iOS Password Mis-Managers

Description: After catching up with the week's news, Steve and Leo examine the inner workings of the most popular password managers for Apple's iOS devices to determine whether and to what degree they offer enhanced security for safe password storage.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-347.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-347-lq.mp3

SHOW TEASE: Steve Gibson's here. It's time for Security Now!, and he's got a great topic for anybody who uses an iPhone or an iPad. Believe it or not, the password managers you're paying for may not be doing the job. We'll talk about how to keep your iOS device secure, and all of the security news as well, including that big credit card breach, next on Security Now!.

Leo Laporte: It's time for Security Now! with Steve Gibson, Episode 347, recorded April 4th, 2012: iOS Password Mis-Managers.

It's time for Security Now!, the show that protects you, your loved ones, and everyone you might know against bad stuff on the Internet. And the guy who does it is here, the Explainer in Chief. What was the other phrase I came up with, Steve?

[Per SN-346, Steve is the Debunker in Chief.]

Steve Gibson: No, that's the one, Explainer in Chief. That's the one.

Leo: Mr. Steve Gibson, of GRC.com, well-known, you know, I could - hacker, programmer, guy who creates the ultimate, SpinRite is the ultimate hard drive utility, I mean, just on and on and on. He's really a great guy to know as a good friend, but also a real expert in these things. And what I love about Steve is he's the Explainer in Chief. He'll take something and make it accessible to us all. Steve, good to see you again.

Steve: Great to be back. Episode 347. And I think all of our iOS Apple device listeners are going to be extra interested because we certainly have a profile of an audience that's interested in security. A well-known forensics company, ElcomSoft, who sells cracking technology to law enforcement, have done an analysis of about 13 of the most popular

password managers which are available. There's tons of password managers for iOS devices, for iPhones and iPads. And the question, of course, is what's going on inside these? Do they actually provide some protection? And the news is, uh, not so much.

Leo: Uh-oh.

Steve: Not in every case, at least. There are, I mean, it's almost comical what some of them do, some of the mistakes they make. So rather than just using that broad a brush, we're going to, because we have the information, quickly poke into many of the most common password managers and look inside their technology. We've laid down enough foundation to understand the terms, and we'll see how these things are being used and what protections - or non-protections - they provide. So I gave the podcast the title "iOS Password Mis-Managers."

Leo: Oh, boy.

Steve: Because some of it's a little frightening. There'll be some people changing their password manager shortly after listening to this podcast, I think.

Leo: Can I do a little coffee talk?

Steve: Oh, please. Absolutely.

Leo: So Steve and I have been going back and forth on various ways to make coffee. And the latest discovery that I've been exploring is cold-brewed coffee. Steve already has decided, after buying the, what was that thing that you bought, the Toddy, that you don't like - you liked a little bite in your coffee. You like the acidity that hot-brewed coffee - and that's the main reason people do cold brew is the low acidity. And it can be a little stronger because cold brew often you steep for 12 or more hours. So I bought - this was kind of crazy. This was kind of crazy. I bought a $200 - you saw it, the tower, the Yama.

Steve: Yeah.

Leo: And in fact I'll play a little video so you can see it at work.

Steve: Does it sit on the - like it sits on the countertop and is, like, several...

Leo: Yeah. It's two feet tall.

Steve: Two feet tall.

Leo: And here it is. Watch. This is it.

CLIP: Question: How do you make eight cups of perfectly brewed acid-free coffee? Answer: The Yama.

Leo: I'm being a little silly. It is a tower. It's furniture.

CLIP: This is the first time I've used it. We start with ice water, literally ice water, dripping, one drop per second...

Leo: See how slow?

CLIP: ...hits that filter to keep it from boring a hole in the...

Leo: And there's a little round filter that's not really about filtering, but more about keeping it from a - distributing it through the grounds.

Steve: Right.

Leo: And then the grounds slowly, through a ceramic filter, give up their liqueur into the decanter. It took all night. And highly disappointing. Highly disappointing. It is not only - it is no acidity, but it's also fairly weak. And considering that it took me all night to make, you get eight cups. And the idea of the Toddy is it's much stronger, so you can treat it as a concentrate. This isn't a concentrate. So that's basically two cups of coffee that took all night, and it's still weak. So unless I'm doing it wrong - I might try some other techniques. But I do like the Toddy. I know you didn't like it because it wasn't acidic enough. But I think I'm going to stick with the Toddy.

Steve: Yeah. My reaction was that it just didn't taste like coffee. I'm used to there being that bite. And...

Leo: That's why some people like it. They like the bite. Some people will like it if it doesn't have the bite. And you know I like it both ways. Today I had the most biting coffee you can make. Oh, look at you. Look at you sucking it down. I had the most - which was that stovetop espresso machine that boils the water and then forces it through the grinds, and it's cooking it. This thing is boiling and boiling and boiling. So by the time you have it, it's like coffee syrup. And that was good. And very acidic. So there you go. But I would say to people, you don't need the Yama. But the Toddy is only 30 bucks. And if you're interested in cold brew, that actually did a good job, I thought.

Steve: Well, I would say, for anyone who is acid-sensitive, if it upsets their stomach - I have the stomach of a billy goat. I just - I do. I could eat anything. Nothing affects me.

And so I don't have a problem with the coffee. But it's a great solution for someone who wants a lower acid coffee.

Leo: And I steeped my Toddy for 24 hours and as a result got a nice, rich brew. And I didn't feel like I had to do eight ounces per cup of coffee. I could just use a couple ounces, and it was delicious.

Steve: Yeah, and then you can control the strength by how much you dilute it down.

Leo: Yeah. So there is a story that I was very curious about. We talked briefly on TWiT. But I thought this is a story for Superman, aka Steve Gibson, and that's the Global Payments breach.

Steve: Yeah. Now, there's a stage in credit processing, credit card processing, that I've been aware of for quite a while because I'm a direct user of a payment processor like this. My eCommerce system at GRC connects to a backend payment processor that is nothing that any user ever sees. It's not a retailer. It's sort of like it's the inner works of how this all happens. And there's maybe a dozen of them. There are not that many of them in the United States, for example. And they're sort of the central hub of the electronic funds transfer system. They've got direct connections to Visa. And so they're sort of the front end to the actual credit card issuers themselves, and they perform all these transactions. So naturally they're a pot of gold for somebody who wants to perform bad acts to acquire credit card information.

Now, interestingly, our good friend Brian Krebs broke the story. He picked up on it. He was able to verify it. He was tweeting gleefully last week about he had more site traffic for his blog than he had ever had in history. And, like, the day afterwards - because these things are very peak-y in their response, there's always something else happening the day after - he tweeted, "Oh, only 190,000 views today." Aw, sorry, Brian. But, boy. So he was on top of it. He was in the center. And quoting from his blog, which was the authoritative location for all this information, The Wall Street Journal picked up on it, the Gartner Group picked up on it, I mean, it was, as you said, it was a big story.

He said, "It's not clear how many cards were breached...." I should mention that the reports were upwards of hundreds of thousands potentially had escaped. So Brian said, "It's not clear how many cards were breached in the [credit] processor attack, but a sampling from one corner of the industry provides some perspective. On Wednesday, PSCU - a provider of online financial services to credit unions - said it [had] alerted 482 credit unions that appear to have had cards impacted by the breach, and that a total of 56,455 member Visa and MasterCard accounts were compromised. PSCU said fraudulent activity had been detected on a relatively small number of those 56,000+ cards - [specifically] 876 accounts - and that the activity was geographically dispersed."

