SECURITY NOW!

Transcript of Episode #529

Listener Feedback #220

Description: In the wake of the news that LogMeIn is acquiring LastPass, Joe Siegrist, founder and CEO of LastPass, joins us to talk about the acquisition and what he hopes it means for the future of our favorite password manager. We then catch up with the week's news, and share and discuss 10 questions and comments from our listeners.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-529.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-529-lq.mp3

SHOW TEASE: It's time for Security Now!. We've got questions and answers. We've got security news. But we're going to kick things off with an interview with Joe Siegrist. You may not know Joe, but you know his product. We talk about LastPass, the password vault, all the time. LastPass just sold to LogMeIn. We're going to talk to Joe Siegrist, the cofounder and CEO of LastPass, and find out what's going on. And can we still trust it? It's coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 529, recorded Tuesday, October 13th, 2015: Joe Siegrist of LastPass.

It's time for Security Now!, the show where we cover your privacy, your security online with this guy right here, Steve Gibson of GRC.com. He's our guru, our fearless leader. If Steve says it's good, it's good. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be with you again, as always. We've got a bunch of stuff to talk about. We've got - this is Patch Tuesday today. And Microsoft just about an hour ago dumped their updates for the month. There's some concern about a new problem that's been found, well, an existing problem that sort of caught people by surprise in the SHA-1 hash that - I saw the statistic, just like during my research. But it was a large number of sites are still using it, on the order of I think it was like a quarter of websites today, still using SHA-1. The press has of course gotten it wrong again, saying that it's broken. But it does take our breath away a little bit.

But there's also news of the CAB Forum, that are the guys that manage certificates, you know, the whole certificate industry forum, essentially, they just put out prior to this news a ballot to consider extending the issuance of new SHA-1 signed certificates for one more year. So we'll talk about that. And of course this is a Q&A episode, so we've also got 10 questions and comments from our listeners that we'll go through and discuss.

But the big news of the week, the Twitter feed-filling event for me was the news that LastPass was being acquired or had been acquired or was in some state of acquisition by LogMeIn. And I thought, you know, there was like a ton of reaction on LastPass's site from users, and lots of people saying, "Oh, my god, is this the end of the world? What does this mean?" And I thought, who better to help us understand this than the founder and CEO of LastPass himself, Joe. So he's our guest for a little conversation here at the top of the podcast.

Leo: It's exciting. And LastPass, of course, is the password vault program that you vetted and picked among all the rest, and I've been recommending for years and using for years. In fact, I just checked, and I have more than 400 passwords in my LastPass vault. And we use it here at TWiT. It's our enterprise solution, as well. We use LastPass Enterprise. So, you know, as anytime a company gets sold, there's a lot of concern. I think we should just jump to Joe right now, and...

Steve: Yeah, I was going to say that, by way of introduction, the reason I am as comfortable and have been as confident of LastPass as I have been is Joe was absolutely forthcoming with - and our listeners who have been following the podcast for a while know this. If I can't get documentation, if I can't get someone to explain to me what they've done, then I can't understand it.

So, for example, famously, BitTorrent Sync came out, and they refused to share the protocol. So people say, "What do you think of BitTorrent Sync, Steve?" And I say I don't know. There's no way to know what it's doing. It's a black box. But from the very start, Joe's entire posture, his whole approach was, "Here's what we're doing, if you're interested." And even to go as far as to create a page that had, I'll never forget this, code which was able to decrypt the LastPass vault in the same way that they were doing it, where the code was very legible and obvious in how it worked. So we were able to essentially sort of do a self-audit to verify that this is how the thing worked.

And so from my standpoint, where I started at the beginning was it was purely that the tech - that I was able to say that this was done right. The technology is solid. And then of course it has succeeded because it's been made cross-platform; it's over on mobile devices; it's got the features everybody wants. And so those are not about the technology, but those are certainly part of what made it a success. But from our standpoint it was I could say I understand what this is doing. I can't see how it could be done better. So this is what I'm using. And so of course the basis of understanding of what it does and how it works is what for us drove our choice.

Leo: Absolutely. And the openness of the CEO and founder, who's joining us right now, Joe Siegrist. First of all, I guess congratulations are in order, Joe.

JOE SIEGRIST: Thank you.

Leo: And the sale hasn't gone through yet, has it?

JOE: So we signed an agreement. But, no, it has not closed yet.

Leo: Okay. When do you anticipate that's going to happen?

Steve: I'm hoping late this week. But it's not, you know, anything can change that. There's a lot of paperwork that has to be done, as you might imagine.

Leo: Sure.

Steve: It is the case that, if you look at the LogMeIn.com site, under Products, LastPass is now listed there. It does just - it's a link that takes you over to LastPass.com. So there's no integration into them yet. But so I guess my first question, Joe, is are you at all taken aback by or surprised by the user base reaction to the news? I mean, did you expect something like this?

JOE: I expected some people to be concerned. I didn't quite expect the, I guess, how vocal some of the minority would be, like how much they cared. And, you know, I think, you know, we had questions ourselves when we went up there. And I felt like I understood everything that had happened at LogMeIn and was very comfortable with it. And they've been very open and forthcoming with me about just how much they want to leave to me to keep running the business and keep driving the product forward and keeping the security model the same. I think all those things gave me a lot of comfort that this would be a great home where we could have more resources, essentially, to keep pushing the product forward.

Steve: So I guess one question is, to the degree that you can share it without divulging any trade secrets, can you give us some sense for Last Pass's future?

JOE: I mean, essentially it's the same future that we were on. It's just an accelerator. More resources, more development resources, more QA resources, additional products that LogMeIn had been working on themselves that we can fold in under the LastPass brand. But LastPass is the brand. LastPass is the product that they are betting on and what's going to be the future moving forward.

Steve: What is Meldium?

JOE: Meldium is kind of a team-based password-sharing program. It has a different technological foundation than LastPass. It has a lot of features that we might pull in ultimately into LastPass. But certainly has kind of a different use case and different foundation of how it works that's really been based around kind of teams sharing passwords, kind of differently than the zero trust, zero knowledge model that LastPass has worked on.

Steve: So I guess what has everyone concerned is that, as a consequence of some of LogMeIn's history, they've not been happy with their experience with LogMeIn. And so the idea that there is any contamination of LastPass by LogMeIn, you know, as you and I corresponded briefly before this, I was explaining that, from my own take on watching what people are saying, we know that the trust in our password manager is difficult to come by. You've earned it over the years, like both with the original design and the way that LastPass has conducted itself. When you have had some security concerns, you've been absolutely forthright and forthcoming. You've explained what's going on. Thanks to the technology, we've been safe from any exploitation. If somebody did get loose in your network, the amount of damage they could potentially do has been minimized.

So everyone, until Friday, was feeling really good about this. And suddenly it's like, you know, I guess I would argue that it would be impossible for change to be good because what we already have is perfect. So, you know, it's like, if your car's running fine, and something changes, well, it's probably not for the better. So what do you think?

JOE: Well, I mean, I understand that people fear change, honestly. And change is a reality, though. We have to deal with it ourselves here at LastPass, too. Like every app is changing. The landscape is changing. How identity is evolving is changing. And when we look around and try to understand where to take this forward, certainly having more resources was a key to being able to kind of dominate the space. And that's what we want to do. We want to keep making the product better, and we want to increase the amount of people working on this, increase the amount of resources that we have to make the product better.

And I know people are kind of fearing that something is fundamentally going to change. But I'm here to say that that's not going to happen. I'm here to continue working on this, to keep pushing forward the vision that I've been working on for the last seven and a half years. I'm not just going to allow that to change. I really want to keep pushing it forward. And I really saw this as kind of the next step. I think, you know, a lot of the people that are complaining are very vocal because something that they had for free was taken away, and people don't like that.

Leo: I'm going to disagree with you, Joe. That's not the issue.

JOE: Oh, yeah?

Leo: The issue is LogMeIn, and I think a lot of people burned by LogMeIn in the past, by what LogMeIn did to Hamachi, what they did to their free product, I think there's a real feeling that LogMeIn is not going to be a good custodian of the great legacy that you've created with LastPass. Have they given you any assurances that you'll have autonomy, and you'll be able to continue to operate as you have in the past?

JOE: Yeah, absolutely. Just today the incoming CEO, Bill Wagner, was here, telling me that, look, you have the ability to say no. It's your vision. It's your team. We're putting resources behind that to drive it forward. And this is the largest acquisition by LogMeIn by more than six times; right? So they are going to naturally have to treat this differently than some of those other products.

And Hamachi is an interesting thing that you brought up because I was talking about that today as a product I used to use, and one that I think should be brought back and could really have a new life breathed into it when you consider you can tie it into some of the other initiatives that we have with identity and have it folded in, potentially, as an additional product. But I think just the size and scale and scope makes that different. And the people behind it, like this office is staying, all the people here are staying, everybody that was part of LastPass is coming onboard.

Leo: You understand why it's a more serious concern. Because we're trusting you -

and I trust you, Joe Siegrist - with our credentials. But if there's a lack of trust for the acquiring company, that raises a cause for concern. And let's be frank, this is a very competitive space. There are more than a dozen other products that do something similar. I've tried them all. None of them are as good as LastPass. But you can see why there's cause for concern. There was a rumor that you have a bonus for customer acquisition. Is that true? Or customer retainment, I'm sorry. Is that true?

JOE: There's a bonus based on our performance, from a bookings perspective, that we keep selling to customers. So I think that's pretty natural in a deal this size, that they want to incentivize the team to keep pushing and growing the product and the business. So, I mean, yes, there is one. That should not be seen as a bad thing, from my point of view. I mean, it means that everybody here is still trying to make the product better, trying to make sure that everybody realizes that it's the same people behind it that are going to be doing the same thing that they've always done for you. It's just they're going to have more resources when they do it.

