Apple Encrypts the Cloud

Description: This week we answer the following questions and more: What browser just added native support for Passkeys and where are they stored? What service have I recommended that suffered a major multi-day service outage? How can you recognize a totally fake cryptocurrency trading site? Which messaging platform has become cybercrime's favorite, and how would you go about monetizing desirable usernames? What's the latest in TikTok legislative insanity, and is it insane? Which two major companies have been hit with class-action lawsuits following security breaches? Was Medibank's leaked data truly useless? And Apple has finally given us the keys to our encrypted data in the cloud, holding none for themselves - or have they?

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-901.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-901-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. And it's again questions and answers. What browser just added support for Passkeys? How can you recognize a totally fake cryptocurrency trading site? And has Apple finally given us the keys to encrypted data in the cloud? Steve analyzes it. All the security news next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 901, recorded Tuesday, December 13th, 2022: Apple Encrypts the Cloud.

It's time for Security Now!, yay. You've been waiting all week, haven't you. Well, good news, it's finally here. So is Steve Gibson from GRC.com, our host, the man of the hour. Hi, Steve.

Steve Gibson: Yo, Leo. Great to be with you. Episode 901. And I was originally going to talk about something else, but this news hit, and it was like, okay, you know, actually it was by far the most tweeted question that I've had in a long time about any news. And that of course is Apple's announcement that they're going to begin encrypting iCloud. So Apple Encrypts the Cloud is today's topic. But that's just what we're going to wrap with. We're going to answer a bunch of questions as we are now poised to do for the last few weeks. What browser just added native support for Passkeys, and where are they stored? What service have I recommended that suffered a major multiday service outage?

Leo: I love, by the way, I love this question format. This is great.

Steve: It works.

Leo: Yeah.

Steve: Yeah. How can you recognize a totally fake cryptocurrency trading site? Which messaging platform has become cybercrime's favorite? And how would you go about monetizing desirable usernames? What's the latest TikTok legislative insanity, and is it insane? Which two major companies have been hit with class-action lawsuits following security breaches? Was Medibank's leaked data truly useless? And Apple has finally given us the keys to our encrypted data in the cloud, holding none for themselves. Or have they?

Leo: Oh, boy. That's a good one. That's a great question. Can't wait to hear that. I knew, you know, you texted me earlier that you were going to cover this, and I told everybody on MacBreak Weekly. Apple just rolled this out. I just turned it on in my phone. Well, actually I didn't because it said, before you turn it on, you have to get updates on all of your Apple devices, of which there are more than a dozen. Which makes sense.

Steve: Yeah, I'll talk about that. You cannot have any older versions. They all have to know about this technology.

Leo: So it's going to take me - I have to go around to a lot of stuff and update it before I can do it, including my watch. Picture of the Week time, Mr. G.

Steve: So rarely does a picture, I think, really work as an analogy as well as this thing does. As a coder, and you're a coder, we know the danger of, as you're writing code, just like not making sure that what you're writing is correct. There is this sense of building a foundation. And you sort of - you create part of it, and then you add to it, and it grows. Well, you know, you want the beginning of that process and all the various stages between the beginning and the end to be correct. Anyway, so the caption on this picture is "Just keep coding, we can always fix it later." And this is so perfect because - so what you and I are laughing at is two bricklayers, I guess maybe this is not...

Leo: They started okay.

Steve: Well, except look at that vertical one.

Leo: Yeah, maybe not.

Steve: I love that vertical one. It's like, so you have to ask, what is the story here? I mean, this is - they kind of know that bricks are supposed to be horizontal.

Leo: Kind of.

Steve: Kind of. But first of all, they seem to have a problem with their brick sizing. You know, these are not all the same size bricks. And so, and there's like some wedgies in

there, and there's, I mean, it's just - it's a disaster. But the beauty of the picture is like way down to the bottom is a brick that it's never going to get fixed because it was four days ago in the process of building this wall that this brick, someone stuck it in vertical because, well, they had a gap to fill or something.

Leo: Eric in our chatroom says that's a go-to statement. Once you see it, you can never unsee it. That's hysterical.

Steve: Yeah. So anyway, I just - it's a great analogy because, you know, these guys just said, oh, well, you know, what the heck, just keep going. And this is never going to get fixed. That brick down there, it will be vertical as long as that wall is standing, just like some bug that got written in the beginning, and they just said, oh, just, you know, we'll fix it later. No, bad idea.

Okay. A good idea was covered by Ars Technica's Friday headline, which read: "Passkey support rolls out to Chrome stable." They said - this is Ars Technica. "With a huge list of caveats, initial Google Passkey support is here." They wrote: "Google's latest blog says: 'With the latest version of Chrome'" - that's 108, I have it, probably everybody does - "'version of Chrome, we're enabling Passkeys on Windows 11, macOS, and Android.'" And Ars wrote: "The Google Password Manager on Android is ready to sync all your Passkeys to the cloud. And if you can meet all the hardware requirements and find a supporting service, you can now sign into something with a Passkey."

So they then in their coverage take some time explaining stuff that we all know about Passkeys that we've talked about. And they get most of it right in kind of a watery down sort of way. Then they talk about compatibility by writing: "Today Passkeys essentially require a portable device, even if you're logging into a stationary PC. The expectation is that you'll use a smartphone for this, but you can also use a MacBook or iPad. The first time you set up an account on a new device, you'll need to verify that your authenticating device, your phone, is in close proximity to whatever you're signing into. This proximity check happens over Bluetooth. All the Passkey people are really aggressive about pointing out that sensitive data is not transferred over Bluetooth. It's just used for a proximity check. But you'll still need to deal with Bluetooth connectivity issues to get started," they say.

"When you're signing into an existing account on a new device, you'll also need to pick which device you want to authenticate with, probably also your phone. If both of these devices are in the same big-tech ecosystem, you'll hopefully see a nice device menu; but, if not, you'll have to use a QR code.