So it makes sense, first of all, that bad guys who acquire this information - and this is everything required to process. This is user's name, address, ZIP code, the CVV2 code, you know, the CSV, it's known by various names, the little three- or four-digit code on the back, all of that had to be provided to - and, like, street address and ZIP code, which are things that are matched. All of that was provided to the credit processor. And now we know that they are archiving that. They're storing it statically. And that escaped. So naturally this is very time-sensitive. These cards are being shut down. They're being replaced. There's certainly a lot of scurrying going on, which means that there's a rapidly

closing window of opportunity for exploitation of the stolen data. The good news is that this Global Payments company reacted responsibly. Although we did hear that this was early in March. So it's been four weeks.

Leo: Now, I'm looking at the press release from Global Payments. They're saying as many as a million and a half cards were "exported."

Steve: I did see that at one point.

Leo: And Visa has dropped support for them. It may be one of those things where it's maybe worse than we thought. By the way, their stock price dropped four bucks, 10 percent.

Steve: Yeah, was it, I think, about 9 or 10 percent.

Leo: Yeah. I'm surprised it was that little.

Steve: Yeah. So we, from this position of scrutinizing security, have seen things like this often, I mean, that's what the podcast is about is how this happens and why and what we could do to prevent it, both on an individual, personal level and on a major provider level like this. I expect we'll have more news trickling out over time. I imagine Brian will be staying on top of it, and I'll keep an eye on his blog to see if he mentions more. Was this their fault? Was this an employee mistake? Was this miscommunication of their stuff?

I mean, that is a big breach. For a million and a half cards to escape is, I mean, like all the information required to process that number of cards, that's big and bad. My sense is it can happen to anyone, unfortunately. It should happen to no one. But we do see it happening. So I wonder if this will be a permanent - if this is a suspension, or if Visa is saying no more. I mean, certainly this hurts them because they've got to go out and replace all those cards. And, boy, clean up any fraudulent activity across a huge swath of cards.

Leo: Yeah, it's ugly. Visa says we're done.

Steve: Wow.

Leo: So but from the point of view of a user, even if your credit card's breached, the law says that you don't owe anything; right? I mean, the credit card - you're not liable for fraudulent charges on your account.

Steve: And in Visa's own statements about this, because they were out there rapidly trying to calm people down and not cause anyone to have any worry, they reiterated exactly that, that the users of credit cards are completely indemnified against fraudulent use of their card. I mean, I've had many fewer problems in the last few years. But it

used to be that when I would be flying up to Northern California to visit my family for the holidays, I'd contact my travel agent, and she'd say, "Steve, did your card get compromised again this year?" And, you know, because she'd...

Leo: Again this year? Again?

Steve: And I'd say, "No, believe it or not, Judy, I've still got the same card. It's a miracle." Because, I mean, it used to be happening. This is before I was able to funnel so much through PayPal, and that's been a real boon, or through Google's shopping service. I work hard not to give the card away, the card number, not to disclose it, if possible. But again, it's the case that not everyone is being careful with it. But as you said, Leo, in no case have I ever had any problem just having those charges reversed. Which of course is the argument that the credit card companies make for charging such high interest. And they say, well, you know, we have to stay profitable, and we're indemnifying everybody, so...

Leo: Yeah, and that's the point. You may not feel like you lose any money. But in fact we're all paying for it.

Steve: It's dribbling out every month you have balances.

Leo: But I have to say, all the card companies are much more proactive about calling about fraudulent charges. I've talked about this on TWiT. I had an order with Shoes.com. It was my first order. I used a credit card and had it shipped to a different address than the billing address. And Shoes.com called me. And when they couldn't reach me, they cancelled the order. And I think that more and more that's what you're going to see. Shoes, because I ordered athletic shoes, those are apparently a red flag. Dvorak says that you can get any credit card canceled by doing this: In the same day, filling up two different tanks with gas and buying athletic shoes. They will cancel your card. He says they'll just cancel your card because that's such a pattern for somebody who has a stolen credit card. He's going to fill himself up, and his friends, and then go out and buy some sneakers. And they just - I don't know if that's true, but it's a great story.

Steve: Actually, I think that's very clever. The multiple fill-ups with a single card.

Leo: Right, that doesn't sound right, does it, yeah.

Steve: That's clever. Well, I had one card, my main card, actually, I cannot buy gas with it. Every time I did, then I'd be in a restaurant, and they'd say, I'm sorry, sir, your card is not - it's like, what? And then I'd call them, and they'd go, well, you used it at a gas pump. And I finally, after several times this happened, I said, look, can you just turn that part off of my fraud protection? She said, no, sir, we're unable to do that. And she explained that the advantage to a bad guy is that they're next to their car if they need to make a getaway.

Leo: They can run. They can run.

Steve: Yes. And they're at an automated terminal where all it can do is say yay or nay. And so it's a way for them to test the card to see if it still works.

Leo: Wow.

Steve: Although increasingly, I mean, now I have to put my ZIP code in every time that I use the card. And so they would have to have that to go along with it.

Leo: We're seeing more - and that's exactly why. We're seeing more and more fraud protection techniques. And it shows you it's not that hard to do.

Steve: But two fill-ups, that's brilliant because who's going to do that?

Leo: That's unusual; right? Yeah.

Steve: Yeah. So another piece of news just hit. Ars Technica reported something that I kind of thought everyone assumed. But I got so many tweets about it that I thought, well, maybe not. And that is that Apple holds the master key to the iCloud. And a careful reading of the iCloud Terms & Conditions says things like Apple can "pre-screen, move, refuse, modify and/or remove Content at any time" if the content is deemed "objectionable" or otherwise in violation of terms of service. Furthermore, Apple can "access, use, preserve and/or disclose your Account information and Content to law enforcement authorities" whenever required or permitted by law. Apple further says that it will review content reportedly in violation of copyright under our favorite DMCA.

Leo: Violation of copyright? Now, see, I could see on court order, a subpoena. On violation of copyright? Oh, that pisses me off.

Steve: Well, so, yeah. The takeaway from this is that, if you use iCloud, it's super convenient, it's all synchronized in the cloud and all that. But it's encrypted in transit, and then it's encrypted by Apple when it's at rest. When your data is at rest, it's under Apple's encryption, not yours. So they can poke in there, peek in there, do whatever they want to, whenever.

I want to talk about, and I'm going to, I think, tentatively in two weeks, if nothing else comes up, about an interesting sort of very security-conscious cloud-based service whose name escapes me at the moment. I wrote it down, and it's been on my radar for a couple months, and I've been meaning to get to it. And I thought, since this would make so much news, with people being upset by this idea, it's like, well, let's take a look because we've often talked about pre-Internet encryption. If you encrypt something, a blob, then iCloud syncs it, well, that's fine because all they ever get is a blob of pseudorandom noise. They have no visibility into it. But if it's just being done by your devices, it's safe in transit, but then it's under Apple's lock and key once it's there. So...

Leo: No privacy.