So I look at all this and say, like, look, we have a great opportunity here to actually go faster and do more. And because it's the same people running it, I'm still going to be in charge of LastPass. I'm still making the decisions. I've been told explicitly not to do anything that I wouldn't do or would make me uncomfortable. I think a lot of that goes a long way to at least giving us a shot to make sure that we can keep doing what we've always done for you because I think I have earned that trust. I would like to think that.

And I hope I can keep it by essentially continuing to do the exact thing that I've always done and keep acting in the same way, putting customers first, making sure security is first, and driving the product forward in the same way that we always have here. You have the exact same team, working in the same place, on the same product. It's just there's some more resources to make things move a little faster. I think it's going to be a good thing for users, despite the reluctance and the fear by a lot of people.

Leo: Yeah. I think it would go a long way, to me and a lot of other users, to hear from you that kind of commitment that you're going to stand up for us and, as long as your name continues to be on that product, that we can trust that it's the same integrity, the same product that we've used for all these years.

JOE: Yeah, no, absolutely.

Steve: I was just going to interject in terms of what Joe was saying he wanted to do. I would say also maintaining the kind of openness and transparency that we've seen before is crucial. And it's been one of the things that has earned the trust, is everyone has had a sense of, like, okay, LastPass is not hiding anything from us. And so, for example, it's great that you're spending some time with us today to sort of help us understand what has happened.

JOE: Yeah, no, and I appreciate you guys having me on. I appreciate all the support you've given me over the years. Like Steve, honestly, I couldn't get people to understand what we were doing in the early days. People just thought, oh, cloud password manager, worst idea of I've ever heard of, until you actually looked into it and understood it, and then we really started moving forward. You were pretty integral to kind of the path that we got to here. And I guess I'm here saying that, look, nothing's really changed from my point of view, other than I have more resources, and I'm going to keep acting how I've always acted, in the best interests of customers, in the best interests of the product and how it should be run because I have very strong feelings, having built this thing over the last seven and a half years, of how it's supposed to be and how it should run. And that is not easily changed.

Leo: Good. I think that really that's what customers want to hear from you, Joe. They want you to - they want to hear from you that you're committed to maintaining the integrity that you've had all along. And I think that goes a long way to keeping us happy customers.

Steve: Yeah.

Leo: So I appreciate you saying that.

JOE: Yeah, no, I appreciate you guys giving me the chance, and hopefully everybody else. I mean, at worst, wait and see; right? Like I think give me another chance to make sure that you see that we're going to keep doing what we've always done. And a year, two years down the line, you'll look back and say, why did we worry so much about this?

Leo: Right, I hope so. Hey, who runs the servers? You? Or do they go into the LogMeIn cloud?

JOE: We're continuing to run the servers for now. I mean, I think one of the things ultimately we need to do is we have two servers kind of in the Northern Virginia area, and we need to kind of get more geographic diversity. Two datacenters, I should say, not two servers. And ultimately we'll change. But we're going to do that in the way that we've always done, which is be transparent about it, tell you about it, give you a lot of notice, and then ultimately do it after all those things have happened, and everyone has been notified, and it'll be done the right way.

Leo: Have you ever - excuse me, Steve. One more question.

Steve: Yeah, yeah, yeah, no, yeah.

Leo: Have you ever considered - because Steve and I were talking, and he kind of shocked me the last time we talked about this, which was right after the - I don't even want to use the word "hack," right after the last thing that happened to you guys, which you...

Steve: The network intrusion.

Leo: Network intrusion, or presumed network intrusion, which you handled so very well.

Steve: Right.

Leo: It can never be a Trust No One solution as long as your passwords are stored somewhere else, in such a way that somebody could get them, try to brute force them, that kind of thing. Have you ever considered a solution that would not involve storing the password vault on your servers, but maybe have your servers act as a transactional server, or maybe WiFi syncing or some other model? In addition to what you do.

JOE: I really think WiFi syncing and some other ways of syncing kind of just aren't the future; right? Like it's just not the way people are going to do this moving forward. Now, a different technological solution that still involves the cloud, perhaps multiple different trust parties, those things I've contemplated in the past. There's interesting ways you can solve this in a different way without fully going offline, right, in that you can solve the problem that you're concerned about in the same way. I mean, I think the fundamentals with LastPass mean that your data is safe so long as you use a strong password. If you use the software without logging in offline, you're, like, guaranteed that you are in a secure position.

Can we improve on that? I think we can. But I don't think we need to go to the extreme of, like, walking around USB thumb drives again. Like I just think the future is everything's going to be connected, and it's all going to be pervasive, and that any way where you just totally avoid the cloud is probably not the right long-term solution, that you can find better technological solutions that still involve the kind of ease of the cloud. And that's really more a directional thing that I think we would be working on.

Leo: Right.

Steve: Good. Thank you.

Leo: I just - I think just your appearance here makes such a difference to me, and I know to a lot of your users. So I'm very grateful that you continue to maintain that openness. And I that we'll always have these dialogues because I think it's so valuable for us, as users, to see your face and to get the trust there because we are trusting you with everything, Joe. You've got it all. All my stuff. Thank you, Joe Siegrist. We really appreciate it.

Steve: Thanks, Joe.

JOE: Yeah, thanks for having me, guys. I appreciate it.

Leo: Joe Siegrist, CEO and founder of LastPass. And I think it's fair to say congratulations, also, Joe.

JOE: Oh, thank you.

Steve: Yeah, yeah. You've earned it.

Leo: Yeah. Take care.

JOE: Thanks, guys.

Leo: Thank you for arranging that, Steve.

Steve: Well, yeah.

Leo: I know you've been in touch with him in the past, vetting this product. And I think it's great that you were able to do that.

Steve: And from time to time when something's happened I've shot him a note and said, uh, okay, what just happened? And so when he's able to tell me something, he's always been available and forthcoming. I was curious to see if I shot him an email yesterday, would it disappear somewhere. And, nope, he was right there, and he said, "Love to come on to the show and talk to you guys."

So as I said to you before we began recording, my sense is - it's sort of a reaction like I had 16 months ago with TrueCrypt, when one morning we woke up and discovered that the site had disappeared, and some people were immediately prone to say, oh, my god, we have to immediately leave. And my feeling was, well, it was fine yesterday. It's still the same code today as it was then. So let's take a measured approach to this. And, I mean, and Joe essentially said what I hoped he would say. Maybe he said what he had to say. But I think it's also true. I get the sense from him that, for today, nothing is going to change.

And as you said, Leo, you've looked around at the alternatives. I have, too. All of them are - they fall short one way or another. I will say that one of the things I have always appreciated about LastPass is it is not doing anything to impede your leaving. Joe has an offline utility which is able to decrypt the database, so you can use it in sort of an offline mode. But if you go in your web browser, where you've got LastPass installed, under Tools > Advanced, there's an export. And you can export your entire vault in a comma-separated value (CSV) file, with a standard format where it labels the columns. And if you are really determined to, you can go somewhere else. But I see no reason to do that today.

Leo: Yeah, one of the problems I've had, and I've ever since this news been looking at alternatives, is it's not that I trust - there's no one else I trust either.

Steve: Yeah.

Leo: So the only clear path is something that's much less convenient, which is an open source solution like KeePass, where there's no trust needed. It is a true Trust No One solution. But those are not nearly as convenient or as easy to use.

Steve: Yeah. Yeah. And then you have the issue of it being maintained across multiple platforms. I mean, the commercial side of LastPass is what has financed the convenience that we all see. And it's funny, too, because Joe mentioned that this podcast played a big role in their early traction. And I was put in mind of Hamachi, which of course Hamachi Dave, as we used to call him, we had him on the podcast. He may have been our very first guest on this show because once again I understood the technology, I loved what he had done, and he said himself that we put him on the map. Unfortunately, we put him on the map, and LogMeIn sucked him up. And so now we're two for two. I think maybe if we find something else that we really love, we just kind of have to whisper it a little bit more and somehow keep it within the family. But then, you know, not have it go, like, big-time because then LogMeIn comes and sucks them up.

Leo: Well, I'm glad we got to talk to Joe.

Steve: Yeah.

Leo: And I guess for the time being, there's no reason to change for the time being because there's nowhere to go, really. And there really is no reason not to trust so far.

Steve: I think that's exactly right. I understand there will be people who just, you know, they don't like it. And it's like, well, okay. If listening to Joe, if listening to us, you don't like it, then there are lots of alternatives, and I just pointed you toward the exit door, showing you how to create a comma-separated value file.

Leo: Right.

Steve: I don't think there's any reason to leave. I see no reason at all. And, for example, in the case of Hamachi, which is a sore point because of course shortly after the acquisition - and I don't know any of the details about like what was going on behind the scenes, what was happening with Dave, or anything. But of course it just collapsed. It failed to be updated. All kinds of problems began occurring. And, I mean, again, I don't know anything about the background. But I think what we need to have is, for something like our password manager, a zero-tolerance policy. And Joe and company, his company, have never given us any reason to bolt, or we would have.

Leo: Right.

Steve: So I think until we're given a reason, this is the best, still the best password manager that is available. And again, if other people feel differently, I completely understand that. But I'm staying.

Leo: Yeah, the problem is, you know, it's not change. It's LogMeIn is really the problem. Had he sold it to a trusted company, that might have been a different thing. But LogMeIn's track record is just not great.

Steve: Yeah.

Leo: I hope that they let him - I hope they understand the importance of the trust that he's built, and they let him continue to run the company autonomously, give him the resources he needs. I feel as long as Joe is there, that will be to me the canary in the coal mine. If Joe disappears...

Steve: Yeah.

Leo: Then I'm going to move.

Steve: Yeah.