"Second big issue," they said, "did everybody catch that OS listing at the top? Google supports Windows 11 with Passkeys, not Windows 10" - what? - "which," they write, "is going to make this a tough sell. Statcounter has Windows 11 at 16% of the total Windows install base, with Windows 10 at 70%. So if you happen to make a Passkey account, you could only log in on newer Windows computers." Okay.

So they continue: "Passkeys get stored in each platform's built-in keystore, so that's Keychain on iOS and macOS, and Google Password Manager or a third-party app on Android, and 'Windows Hello' on Windows 11. Some of these platforms have key syncing across devices, and some do not. So signing in on one Apple device should sync your Passkeys across to other Apple devices via iCloud, and the same goes for Android via a Google account, but not Windows or Linux or Chrome OS. Syncing," they write, "by the way, is your escape hatch if you lose your phone. Everything is still backed up to your Google or Apple account. Google's documentation mostly doesn't mention Chrome OS at all, but Google says: 'We're working on enabling Passkeys on Chrome for iOS and

Chrome OS.' There's also no support for Android apps yet, but Google is also working on it." Which makes me wonder, like okay, a lot of these limitations seem significant and weird.

Anyway, they wrap up this news of Chrome's emerging support by writing: "Now that this is actually up and running on Chrome 108 and a supported OS, you should be able to see the Passkey screen under the 'autofill' section of Chrome settings." So, you know, of a Chrome browser's settings. So you can go to chrome://settings/passkeys. Put that into the address bar. And they said: "Next, we'll need websites and services to actually support using a Passkey instead of a password to sign in." They said: "Google Account support would be a good first step. Right now you can use a Passkey for two-factor authentication with Google, but you can't replace your password."

And they finished: "Everyone's go-to example of Passkeys is the Passkeys.io demo site, which we have a walkthrough of," and then they do that. So, you know, I've got Chrome 108. So I put "chrome://settings/passkeys" into Chrome's address bar, and I was greeted with a little thing that said - okay, this was on Windows 10. It just said: "To manage Passkeys, use a newer version of Windows."

Leo: Oh, god.

Steve: And it's like, wow, really? I mean, that's what you're going to get on Windows 10? So presumably it's the Windows Hello which, I mean, it's very cool that the browser is not storing your Passkeys, that the browser manages this process, but it's in the substrate. It's in Windows itself where the Passkeys are stored. That seems like a much better idea than having them in the browser. But wow. You're not letting people with Windows 10 have it? Good luck with that.

So, you know, 70% of the world won't be able to use it. These feel like arbitrary limitations. Lack of syncing among competing platforms and devices feels like the attempt to create walled gardens. It feels to me as though Passkeys, the way this is going, Passkeys, like passwords, may also become the domain of our existing password managers. We know that any password manager that has a pulse has got to be racing as fast as possible to getting support of Passkeys up and going. And of course they will provide cross-client synchronization. And none of this, sorry, you can't use it on Windows 10 nonsense. So, you know, we can hope that that's coming. We still have the chicken-and-egg problem, of course, of getting it to actually work and then having places where you can use it to sign in. But you and I, Leo, are old enough to remember when people thought that the web would never happen because it's like, well, you know, why is anyone going to put a web page up...

Leo: What do we need that for?

Steve: ...when there's only five people who are using the Internet?

Leo: I've got Gopher. I don't need a website.

Steve: Yeah, exactly, exactly. Okay. So while we're talking about synchronization, I thought I should mention that my favorite cloud synchronization platform, Sync.com, had something happen to it. The problem first surfaced last Wednesday, apparently after a scheduled maintenance somehow went wrong, and things didn't appear to be fully

restored until just yesterday. I utterly depend upon Sync.com, and the outage had me revisiting the wisdom of that dependency. I'm not a typical user since I also run a pair of NAS boxes, you know, Network Attached Storage boxes, at each of my two locations. And as we know, there are many other syncing alternatives. Reading between the lines of Sync's frequent online status updates through these slowly passing days, you sort of got the sense that this was causing a major problem for their customers. You know, there was a lot of, like, we really understand how much you need this back. And believe us, we're working on this as hard as we can. Yet they never really told us what was going on.

Anyway, I came away - first of all, I thought it was my problem. I didn't immediately - I didn't even know that there was like a status log page until I dug in. So one of the things that I discovered, I know that a lot of our listeners are now Sync.com users, probably as a consequence of me having said, yeah, it's been years, and I love it. I'm still using it. Anyway, what I discovered was that the client, the desktop clients do not update themselves. Or, if they do, mine weren't. Like they got stuck or something. Anyway, the world, the Sync.com world has gone to 2.1.7. What am I saying? 2.1.4. Sorry. Don't go crazy. 2.1.4. I had to manually get that and run the latest version in order to bring my clients current. They were, you know, I've had Sync for years; and, like, they were really old. So everything seems to be like working really well now that I actually have clients that were written in this century.

The good news is when you run it, it seamlessly installs itself and, like, removes the old one, puts in the new one, gets us all set up and going. So I just wanted to say, yup, if you were affected by this Sync.com update, I feel for you. I was, too. They were saying, oh, some of our users are experiencing problems. Really? Okay. I would love to hear, for example, if there are Sync.com listeners of this podcast who had no problems at all for the last week. That would be interesting to me because maybe it was just some people. I don't know. Okay.

Leo: By the way, you use, you mentioned Syncthing.

Steve: Yes.

Leo: And of late, since Syncthing is open source and completely local, I feel like I don't know if I need a cloud because I have everything on every computer.

Steve: Yup.

Leo: And then I was thinking, well, one advantage of the cloud is it's always on. So you use a NAS, as I do, a Synology NAS. You could put Syncthing on your Synology NAS. So I'm basically treating my Synology NAS as the canonical copy of all that stuff.

Steve: Yup.