Steve: Yeah. I didn't assume anyone would think otherwise, but I thought it was worth pointing out that this is - you get the convenience, but you're not doing device-level encryption for - I don't know if some of the services they're offering might require them to have visibility; but in any event, they do. And that's sort of part of what you get, I think, from using a big bulk public service like Apple.

Leo: Well, and that's something I talk about with Carbonite, who's one of our sponsors, is that - in fact, I remember having a conversation with the CEO of Carbonite. He says, "We get subpoenas all the time. We just say, sorry, can't help you," because they do pre-Internet encryption. They support encryption, and you keep the key.

Steve: Right. And, of course, famously, Dropbox wasn't doing that.

Leo: And Dropbox still doesn't.

Steve: Yup.

Leo: And, I mean, yeah. There you go. It's one thing to say, look, we'll comply with a court order from law enforcement. It's another thing entirely to say, oh, and by the way, if the record industry asks, we'll hand you over.

Steve: That's right.

Leo: To me, that's another thing entirely.

Steve: So we were right in our pretty much tossing off without much thought that claim that we discussed last week about this XRY's company video. Remember they showed a video which claimed to allow them to hack a password-protected or passcode-protected iPhone instantly, in a matter of seconds. And we both talked about how - and it showed them holding the button down while they powered it on, and we realized that was about the phone being a RAM disk, and that Apple had fixed that some number of versions ago. And there has since been a bunch of public debunking of that video, which they have removed from YouTube.

Leo: Oh, man.

Steve: They've taken the video down. Now, people that have looked at it closely confirmed what we believed. But we'll be coming back to this later in the podcast. But it's worth talking about what can be done and what cannot be done. What has happened is that, as we mentioned, the iOS security and the device, the physical device security has

been improved dramatically over time. And as I've had to look at what iOS is doing and the devices are doing much more carefully for this podcast, I have to say I'm impressed with what Apple has done, that is, the very first iPhone offered just UI protection. There was no encryption of the device. It was just - the passcode you put in sort of just kept you from getting past the locked screen. But there was nothing else going on. And the forensic companies were having a field day with that because naturally a phone is a wealth of information for law enforcement. They would love to have access to everything in someone's phone.

And so as the iPhone has become increasingly popular, as we've moved from v1 to 2 to 3 to 4, now we're at 5.0.1, I think is the latest, Apple has really taken measures to increase the strength. There are, for example, they have added full file system encryption, although there are a couple little catches. For example, if you never - if you are on iOS 3, and you never wiped the device and then reinstalled under iOS 4 or 5, if you simply updated iOS itself to 4 or 5, then you still don't have an encrypted file system, which some people may not be aware of. It turns out that the encrypted file system is super important. I mean, really it's what everyone should have and want because it's zero hassle, Apple manages it beautifully, and it really does protect users.

Leo: I feel like I take a performance - you're talking about FileVault, their built-in FileVault. Yes?

Steve: Yes.

Leo: I feel like I take a performance hit with that.

Steve: Well, now, not FileVault, but the actual, I mean, the entire device.

Leo: Oh, I see, okay.

Steve: Yeah, the whole...

Leo: That kind of like Intel's TPM thing, where it's just built in. Then it's done by the CPU automatically, using its own...

Steve: Yeah, there is hardware crypto now in the latest devices. And the forensics companies are not happy. The iPhone 4S and iPad 2, it's really been locked down.

Leo: So it's automatic. There's nothing I - it's not like Vault - okay. I understand. FileVault's on the desktop.

Steve: Correct.

Leo: This is automatic on the iOS stuff. There's nothing you can do about it.

Steve: Yup, exactly.

Leo: I got it. I got it.

Steve: Yeah. And so, for example, one of the things that they're doing, we'll be talking about key strengthening because there's two places that users will get security. And this is really where this XRY company was misleading people because, even if you have access to the device, what Apple has done is they've used very good key strengthening, or key stretching. The acronym is a tongue twister. It's PBKDF2, which stands for Password Based Key Derivation Function v2. And I've seen people say, well, you can remember that by Peanut Butter Keeps Dogs Friendly, Too. It's the same acronym.

So what they do is - and we've talked about this PBKDF2 before because, for example, WPA, the WPA2 encryption, the good, strong encryption, what it does is it takes the user's passphrase and the SSID and essentially hashes it with some salt 4096 times. It does it 4096 times, essentially in a loop, taking the output from the first one, putting it into the second one, hashing that, putting that into the third one, hashing that, into the fourth one, hashing that, and so forth. Because it just makes it computationally infeasible, I mean, it's like it slows down any guessing that you do by the factor of how long it takes to perform that operation.

So Apple does this 10,000 times on their iOS devices. So even if you have some access to the phone, talking about this XRY video, for example, even if they had access to the phone, because of the fact that anything you put in has to run through 10,000 of these complex hashing functions, in order to get the key which you can then test to see if it will decrypt the phone, the best you can do - oh, and it has to be done on the phone. This is not an offline attack. So the phone itself, because it also uses some non-public key as part of this password strengthening, the phone itself has to do it. So you can't use GPUs or anything else. You have to do it on the particular device that you're trying to crack because the point is, if you put the same - say you just did a four-digit passcode. You put the same four-digit passcode into a different phone, it comes out of this strengthening function with a completely different 256-bit key.

So because every phone is different because every phone has its own secret keys that it never publishes, I mean, I'm very impressed with the technology that Apple has. They've done a good job. The point is it takes about a quarter second, I mean, you could only do four four-digit passcodes per second. Now, that's not super strong security because it means, if you just do the math, that it takes about 42 minutes to try 0000 to 9999. So one of our takeaways from this analysis today is you really do want to use, if you're relying on this Apple security, you want to use a stronger passcode because 42 minutes is not very long to crack...

Leo: Ah, but remember that you also have this feature that, if they try 10 times and fail, it erases everything.

Steve: No. This is, well, I mean, yes, if you use the UI.

Leo: Oh.

Steve: Not if you're attached to the phone forensics.

Leo: Oh. So it's not paying attention to the count forensic.

Steve: Correct.

Leo: Oh, interesting, oh.

Steve: Correct. But, so that's one takeaway. So we'll come back to this a little bit later because what we're going to see is that many of these password managers provide virtually no additional protection.

Leo: So you really want the OS protection to be tiptop.

Steve: Yes. And when you talk about backup encryption also because docking our devices to our machines, it turns out that using a really strong backup password is equally important because that's another place where the entire phone set of data is sitting and is available for forensics. And law enforcement might often have a good reason for getting it from bad guys. But we want to control that ourselves.

I got a great tweet this morning from Andrew Mason, who's in London, tweeted from @amason, who told me about a site I hadn't seen, AreWeSlimYet.com. And this is not about body weight.

Leo: Okay, because I know the answer. I don't really have to check a website for that.

Steve: Yeah, Leo, you stand on your keyboard and - no. So AreWeSlimYet.com is Mozilla's self-monitoring of Firefox's memory consumption.

Leo: Oh, how clever.

Steve: Over time.

Leo: How clever. Now, you have to be using Firefox. Do you have to go to that site in Firefox?

Steve: I don't think so. I did because I'm still very happy...

Leo: I'm on Safari here, and I'm getting information, so...