Leo: But as long as Joe is there, I feel like, well, and that's why I asked him for that commitment. You'll continue to maintain this integrity as long as you're there; right? And if you don't, if you can't, if you won't, if LogMeIn says, no, no, guy, we're going to sell these addresses to the highest bidder, then you will leave, and we will know. And I should have probably made that more explicit, but...

Steve: Well, and you're right about LogMeIn. I did a little poking around in the last couple days because I was curious about this backlash. And, for example, they once, on their Facebook page in 2011, said we receive a lot of messages - this is LogMeIn. This has nothing to do with LastPass. LogMeIn: "We receive a lot of messages thanking us for making LogMeIn free." Or, I'm sorry, LogMeIn Free, free, because that was the name of the product. And they said, "Let's make this official. There's no need to thank us. LogMeIn Free is and will always be free."

Leo: [Mimicking buzzer]

Steve: Uh-huh. "For today, you can just pay us in 'likes,'" they said. And then a couple years later, on their blog on LogMeIn.com, it was titled, "Changes to LogMeIn Free." And it reads: "After 10 years, LogMeIn's free remote access product, LogMeIn Free, is going away. We will be unifying our protocol," I'm sorry, "unifying our portfolio of free and premium remote access products into a single offering. This product will be a paid-only offering." So it's like, okay, you know, they're on the record of not living up to their own commitments.

Leo: Right.

Steve: And so, and even on MacBreak Weekly, when you were talking to Alex, Alex sort of like, "Uh, well, uh, you know, I've had some bad experiences with them." So again...

Leo: I think that really is the source of all this...

Steve: Angst.

Leo: ...upset, yeah. And it's, I think, completely understandable. But, and I should also point out I've been through acquisitions. There's always a honeymoon period. And the companies always say, oh, we're not going to change a thing, until they do. So we just have to watch; right?

Steve: So I would say this has probably been good for Joe and company, that is, to witness this. I didn't verify, but some people said that they shut down posting to their blog announcement because there was so much negativity from their users. And, yes, I completely get it that this is a vocal minority. This, however, are the opinion-leading minority, the people who know what this means and care. We're the people that drive, you know, Jenny's using LastPass because that's, I mean, and everybody I know is because that's the one. And so I think maybe it's been good for Joe, and one step removed, for LogMeIn to understand that behavior really counts here. And as you said, Leo, there's lots of alternatives. I'm still happy here, but everybody is watching.

Leo: Yeah.

Steve: And so I think, again...

Leo: I think you're right. I think, if he wasn't clear about that before, he is now; right?

Steve: Right.

Leo: He's learned, oh, my god. But that's good, in a way. I mean, it really shows people love LastPass, and they really want to use it, and they want to keep using it.

Steve: Yeah. And as I, in my notes and in a conversation with him, it is all about trust.

Leo: Yeah.

Steve: This is our entire Internet online experience we're trusting to a third party. We're saying, well, yeah, we're saying, encrypt this in a way that we believe you cannot, no aberrant employee can decrypt it, and put it in the cloud, and we're going to trust you with it. All of our website passwords. So it was difficult to create that bond of trust from the beginning. And it's fragile. It's brittle. So I think both LastPass and LogMeIn need to understand that we're here as long as things continue as they have been. But there's a zero tolerance policy on our end.

Leo: And if you keep listening to this show, I guarantee you, you'll hear if there's a problem, yeah. I'm going to look at - I'm going to set up KeePass, the open source solution, and just see how much harder it is. I know it will be less convenient, but let's see how much harder it is. And of course, you know, if you're carrying about a USB key with your password vault on it, that's maybe not such a good idea, either. So, all right. What's in the news?

Steve: At least you'll be as clean shaven as I am.

Leo: You'll be as clean shaven.

Steve: That's right. So, Patch Tuesday. And when I was putting things together this morning, there had been no update yet. So I left a little spider on their page. And I have to tell people, I've mentioned it before, but this thing works so well. And now I've forgotten what it's called. But if I right-click on this tab, it's called Check4Change, with a numeral "4," Check4Change. It's a Firefox add-on. And when you're on any page, you highlight a region that you care about, and then you just - you right-click on the tab, and then you tell it, check every minute, or maybe it's even every 30 seconds, every minute, every five minutes, every 10 minutes and so forth. And it automatically refreshes the page and sees whether that marked region has changed. And if it has, it plays an annoying audio file, "ch-ch-ch-changes, da da da da." And it's, you know, very short.

Leo: It plays Bowie? Oh, my god.

Steve: Anyway, so like when I'm waiting for the Apple Store to come back online and be the first person to purchase a new i-something, or the other day I was waiting for - it was to go see "The Martian." I was waiting for the theater that I wanted to see it at to refresh their schedule, and I wanted to immediately nail the reserved seating that I wanted. And just this morning on the Microsoft page I marked the top of their table that showed September's updates, and then said "Check every minute." And the moment that page changed, I got "ch-ch-changes." And it's like, okay, good. And so now I have - I'm able to tell our listeners. But anyway, Check4Change. It's just innocuous. It sits there. But any time you, like, care about knowing when something changes, this does it. That's perfect.

So we have six patch bundles, and they're split, three critical and three important. There are two critical problems which - and one of them is a little blood-chilling. So this is high up on the list of update your Windows. The good news, though, is the blood-chilling one is only Vista and Windows Server 2008, nothing later. Presumably XP. I don't know that for sure. They don't tell us because of course that's unsupported now. But what this is, the reason this is a little chilling is this is a remote code execution vulnerability in Microsoft's implementation of JavaScript, or as they call it, JScript, and VBScript, which of course is completely exposed to the Internet.

So we've been talking lately about attack surface, and this represents a frightening attack surface. And Microsoft said of this, with the same sort of jargon we're used to from them, but there's some interesting stuff in here: This security update resolves vulnerabilities in the VBScript and JScript scripting engines in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if an attacker hosts a specially crafted website that is designed to exploit the vulnerabilities through Internet Explorer." It says in parens, "(or leverages a compromised website or a website that accepts or hosts user-provided content or advertisements.)" So find one that doesn't, in other words, all websites,

"and then convinces a user to view the website."

Now, yes, those of us with adblockers, we're being protected because we're not receiving script in these ad blanks which our browsers are then receiving. "An attacker could also embed," Microsoft continues, "an ActiveX control marked as safe for initialization in an application or Microsoft Office document that uses the IE rendering engine to direct the user to the specially crafted website." And then it goes on.

But anyway, point is there's a bad one here. It's not in the wild. It's not being exploited. But we now know that the way, the course this will take is that bad guys who see something as juicy as this is know that they've got some window of opportunity, especially if this goes back to XP, as I suspect it probably does. It looks like it got fixed in the jump to Windows 7 and Server 2000 R2, or, I'm sorry, 2008 R2 and subsequent. But probably this is XP. Those are not being patched any longer. And there's a dwindling population, but they're still around. Does need to have access to IE. So those would be people using, what, up through IE8 I think is where it stops.

But still, the point is they will examine the patch, reverse engineer what changed, and then figure out what was not known at the time of the patch. It will become known afterwards. And for something like this, this looks like it's an easy way into Windows machines. And Windows machines are not being kept patched. So you don't want to be one of those. Again, XP and Vista and Windows Server 2008 only, nothing subsequent. And of course those numbers are dwindling, too.

This podcast's chosen power user adblocker got updated with the one feature that it needed. So I thank those guys for that. And that is - so of course we're talking about 1Blocker, which is the fancy one. They added easy access site whitelisting so that, when you're in Safari, you touch the little "send the page somewhere" arrow, whatever that's called, which pops up a list of things like that you can do with the page. And it's now possible - it was not turned on by default, so you'll have to go into the dot dot dot at the end of the far right-hand end of the list. That opens up the dropdown of switches. And then down at the bottom it'll be switched off. So you probably want to turn it on and then use the little drag bars to drag it all the way to the top so that it then appears as your first choice.

So I had some fun with it today, for example. I was on Google, and after updating to 1.1, I whitelisted Google and then went into 1Blocker. And the thing I like about it, the reason it's the power user's choice, is there under whitelisting was www.google.com, with its own little switch. So this is, you know, the other adblockers are preferred for just set it and forget it, simple sort of users who don't want any extra features. And Purify is our choice there because it does have whitelisting, and it is a sort of a set it or forget it. But for the typical Security Now! listener, being able to, for example, browse your whitelisted apps and say, oh, why is that in there, and then, like, turn it off or remove it, this gives us that kind of power. So I wanted to let people know that 1Blocker v1.1 is out, and it's got easy whitelisting.

And I did, in listening to MacBreak Weekly just before this, Leo, I heard Rene give a shout-out to Tweetbot v4. And I say, oh, thank god, yes. I've been using it for a couple weeks. The Tweetbot for the iPhone had been kept kind of current. But the version for the Pad had, you know, they hadn't fixed it for years. And so things like the new free size DM'ing was not available. And there were just a whole bunch of other annoyances with it. And it's back, and I'm so pleased. Tweetbot is my Twitter client for iOS. And I use TweetDeck in Firefox on the desktop. I just think it's the right one.

So there was some concern, late toward the end of last week, about so-called "freestart collisions" are what they're called, in the SHA-1 secure hash algorithm, which a large percentage of sites are still using. And I'll say I'm there, I'm among them. GRC currently has my certs signed courtesy of DigiCert with SHA-1, but those certs expire on December 31st of this year. That's the only way to slice this so that Chrome is not punishing GRC and frightening its users, yet people who still need SHA-1, that is, who don't have clients which understand SHA-256, are still able to use GRC. I already have SHA-256 certs. Actually DigiCert made both for me. They made midnight on New Year's Eve expiring SHA-1 certs. And I already have my regular ones. And so a day or two before the end of the year I'll switch over.