Leo: And it's pretty fast. I use Syncthing to update source code. I know that's one of the things you do is so that you can work at Lorrie's and at the office. So it's pretty fast. I will finish a project, close a window, go over to my other computer, and it's almost always there by then.

Steve: So I'm glad you mentioned it because I should have. I have Syncthing on both of my NASes, both the Drobo and the Synology. I use Syncthing to synchronize some directories between them. And Syncthing is what we use with Lorrie's fleet of laptops which she has out to her clients to keep them all synchronized.

Leo: Smart. So they all have the same stuff on them. That's smart.

Steve: Yeah, yeah. It is absolutely a win.

Leo: It's free. It's open source. It works. It does NAT traversal. No, I just - I love it. It's really, really good. In fact, it's really made me rethink how I back stuff up since I have a copy of everything everywhere.

Steve: Yup.

Leo: Without being in the cloud at all.

Steve: Yup. Okay. So I titled this piece "Medibank Reboot" because that might literally be what happened this past weekend. We've been recently following the drama with Australia's latest private medical insurer, Medibank. That's the one that exposed a huge number, well, a huge number of its current and past customer data. 9.7 million clients got exfiltrated on the dark web, and then it got released into the public when they refused to pay. Well, on Friday the Sydney, Australia Morning Herald had an interesting bit of news. Their coverage began: "Private insurer Medibank's app, stores, contact center, and IT systems will all go dark this weekend as it overhauls its cybersecurity following the nation's worst data breach in corporate history."

They said: "From 8:30 a.m. Australian Eastern Daylight Time on Friday" - I'm sorry, p.m., 8:30 p.m., end of the day in Australia on Friday, p.m., Eastern Australia. They said: "Australia's largest health insurer will shut down its IT systems followed by retail store and customer contact center closures on Saturday to 'further strengthen systems and enhance security protections,'" was the official line from Medibank. They said: "The company expects normal activity to resume by Sunday at the latest."

They also said: "Microsoft IT security experts from the Asia-Pacific region will travel to Medibank's Melbourne headquarters to assist with the operation." And then I kind of quipped to myself, I guess Microsoft is going to show them where the Update button is located on their server. And they said: "This was said to have been planned over several weeks and will be Medibank's first shutdown of such scale." Well, yeah, you can imagine. This is, like, for a massive private insurer to shut down everything. So in other words, you know, shut down, update software and firmware and everything else, then turn everything back on again.

So the Herald finished by saying: "The overhaul is part of a series of maintenance strategies, termed 'Operation Safeguard'" - so, right, they gave this a big banner as part of this - "established after the personal information," they said, "of up to 10 million current and former Medibank customers was breached in a cyberattack. The data was released on the dark web when Medibank refused to pay a 15 million" - we never had numbers before - "a $15 million ransom demand by the hackers, who police have said were based in Russia. The company said the damaging cyberattack will cost the firm at

least $35 million in initial recovery costs, though that is likely to grow as law firms and regulators circle. A Medibank spokesperson said, although there had been 'no further suspicious activity' detected inside its systems since October, the insurer was carrying out further maintenance to strengthen its online security."

Now, okay. If we can read between those lines, what might be happening is a complete wide-scale coordinated reinstallation of system software. I mean, not just an update. As we've noted before, and Leo, you and I have talked about the problem after something has been compromised is, in a complex system, you can never really be certain that something isn't still hiding somewhere. So, you know, imagine you're in their shoes, and there was - and we don't know, right, what the forensic examination actually found. It might have left them horrified or terrified, you know, and feeling that they had no choice other than to just wash everything clean and reinstall. And boy, if so, what a nightmare.

Oh, and they did say: "Since the hack, Medibank has bolstered monitoring, added detection and forensics capability across its system, and scaled up analytical support via specialist third parties." Right, so they brought a bunch of people in. And they said: "It also recently introduced two-factor authentication" - oh, imagine that - "where access is granted only after providing a code sent to one's email or SMS." Oh, okay, so not very good two-factor authentication, but better than none. Anyway, so being completely down and offline for as many as two days sure does sound like a major sweep cleaning of all mission-critical systems, and they probably had no choice.

It was P.T. Barnum who is credited with the saying "There's a sucker born every minute." I was reminded of that when I came across this bit of news about a cybercrime group that's been named "CryptosLabs." The cybercrime research group known as Group-IB, which we talk about from time, identified a new cybercrime operation which they named CryptosLabs. Okay, get this. Since 2018, so four years, this CryptosLabs group has operated a network of more than 300 scam websites posing as fintech, you know, financial technology, and cryptocurrency trading platforms.

Group-IB says the group used search engine ads and social media posts to trick French-speaking users across Europe into investing more than 480 million euros, okay, so nearly half a billion euros, in these scam websites by leading them to believe that they would get to trade in stocks and crypto assets. But researchers say that once users put money into their accounts - their, you know, bogus accounts - the crooks either asked for more, you know, get as much as you can; right? Or ignored their customers before shutting down platforms and moving to a new domain.

Group-IB said it named this group CryptosLabs after the kit they used to automate the deployment of fake trading portals. Right. Since we're going to be doing this a lot, let's create a kit that makes it real quick to set up a new fake trading portal because, you know, we're not going to be there long. We're going to have to do it again soon. Okay. It typically, these portals typically mimicked 40 different popular banking, fintech, and crypto brands. So, you know, these guys were pretending to be Coinbase, and set up one fake cloned Coinbase site after another.

People, you know, had heard of Coinbase. Their friends were talking about it. Then they encountered an advertisement in a search engine or in social media, and they thought, hey, I just got paid, now's the time. They didn't really know what Coinbase's domain name was, so they just clicked the advertisement and went to Coinbases.org. And since everything looked quite official, they never thought that it might be an illegitimate ad and site. People would transfer money in; and, at some point, once enough had, or someone wanted their money back, the fake domain would be shut down and another would be set up in its place using this crypto slab tool that just, you know, just spits out these fake platforms.

