and it often is not the full address, but it's did you ever live at Page Road? And they'll give you four addresses. And you pick the one that you did live there.

**Steve:** Right.

**Leo:** And that's direct from your credit report because of course all of that stuff is

stored on your credit report.

**Steve:** Right. So they're matching up your real world identity with your cyber identity.

**Leo:** And they're not gathering new information at all. It's like secret questions, but you just haven't prearranged the answers.

**Steve:** Right.

**Leo:** So I don't - unless you can think of a - I guess one issue would be if the third party were intermediating. So if FedEx saw the questions, got the answers, and then - if it made the quiz based on downloading your credit report, well, but they have access to your credit report if you're applying for credit. You have to give them access to your credit report in some cases, at which point they know all that anyway. If you've ever given any company your Social Security number, that's because they use it to access your credit report.

**Steve:** Right.

**Leo:** Date of birth - name, date of birth, and Social is enough to get your credit report. So I don't, yeah, I don't think it's an issue. But you have to be the judge, of course. I think it's just - it's solving an interesting question. How do you authenticate somebody you've never met?

**Steve:** Yeah. How do you match their real-world true identity with their cyber personality?

**Leo:** Yeah, and the only way you could do that is with a third party that did know something.

**Steve:** Yup.

**Leo:** Mike Vore, Columbia, Maryland, wonders about Sony exfiltration. I love that name, that word, "exfiltration." I've been wondering, how could that much data be taken offsite without the NOC noticing that much traffic [the network operations center]? Even with fast fiber it takes a lot of sustained bandwidth to move that much data. An extra megabyte or even gigabyte a day might not be noticed, but we're talking 12TB. That's either high bandwidth or a long time. What is - see, Sony of course is not telling anybody, the FBI isn't telling anybody how any of this happened.

**Steve:** I know.

**Leo:** What's your speculation about how this might have happened?

**Steve:** Many people asked this question, and I just, when I encountered it, the first time I encountered it I added it to the show today because I wanted to respond to it. I had the same thought myself when we learned how much data it was. But then I thought, can you - we're talking Sony Pictures Entertainment. Can you imagine how much content, how much media, how much data they must have transacting over their Internet, I mean, over their Intranet to the Internet? And the fact is, you know, 12TB for a major corporation's network, eh, that's in the noise. I mean, that's - and we do know that some of the data was snapshotted on November 23rd and, what, maybe a week later? So we don't know how long they were there pulling other stuff.

We do know, for example, that they used Sony's own servers to seed some of the torrents, which is so ironic. I just love that. So there it's sort of like trickling out over time, and as people use it, you know, the way torrents will. So anyway, I just think, if it was our network, our individual networks, yeah, we would notice if 12TB was trying to leave. But, boy, a major media corporation the size of Sony, eh, I just - lord knows how much bandwidth they must have. And, yeah, I just think it actually could. If spread out over time, it would just probably sneak right out, just they wouldn't even know. They wouldn't see it as a blip compared to, like, movies that they've got coming and going across their fiber connections.

**Leo:** I would bet that, you know, digital movies now are distributed over the Internet as downloads. I would bet that some of that came from Sony servers, among other things.

**Steve:** Yup. Yup.

**Leo:** I also think...

**Steve:** Well, actually we know because a bunch of movies were exfiltrated.

**Leo:** Well, but those weren't projection copies. Those were the screeners. Kind of low quality, in fact, DVD copies that leaked out, as far as I - I have not downloaded them. I'm told.

**Steve:** Hardly worth going to find.

**Leo:** Really. No kidding.

**Steve:** Besides, "Annie" I can live without, I think.

**Leo:** I can wait till Christmas Day, thank you very much.

**Steve:** Yeah, okay.

**Leo:** And then there's also the suspicion, you know, I wonder, I guess we'll never really know what really...

**Steve:** I'm hoping, I'm hoping that - because it would really be fun to get the technical readout.

**Leo:** That I would have no problem revealing, that kind of information. Even if we came by it illegally, I would absolutely reveal that information because that is something very, very valuable. The public does have a right to know how did Sony get hacked, what happened, et cetera, et cetera. There is some suspicion, you know, Sony got hacked and didn't want to talk about it in February. It maybe is even part of the treasure trove that's been leaked. There was a memo saying we're not going to alert the affected parties that we got hacked. And that was in February. So it wouldn't - and, by the way, there is a little bit of a nexus because that hack was some - it had something to do with Brazil, and there was a significant number of Portuguese and Brazilian documents in the trove.