And so GRC will never be down, but I will have waited, I will have extended GRC's availability for down spec clients to access my site securely because the only way you can access it is securely. That was the point, is that you can't get to GRC anymore other than HTTPS. So I didn't want to cut people off prematurely, even though Chrome started scaring people about it.

So years ago Bruce Schneier predicted when, based on the rate of increase in processing power and the level of difficulty that we know that SHA-1 hash has, when sort of the lines would cross so that it would become technologically feasible for a nation-size, nation-state actor to put the screws onto SHA-1 with lots of processing power, that is, in terms of what it would cost, and be able to deliberately forge a signature. That's what this is all about. This all comes down to signature forging because, if somebody could forge a signature on an SHA-1 signed certificate, then that allows the certificate itself to be forged because it's the signature that protects the certificate.

So Bruce's guess, and this was, like, maybe five or six years ago, was 2017 at the earliest, maybe 2018. Well, what's happened is that processing power, or the cost of processing power, has fallen, thanks largely to GPUs and ASICs. And a lot of this, of course, has been also driven by the Bitcoin phenomenon that no one could have predicted, that put a huge amount of resources behind increasing hashing performance.

So researchers will be shortly releasing a paper where, for the first time, a non-reduced-round SHA-1 compression function - which is not the whole SHA-1 hash, but it's the meat of SHA-1, the so-called "compression" function, a non-reduced-round - they have been able to synthesize, academically, a collision in that function using a 64-GPU cluster with 10 days of work. Now, this is not the same, and they acknowledge this, as a full SHA-1 collision, because that would require the entire hash function. And there's a lot of preamble and postamble work on each end, on the incoming and outgoing of the compression function. But the meat of SHA-1 is this compression function.

Previously, so-called "reduced-round collisions" had been found. This is always the way it is. For example, even our beloved AES cipher, Rijndael, is, now, it's been a while since I looked at it, but it's something like 13 rounds. And it's a little scary when you see them saying, well, you know, an eight-round reduction is giving us compromised security. But this is all something the designers understand, and they're trading off additional rounds which slow down processing versus brute-force protection. The more rounds you have, the stronger it is. But at some point it's just stronger than you need, and so that's just wasted computational time. So that has all been set.

In the case of SHA-1, this is a bit of a surprise. So again, this is not the whole hash. It's not like SHA-1 has been cracked or hacked or broken, or somebody found a magic key to it or anything. It's just that we really do have lots of processing power. The processing power is getting less expensive more quickly than we, and then Bruce six or seven years ago, anticipated. And so what that means is that we're moving the time at which it would become cost-effective for somebody who really always wished to pay for compute time or for hardware or whatever to create a spoofed certificate.

Now, people could argue, oh, the NSA has got all these resources and super crypto everything. It's like, yes. And they also probably have control over a handful of certificate authorities that all of our technology trusts implicitly, so they don't need to forge anything. They can just make their own certificate because there's no doubt that all of the major nation-states have control over certificate authorities that are signing certificates that we trust. We have to assume that that's the case. So these are more other actors who it's suggested for a cost of $100,000 of computing cost could do something like this, although that still isn't allowing them to create a fraudulent certificate. Anyway, so the point is this argues that the sunsetting of SHA-1 in a timely fashion is an absolutely good thing. This is another milestone along the path to its graveyard.

But what's interesting is, just before this announcement, on Friday, two Fridays ago, I think, what, October 3rd, some people at the so-called CAB Forum, which is the industry's certificate authority association, they put forth, for a two-week vote, the proposal to continue issuing SHA-1 signed certs through 2016. As it is now, the signing of new SHA-1 certs is due to stop at midnight at the end of this year. So certs can continue to live into 2016, although Chrome will frighten people, but they can. But the idea would be that no certificate authorities would issue any after midnight of New Year's at the end of 2015.

So the following motion was proposed by Rick Andrews of Symantec, endorsed by Bruce Morton of Entrust, and Judy Cloutier of Microsoft, oh, and Kirk Hall of Trend Micro. So four major participants and players in the CA Forum. So I'll just read a couple paragraphs of this so you get a sense for why. So they said: "The purpose of the ballot" - and the voting ends in three days, at the end of this week. And remember that this did, this was floated before the news of this SHA-1 weakness sort of frightened the industry.

They said: "The purpose of this ballot is to allow the issuance of SHA-1 certificates through 2016, with maximum expiry date of 31 December 2016." So they're still talking about - so it would have a one-year or less lifetime. "Although the vast majority of customers have been able or will be able to transition to SHA-2 certificates" - and remember that's like 256 because SHA-2 is actually a family of different size digest hashes - "will be able to transition to SHA-2 certificates by the issuance termination date of 31 December 2015," that is, the current termination.

They say: "A very small number of very large enterprise customers have disclosed to us that they simply cannot complete this work before the issuance deadline. This is attributed to the sheer volume of certificates that they need to migrate (numbering in the thousands), and their end-of-year blackout period." I don't know what that is. Maybe Christmas vacation. "These customers accept the risk of continuing to use new SHA-1 certificates and assert that, if they can continue to enroll for and receive SHA-1 certificates through 2016, all with an expiration date of 31 December 2016 or earlier, they will be able to complete the transition by the end of 2016." So basically a very small number of very large corporations are saying "We cannot be ready in time." Which must mean that they've got clients that cannot accept SHA-2 certs, and they can't fix those clients in time.

So then the CAB Forum says: "We realize that extending the issuance period will extend the collision attack period," meaning this is the problem of certificate collisions, which is what we've been talking about. "Although we feel that the BRs [as they call them], the Baseline Requirements, already mandate enough entropy, typically in the certificate's serial number, to guard against that attack." Now, of course that - we'll see how they feel now that this full non-reduced-round collision has been created. They say, "It can be further mitigated by limiting SHA-1 certificate issuance to subordinate CAs that have a basicConstraints pathLength of zero," meaning that those CAs are unable to issue them any further.

So they said, just finishing: "The intent of the ballot is to allow limited issuance of SHA-1 certificates through 2016, as long as any SHA-1 certificate created in 2016 expires by the end of 2016. We also correct the number" - and blah, blah, blah, it goes on. And this voting then ends this Friday. So I will keep an eye on this, just because I'm curious, and we will see whether people decided, eh, you know, this seems like a bad idea. It does sound like, I mean, it's not clear whether these are public-facing servers, or maybe internal, so they may be asking for non-public-facing certificates only for clients of theirs that they are, for whatever reason, unable to upgrade in time so that they're able to connect to servers with SHA-2 certs. In which case it wouldn't affect the broader public, and what Google does with the browser wouldn't matter.

But I just thought this was interesting and a weird coincidence that here as the deadline approaches we have not only an improvement in, another sort of proof of concept of, yes, folks, we really do need to get serious about moving away from SHA-1, and there being some entrenchment of why this is so hard to do. It's like the move from IPv4. It's like you just - people have to be forced to make this change for their own good. And so it'll be interesting to see how this vote turns out.

I did want to note that the Obama administration has opted for now not to force firms to decrypt data. Which is to say, the administration has decided that they will not request legislation making that a requirement. The New York Times, Nicole Perlroth and David Sanger, broke the story, and I'll just share the beginning of it because it's succinct.

They said: "The Obama administration has backed down in its bitter dispute with Silicon Valley over the encryption of data on iPhones and other digital devices, concluding that it is not possible to give American law enforcement and intelligence agencies access to that information without also creating an opening that China, Russia, cybercriminals, and terrorists could exploit. With its decision, which angered the FBI and other law enforcement agencies, the administration essentially agreed with Apple, Google, Microsoft, and a group of the nation's top cryptographers and computer scientists that millions of Americans would be vulnerable to hacking if technology firms and smartphone manufacturers were required to provide the government with backdoors or access to their source code and encryption keys."

So, boy. I mean, it was not only the right decision, but the correct understanding of the problem. So I say, yay. And I made a note here. I said Security Now's take, our take, is even if they did, that is, force backdoors and so forth, it wouldn't matter since strong and unbreakable encryption is already and always will be freely available because it's just math. It's loose. It's late. It's too late. Even if it were outlawed, bad guys will always be able to use it, if they wish, because it's just math. And you can't take it back. It's already out there. So it wouldn't have helped. Anyone who needed to stay cloaked, could have, even if the manufacturers were forced to create backdoors, which as we've often said, there's just no way to see how that can happen safely.

So I went to PrivacyTools.io, and I got a big kick out of the top of the page. Our listeners will remember PrivacyTools.io was the site that I stumbled on, thanks to somebody who tweeted to me about it, asking for what I thought. This great compendium of all things like - it's a recommendation site of privacy-related tools. And the huge, on the page, top of the page is their feelings about Windows 10, which I got a big kick out of. You know, listeners of this podcast can imagine what's there.

But I saw something, a quote, that just hit me between the eyes, that Edward Snowden posted on Reddit about four months ago. And I want to share his whole statement from which one line is like, I think, just perfect. And this is regarding privacy. In my notes I called it "Another way to look at privacy." This is a whole, I'm not overly concerned about privacy because I have nothing to hide approach.

So Snowden wrote: "I think the central issue is to point out that, regardless of the results, the ends (preventing a crime) do not justify the means (violating the rights of the millions whose private records are unconstitutionally seized and analyzed).

"Some might say," wrote Snowden, "I don't care if they violate my privacy; I've got nothing to hide." Snowden says: "Help them understand that they are misunderstanding the fundamental nature of human rights. Nobody needs to justify why they need a right. The burden of justification falls on the one seeking to infringe upon the right. But even if they did, you can't give away the rights of others because they're not useful to you. More simply, the majority cannot vote away the natural rights of the minority."