So this is not the Internet that Tim Berners-Lee envisioned back in 1989 when he originated the concept of an Internet full of interlinked HTML documents that anyone could create and publish on their own. It's not as if crime hadn't existed before. It's just flowed into this new medium. So that's going to happen.

Two interesting pieces of news about Telegram. First, malware on Telegram. The Russian security firm Positive Technologies published a report on Telegram's budding cybercrime ecosystem. According to the company's scans, Telegram has slowly replaced hacking forums and is currently being used for advertising a wide spectrum of hacking services and malware. The sale of remote access trojans, corporate network account credentials, and cash-out services are among some of the most popular topics on Telegram now.

Okay. So there's one tidbit. But get a load of this one. Telegram, which now we know is generally becoming the favored hangout of the crime underworld, has decided to further expand their subscriber base by allowing users to sign up without needing one of those pesky SIM cards to anchor their identities. Telegram wrote: "Today starts a new era of privacy. You can have a Telegram account without a SIM card, and log in using blockchain-powered anonymous numbers available on the Fragment platform."

Okay. So, what? I thought, what's Fragment? So I followed a link, https://fragment.com, and I was told: "Oops. This service is not available in the United States." Okay. That's interesting. I wonder why not? So I thought that Wikipedia might know about Fragment, and perhaps it does. But the word "fragment" is so common that I wasn't able to find it there among all of the other fragments. Googling turned up an abbreviated reference that was more tease than anything else. Google said: "Buy and sell usernames. Secure your name with blockchain in an ecosystem of 700-plus million users and assign it as a link for your personal account," dot dot dot. And that's where the little summary cut off on Google Search.

I thought, buy and sell usernames? What? Now, I know that Kevin Rose might be willing to sell you an icon of a zombie. But what's Fragment? So I dug in some more, and I found some news about Fragment over at Crypto.news, where their coverage had the headline "Telegram now allows users to buy and sell usernames via auction." And then it goes on to explain: "Telegram releases new feature, transforms usernames into digital assets." Then it says: "Popular cloud-based instant messaging app Telegram has just launched a new feature to allow users to buy and sell short, recognizable '@usernames' for personal accounts, public groups, and channels.

"Telegram has commenced an auction for the best usernames on Fragment, a free collectible trading platform. With this new feature, Telegram usernames have become digital assets that can be secured and sold between parties. According to the innovative platform's unveiling note, ownership of the collectible usernames is secured in the immutable ledger of TON" - (T-O-N), and it goes on - "a fast and scalable blockchain network," which no one's ever heard of before. "Interestingly, the new feature allows owners to add multiple username aliases to their personal accounts, group, or channel. Also, each collectible name can be accessed with its @username on Telegram or outside Telegram using links such as username.t.me and t.me/username.

"To acquire usernames on Telegram, buyers visit Fragment, search for their desired" - unless you're in the U.S., I guess. For whatever reason you can't have a Fragment in the U.S., but here a VPN might be your friend - "search for their desired username and click on auction if that username is still available." So, okay. Telegram is like tied in with Fragment somehow. And now you have to buy your Telegram username on the blockchain. So then it says: "Buyers will then be redirected to a page which shows the highest bid along with the bid setup and minimum bid."

Okay. So earlier this said that TON was an immutable ledger. Apparently it's also a currency. I went over to CoinMarketCap.com/currencies/toncoin, and I learned that a TON has a current value of $2.10 U.S. And it was fluctuating as I was there at that page, couldn't make up its mind between $2.10 and $2.11. Also it's got a 24-hour trading volume of $44 million.

Leo: Whoa.

Steve: Yeah, $44,628,950. That was yesterday, 24-hour cycle. And I saw that there was a TON.org. So I went over there, and I discovered that TON stands for The Open Network (TON). And from the TON homepage we learn that: "TON is a decentralized layer-1 blockchain designed by Telegram to...

Leo: Ah.

Steve: Uh-huh, so the loop closes. "Designed by Telegram to onboard billions of users." They hope. "It boasts ultra-fast transactions, tiny fees, easy-to-use apps, and is environmentally friendly."

Okay. So let's get this straight. Telegram noticed that they had a lot of users and a popular platform. So they decided that they wanted to monetize the ownership of Telegram usernames. They wanted to create a marketplace which would allow Telegram usernames to be bought and sold. So they created TON, their own cryptocurrency, anchored it with their own blockchain. They then established an auctioning system which uses the TON as its exchange currency to allow their users to bid for, purchase, and sell Telegram usernames. The rest of the coverage of this, the first part of which I already shared, tells us how this is going.

Under the heading "Massive instant adoption of new feature; millions of TONs earned in username sales," we have less than - this is the reporting of this. "Less than six hours after the launch, thousands of usernames featuring international brands and celebrity accounts have been put up for sale. Still on auction are @nike, @king, @esport; while others such as @auto, @avia, @fifa, et cetera, have been sold for as much as 900,000 TON." Now, we don't know what the TON was worth when it sold. But the TON is now $2:10. So that's, what, $1.8 million, thereabouts.

Judging by data on the Fragment platform, millions of TONs, you might say a ton of TONs, have been earned by Telegram users from the sales of their short usernames. So users who were on Telegram early, got in, got a short name, those are desirable, they're now able to cash in on their short username by selling them for TONs, and then liquidating TONs for cash. There's still more to be made as there are still lots of usernames currently on auction, the report says. "An example is the popular shoe brand @nike, which has over 300,000 TON bid for it at the moment. Telegram is affording its users full ownership of their usernames, and they are embracing the idea." So think about that. There's no trademark protection, I guess. So anybody could buy @nike on Telegram who is willing to pay enough. And that's got to make Nike a little nervous; right? Because Telegram, you know, it is a happening place right now.

Leo: So I think it's more complicated because I don't think they actually own TON. Telegram - I love Telegram, by the way. And, you know, you can look at what you just described in, as you did, kind of...

Steve: Askance. Askance.