Steve: Yeah, I don't think you need to use Firefox. You have to have scripting because they're very script - it's like a whole bunch of - you can, like, zoom in on these charts and things by moving your mouse around and then clicking. But here is this AreWeSlimYet.com shows over the history of Firefox versions how they're using memory and graphically demonstrates their determination to just fight that down. And I love the tabs on the side, and my tools I have in Firefox. Now that I'm at 11, and they really did solve the memory bloat problem, where sometimes I'd wake the machine up after it was on overnight, and it used up all my 3GB. It's like, okay.

Leo: Now, is this information from my machine or their own stuff?

Steve: This is their own forensics over time.

Leo: Got it, got it.

Steve: So it's sort of static, just sort of...

Leo: It's not my number, yeah.

Steve: Right, right.

Leo: I get it. I was saying, how do they know? How do they know? All right. So they're getting slimmer, aren't they.

Steve: Yeah, they're doing it. I'm impressed.

Leo: Especially with tabs closed.

Steve: And now that we're not sure how much we love Google, I thought, well, that's good. I'm happy I've got Firefox. On April 1st, and I was conscious of the fact that it was April 1st, was the news that Ashton Kutcher - Kutcher?

Leo: Kutcher. Now I don't know. I want to say Kutcher. Kutcher. Oh, forget it. Who cares? Who cares?

Steve: Anyway, well, we might care. He's been chosen to play Steve Jobs.

Leo: Yeah, but just in some indie flick.

Steve: Well, I know, but...

Leo: There's a big biopic from Sony coming up. Actually, this is better news than you think.

Steve: Okay.

Leo: So he's been picked because he has a stringy beard and stringy hair, and he looks like a young Steve Jobs.

Steve: He actually does. I had never really...

Leo: Yeah, but anybody with a stringy beard and stringy hair would look that way.

Steve: Okay.

Leo: And it's in an indie pic, which means he won't be able to play in the really big one based on the Isaacson biography when Sony does that. Thank god.

Steve: Ahh.

Leo: I'm not an Ashton Kutcher fan, as you might determine.

Steve: I think you just pronounced his name correctly.

Leo: I think I did. As soon as I was angry about it. Are you excited that he's going to play it? I mean, he does look like - he does look the part. And he's a good actor.

Steve: Yeah.

Leo: It's not that he's not a good actor.

Steve: Yeah.

Leo: Yeah. But...

Steve: I have no bias one way or the other. I don't like him or dislike him. I'm maybe a little jealous of him, but...

Leo: I'm very jealous of him. You know he's not dating Demi Moore anymore, though, so that's...

Steve: Oh, okay. Well...

Leo: So you don't have to be jealous about that.

Steve: He seems to be a good guy. He and Bruce and Demi were all getting along. Sort of strange.

Leo: So the interesting thing, I don't know how we got in this Hollywood gossip thing, but the interesting thing, I talked - we did an interview with Dana Brunetti, who's an old friend. He's a Hollywood producer. He produced "The Social Network." And they tried - Trigger Street, his production company with Kevin Spacey, they tried very hard to get the Walter Isaacson biography, but lost out to Sony. But he in the process was spending a lot of time thinking about, well, who do you get to play Jobs? And the real problem is the age range because Kutcher can play the young Jobs, but he can't play the older Jobs.

Steve: Good point. Right.

Leo: So it's actually a very tricky casting decision. I'm sure that this pic will be mostly about the young Steve Jobs, the hip Steve Jobs. Well, he was always hip.

Steve: You think so? Because, I mean, he was - it was the later Steve Jobs that changed the world. I mean...

Leo: Right. Kutcher is - comparing him to a 23-year-old Steve Jobs.

Steve: Yeah.

Leo: So how do you - somebody was suggesting Tom Cruise. I don't know if that's a good pick, either, but...

Steve: Oh, please, no.

Leo: Fortunately, it's not our decision.

Steve: Well, it'll be fun that we're going to get some movies.

Leo: Oh, yeah, we're going to get lots of movies. Are you kidding? Absolutely.

Steve: Yeah, that's neat.

Leo: Yeah.

Steve: So I did poke just briefly, to talk about health, I poked a little bit into this Dave Aguss, whose book "The End of Illness" you mentioned last week.

Leo: Yeah, what did you think?

Steve: Well, I was a little put off because I went to his website, and he has a video on there where he's talking about how supplements are harmful. And he quoted, he said, he quoted a very bad Vitamin E study.

Leo: Oh, dear.

Steve: Well, first of all, yeah, anyone who just says "Vitamin E," immediately I'm worried because there isn't anything called Vitamin E. There's eight Vitamin Es. There's alpha, beta, gamma, and delta tocopherol, and alpha, beta, gamma, delta tocotrienol. There's a family of eight. And unfortunately, because early nutrition scientists saw that alpha tocopherol seemed to be what there was most of, that's what all the supplements have.

Leo: Right.

Steve: And that's what you'll see if you look at your bottle on a multivitamin is alpha tocopherol. Well, what was found was that in people taking huge amounts of alpha tocopherol, there seemed to be a correlation with an increase in prostate cancer. Thus, unfortunately, David says "Supplements are harmful." Now - and Vitamin E causes prostate cancer. The fact is, ill-advised, uninformed use, over-consumption of one of the eight Vitamin Es does. Gamma tocopherol turns out to be the one that we need. And because the molecules are so similar, if you overload on alpha, it competes with the other tocopherols and tocotrienols and keeps them from having the effect that they should. So what you want is a Vitamin E which is full spectrum, that contains all eight of the different types in the same ratio that they occur in nature. And that's the E that I take and have been taking. And if you do that, then you're fine.

And then of course the other problem is, arguably, almost everyone needs to supplement their Vitamin D. It's been our own purely anecdotal experience with the podcast I did where I got flooded with people after the holiday season saying, hey, this is the first season I never got sick, probably thanks to Vitamin D. I mean, and since then, it's been several years since we did that, there's just constant reports about the benefits of

Vitamin D supplementation. So anyway, the guy seemed like a little bit of a populist and like...

Leo: Read the book because I think that what you see on the website is a summary. He may not say don't take multivitamins. He has some interesting - I think the larger story is still accurate, which is that we don't treat people as systems. Because we've had such success using antibiotics to target a particular illness or antivirals to target a particular illness, we have changed our model of medicine from thinking of it as a systemic model to you've got an invader, aim a weapon at them. And, now, he's an oncologist, a cancer doctor, and he says that that doesn't work because cancer is a systemic issue, and that many of the illnesses we see come from systemic issues, and that we've kind of gotten away from that in medicine because we've had such success with the magic bullets.

Steve: Yeah, I think that's true.

Leo: And I think that's probably what he means when he's talking about supplements, that you can't treat them as a magic bullet. You have to think systemically. One of the things he does recommend is getting blood work on a regular basis, looking - he says everybody's individual. You need to look at what these things are doing. And so I think in that regard he probably does say supplement your Vitamin D if you need Vitamin D. I think what he's against is just kind of take vitamins because it's good for you attitude.

Steve: Right. So I do, however, have a book recommendation.

Leo: Oh, good.