And finally he said: "But even if they could, help them think for a moment about what they're saying." And this was the phrase that got me. "Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say." So I just - that just hit me because the point being that I may not be concerned about privacy, but I absolutely know the world is full of people who are. And I won't have access to their honest thoughts and feelings and truth, and I'm interested in that, if they are muted because they don't feel they have the freedom to express themselves, because they're worried about the world that they're in from a privacy standpoint. So I thought that was a really great point. And so I wanted to share that.

And finally, before we take a break, I got a - I guess this was a - oh, I found it in the mailbag when I was going through the Q&A stuff, David in Montreal, Quebec. He wondered whether I use SpinRite myself. He wrote: "Hi, Steve and Leo. I know that your backup strategy is very good. But have you had a situation where you had to use your own product for maintenance or to recuperate data for any reason? How many times over the years?" And he says, "Thank you, and keep up the good work."

And I was put in mind of two things: the event which created SpinRite, like 25 years ago or however long it was, and then my most recent use. It was created when the hard drive at the company that my girlfriend owned, which was like, these were in the days when computers were, PCs were $10,000, and the hard drive itself was $5,000, and it was 10MB. And three years of accounting information that had never been backed up was inaccessible. And I had to get it back, yet it was inaccessible.

So that experience - I succeeded. That experience was what started me on the path of turning the quick code that I wrote in order to perform the data recovery for her into a commercial product. And then I had mentioned it before, I'll remind David and our listeners, that my most recent use was edge of my seat because my own operations officer, Sue, I had set her up with a full RAID-based system, with drive mirroring, so full redundancy. And the RAID began complaining, when she booted her system, with a critical failure of the RAID, because one drive had died. And then unfortunately, under the critical message, it said: "Press Escape to continue." And so she didn't want to bother me, so she tried pressing Escape. And, oh, what do you know, the computer booted. So that's what she kept doing. Every time she needed to boot, she'd get the critical error message. But, well, apparently it's not that critical.

Leo: Still works.

Steve: Yeah, boy. Until, of course, that fated morning when that drive died. And I got email from Sue saying, "My computer has crashed. I can't get in." And so forth. So it's like, oh, no. So, and I thought, okay, wait a minute. How could this happen? You know, because she's got a mirror, and we would know. We'd have lots of notice. Well, yeah, like a year's worth of notice, as it turns out.

Leo: Exactly.

Steve: But if you ignore the notice, or if you don't understand what it means. So, I went down, and she said, oh, this'll come up and say "Critical error." But if you just hit Escape, normally it goes past it.

Leo: Oh, my god.

Steve: And I said, "What?"

Leo: What?

Steve: So I brought the computer home. I set it up. And I did what everyone who knows does. I became a SpinRite user. I mean, I didn't have to reach very far for my disk. And I booted SpinRite, and I let it run overnight. And in the morning everything was fine. Now, yes, she was all backed up. She was in the cloud. We have nightly backups of the accounting system and so forth. But as everyone knows, you still have to rebuild the system and then reconstitute it and then restore it and all that. It's just - and then you've got the changes that occurred since that backup.

So it's just better if you can get the disk recovered. And so, whew. I did, and we all learned a lesson. Sue now knows how close we came. Like we were right on the edge. It complained for a year. And I really learned, too. RAIDs that are in front of consumers, they need to stop working when the first drive dies. Even though, you know, it's the IT people that cross themselves and say, thank you for there being redundant drives. We know what to do now. But the consumer, when the first drive gives up, that's when it needs to say, okay, you can't, sorry, no computer today. Call your computer person, and they'll know what to do. So David, that's the story. Yes, indeed, it is my goto tool when...

Leo: It's a true story.

Steve: When it hits the fan.

Leo: All right, Steverino.

Steve: Yay.

Leo: Time for Q&A. This has been a jam-packed episode, hasn't it. Holy camoly.

Steve: Everybody's getting their money's worth today.

Leo: Yeah. That's one way to put it. You're getting your money's worth.

Steve: That's right.

Leo: You get your money's worth. If we just show up you're getting your money's worth since we charge nothing. Let's see, today, questions...

Steve: That's right. They can get a refund if they're not happy.

Leo: Yeah, we'll give you - every penny you pay comes back to you. Let me go full screen. This is Question 1 from David in Washington State. Maybe he's from Walla Walla, I don't know. He writes that "a friend of a friend" may be a reason to "_optout" of WiFi Sense: In Episode 527 you stated that renaming your WiFi SSID to include _optout is primarily useful for owners of public hotspots. That was my guess. It wasn't based on anything I knew. He said: That's certainly true. But if you manually share your WiFi with a Windows 10-using friend, they could choose to auto-share your network's login with all of their friends, which may not be what you'd prefer.

Steve: Yeah.

Leo: So, in this Windows 10 world, if you ever give your network password to anyone using Windows 10, adding _optout to the SSID is probably a good idea. But as you point out, it's not as bad as everyone initially feared. But just so you know, that's the value of it. I didn't even think of that, yeah.

Steve: Yeah, I thought, yeah, I thought that was a good point is that Windows 10 has no way of knowing, when your friend enters your password, that it's not a system that belongs to the household.

Leo: Right.

Steve: And so, again, they would have to manually share it. But nothing prevents them from doing that. Or they may not understand that they don't have to turn that on. Who knows? So if they had enabled sharing on their, for example, their Windows 10 laptop, and for whatever reason got onto your network and then chose to share it, then it would extend out into their friend field unless the SSID had _optout in it.

So I think probably in the future, I mean, it's a shame that it's not opt-in. That would be nice. Then if you wanted to have your network automatically shared, you add _optin to the name, otherwise it defaults to _optout. I mean, I think that's the right way to do it. But that doesn't make it all just sort of magical and automatic and, oh, look, I'm already on your network, and you didn't even have to tell me. It's because we're Facebook friends. Oh, isn't that wonderful. Anyway, yeah.

Leo: Yeah. You can also opt out by not turning it on in the first place. And it asks you every time. But, yeah, okay. I have to check that thing, a friend of a friend shares it. Is that true? That doesn't sound - that isn't right, that just because you shared it with a friend, that they can share it with somebody else. That doesn't sound like a good thing to do.

Steve: And that's my point, is that Windows 10 has no way of knowing it's not your laptop.

Leo: Yeah. Dale Freye in Grand Haven wonders about "The Filter Bubble": In light of the recent focus on tracking our browser usage, could you and Leo say a few words about how this affects the search results we get when using Google? If you've read "The Filter Bubble" - that's Eli Pariser's book about this - what views does it put forward, and do you agree? Do you know "The Filter Bubble"?

Steve: I do, and you referred to this phenomenon on some other podcast on your network.

Leo: "This Week in Google," yeah.

Steve: Oh, okay. And I just thought, I thought this was a good - we've never discussed it on the podcast. But it is an interesting phenomenon. And that was the observation that, in Google's trying to provide you with, well, first of all, Google learning who you are, looking at your past history of searches and essentially working to be, to do, they say, the best job they can, when I search for something and you search for something and Dale searches for something, we actually get different search results because Google filters this through what it knows about us in order to try to select what we want.

And so, for example, take a simple black-and-white case, politics, where you've got

Republicans and Democrats, you know, left and right. You might do a search, and Google has algorithmically determined your party affiliation without knowing it, but just sort of by understanding that other people who have searched for things you've searched for have also searched for these things, so we're going to give you the same sort of results. Well, as a consequence, you end up with sort of a skewed view to the degree that Google is the Internet, and we've laughed about that and chuckled about it even last week, that many people don't realize Google is not the Internet because it's the way they have any visibility, but that it actually does skew individuals' views into the Internet.

Leo: Yeah, I mean, you can always, I guess, use the incognito mode, if you want. But then you wouldn't have your login there. Rick in Colorado feels...

[Crosstalk]

Leo: Go ahead.

Steve: I was just going to say, yeah. So Dale, I do agree that it is an interesting and maybe important thing to keep in mind, that as you say, Leo, somebody who very much wanted to get unbiased results just needs not to be known by Google. And are you sure that incognito - I know that it doesn't record what you do. But does it...

Leo: It says if you're not logged in.

Steve: Okay, good.

Leo: This only works if you're logged in, obviously, because it can't collect signals if you're not. And I'm not convinced the filter bubble is as dramatic as people say.

Steve: Is a big deal?

Leo: Yeah. I know Jeff Jarvis thinks it's not. But I'm not convinced. If you search, you can still search for anything you want. What it's trying to do is give you, in the whole, what Google wants to do is give you the best results for your interests, give you the top results for what you're searching for. And if it can add signals from other sources, including your own previous searches, it's going to do that. But I'm not sure that it really conditions the searches as badly as people might say. You still see other stuff.

Rick in Colorado feels that the iPhone fingerprint unlock is worthless: Someone can force you physically to apply your fingerprint to various sensors. iPhones can get around this by turning off your phone, after which you must enter your passphrase. He probably means iPhone users. If you turn off your phone, you have to enter your passphrase before you can use the fingerprint again. But why doesn't Apple offer a "fast lock" for their products? I would recommend that a different fingerprint be used as a method of instantly locking the phone so that it once again requires the entry of the passphrase. You agree?

Steve: So, well, this was an opportunity to talk about a couple features that people may not be aware of. First of all, the way the legislation stands at the moment, you can be compelled to relinquish a fingerprint because...

Leo: It ain't legislation. It's called the Constitution. That's the problem. Courts have held that the Constitution says, just as you can be asked for a fingerprint or your DNA, you can be asked to unlock a phone with your fingerprint.

Steve: Correct. However, the recent legislation has held that a user cannot be forced to divulge a passphrase. So passwords, something that we know is protected. Something that we are is not protected. So that's the first thing, I mean, to note. But the features that people may not be aware of is that there is granularity in the settings for the iPhone fingerprint. You can specifically disable its unlocking, yet leave its other utility in place. So if you go into Control Panel and Touch ID and something, I think it's lock screen or whatever that's called, there you'll find settings.