Leo: Askance. But also if you're trying to solve this issue of, and this is an issue, it's an issue with Signal, having to tie your account to an actual phone number...

Steve: Yeah.

Leo: ...you'd need to do some sort of - I think blockchain is actually, this might be one good application, blockchain, some sort of decentralized authentication system. My short name is @leolaporte so, you know, I own that. But I didn't buy it with TON. I just always have had it.

Steve: Right.

Leo: So when you started talking about this, I said, well, wait a minute, doesn't Telegram have its own crypto? And they did. They started something called the Gram in 2018, which the SEC...

Steve: That's kind of a good name. I like that.

Leo: It was a great name. SEC halted it because they were doing an ICO. Remember when that was the big thing, the Initial Coin Offerings?

Steve: Right.

Leo: And they had registered the ICO. So the SEC halted it. So Telegram abandoned TON, which stands for The Open Network. And it's open source. So developers have kept it going.

Steve: Ahhh.

Leo: According to The Verge, Pavel Durov, the owner of Telegram, said he supported the project a year ago, saying I'm proud that the technology we created is alive and evolving.

Steve: Cool.

Leo: So it is a third-party effort. And I agree, anytime I hear crypto I go, okay, what's - and especially if you're selling usernames. You know, this is a - you know. But if you think about it, if you wanted to replace phone numbers, you need some sort of unique fingerprint; right?

Steve: Yeah.

Leo: Could do what Threema does and, you know, meet in person and do it. But there's some sort - Threema generates basically a private and public key chain.

Steve: Correct, correct, correct.

Leo: Key pair. But how do you get your key out there is the problem. So this is an interesting solution. I wish Signal would do something that didn't require a phone number because I think that's a problem.

Steve: Yeah. And it definitely is a privacy concern, right, because you've got to have something that is, you know, anchored to a SIM.

Leo: Plus Signal might - any Signal app I run is attached to a one phone. I can't put it on another phone without...

Steve: Right. You're only able to have it, like you're able to sync a desktop, but not another phone.

Leo: Exactly. And with Telegram I can. I have Telegram everywhere. So, you know, different strokes. I agree there's, you know, potential for misuse, obviously.

Steve: So I just - I wanted to mention, because this is in the news, in the technology, that the TikTok banning has continued. Texas has now joined the ranks. And I was going to say that Texas was the latest, but that was yesterday. So who knows what's happened since then. Texas Gov. Greg Abbott has banned the use of TikTok on the devices of state employees, and in doing so becomes the fourth, happens to be Republican-led state to ban TikTok on employee devices. That follows Maryland, South Carolina, and South Dakota. Remember that last week it was South Dakota that I noted was first, with their Gov. Kristi Noem saying that she hoped other states would be following suit. I guess her wish is coming true. Greg Abbott also ordered state agencies - this was interesting - to come up with plans to govern the use of TikTok on state employees' personal devices, not owned by the state.

Leo: Yeah. Good luck. You can't do that.

Steve: So yikes.

Leo: That's just performative. You can't do that.

Steve: Yeah. He wrote in a letter to state agency leaders that there are "growing threats posed by TikTok" to the state's sensitive information. "TikTok harvests vast amounts of data from its users' devices - including when, where, and how they conduct Internet activity - and offers this trove of personally sensitive information to the Chinese government." Okay. But wait, there's more.

Indiana's attorney general brought a pair of lawsuits against TikTok, accusing the company of deceiving users by claiming that their data was protected from the Chinese government and for exposing Indiana children to adult content. The lawsuits claim that the Chinese-based social media giant has deceived and harmed Indiana residents. Indiana's first lawsuit alleges TikTok has marketed its video-sharing platform as safe for teens, even though its algorithm "serves up abundant content" depicting drugs, sexual content, and other inappropriate themes. The second lawsuit asserts that TikTok has deceived consumers by suggesting their personal information is protected from the Chinese government and the Communist Party.

Okay. So the attorney general said in a statement: "The TikTok app is a malicious and menacing threat unleashed on unsuspecting Indiana consumers by a Chinese company that knows full well the harms it inflicts on users. With this pair of lawsuits, we hope to force TikTok to stop its false, deceptive, and misleading practices, which violate Indiana law." So the attorney general is asking for emergency injunctive relief against the company and is seeking monetary penalties for every time TikTok violated Indiana's Deceptive Consumer Sales Act. Wow.

Leo: How do you violate a sales act if it's free?

Steve: Yeah. I was wondering if maybe there was something I had missed. So I have it in the show notes. I'm not going to drag our listeners through it. But Kaspersky has a very useful, factual, piece-by-piece walkthrough, and the upshot is there is no smoking gun here. There's nothing that TikTok is doing that any of the other social media platforms, most notably Facebook, being the largest and here in the U.S., isn't also doing. I thought, okay, what's on the other side of this? How about a balanced look? So I found some coverage that NPR offered from less than a month ago about the FBI's raising of concerns, which apparently is what started all of this, over what TikTok might be capable of doing. And what's interesting is the quotes from FBI Director Christopher Wray during a Homeland Security Committee meeting. So NPR's story says: "The FBI alleges TikTok poses national security concerns." Right? Okay. So, okay. That's a concern.

So NPR says: "The head of the FBI says the bureau has 'national security concerns'" - and they even quoted that - "about the U.S. operations of TikTok, warning that the Chinese government could potentially use the popular video-sharing app to influence American users or control their devices." Gee, like what? Facebook? Like Twitter? Like everything; right? Anyway, sorry.

"FBI director Christopher Wray told a House Homeland Security Committee hearing about worldwide threats on Tuesday" - this was middle of last year, it was like the 17th, I think, of November - "that the FBI has 'a number of concerns' just days after Republican lawmakers introduced a bill that would ban the app nationwide." How do you do that? Okay. Anyway, Wray said, I mean, this is sounding like, right, some other country we talk about somewhere else. Wray said: "They include" - the concerns, that is - "include the possibility that the Chinese government could use it to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations if they so chose, or to control software on millions of devices, which gives it an opportunity to potentially technically compromise personal devices."