Steve: I'm at the end of this book. I am so impressed by this book. It's funny, too, because as I was reading it - and this is the one I've mentioned a couple times that was about nutritional anthropology, essentially - I was thinking, wow, I hate the title of this book because it's just not serious enough. And I was telling people, in fact I may have mentioned it to you on the podcast, that I would imagine that, when this book was first written, the author, whose name is Geoff Bond - actually his middle name is James, so Geoff James Bond. He is from the U.K., but it's G-e-o-f-f Bond. I could imagine that, when he submitted his galleys to the publisher, it was probably titled "Nutritional Anthropology" or "Applied Practical Nutritional Anthropology" or something, and the publisher said, uh-huh, yeah, well, we'll never sell it if that's what we call it. What's funny is that this is his second book. And I did find his first book, which is titled "Natural Eating," and then the subtitle is "Nutritional Anthropology: Eating in Harmony with Our Genetic Programming."

Leo: Oh, see, this is the new thing everybody's talking about.

Steve: Well, and frankly, I'm now self-conscious about ever having mentioned Gary Taubes because I ran across a quote from him about what he eats, and it's like, oh, boy, that's nothing that I'm able to endorse from all the research I've done. Anyway, the book

is unfortunately titled "Deadly Harvest."

Leo: Oh, dear.

Steve: Which is, I know, which is meant to sell copies.

Leo: Absolutely, yeah.

Steve: But it is a serious piece of work. He and his wife have lived among aboriginal tribes and eaten what they eat. It is massively referenced and researched. The last third of the book is the references to everything he refers to through the book. For people who haven't studied, as I have, things like evolutionary psychology, there's a whole chunk about, like, pressures that, like more than just eating, like societal and familial relationships and interpersonal relationships and how our past formed who we are today. Anyway, it's been a fantastic read. I recommend it without reservation for anyone who is curious about sort of where I've gone with my reading: "Deadly Harvest" by Geoff Bond.

Leo: I've ordered it, yeah.

Steve: It was all good.

Leo: And I've been reading a similar book called "The New Evolution Diet" by this guy, Arthur De Vany, who's an economist, but similar nutritional anthropology. I presume that all of this stuff is around the same idea, which is that we stopped evolving about 40,000 years ago, and we should eat as our - and exercise, in this case, he talks a lot about exercise - as our Paleolithic ancestors did.

Steve: Yeah, the way - I don't want to spend too much time on this. But the way I would sum it up is that we evolved in a world of scarcity. Meat was scarce. It ran away, so it wasn't staying put for us to get it. Sweet stuff was scarce. Like the only real source of sweets was honey in African killer bee nests, and they tended to protect their honey, too. And so we wanted things that were high calorie, but we couldn't get them. They were scarce. So we largely supported ourselves eating a lower calorie, which is to say plant-based and slow-moving animal, like crickets and locusts and slugs and snails and things, that was our diet.

Now, but we were built to want the higher calorie foods. So what happened, of course, in summary, is we got very smart with agriculture and with industrialization and with farming. And so today we have all this technology that lets us have anything we want. And unfortunately we're still programmed as we once were to want high calorie things. And now we can have all the meat we can imagine. We can have all of the grain, which didn't exist back then, and all of the refined sugar.

"60 Minutes," as a matter of fact, did a piece that was really interesting just this last Sunday on raising the question, is sugar toxic? And I'm convinced it is. And what they weren't quite ready to go into yet is so is white bread, so is grain, because it converts immediately into sugar and has almost all of the same effects. So those were things that

we just weren't designed to handle. Our bodies weren't designed to handle them. And you look around at what's happening to us as a consequence. So we're smart, and unfortunately we're able to now give ourselves anything we could imagine we want, and that's not necessarily good for us. But something is good for us.

Leo: Yes.

Steve: And that's SpinRite.

Leo: Yes. How did I know?

Steve: On March 30th I got a nice note from a Gregg Dille, I think that's how I pronounce his name, D-i-l-l-e. The subject was "Process control site license/SpinRite." And he said, "Steve, just wanted to let you know, I work at a major chemical plant refinery. Check your recent purchases of four copies to match it up. We bought a copy of SpinRite, one copy, a while back and had been using it quite successfully in our process control environment. Shortly after purchase, I sent a note to our group stating that we should acquire a site license, but the powers that be did not take me seriously. I've tried to advocate the use of SpinRite out here whenever I felt the situation warranted it, as we have some nodes that are really old, and there is no plan to replace them. They're working, so why fix them?

"During this year's software license true-up" - which I thought was interesting, it must be like where they decided to get themselves current - "I brought it up again, and others have since realized the value of SpinRite. So we just made the effort to purchase four copies so that we would have a site license. Thanks for all you do. Gregg." And that's, you know, thank you, Gregg. I really do appreciate that.

Leo: Yay.

Steve: It's an honor system, but that's what keeps us going.

Leo: All right. Let's talk about iOS. I use LastPass on iOS. I hope that's still safe.

Steve: They've done a good job. I did vet them extensively. What seems to be the case is that I can't quite understand the thinking on the password manager developers' part of not making them as strong as they can. It appears that in some cases they just don't care. It's a free app, for example, many of them are free. And they've just sort of said, well, some people are going to buy them. People who don't know any better will buy them, and so it doesn't really matter. It's like, okay. I mean, certainly a takeaway, by the time I'm through enumerating the specifics, our listeners are going to know and understand clearly that it's not enough for the thing just to say, oh, you have to put a password in to get to your passwords, and we're going to protect them from you. It's like, well, okay, we really do need to know the details.

Now, but this all starts from sort of the forensic attack angle, the idea being, of course, that somebody, presumably law enforcement, or a hacker who's got access to the same

sorts of tools, is trying to get to your stuff. This ElcomSoft is one of the leading suppliers of forensic tools. On their page - it's ElcomSoft.com. On their page they talk about, they say "Enhanced forensic access to iPhone/iPad/iPod devices running Apple iOS." And then they say "Perform the complete forensic acquisition of user data stored in iPhone/iPad/iPod devices running any version of iOS. ElcomSoft iOS Forensic Toolkit allows eligible customers acquiring bit-to-bit images of devices' file systems, extracting device secrets (passcodes, passwords, and encryption keys) and decrypting the file system image. Access to most information is provided instantly." And it goes on to enumerate features and benefits all in one complete solution; quick file system acquisition, 20 to 40 minutes for 32GB models; zero footprint operation leaves no traces or alterations; and so forth. So this is something which is used to access the innards of these phones.

Now, they published a paper which explains sort of the background of the environment that they're trying to operate in. And one of the things that they make very clear is that they look at iOS and BlackBerry. There's no coverage here in their paper of Android devices. I'll keep my eyes out for anything that gets published like that so we can talk about that when something exists. But as I was mentioning it earlier, it is the case that Apple has gone to great lengths and, I think, very impressive lengths to provide security to their users.

Now, as we also mentioned in another context earlier, as soon as you synchronize with iCloud, that's out the window because Apple holds the encryption, and you don't. But as long as you don't do that - we don't know for sure whether Apple holds the keys per phone. Each iOS device - iPhone, iPad, iPod - has unique hardware encryption keys. And those are used as part of the unlocking process to develop the - when you actually enter this little passcode to unlock your device, to us it seems like all it's doing is sliding the screen over. It is in fact producing a very strong 256-bit symmetric cipher key. And it is only that that allows the file system to be viewed. The file system is stored, given that it is encrypted, as long as that's the case, as pseudorandom data. It is completely unavailable unless you have that 256-bit key. And the only way to get it is by running through this process.