And there are three switches. Normally they're all on. The first one is "unlock the phone." So you are able to turn that off, if this was a concern of yours, then still use it to authenticate your identity to applications and iCloud and so forth while you're using the phone, after it's already been unlocked, but it won't - but your fingerprint won't take it out of the locked state. And we've talked about this, the fact that Apple requires an unlock, a passcode unlock, coming in from a reboot or power off.

And so, for example, if you were using your phone normally, the thing to do if, like, you were crossing the border, or entering some situation where it might be necessary or you might be subjected to forced unlocking, do just power down your phone. Sort of keep that in mind. And I will finally say that I use the full alpha keyboard. We know that with iOS9 they went to a six-digit passcode, but still better to use the keyboard.

For me, the whole keyboard comes up - and I don't have a big, fancy, impossible to type on a horrible touch keyboard. But I've got - but just because there are so many more buttons there, I type a few things, and my phone is up and running. The point being that the iPhone is very good about counting those guesses and shutting itself down if somebody guesses wrong. And so using the full ASCII keyboard, and something that is, you know, it doesn't have to be super long and difficult because it just means that it's going to be far more difficult for someone to guess.

Leo: It's the Fifth Amendment, your right against self-incrimination.

Steve: Ah, right.

Leo: So courts and the Supreme Court even have ruled that you can be compelled to give up physical evidence, like your fingerprint. If you're arrested, you can't say no, I'm not giving you my fingerprint. But that stuff that's in your head?

Steve: Right, self-incrimination.

Leo: That's equivalent of testifying against yourself.

Steve: Yes.

Leo: And that makes sense, doesn't it.

Steve: Yes.

Leo: Amazingly.

Steve: Odd, but I'm glad to know. And our listeners who are really concerned just need to understand that no one can make them tell, you know, give up a password. They can just say no.

Leo: Right, just say no. Or plead the Fifth. Conor in Castlegar, British Columbia asks - I don't know what happened with the accent there. Steve, it's the Castlegar. That sounds like Scotland.

Steve: Eh, just mix it up.

Leo: Steve, I'm running Windows 7 Pro and considering upgrading to Windows 10 Pro. But is there any privacy difference between paying for a new license or getting the free upgrade? Regards, Conor.

Steve: No.

Leo: That was a short one.

Steve: I thought that was an interesting question. You know, the idea being that, well, is the freeness of Windows 10's upgrade a tradeoff that you're making in divulging all this, the advertising ID and everything? And so, if I were to pay for it, could I not have that? And so the answer is, uh, no, that's Windows 10. That's the way [crosstalk].

Leo: There is one difference between the paid and the free upgrade. The free upgrade you agree to accept updates. You can defer them, but you can't prevent them. If you take the free upgrade to Windows 10, you are then bound to accept all Windows updates from then on. You can put it off...

Steve: So it might even - it might shut off or shut down or, like, say, hey, look?

Leo: I think that - yes, it might. I think you'd have a cause for upset if that happened. But I think the real intent from Microsoft is that they want to really get people to do automatic updates.

Steve: Yeah.

Leo: And one way to do that is to say, look, you've got to accept automatic updates if you're going to accept the free upgrade. That's just the deal. If you pay for it, you don't have to.

Steve: Hmm.

Leo: And I don't know, you know, that's because businesses, some businesses don't want to do that. But the free upgrade is only for consumers. Businesses still have to buy it.

Steve: Ah. And I wonder, I didn't even look, I wonder if the free upgrade lets you turn them off. They might have just taken the switch away.

Leo: No. Yeah, you can't. You can defer it. You can say put it off. I don't want to do it this week; let's do it next week.

Steve: Okay.

Leo: But you can't put it off forever. And actually I don't know what happens if you put it off forever. I think at some point they spank you. Have to ask Paul Thurrott about that.

Steve: Paul, Paul, yeah.

Leo: Kevin Schwartz, Kansas City, Missouri had a website security question: Steve and Leo, I've been a dedicated listener to Security Now! since Episode 1. Thank you both for keeping us up to date on what's happening out there. I want to share something with you and your listeners with regard to security questions on websites. I'm talking about those questions you provide answers to in case of a forgotten username or password. Leo has often said he never answers these questions truthfully because the correct answers might be available somewhere online or even known by someone you know.

Lately, I have been using LastPass to generate 30-character passwords for these answers. Good thinking. I put the questions and passwords into a secure note inside of LastPass for safekeeping and easy lookup. There are times when I've had to remove the option of including special characters because they aren't accepted. But with the 30 characters I use, I feel safe. Frankly, any random data would be fine.

Steve: Yeah.

Leo: Or even data you could remember, but just is wrong. I suppose you could even go longer than 30, but that's what I choose. I don't think anybody brute forces security questions. Maybe they do. I don't know. I know this might be a pain if you have to answer those questions, but it really does happen very often. I've got a story for you, Steve.

Steve: Oh, good. Let's hear yours first.

Leo: I was trying some password vaults.

Steve: Alternatives, yeah.

Leo: The No. 2 password vault, it's used by I think 13 million people, is Keeper. And I was somewhat taken aback when it said, oh, and now here's your security question. Because normally a company, good company like LastPass, says don't forget your password. We can't recover it.

Steve: Right.

Leo: Keeper says, oh, just tell me. And so one security question, and I can recover my password.

Steve: Ooh.

Leo: Now, that raised two problems for me. One is the security question in general. But, two, doesn't that mean they have access to my password?

Steve: I mean, I could - there could be something in Keeper which uses your answer to the question to decrypt the password.

Leo: Okay. So you'd need to know the answer.

Steve: Right. You'd have to have the exact answer. Then it could decrypt using that answer as the key to its encryption. So I could see how it could be done right, and let's hope that that's what they did.

Leo: But it's inherently done wrong, and there shouldn't be a security question, period. That's a huge security hole; right?

Steve: Yes. I mean...

Leo: Because most people are going to use mother's maiden name, and boom. That's the password to your master vault now.

Steve: And the problem is it's always struck me as being a soft answer, that is, wait, did I spell my teacher's name with a capital letter or not? Did I put his full name? Because I remember his first name. Did I say Mr. Fearon or Harold Fearon? He was my electronics teacher in high school. You know? And so, I don't know, I've never been really comfortable with those. The kick I got out of this question that Kevin asks is he's using LastPass, which prevents him from ever needing to remember his password...

Leo: Right. Occasionally the banks will use secret questions, even if you knew the password.

Steve: Oh, that's true. They'll just say, you know, we're tired of accepting your password on blind faith, so prove us that you still remember your mother's maiden name. And lord help you if that's the question that you chose. So anyway...

Leo: And somebody's point out, LastPass has a time-limited password recovery. When you create a new password, you have 90 days if you forget it. But the way they do that is you have to know the old password. So clearly they used the old password to encrypt the new password.

Steve: It's called a bootstrap, yes, so you're able to bootstrap yourself. And again, every step of the way, everything Joe has designed, he's, like, he's clearly spent some time.

Leo: Very thoughtful, very thoughtful.

Steve: And then what is the least exposure that we can have, which is exactly what we want, yet we can offer the service to our customers. And clearly, LastPass exploded in popularity. People who are not super savvy, like Jenny, my Jenny, is using it. She might mistype her new password, or forget what she changed it to, but still know her old one. And so Joe is like, okay, wait a minute. We don't want, we do not want this information. But what's the perfect tradeoff? And the perfect tradeoff is a forgiveness period where, until it expires, we'll forgive you if you forget the change you made. But otherwise, after that point, you've proven you have the new one. So now we're going to forget the old one. I mean, that's brilliant.

Leo: Right.

Steve: That's exactly what you want.

Leo: Yeah, I think so, yeah.

Steve: Yeah. So it's why I continue to be encouraged that they're going to, you know, that they're the right choice. Let's hope it remains so.

Leo: Jim in Chicago comes to us with Question No. 6 - that's no language. There's no language that says that. Jim in Chicago, Illinois wonders about adblocking at the network level: Steve, you and Leo have done a great job covering adblocking in iOS from every possible angle. However, those adblockers only work on an iPhone or iPad. Is there a way to block ads across an entire network? I have a ASUS AC3200 router, same as Leo, I believe - yes, love that router. And I've looked for ways to block ads at the router level, but I haven't figured out how. So how?

Steve: Okay. So first of all, it's probably not going to work for long. As we predicted, the first response to the increase of use of adblocking will be that sites will detect it. And as we know, there's already a publicly, or at least a privately financed, but a venture financed company that is offering this as a service. So it's even been subbed out so that a site can say, okay, we want a service to detect adblocking and notify people who visit our site that, like, either blank the site or beg them or whatever. There is a range of things they can do.

So the point is, I don't think it will be feasible to operate without the ability to whitelist. And a network-wide facility is going to make whitelisting more difficult. But the way it's done is with DNS, the idea being that all of the devices in your network rely probably on the DNS that they receive from your router. Routers certainly do provide the DNS IP. They may provide their own IP, in which case everything in the network asks the router for the IP address of a given domain. Then the router turns around and asks the DNS servers that it's been configured with, so it's a proxy for the network's DNS. And then it returns the answer to the requester.

Or a little bit sort of older school is that the router will simply pass on the DNS IP addresses that it's received from upstream, or that it may have been overwritten with. You may, for example, want to use Level 3's DNS or Google's or OpenDNS or some other DNS. So you can tell your router, offer the following DNS, or use the following DNS for your queries. The point is that's the way to do it. There are, you know, the way these adblockers work, these lists of adblockers or lists that the adblockers use are just domain names. DoubleClick.net is just, all you have to do is say that that's a bad domain name, and everything in your network will fail to look up the IP of DoubleClick.net and won't be able to retrieve any ads.