And then NPR reminds us: "TikTok, which hit one billion monthly active users in September 2021, is owned by the Chinese company ByteDance. Chinese national security laws can compel foreign and domestic firms operating within the country to share their data with the government upon request, and there are concerns about China's ruling

Communist Party using this broad authority to gather sensitive intellectual property, proprietary commercial secrets, and personal data." Blah blah blah.

So, you know, concerns. And based on concerns and China and communism, what we see to my reading is a bunch of grandstanding by governors and attorneys general who want to make a big deal about this because it's owned by a Chinese company. We've seen misbehavior on the part of our domestic firms, who are looking at things that they shouldn't. There was some BuzzFeed news had some audio. Because I spent some time digging into this, wondering what the heck. There was some audio that BuzzFeed's News found of some TikTok employees clearly looking at the data of some TikTok users, much like Facebook has been caught looking at their own users, and Twitter was caught doing the same. So anyway, to me this looks like a bunch of nonsense. We'll see where it goes. I would be surprised if we end up with legislation banning TikTok.

Leo: Did Kaspersky go into what information TikTok knows about you? I mean, because that's I guess the fundamental question.

Steve: Yes.

Leo: There's two parts to this. A, is TikTok giving information - let's assume the Chinese government has a pipeline into ByteDance. I mean, that's a big assumption, but let's assume they do. Is TikTok gathering - what kind of information is it gathering from my phone that it's sending to the Chinese government? That's problem number one. And then problem number two is people say, well, you know, they could use the algorithm to propagandize us, you know, to convince us of something. Which is legit, although the Chinese government is not unhappy to use Twitter and Facebook and YouTube to do that, as well.

Steve: Right, they don't need TikTok.

Leo: They don't really have to have some other way to do it. But what did Kaspersky say about - is it any different from any other app on the phone?

Steve: No. Kaspersky directly addresses the question of privacy concerns. They wrote: "One of the most viral aspects of TikTok has been privacy concerns, with questions like 'What data does TikTok collect?' and 'Does TikTok steal your information?' regularly circulating online." They wrote:

"Like many other social networking platforms such as Facebook, TikTok collects a lot of information about its users. This includes every TikTok video watched, and for how long; the entire contents of every message sent through the app since messages are not encrypted; the user's country location, Internet address, and type of device being used. And with the user's permission, TikTok also captures its user's exact location, rather than just their IP address; their phone's contacts and other social network connections...

Leo: But you have to give them that because...

Steve: ...in order to build a graph.

Leo: It's always asking for my contacts, and I always say no.

Steve: Okay.

Leo: I think I'm assuming that Apple blocks it if I don't say yes. I mean, that they're not sneakily, underhandedly...

Steve: Oh, I bet Apple would.

Leo: Yeah.

Steve: And finally, their age, phone number, and payment information. Again, if you say yes, you allow it.

Leo: You provide it. Unless you say you're 98 and you live in Muncie, Indiana. Which you could, yeah.

Steve: Yeah. So Kaspersky says: "This information can be used to assemble a detailed profile for advertisement targeting - by understanding who its users are, who their friends and family are, what they like and find entertaining, and what they have to say to their friends. To use the app, users grant access to their microphone and camera. If they create videos, the app captures close-ups of their face. Potentially..."

Leo: And by the way, again, you have to do that only if you're going to use it to create videos. I don't. I use it - and most people don't. They use it to look at videos.

Steve: To watch, yes.

Leo: And every time it says you want the camera access, I say no, you can't - no. I don't want you to have that. So that, again, that's something you turn on.

Steve: Right. So they said: "Potentially, this provides biometric data which could be used in conjunction with other images which exist online. TikTok also uses technical measures to encode its activity. This means that some of what it does is hidden from external researchers, which all the apps do. TikTok says this is to disrupt hackers and other malicious actors. There's been extensive media coverage of TikTok privacy concerns. However...

Leo: Yeah, think how mad we'd be if TikTok was sending all that information in the clear. You know? That's not good either.

Steve: The way all of our web pages used to be.

Leo: Right, right, yeah.

Steve: And Kaspersky said: "However, most social media platforms worldwide collect, use, analyze, and ultimately profit from users' personal data. TikTok argues that it collects less data than platforms such as Facebook or Google since it does not track user activity across devices." So again, to me this is all just, you know, the FBI saying, well, we have concerns because maybe, you know, "an opportunity to potentially technically compromise personal devices." Right. Because you loaded an app. All apps have that opportunity to potentially technically compromise personal devices. Anyway, to me this is protectionism; right? It's xenophobia and protectionism and an opportunity for so far it's all been Republican political people.

Leo: It's performative. It's performative.

Steve: To say, yeah, the Commies are going to get our kids. Okay. And while we're on the subject of nonsense, filed two days after LastPass's November 30th disclosure, password management company LastPass has been hit with a class-action lawsuit after experiencing two data breaches in the past three months, which we've talked about. In fact, it was the title of our podcast a couple weeks ago. The plaintiff in this case, DebtCleanse Group Legal Services LLC, filed the class-action complaint against LastPass US LP on December 2nd in a Massachusetts federal court, alleging negligence and breach of contract. The Chicago-based debt relief firm said it used LastPass to manage its passwords. However, it says LastPass was negligent in its duties, evidenced by the fact that it has experienced two data breaches in the past three months.

The class-action lawsuit alleges that LastPass was negligent with data security, stating that LastPass used ineffective data security measures to protect its customers' information. The lawsuit states: "There is a strong probability that entire batches of stolen information have been dumped on the black market, or are yet to be dumped on the black market, meaning plaintiff and class members may be at an increased risk of fraud and identity theft for many years into the future."