Now, if you do it through the UI, as you mentioned, Leo, as long as you've got the wipe after 10 mistakes, you're probably safe. If there is a way to get past that, if the phone, first of all, if the phone is jailbroken, all bets are off. So you absolutely don't want to jailbreak any of these iOS devices because that breaks down the fundamental protections that keep people from getting in. It may be the case that there are ways in, and that the forensics companies have a way in. But even if they do, then they are prevented from trying any more than about four passcodes per second. Them getting a way in bypasses that 10 mistakes file system wipe feature. My advice would be always run with that.

The downside is, if a toddler grabbed your phone and was playing with it and made 10 mistakes, you'd wipe out your phone. But then you've got your backup. So hopefully you're docking with iTunes from time to time on a base-station computer, and it's kept synchronized. Or you're using iCloud. You're not that concerned about Apple's having access, so you're backed up very currently that way. Certainly makes sense to turn that on.

But if there's a way to get to the device underneath this - in a jailbroken style, by somehow hacking to it, then anyone forensically analyzing it is still going to have to come up with this 256-bit key. And Apple does a 10,000-round password strengthening which has to be done on the device, using the device's hardware, because it mixes in the device's individual hardware keys as part of that. So that puts an absolute limit of about four tries per second when you have that kind of access. So that says about an average

of 20 minutes to guess a four-digit passcode.

Now, to me that says, if you really do want security, you can't settle for a four-digit passcode. You need to go to the more complex, turn off the simple passcode, get yourself a full keyboard, and then do whatever you want. This is really where there's a tradeoff between convenience and security because this is something you've got to be able to do every time you unblank your device or turn it on. I mean, it's on all the time actually. But go to use it, you need to say hi, it's me, and prove that's you.

But this is where something like Password Haystacks, the haystacks concept comes in because length here can really trump complexity. Yes, you want, yes, I know, nothing's better than pure entropy. But still, there's a tradeoff with what's easy and feasible to enter. But the bad guy doesn't know anything about your strategy for having padded a password. Use the haystacks approach. So what you want is something long, but also something you won't go crazy having to type in all the time.

Leo: Well, and that's kind of the issue on iOS. It's one of the reasons people like those four digits is I'm doing this, on a phone anyway, with my thumb, and I want to do it quickly.

Steve: Yup.

Leo: And so, yes, you can have a long password, but who wants to sit there every time you turn on the phone, type type type type type type type type.

Steve: Right. So all I want to do here is explain what the tradeoff is, which is, if it's digits only, I mean, actually you can do the math. You can go to GRC.com/haystack, and it'll do the math for you of using different alphabet complexities and different lengths. And then you can figure that there will be four attempts per second. Which, I mean, that is slow. Apple's done a nice job of making it that slow because that's no stick it on a GPU and do a billion per second. That's four per second, which is pretty slow. And somebody has to have your phone for that length of time. But if you just make it six digits and a bigger alphabet, then it goes quickly to years to crack it. And I think there was, like, six digits with a full alphabet, I did some math, I think it was like 88 years. It's like, okay, that's probably enough, on average, to crack something. And six characters isn't that hard to type. So that's where that tradeoff is. But that's getting into the device.

Now, what it turns out is that, once in, many - well, first of all, some users might not be locking their phone at all, or their iPad. They may just want to access it. They figure, hey, there's nothing I'm storing here that I care about except my passwords. And so the idea being that people want the convenience of turning the phone on and just having it right now, right now access. But they go, hey, I've got a password manager that I have either free or purchased, because both types are available. And that's where I'm going to put the responsibility for keeping the things that I really care about. I'm going to lock them up under a password manager. But otherwise, who cares about my contacts and my web browsing history and things? I'm not doing anything on the phone that I don't mind if somebody looks at.

So the question is, how secure are the password managers? Oh, I need to also mention the backup before I move on. One access point that the forensics guys have is the physical phone. The other is the backup. Now, again, I was impressed when I learned

that Apple encrypts the backup before it leaves the phone, using the phone's keys. So the backup is not encrypted, I just assumed it was encrypted on the PC, the Mac or the PC, whatever you're synchronizing your phone to. It's not the case. It's encrypted by the phone, in the phone, and only the encrypted result is stored. Except that the backup password complexity definitely matters because that can be attacked in an offline attack. So again, Apple's done a good job of making it secure.

But if you use encrypted backups, and you absolutely definitely want to, I'll wrap this up with some bullet points of sort of a checklist of things Apple users, and to a lesser degree BlackBerry users, need to do. They're pretty much the same. But a really good - first of all, using backup encryption is important especially, as we'll see in a second, because the password managers, many of them are not providing much, if any protection. And if you do encrypt your backup, you want to use a good strong complex password because there an offline attack is possible.

Okay. So what are the password managers doing? I've separated them into three categories: brain dead, brain challenged, and useful.

Leo: Oh, I'm getting a lot of people hoping they don't get in that first category. Okay.

Steve: So under "brain dead," there's something that just - there's a free password manager called "Safe," Safe Password, and it's also known as Awesome Password Lite and also as Password Lock Lite. And in this case, heavy on the "lite." Nothing is encrypted. All user data is stored in plaintext.

Leo: For crying out loud.

Steve: The master password is limited to four digits, and it's stored in plaintext. So password recovery, such as it is, is instantaneous. Not that it matters much because everything's in the clear anyway. Just couldn't be more ridiculous. So nothing safe about Safe Password.

iSecure Lite Password Manager, also no encryption. All user data stored in plaintext. The master password in plaintext. So that means, to be clear about what that means - or I'll finish one more. Ultimate Password Manager, their free version. No encryption. This is the Ultimate Password Manager, Leo. No encryption. All user data stored in plaintext. Master password stored in plaintext. Okay.

So what those are doing is nothing. You go to the app, and it says, "What's your password?" You type it in, and it sees that it matches the plaintext copy that it has stored; and, if so, it lowers the drawbridge. It lets you look at your passwords and data that you've stored in there, which are also stored all in plaintext. So if somebody had access, got access to your phone and could get past its lock code, or if your phone is not locked, if you don't use that, then anybody can read out all your passwords if you're using any of those first three brain dead ones. Or, if you're not encrypting your backup, and someone has access to your PC where you have backed up your machine, same story. There's all your passwords just laying out there. You'd print the file, and there would be all of your data from these password managers.

Now, there's also, under the brain dead category, the last one is Secret Folder Lite, which

is the same author as Password Lock Lite, which I mentioned. That was the first one I talked about, heavy on the "lite." And it's just as lite. It protects folders, the photo and video files, but the passwords are all in plaintext, and they can be instantly recovered. So none of those offer any protection.

Now, stepping up a little bit, we come to the "brain challenged" two. There's something called Keeper Password and Data Vault. Now, this one uses encryption, AES-128. Most of the things we'll talk about from here on out use encryption, and most of them use AES-128, sometimes 256. We know that 128 is just fine for today. It encrypts in CBC mode, Cipher Block Chaining, which is one of the standard modes for using AES encryption, so that's good. The encryption key uses the first 16 bytes, which is 128 bits, of the SHA-1 hash of the master password. So that's pretty good. You put in any length password you want. It hashes that to 128. It does it as an SHA-1. Then it uses the first 128 bits of that as the key for the AES encryption.