If you want to pursue this, though, there is a very nice solution based on a Raspberry Pi. It sort of combines the name Raspberry Pi and the notion of a black hole because essentially you are, and this is the networking term, you're "blackholing" those domain names. You're telling this set of domain names, go nowhere. We don't want lookups to those domain names to succeed. They are blackholed. So the project is called "Pi-Hole."

Leo: As in shut your.

Steve: As in, yes.

Leo: Shut your pi hole.

Steve: P-I dash H-O-L-E dot net [pi-hole.net]. And this is a nice little project. You spend, what, 20 or 30 bucks for a Raspberry Pi. You use this software. It turns it into an advertising-aware DNS server.

Leo: Ah.

Steve: So that it sits on your network, and it provides - it fields all of the DNS requests within your network. And it is updated in the same way that our adblockers are updated, in the background, with any new additions or removals from the list. So it's a nice, simple way of performing network-wide adblocking and, for 20 or 30 bucks, the cost of a Raspberry Pi, provides Jim what he wants. So it was cool, and I thought that would appeal to a subset of our listeners, so I wanted to make sure everyone was aware of Pi-Hole.net.

Leo: So really somebody, some enterprising person, could set up a DNS server that does the same thing, and all you'd have to do is change your router to point to that. I wonder why no one's done that?

Steve: Actually they exist. You can also google "DNS adblocking," and you'll find all kinds of projects like that.

Leo: Yeah, I mean, I just need a number. OpenDNS could do it, for instance.

Steve: Yeah. They're unlikely to, of course, because they're too high-profile.

Leo: Yeah.

Steve: But some sort of off the beaten path, somebody who's got a real thing. The problem is I expect it's going to be infeasible, and that's why I led with that, is you'll hit a site that refuses to let you proceed. And now you're stuck because you don't have the ability to whitelist because somewhere else in your network a DNS server is refusing to give you the IP for that site. So I wanted to let everybody knows it exists as an option. But unfortunately I think that local blocking that allows local whitelisting is probably going to be the solution.

Leo: Yeah. Steve Bourgeois in Paris - I wonder if that's really his name - wonders about web encryption strength: Hello, Steve. I've been trying to find an alternative to LastPass after the latest announcement. So I checked the two next in line, which are supposed to use the same process, Dashlane and 1Password. They both advertise an AES 256-bit encryption process. But when checking the Dashlane website certificate, it was AES-128.

Support replied: "Oh, AES-128 is just the way our website's encrypted before being transmitted and displayed in the user's browser. AES-128 has nothing to do with the data of our users, which is encrypted using AES-256." But when I upload updated data via my browser to my vault on their site, isn't the data transmitted at AES-128? Could you please explain? Sorry for my noobness in this matter. I like to listen to your show, even if I'm lost some of the time. Steve from Paris. Yes, I am French, and I am called Steve.

Steve: Or Esteban, I think, probably.

Leo: No, that's Spanish.

Steve: Oh, that's right, that was my Spanish name. I don't think I ever knew what my French name is.

Leo: Esteban. I like it.

Steve: Anyway, okay. So there's a couple things here. I'm sort of trying to decide which to do first. First of all, 128 bits is what pretty much everybody is using now. The various encryption systems - LastPass, Dashlane, 1Password, whatever - are using 256 just because they can. It's, I mean, there is no 128-bit AES. Is there? I don't think so. I think there's, no, 256, 384, and 512 are the three different key lengths. But a 128-bit key is still just fine. It's what the web is using. For example, if you go to Google, of all people, https:// because Google is now HTTPS, just bring up the Google page. And then look at the certificate details. You will see AES-128 is the cipher that they used, meaning a 128-bit key.

So from a practical standpoint, to address that aspect first, 128 bits is nobody is worried about that today. It is absolutely fine. We're hoping to be with AES for a long time. So that's why 128-bit keys were not part of that competition. We went 256, 384, and 512, which will last us, you know, we will know about aliens by the time AES-512 is a problem because even though the key lengths are only doubling, that is, the point I've tried to make is, you know, every bit you add doubles the difficulty. So we've added, to go from AES-128 to 256 is - wait a minute. AES-128. Is there a 128-bit AES?

Leo: He's probably just confusing SSL.

Steve: He might be.

Leo: That's where he gets the 128.

Steve: Or it might not have...

Leo: Yeah, there is, there's an AES-128.

Steve: Okay. I'm sorry, it's been a while since I've looked at the protocol.

Leo: Yeah, yeah. AES-128, 192, and 256.

Steve: Okay. Those are the three. So I was up by a factor of two. So, yes, 256 is there because we can. So that's AES-128 that nobody is worried about. That's what all of our Internet use is often being encrypted by, if that's what the client and server agree to. 256 is there - oh, I know, I was confusing it with hash lengths because there are longer hashes. 256 is there because it was part of the spec. And so in creating these systems - LastPass, Dashlane, 1Password - they're like, well, more is better. More is going to make our users feel better. So let's make them feel better. Let's use 256. Absolutely no benefit today because, as I was saying, if you make the cipher stronger than it absolutely needs to be, you're just spending time computing. But there's no reason not to.

So first off, AES-128, just fine. That's what the web is using. But the tech support guy who talked to you, Steve, did say it correctly. That is, assuming that those other products work the way LastPass does - and I'm not vouching for them, I haven't looked at them, I don't know them, I know LastPass - LastPass absolutely pre-encrypts the data that they're sending. So you would never want it to be over an unencrypted connection because that would also be unauthenticated. And we absolutely care about the authentication to make sure that we are talking to LastPass's servers, even though this blob is encrypted.

So the blob of our vault is encrypted in all these cases with 256-bit encryption, even though that's way more than necessary. Then it is sent over a 128-bit encrypted channel which, again, is plenty. We're pre-encrypting it, not because we're worried about it in transit, but because we never want to give it to the other end in a non-encrypted form. That's why we encrypt it before we send it. So it actually is the case that the channel's security matters much less. But 128 bits is just fine.

Leo: Don't worry, in other words.

Steve: Yeah. And I was thinking about SHA because, for example, SQRL uses SHA-256 and 512 at various points. So that's what I was - I was confused between that and AES.

Leo: Yeah. Paul in London, Ontario, Canada wonders about Dynamic DNS providers: Steve, great show. I listen to you and Leo every week without fail. Great podcast. I've been looking into Dynamic DNS providers and was wondering if they are more secure than my ISP DNS, and if it's a good idea to use one. I have a Netgear Nighthawk R7000 router, and they have partnered with No-IP to provide this service. Are there any advantages or issues with doing this? Thanks, Paul.

Steve: So, Paul, these are sort of two different things. And so I thought I'd take this opportunity to explain. What Dynamic DNS is used for is for any situation where the endpoint may not have a fixed IP. So, for example, all of us, and I'm including myself now, having lost my two T1s, I'm now a cable modem user, my IP never changes unless I disconnect my router from the 'Net for a long time. Or typically it just doesn't change. So it's largely static. But it was an IP that the DHCP client in the router received dynamically from the ISP. So it can change, and it has changed since I began using the cable modem, for example. It's changed a couple times, but only as a result of major upheavals of things.

So the idea is you, your home has an IP, but it might change. And say that you had an OpenDNS server running on and deliberately exposed publicly so that, when you were traveling, you could use OpenDNS to create - I'm sorry, not OpenDNS, OpenVPN. You had an OpenVPN server running on your home network, so that you could use OpenVPN to log into your OpenVPN server at home to access your internal network. I actually have a setup like that. So it's one that's very convenient.

The problem is, what if you were away, and the lease expired on your router's public IP, and as can happen for whatever reason, it obtained a different IP. Normally the lease expires, and it says to the ISP server, hey, I used to have this IP, my lease is expired, what's the story? If the ISP had some reason to move your IP, they could. Normally they just reissue the same IP, just sort of for the sake of letting everything stay the same. But there's no guarantee. So if you were away from home, and your lease expired, your home's IP that was available to the public would change, and you wouldn't know what it was. You would not be able to log into your network.

So that's the problem that Dynamic DNS solves. And that's why it's in your router, is your router partnering with the No-IP service means that your router will inform No-IP if its IP changes. And No-IP is a DNS server and service where you can create an account with them and say, paulinlondon.noip.com. That would be a sort of a pseudo domain name. And, I mean, it's a real domain name, but it's sort of like a machine underneath the NoIP.com. So paulinlondon.noip.com would resolve to your router's IP, even if that IP changed.

So what this whole thing is, is it's a means for anyone who needs remote access to a network whose IP may change to have that change tracked by a service that they're able to ask, essentially, uh-oh, what is my current IP? And this system makes that happen. So this is not at all the same as your ISP's DNS, which is why the question of is it as secure as your ISP's DNS, it's just an entirely different thing. Your ISP provides lookup for all IPs that are on the Internet based on name. This is a facility that allows your IP to sort of be mapped into a domain name that you would use in order to always be able to find your network. And most of the high-end router firmware allows Dynamic DNS support. Basically you give the router the information, your account information, and it's able to update that public provider with any IP changes that it experiences. Very cool.

Leo: And I suppose in these days of limited IP addresses, you probably can't count on having a static IP address. It must probably cost a lot. I haven't looked. But I can only imagine.

Steve: Yeah, I think, for example, Cox will, for example, the business services version will give you a static IP, and you just pay more for it. So if you absolutely needed one, you could buy it. At this point I have no need for it, so I'm just not worrying about it. But it...

Leo: Right. And you know what, my experience has been, and a couple of people are talking about this in the chatroom, it's rare that your IP address changes.

Steve: Yes, it really is.

Leo: They reserve the right to do it, but I don't think they ever do. Or maybe it's just a way of getting you to pay.