So DebtCleanse responded to news of the breach by changing all of its employees' passwords for accounts that used LastPass, which took considerable resources, it said. It seeks to represent all LastPass users whose information was accessed in the breach. Well, that's a very small number. It seeks certification of the class action, damages, fees, costs and a jury trial.

So, okay. The geniuses over at DebtCleanse freaked out and totally unnecessarily changed all of their passwords for everything. They noticed that LastPass made an announcement of a secondary breach following on from the first one. But they somehow failed to heed the statement - which was also right there, both times - that no user information or passwords were at any time at risk or exposed as a consequence of either of those two breaches.

Now, Leo, I know you and I feel quite similarly about class-action lawsuits. You know, from time to time I'm awarded something like 92 cents from something I purchased once that faded too quickly if it was left out in the sun or whatever. Somewhere some lawyers made some money.

Leo: Yeah, that's really it, yeah.

Steve: The individuals in the class on whose behalf the action was taken netted 52 cents, you know, or whatever.

Leo: There is one secondary value to class-action lawsuits. Companies still have to pay that money. And it certainly has sometimes a salubrious effect on the company, maybe stopping them from doing that again, if you know what I mean.

Steve: Yeah.

Leo: So there is that.

Steve: Well, and unfortunately, I mean, I can't even imagine what a trial would look like because this is technical stuff. I mean, you would like it just to be dismissed when under deposition LastPass techie says nothing that happened could have possibly compromised anyone's passwords.

Leo: Yeah, and how do you prove that to a judge and jury who are not technically sophisticated?

Steve: Oh, oh, oh.

Leo: They bring in you, somebody like you, to say, well, I'm an expert, and in my judgment it's safe. And what else are they going to do? And just, you know. You used to do that, didn't you, testify?

Steve: I did. I did. And when I tried to explain to a judge who literally had - I will never forget this - to his right was a green oxygen tank.

Leo: Oh, geez.

Steve: And he had the nasal cannula up his nose and a mask in case he needed a little extra hit, you know.

Leo: Holy cow.

Steve: I mean, this is who was, you know, judging this. And it went the wrong way. And I thought, okay, I'm done here. This is dumb.

Okay. But we're not done. A tiny piece of Rackspace's overall cloud hosting business hosting Microsoft Exchange email services, was hit 11 days ago by ransomware. Things have not been going well for them ever since. An article published yesterday in IT World Canada summed things up and offered some interesting perspective on the cloud industry overall. Here's what IT World Canada wrote.

They said: "On December 2nd, Rackspace experienced an outage for its Hosted Exchange environment. The company blamed a 'security incident.'" Unfortunately, first mistake was they didn't say what it was. "A status update issued by the company noted: 'We proactively shut down the environment to avoid any further issues while we continue work to restore service.'" Okay, now, that really stretches the phrase "putting a good face on the problem." What, they were too embarrassed? I guess. They should have just said "We got hit with ransomware" right from the start because that happens now, unfortunately. Anyway, back to what IT World Canada said. They said: "One week later, the outage continues."

Leo: Wow.

Steve: Yes.

Leo: Sounds like that Medi story, wow.

Steve: "And the company has confirmed that it is due to a ransomware attack. Rackspace has not indicated how much data might be lost, whether it will pay the ransom, or when the managed exchange service will resume. This is the only information from the section of the website dealing with the press. However, in an announcement on its investors page, the company notes that the hosted exchange business accounts for less than 1% of the company's revenue." Which, by the way, is a hefty $3 billion per year. And on the page they reassure investors that the company has cyber insurance. And I guess they're going to be needing it. We'll get to that in a minute.

But World IT said: "But the attempt to reassure investors may not be working. In an article on December 10th" - so that would be last Sunday - "investment blog MarketWatch criticized the company for being "frustratingly closed mouthed" about the incident, and noted that the company's stock price had declined. The article notes: "Since the incident came to light, Rackspace shares have tumbled by a third. This is a relatively small part of the company's business, only about $30 million a year in revenue," right, against 3 billion in total, so yeah. That's 1%. "But the bad blood that Rackspace is generating will leave a lasting stain."

The stinging critique of the company's communication is significant, but another quote from the article raises an issue that could extend beyond Rackspace to the entire cloud industry. The writer notes: "While I remain a big believer in cloud computing, the Rackspace attack is an urgent reminder of the risks in relying on cloud for mission-critical applications if your provider isn't keeping up with software patches and paying attention to security risks." So the use of cloud computing, even for mission-critical applications, has grown rapidly for years, but that growth has accelerated in the past year and is predicted to further accelerate in the next 24 months.

And, you know, when we had Paul and Mary Jo on Windows Weekly, they were often talking about how Microsoft is like, Microsoft doesn't really care about desktop anymore; right? They just - it's all Azure. And we know that AWS is a massive thing for Amazon. So sure enough. And it's funny because I so clearly recall the looks I received from the IT guys who attended DigiCert's Customer Advisory Board meeting six years ago that I was also invited to. I made some offhand comment about the rack of gear I had over at Level 3 which brought all discussion to a halt. I said, "What?" And one of them replied, apparently for the entire group: "Nobody does hardware anymore." Oh. Well, I do. You know, I like hardware with lots of little blinky lights.

But anyway, this piece ends: "Senior management has bought into cloud in a big way. But could investor nervousness from the Rackspace outage have an impact on attitudes in the boardroom? When a service that gives you 1% of your revenue leads to a 30% drop in your market share, cloud proponents may, to quote Ricky Ricardo," says the article, "have some 'splaining to do."

And that was just the first shoe to drop. The second shoe was, yes, Rackspace is now facing not one, not two, but at least three class-action lawsuits. Reports are that Rackspace will need to defend themselves in so far at least three different class-action lawsuits related to this recent ransomware attack from which they're still recovering and may never be able to fully recover from. The attack left countless companies - unfortunately it was tons of small and medium-size businesses that had all outsourced their email to Exchange Server hosted by Rackspace, and they just got wiped. So it's not clear that it's coming back.