But the master password is verified by comparing an MD5 hash of what you enter with the MD5 hash of the password when you set it. So when you're setting this up, it says give us your master password, and you enter it. And it says, oh, verify that. And so you put it in a second time. And it's like, oh, very good. You put it in twice correctly, so we believe you're going to be able to do it in the future. It then makes an MD5 hash of that, and that's what it stores. So the crypto is good, but it stored an MD5 hash, without any salt, of your password. Which means any rainbow table with MD5, which is one of the older hashes that has been rainbowed to death, can be used to look up your password. So not so good.

All they had to do was salt it, just add some salt to the hash, and then rainbow tables wouldn't be - precomputed rainbow tables couldn't be used. But they didn't do that. So you just - so anyone who has access to the raw data would take the MD5 hash of your password, look it up in an online rainbow table, which would give them the password. And then they put that in, which it then SHA-1 hashes to get the decryption key, and they can decrypt your data. So it's better than nothing. But they could have easily made it a little stronger. And, I mean, any listener to this podcast knows 25 ways that these things could be made stronger. But the authors of these programs apparently don't or didn't care.

Now, that one is free. Everything we've talked about so far is free. Also under brain challenged is, for $9.99, something you pay $10 for and think, oh, well, if it's 10 bucks it must be better, this one is called SplashID Safe, SplashID Safe for iPhone. Now, this uses Blowfish rather than AES. And it's one of several, only a few, that do use Blowfish. Blowfish is interesting. It was designed by our friend Bruce Schneier back in 1993. So it's been around a long time, and it has withstood all attack.

The problem with Blowfish is that it uses, because it's so old, it uses a smaller block size. It's a 64-bit symmetric cipher, meaning you put in 64 bits at a time and get out a different 64 bits. That's significant because there aren't - there are, what, we know that there are four billion combinations of 32 bits. That means there's 16 billion billion combinations of 64. Once upon a time, back in '93 when Bruce did that, that was enough. But that was - that's a long time ago in terms of computing power explosion. So 64-bit block ciphers are really no longer considered secure enough for industrial work.

But what is significant about this is that it uses a highly complex key setup, which is to say, remember the way these ciphers work is there's something called a "key schedule" is the technical term, the idea being you take the key, and you do a bunch of stuff to it to create some raw data based on the key, which is then used, for example, by successive rounds of the key. This is the way AES, for example, works, where it's like an 11-round

process for, I think it's AES-128 uses 11 rounds. Each of those 11 rounds uses different data from the key setup.

Well, normally a cipher wants a fast key setup, that is, it doesn't want much overhead associated with getting going. Blowfish has a particularly onerous key setup that involves preprocessing of a block of about 4K. So it's very slow to set up the key. But that's a good thing when you're wanting to prevent guessing because any brute forcing is by its nature requiring you to try this key, which means you've got to go through all this, in this case with Blowfish, a lot of work to get this thing set up.

So all of this sounds really good. In fact, I should mention that OpenBSD uses for some of its security Blowfish on purpose because it's so complex. It's just burdensome to guess what the key is. So all of this good stuff was used by SplashID Safe for iPhone for $10. After they did all this, the master password is encrypted under Blowfish - you're giggling, Leo.

Leo: I can just tell something bad's coming.

Steve: Something bad's coming. Master password is encrypted under Blowfish using a fixed key. Which is - I'll spare everyone saying upper and lower case. So it's "g.;59? ^/0n1X*{OQIRwy." Now, clearly someone went to some serious trouble coming up with that.

Leo: Nice random password. But it's the same.

Steve: And it's always the same.

Leo: On every - I can't believe it.

Steve: It's built - I know, I know. It's built into the software. That's the magic key. So when someone sees that you're using SplashID Safe, for which you paid $10, and they have access to your raw data, they go, oh. And they simply use Blowfish to decrypt the stored encrypted key using that secret magic phrase. Then that gives them your actual Blowfish key, which allows them to decrypt all your data. So it doesn't matter how long it takes Blowfish to get going and set up its key schedule because they only have to do it once because they can decrypt your key using the secret passphrase built into the application. Not so good.

So now, under "useful security," the good news is the bulk of the password managers are there, under this category. But unfortunately there are still some problems. A free version called Password Safe - and it says "iPassSafe free version." It uses AES-256, so nice big key. And it uses encryption in CBC, Cipher Block Chaining. The master key is randomly generated. So it pseudorandomly generates a master key, then encrypts that using the user's password, the user's master password, and that's what it stores. So that's nice. But the master password is not hashed. It is directly encrypted. It's padded out to 32 bytes because we have AES-256, so that's 32 bytes used for the key. But most users are not going to use a 32-character key. They're going to use whatever, whatever they think is enough. Who knows? Say they used 10 characters, which is probably more than usual. Well, that means that we actually need - we need 32, and the user gave us

10. So it would be nice if they hashed it. Then they'd come up with, instantly, 256 bits of garbage-looking stuff, like the output of a hash is just going to be debris, but it's going to be based on what you gave it. No, these people just use it directly. They pad it out with nothing, essentially zeroes, to the full 32 bytes. And that's what they encrypt.

So the problem is, although you would have to be doing AES-256 decryptions, the idea would be you would guess the password with AES-256 and decrypt it. The instant you see that the end is all zeroes, you know you guessed right. So it gives you, you know, it's nice encryption. It does require you to use AES-256. You can, however, do this in an offline attack. So if you got a hold of the data, you'd take this somewhere with GPUs that are set up for fast AES decryption. And you can do this in parallel. You start pounding on it. And the instant you decrypt such that the whole end, the tail of this is all zeroes, you can be very sure that you've got a candidate, at least. So it makes it very quick to crack this under testing, under brute force, if you wanted to. Still, I mean, it's not bad, and it's free. So it certainly beats the pants off any of the other free things that we've looked at so far.

There's My Eyes Only Secure Password Manager, stores the master password, the answer to the secret password recovery question, and it uses RSA. And it's unique in that. It's the only one that we looked at that uses both asymmetric encryption, uses RSA public and private keys, and it stores all those in the iOS keychain. So iOS manages some of the data for this password manager, which provides some good security. iOS keychain has different attributes that you can store things under. This is stored under the attribute of "accessible when unlocked." So when you unlock your phone using the normal procedure, then these things stored in the keychain are accessible to the password manager, which is reasonable, which means when it's not unlocked, then they're encrypted securely. So it does mean, though, that if you had an unencrypted backup, then that would be a problem.

So the problem is the users, all of that same data, the master password, the secret recovery question, and the RSA public and private keys, are also all for some reason encrypted in the same database using RSA. But it's only 512 bits. And we were just talking recently about how 768 had been cracked, and it gets much easier to crack it as the RSA modulus shrinks. So this is only 512-bit RSA, not really strong enough because factoring 512 bits is now feasible and is getting more so all the time. So again, you've got some good security; but it's like, okay, why didn't they use 1024 or 2048? Because it doesn't take that long to do it with contemporary devices.