Steve: For example, I did something, I guess I changed cable modems and routers at the same time because now I'm using a pfSense-based FreeBSD router. In that change, my IP did change. So I was off the 'Net, needing to pair with a new cable modem. And I think it was the new cable modem, in fact, that Cox sort of thought, oh, whoa, what, okay, and just gave me a new IP when I came back up. But since then, absolutely rock solid. I can't really - unless they were, for example, say that they needed to migrate their huge block of users off of a certain chunk of IP space over to somewhere else, for some network architecture means. They would have the ability, knowing that leases are going to expire, typically it's a 24-hour lease that you receive, they would know that they could force the migration. It would upset some things that were sensitive to it. But generally not.

Leo: Are you ready? Because Ben Shipley in Atlanta, Georgia wants to get quite techie: I've been a continuous listener since 2011. I am an undergraduate student in the Atlanta area. In my hardware/software concepts class, my professor has asked the class to figure out - oh, he's going to have you do his homework.

Steve: He is.

Leo: Why a VPN software application would use UDP for communication between a PC and the VPN concentrator. I have found no mention of this in our class textbook - Irv Englander's "The Architecture of Computer Hardware, Systems Software, and Networking: An Information Technology Approach" - so I figured I'd consult the legend himself. See, he throws in that little, that praise, a little bit of - you're a legend, Steve. Surely.

Steve: That's right.

Leo: And then he says, "Steve, do you know?" Of course Steve knows.

Steve: It just so happens. Of course...

Leo: I think that it's not in the book. It's an exercise in logic. You should be able to figure it out; right?

Steve: Actually, well, you would really have to pretty much have a grip on how networking works. It's something that we've talked about because it's an interesting fact. And that is that TCP, which is the normal communications protocol, which you would expect to use, it has a - what it guarantees is when you send packets in one end, they come out the other end with none lost, and in the same order as they went in. So lost packets end up getting detected because the far end doesn't acknowledge their receipt, and so the sender always holds onto the packets it has sent until they've been acknowledged by the other end, so at that point it's able to let go of them. But it holds on, it holds them, it buffers them until it gets that acknowledgement of the highest byte number of any packet the other end has received. That's the guarantee that TCP provides.

UDP has none of that. UDP is we squirted off a packet, and we don't know what happened to it. We're not worried about it. It's gone. So, and here's the trick. This is going to get you an A, you and your class, on your homework, Ben. Let's hope that your professor is not a subscriber and listener to Security Now!, or you've been had. But what you're probably trying to do with a VPN is tunnel other TCP connections, like browser connections that are all TCP. And something really ugly happens if you tunnel TCP in TCP, that is, if you use a TCP connection to carry TCP protocol, because then you've got both TCPs trying to correct for problems. And you don't want that.

Leo: Unh-unh.

Steve: So a packet gets lost, and the carrying tunnel recognizes that it never got an acknowledgment for the packet. So it resends it. But the packet that that was carrying was also sent by the TCP protocol that was going through that tunnel. So, that is, the payload also got lost. So that TCP realizes it never got an acknowledgment. And so it resends it. So you've got the VPN resending and the client resending, and it could be a mess. In fact, it can create a complete collapse of the VPN. It can stall the tunnel. And that's one of the things that happens when people try to use a TCP tunnel to carry TCP data, which is mostly what people are carrying.

What you want, then, for a VPN, is you want the VPN to simulate the Internet. And the Internet doesn't care. If a packet gets lost, oh, that's the way it was designed. Buffers got full on an interface, and there's too many coming in and not enough bandwidth going out. A router, as we have often discussed, is completely free, by design, to just drop the packets. It figures somebody is going to figure that out. If they care, they will send it again. So the bottom line is you want UDP protocol to be used for the VPN because it, like the Internet, doesn't care. And that way the client protocols being carried by the tunnel, they can do the packet recovery, sending again, and then causing another UDP packet to be sent; whereas the UDP protocol, eh, you know, stuff happens on the Internet.

Leo: You know, I think we did cover this. I remember talking about this.

Steve: Really, it's really - I love the concept. It's pure Internet theory.

Leo: Yeah, yeah.

Steve: Really neat.

Leo: Which means that the professor listens to this show.

Steve: Oh, that's where he got it.

Leo: And that's where he got it. Bet you anything. Last question comes from Kelly Shipp in Conway, Arkansas. Kelly wonders, how do you search episodes? You should offer a way to search all the Security Now! episodes by keyword or phrase. This way we could check to see whether you have discovered or reviewed something yet. It could keep you from getting repetitive topical emails, et cetera. Surely you have the episode text already database searchable. Thank you.

Steve: You know, I put this in here just to wrap up our Q&A because I get the question all the time. And if you go to the page that Leo always mentions at the end of the podcast, where all Security Now! things happen, GRC.com/sn, there is a search box in the upper right. And it's not very big. It's not in your face. But it's there. Actually it's on every page of the website. It's in the main menu for GRC.com. And all of the, thanks to Elaine and her transcribing, she's busy right now, as I say this, she's typing these words, and these words, and these words, and these words.

Leo: That's mean.

Steve: And they're all going into the transcript and being indexed by our favorite search engine, Google. And it knows about all of the podcasts and when they occurred. And I use it all the time myself. And you've often heard me say, oh, back in this episode, well, I don't know, I don't have all this memorized. I put a few terms into the search box, and it finds what episode we were talking about that in. So, yes, Kelly, just go to GRC.com/sn for Security Now! and search to your heart's content. And thank you for asking so that I could tell everybody else because lots of people ask for that, and it's right there.

Leo: You can also do it right on Google, if you just do site:GRC.com and then whatever your topic. And as you say, Google does do a good job of indexing, not just the transcripts, but everything on your website. So I put in the word "LastPass," and there's an episode from 2010 in which we reviewed - Security Now! 2010. That's odd. That must be a typo or something. Anyway, in which we reviewed LastPass. Transcripts from Episodes 256, 512, the PDF of your show notes, the download, you can pretty much get everything you need. Google's very good at that. That's a good Google tip. "Site:" will constrain the search to a particular site.

Steve: It's funny, too. When I'm searching around for various topics, I'm now finding GRC coming up. I guess it's probably because Google knows me, come to think of it. Maybe it wouldn't happen for everybody. But like there are obscure pages on GRC that I have not thought of for a long time, often like branching off of the health tree. And I'll be searching for something, and it will find a PDF that has been indexed on GRC. It's like, what? Oh, yeah, I guess that is there. So, yeah. That's sometimes surprising.

Leo: Yeah, it's very handy, yeah. Google's everywhere. Well, that was fun.

Steve: That was, I think...

Leo: A new record.

Steve: I think useful. No, we're about two hours and five minutes.

Leo: Oh, that's not so bad.

Steve: And we're getting out of here in time for your Tech News 2Night.

Leo: That's right.

Steve: So that timing works. And I'm glad we heard from Joe.

Leo: I am, too.

Steve: I feel good about where we are. I'm glad he knows that the industry is really concerned.

Leo: Yeah.

Steve: And I think that'll help. Not that anyone is ever suggesting that he needs to be kept honest. But, you know, maybe it's LogMeIn who wants to get some value for their 110 million. And you were right, by the way, Leo, it was 110 million, and with a 15 million bonus that bumps it up to 125 if they meet some future goals. So LogMeIn doesn't want to do anything to cause their investment to be worth less than was negotiated. So they need to understand, this is different than Hamachi. This is, you know...

Leo: Yeah, don't screw with this, yeah.

Steve: This is competitive, and we're very skittish because it's all about trust. We trust Joe. We don't trust them. And they've given us lots of reason not to. So don't screw with this, LogMeIn. Leave LastPass alone. And leave Joe and his people.

Leo: And that's an important message.

Steve: It really is.

Leo: It's great that everybody made such noise about this, and I hope they keep that will because that really sends a signal to them. If you want to get your money out of this company, you'd better do right by us.

Steve: Well, they will see a hit. There will be a notch in, I mean...

Leo: Anyway.

Steve: Yes. There will be a notch anyway. And so that's Lesson No. 1. But those of us who understand, who believe in Joe and LastPass and the technology, we're not going anywhere because there's no reason to today. But let's hope for continued good behavior. Otherwise, believe me, I will find us an alternative.

Leo: Well, you know, I keep looking because that's the other problem, is who knows who these other guys are? Do you trust them? Do they have a track record? You know, I mean, 1Password's been around for a while, but you'd have to really look deeply, as you have already done with LastPass, to figure out everything that they're doing.

Steve: Yeah. The problem is, though, the things we love end up succeeding and then getting bonked. So I think we're just going to whisper it. We'll just whisper the next one.

Leo: Yeah, yeah.

Steve: For now, I'm staying put.

Leo: Hey, thank you so much, Steve. Steve's at GRC.com. That's where you go to find SpinRite, the world's finest hard drive recovery and maintenance utility. You can also find his Password Generator, his Perfect Paper Passwords...

Steve: Off The Grid.

Leo: Password Haystacks, Off The Grid, all sorts of free software, lots of information. And, yes, this show, both audio and written transcripts, which are very handy if you like to read along. GRC.com. We also have copies at TWiT, of course, it's a TWiT podcast, at TWiT.tv/sn; audio and video, as well. And you can get it, you know, easiest thing is to subscribe because it's all over the place. Anywhere you get your podcasts you'll have Security Now!.

We do the show Tuesdays, 1:30 Pacific, 4:30 Eastern time, that's 20:30 UTC. If you want to watch live, you can at TWiT.tv/live. All our shows we stream live as we're producing them. And that's about it. If you want to be here, email tickets@twit.tv. We have limited room, but we've got some very nice people from Washington and Chicago here, and they're big fans of yours, Steve, and they say hi.

Steve: Cool. Hi back.

Leo: What's the French word - his name's Steve, too. What's the French for Steve? You don't know either. Esteban. I'm sure we'll hear. Thank you, everybody. We'll see you next time on Security Now!.

Steve: Thanks, Leo.