**Steve:** Yes. We talked about that last week. And I also heard you say on The Tech Guy over the weekend, to somebody who had a virus, you correctly said there's no way to get rid of it.

**Leo:** Right.

**Steve:** Once it's in there, you can never know.

**Leo:** That could have been the vector, back in February. And who knows, maybe they've been leaking data, a terabyte a week, since then.

**Steve:** I mean, there is this notion of a foothold. You get in, and then you go quiet, and you protect yourself, and you scrounge around.

**Leo:** Really interesting. I wish we could know the truth of this. And that I think would be very useful for prophylaxis, for future.

**Steve:** Yeah.

**Leo:** Stephane Blais in Gatineau, Quebec, Canada wonders: What if Sony was a bank? Steve and Leo, longtime listener, big fan, yada yada. As big as Sony's recent hack was, I can't help getting shivers when I imagine how devastating an attack like that would be if it were a bank instead of Sony. How disruptive would that be? And for all we know, those things are happening, too. In last week's podcast, SN-485,

you mentioned how impossibly hard it would be to secure Sony's network. Would it not be just as hard to secure a bank from a determined attacker? Are banks really that much ahead of the game, or are we all in denial? I don't want to be unfair to banks, but I do have a vested interest since my bank has my money. And I expect it's the same for you. Thank you.

Optional yada yada extra: On a personal note, I want to thank you both for the amazing education I'm getting from Security Now!. I work as a security professional, and it's amazing how many times I look smart because of stuff I hear on your show. I'm also convinced I passed my CISSP exam because of you. Thank you both, and keep up the great work. Stephane.

**Steve:** So I think it is without question that banks are more secure, in the same way that casinos are more secure. And we could almost look at Sony as an example of the other end of the spectrum. That is, if nothing else, how many attacks has Sony suffered? How many password breaches? I mean, Sony has been a constant victim over, you know, we've talked about multiple Sony problems over the years. And for whatever reason, they seem to keep having them. So it is certainly the case that lax security makes you more likely to get attacked, and that a bank by its very nature is about security and privacy and secrecy. Sony, as sort of like the generic business operating corporate side, they're not. They're about Donald Duck and Mickey Mouse and movies and...

**Leo:** That's Disney.

**Steve:** Oh, yeah, well, okay. Movies and actors and all that.

**Leo:** They're artists. They're artists. They're not security professionals.

**Steve:** Perfect. Perfect. Yes, artists.

**Leo:** Although a couple of things. We know banks get hacked all the time and don't report it, A, they just absorb the loss. And we know that happens every day. It's not like the Sony hack because the Sony hack they got everything. Although who would care if they released a bank vice president's email, really?

**Steve:** Yeah. What is being - the loss that they're absorbing, though, is more of, like...

**Leo:** Funds.

**Steve:** ...vendors losing their credit cards, who then turn to the bank and say, okay, you're going to have to replace all these cards.

**Leo:** Yeah. I think that banks also lose money.

**Steve:** Yeah.

**Leo:** They lose money to hacks. And they just cover it and move on.

**Steve:** Well, and that's a good point. We also know that banking customers lose money. There is all kinds of wire fraud and money transfer fraud, where somebody says, hey, all the money in my account is gone. And we've discussed who is responsible in that event, and I erroneously said that the user, the victim was responsible. But it turned out that there was a difference between personal and corporate accounts in terms of what was insured and what wasn't.

**Leo:** And then Sheldon Adelson, who is probably as protected as most banks, got hacked. Right?

**Steve:** Yeah.

**Leo:** Chase Bank was hacked, info stolen for 83 million accounts. That was in October. Hackers attack, crack 10 financial firms in major assault. That was in October, including JPMorgan. Remember?

**Steve:** Yup.

**Leo:** I mean, this stuff...

**Steve:** Yeah, it just happens all the time.

**Leo:** We're just used to it. You know what? We're just used to it.

**Steve:** Yup.

**Leo:** It's not not happening. It isn't. We're just used to it. In fact, I don't think, you know, we didn't talk much about - that's where the - see, maybe they, okay, you know what? This backs what you're saying up. Because JPMorgan got hacked badly last - for 83 million accounts, an untold amount of money, just a couple of months ago. And nobody talked about it that much. Sony gets hacked, and a few stars' salaries get revealed, and it's the talk of the town for weeks. So that does back up your argument that it's not a bad thing to reveal this because it just does raise awareness.