Strip Lite Password Manager uses AES-256 encryption. And these guys did a good job. It's one of the first that is really pretty strong. They compute the encryption key using password strengthening, that PBKDF2, 4,000 times, using the master password that the user provided and a per-database salt. So again, they protect themselves from any precomputation attacks and do this 4,000-round password strengthening. So that looks pretty good.

Safe Wallet Password Manager, for $4, uses AES-256 encryption also. And they do also password strengthening 10 times, so not quite as strong as Strip Lite, but still pretty strong.

DataVault Password Manager uses AES-128 encryption in ECB - that's Electronic Code Book - mode where there isn't any block-to-block chaining. You just use each block and encrypt it separately, which is probably fine for this kind of data. They encrypt the key using the master password, pad it out to 16 bytes. So that's a little bit of a concern because when we don't hash, and we just pad, then it is possible, as we saw earlier, to quickly determine whether we've hit the right password because we're going to end up

with an obviously padded result and not just pseudorandom noise in our test decryption. But they also use the iOS keychain to store everything, so they're pretty safe.

mSecure Password Manager, for $10, uses Blowfish encryption. The encryption key is an SHA-256 hash of the master password, so that's pretty strong. They do password verification by performing a trial decryption of a known verification value for comparison. So when you enter your password, they hash it and then perform a trial decryption of something whose decrypted value they know. And if it matches, then it's safe. So that means, okay, you could perform an offline attack. Password recovery would require one SHA-256 process and a Blowfish key setup. And that's significant because that's very slow. So I think mSecure looks like they did a good job.

And finally LastPass - which is as we know $1 per month for the premium, Last Pass Premium, but they use the same technology even for their free, uses AES-256 encryption, so nice strong key. They use an SHA-256 hash of the username plus the password. So that's got the advantage of probably being longer than if you were just using the password. Essentially the username becomes the salt when you're entering the password every time, after you've set it up. And they verify by decrypting the 256-hash of the encryption key. So password recovery for LastPass requires two SHA-256 hashes and an AES-256 decryption. So that's also pretty strong.

So what we see is there are some password utilities which have done a very good job. There are some that have tried, but have made some simple mistakes that render them essentially useless because it's very easy to look up the password or decrypt their secret key because they encrypted it with something that was known, even though it was random gibberish. It's like, okay, well, this is a reverse engineer's joy. And there are many that perform no encryption at all. Everything is stored in plaintext. The password just is checked to see if it's the same as what you put in before. And if it is, it lets you look at your data, you and anybody else who might have it.

So strength varies across the complete spectrum. There's no way to know what you've got unless someone - unless they disclose to you exactly what algorithm they are using, which would be nice. Most people don't. They just say, oh, military-grade encryption, if they have any encryption. Again, as we know, as we well know from the podcast, just saying that means nothing because you may be using military-grade encryption, but storing the unencrypted data in the file. So...

Leo: It just shows how tricky it is.

Steve: Yes.

Leo: I mean, it's not - you can know a lot and still do it wrong.

Steve: Yes. It is very - we see that all the time, people doing a good job with encryption and making a simple mistake that allows the bad guys to get around it.

Leo: Did you look at 1Pass - I think it's called 1Password? Because that's kind of the best known one.

Steve: Yeah. 1Password...

Leo: 1Password, that's it.

Steve: Yes, the numeral 1Password.

Leo: Yeah, yeah.

Steve: And they're good people. I did look at it. I looked at several of their blog entries. This report from ElcomSoft was a little harsh about them.

Leo: Really.

Steve: Well, but...

Leo: They're probably the No. 1 iOS password manager.

Steve: Well, yes. And they are absolutely strong. They're as strong as any of the good ones.

Leo: Oh, okay.

Steve: And from looking at the blog postings, they're going to make it stronger. They weren't, as I recall, they weren't doing any password strengthening, though all of their crypto was absolutely good and solid. I can probably - I didn't have it in my notes, but I think I've got the - I've got it right here in front of me, the ElcomSoft deal, what they said about 1Password. Yeah.

1Password Pro, it is $14.99. And it actually uses a bunch of MD5 hashes with salt, so rainbow tables cannot be applied. And it uses AES-128 encryption to generate database keys and strong validation. And I do know from reading their blogs that, if they haven't already, they're just in the process of adding some good strengthening to bring it up to speed. But I was impressed by everything that I saw on their website. So I think 1Password Pro is - and it looks like it's the priciest one of the ones we've seen. But they've done a good job. So I would absolutely trust them. There is no backdoor, no shortcut into passwords stored with them.

So takeaways are that many popular password storage apps provide little or no actual security. They're just pure eyewash. It just prevents you, the user, from...

Leo: [Laughing] Eye wash.

Steve: ...from getting past the front door. But anyone with access to an unencrypted

backup or to the device itself, if it's not locked, or if there's a way that the lock can be bypassed, although we see that Apple has done a very good job of that on the later devices, many of them just won't prevent you from getting in at all. We see that Apple's own protection is typically far superior to what certainly some of this password software provides. But the better ones that we talked about really, I mean, it requires full-on brute-force crypto in order to crack them. So you want to use a good, strong password. That advice still applies.

And so Apple users, and same thing for BlackBerry users, BlackBerry also does good - BlackBerry's been a crypto leader for a long time. So they use actually twice the password strengthening that Apple does. They use 20,000 iterations of the strengthening algorithm in order to generate their final key. Not that it really matters because you just do that once. And all you'd really see from a UI standpoint is a slight pause as it accepts your key, which is entirely acceptable because the bad guy is going to face that pause every single time they guess. And so you want them to be slowed down.

So complex backup passwords. Use the best strongest daily unlocking passcode you can. And length matters, so do something easy to do but hard to guess, especially when the bad guy doesn't know what you've done. And absolutely encrypt your backups. And listen to this podcast...

Leo: For more.

Steve: Yeah, well, use one of the better password managers.

Leo: Yeah, yeah. LastPass continues to impress.

Steve: Yup. They understand crypto. They've made no mistakes.

Leo: And they're totally cross-platform, a buck a month for the pro, which you don't even have to pay for, but it's worth.

Steve: Yup.

Leo: I think that's probably a good choice.

Steve: It's what I use.

Leo: Yeah. Thank you so much, Steve Gibson. He is the man in charge at GRC.com, the Gibson Research Corporation. That's where you'll find him. You'll find him on Twitter, @SGgrc or @SGpad, and I presume you're putting some stuff up there because of your new iPad.

Steve: Yup, have been.

Leo: Lots of thoughts there. And don't forget SpinRite, please, the world's finest hard drive maintenance utility. That's at GRC.com, the one thing he charges you for. Everything else is free, lots of freebies including ShieldsUP!, which everybody knows, but lots of free security programs, utilities, information about things like Password Haystacks, which Steve referred to. If you want to know more, that's there. And don't forget that there are 16Kb versions of this show, for those of you with bandwidth caps or bandwidth impaired or on dialup, as well as full transcripts at GRC.com. We have the audio and video at our site, TWiT.tv, and we do this show every Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern, if you'd like to watch live. Next week Q&A. And if you've got a question for Steve, go to GRC.com/feedback. And I'm sure he's collecting them even as we speak. Thanks, Steve. We'll see you next week.

Steve: Thanks, Leo.

Leo: On Security Now!.