**Steve:** I think it's human nature. It's got to be bad for anyone to say, oh, I really don't want that to happen to me.

**Leo:** And by the way, Chase didn't want to reveal that it had been hacked.

**Steve:** No, it hurts its reputation. And their reputation really matters.

**Leo:** Yeah, yeah. Well, Steve, I think that's it. I don't see a Question 10.

**Steve:** Nope, we're done.

**Leo:** I think once again you've aced it. You are an A+ student in my book. I don't care what SSL Labs says. Thank you so much for the good work you do. And it is, it's always - it's an education listening to Security Now!. We do it every Tuesday, 1:00 p.m. Pacific, 4:00 p.m. Eastern time, 2100 UTC. Do stop by and participate live. It's great. You can even come by the studio, if you want. We always have somebody in this - people love you. There's always people watching, you know, in the studio. Email tickets@twit.tv, and we'll make sure we have a seat for you. This, my studio, the little one, is a little constrained. There are only really three good seats. We could fit...

**Steve:** Well, four.

**Leo:** There's a few obstructed views.

**Steve:** Yours is one of the best seats.

**Leo:** I have a good seat.

**Steve:** You've got the best seat in the house.

**Leo:** But there's a couple of obstructed views. So let us know ahead of time. You can also get on-demand versions of this show in several places. This is one show where Steve has a copy of it, which is unusual, but Steve likes to host 16Kb audio versions and handcrafted transcriptions at his site, GRC.com. We have the larger audio files and video, too, at TWiT.tv/sn. And of course you can always subscribe on your favorite catcher, iTunes or Xbox or whatever it is you use to listen to podcasts. Don't forget to go to GRC.com to get SpinRite, the world's best hard drive maintenance and recovery utility. There's lots of freebies there, too, and you can find out more about SQRL.

Next week it's your talk from, what was that, a Vegas hacker con or something?

**Steve:** Yes, it was November 7th. It was DigiCert's Security Summit.

**Leo:** Ah, okay.

**Steve:** And I gave a really nice presentation, if I do say so myself, of sort of soup to nuts, if I may, for SQRL. And so that'll be the Christmas Special content.

**Leo:** Next week, December 23rd. And then we will be back live on December 30th. We can wrap up the year in hacks.

**Steve:** Yup, will do. And I'm going to give a SQRL demo during that podcast.

**Leo:** Oh, we're that - oh.

**Steve:** It's running.

**Leo:** Yay. That's exciting.

**Steve:** Yup, yup.

**Leo:** So next week our holiday special.

**Steve:** It's going to - you're going to - your mouth is going to hang open.

**Leo:** Can't wait.

**Steve:** You're going to say, wait a minute, that's actually - that works? That's secure? I'll go, yup, that's all there is to it.

**Leo:** So exciting. That's really exciting. So that's December 30th. Make sure you tune in for that. Steve, I'm not going to see you till New Year's. I know you're coming up for New Year's Eve. That'll be fun.

**Steve:** Yeah. I'm going to come up a few days before and join you guys in the...

**Leo:** In a washed-out house.

**Steve:** ...host party and then be hanging around.

**Leo:** That'll be a lot of fun. I can't wait.

**Steve:** It will.

**Leo:** Three a.m. New Year's Eve, 3:00 a.m. to 3:00 a.m. New Year's Day, 24 hours of 2015. I'm going to stay up late. Steve did it last time with me. I bet he'll do it again.

**Steve:** I also signed up, I signed up for doing something in front of a green screen with you. I'm not sure what I got myself into, but some sort of, like, I don't know.

**Leo:** I think we're doing - I think we're acting out a Flintstones episode, and you're Bamm-Bamm.

**Steve:** Oh, good.

**Leo:** No, I'm just kidding. I don't know what it is. We're doing it for a charity, though, so you should really do any, you know, you should really step up because this is all to raise money for UNICEF, the United Nations Children's Fund, which does great work all over the world, including in the Ebola-ravaged areas of Africa. They've really been doing good stuff there. So we thought it would be good to take - we were going to do it anyway. Why not do it for a good cause?

**Steve:** Yeah.

**Leo:** We're going to have auction items, giveaways. It's going to be fun.

**Steve:** Neat.

**Leo:** Thanks, Steve. Have a great Christmas. Won't see you till after the holidays.

**Steve:** Right. Have a great week, and I'll see you week after next.

**Leo:** Take care.

**Steve:** Bye.