In an interview last week, Rackspace suggested they may not be able to recover all their customers' data, which they referred to as "legacy data." The company also appears to have given up on hosting Exchange email servers in its cloud - yeah - and said it was migrating all its existing customers to Microsoft 365. Right, give it to Microsoft. Which, according to documents Rackspace filed with the SEC will cost the company 30 million, right, because that's that 1% of its revenue. But who cares? It's certainly not worth the headache. I imagine that hosting Exchange Server was more of a means to an end for Rackspace, you know, a way of establishing a relationship with an enterprise and then, over time, probably moving more of their non-email business into the cloud. You know? That didn't work out so well.

Okay. The trend appears to be, what we're seeing broadly, is everyone is getting very tired of the consequences of these apparently never-ending attacks. Governments are going on the offensive, saying that they're no longer going to be waiting to be attacked. They're going to go proactive.

Leo: Australia.

Steve: Yes. Other governments are calling their own employees criminally negligent and bringing them up on criminal charges.

Leo: I don't know if that's fair.

Steve: Right. And the class-action ambulance chasers now only take a day or two to file their lawsuits. Why is all this happening all of a sudden? Well, we know, because criminal organizations, apparently some with state-level sponsorship and protection, have realized that the cryptocurrency boom, coupled with the presence of exchanges to local fiat currencies, provides them with a means of being anonymously paid. That provided the motivation. Clever hackers provided the means. And the final piece, endless opportunity, was readily supplied by the industry's historically lax cybersecurity.

So today everyone is furious, beside themselves, pointing fingers and suing. But who's still never being held to account? By a perversion inherent in the system we've built, the suppliers of the buggy, brittle, and breakable systems are never to blame. I would say stay tuned. That's going to be next. Juries are made up, after all, of end users, and they're not going to be sympathetic after everything this industry has been putting them through lately.

Oh, and one last piece. Speaking of losing patience, another country goes on the offensive. On December 11th it was reported that Japan, kind of quiet, peaceful Japan, intends to establish a legal framework that will allow strengthening of defense measures in cyberspace, including the ability to attack preemptively. The Japanese government intends to change the rules so that it can start tracking potential attackers and breaking into systems, the attacker systems, as soon as there's a potential threat. Current regulations make it extremely difficult to apply such measures unless there's an emergency situation that requires the mobilization of defense forces after a military attack. The plan is reflected in a proposal to amend the National Security Strategy that has just been submitted to the governing coalition. The draft amendment is expected to be approved by the cabinet before the end of this month. So we're clearly seeing a changing of attitudes across the board. Wow indeed, my friend.

Okay. Get this, Leo. The following was sent to me via Twitter DM, and I'm not sure this individual would want his name published so I'm not sharing it. But he's the Australian cybersecurity person who was tasked with finding and downloading the Medibank data from the dark web for analysis. He sent the following. He said: "Hi, Steve. I just wanted to drop you a line about the Medibank data. You mentioned in Security Now! 900 that you didn't know what use the data would be if it wasn't formatted properly. I'd like to offer one way it could be useful in the wrong hands.

"I work in cybersecurity for a law enforcement government department in Australia, and I was tasked with finding and downloading the Medibank and Optus data. I absolutely agree, the data held within the extracted data was not formatted and was of limited use in its raw format," he says, "(all CSV files with different structures presumably depending upon the database it was extracted from)." He said: "It's true that the data is of limited use as the medical information about the patients was all in code format which meant nothing without the application to match the code to the treatment the patient received.

"However, my job was to search through the data to see what law enforcement officers' details were leaked. Can you imagine how bad it would be if an individual used their government-issued email address, which has their law enforcement division within the domain of the email address, to sign up with Medibank? Suddenly you would be able to match a name and home address of a person, and verify it was a person working for the law enforcement division thanks to their email address. In the hands of the wrong people, such as criminal gangs, this information could put these law enforcement officers in serious danger. Sadly, data of this nature was leaked, and our organization now has to help protect these individuals. I'm sure you've already considered this scenario with leaked data. Really, any leaked data could be used this way. But considering the high-profile nature of this leak, we're having to take it very seriously. Thank you for such a wonderful podcast."

And thank you for the very interesting note from the field. You know, it's abundantly clear that this podcast has aggregated quite an amazing group of listeners. I am continually humbled and flattered by the people who take the time to listen to these ramblings every week. So thank you all.

Paul Jolley wrote: "I know you've spoken of UTF-8 in past episodes, but was left asking myself what could possibly be the legitimate purpose of some characters after I encountered [and then he has a] U+200B [so that's a Unicode character] recently." He said: "I appreciate English isn't the only language used in the world, so I understand why this extended character set is useful; but, as previously described on the podcast can also see how it can be abused - typo-squatting in domain names, for example - by using characters that look like their ASCII equivalents.

"Getting back to my recent experience," he said, "I received an email where the sender name would not sort alphabetically in my email client. I didn't think much of it at first,

but then decided to investigate. It turns out that they had inserted a 'Zero Width Space' character..."

Leo: Wow. Wow.

Steve: ...before the first letter of their name, making it appear at the top of my sorted list.

Leo: That's very sophisticated. Holy cow.

Steve: Yeah. "The three bytes could be seen in a hex editor as E2, hex 80, and then hex 8B; but would not visibly appear in Notepad." He said: "I've never encountered this kind of whitespace before and thought it would be worth mentioning because I expect something like this will only be used for mischief. Try it yourself by renaming a folder in Windows and putting this special character at the beginning to make your folder appear at the top of a sorted list without any visible whitespace, or paste it in Notepad a few times and see the file size increase when you save the file but there's nothing to select or highlight on the screen. The world doesn't need this." So anyway, another lesson here is that for every useful thing we create, there are clever people who will subvert that use into abuse.

Leo: Yeah.

Steve: A SpinRite note. SpinRite is currently at alpha release 5 with many further improvements already implemented for its next alpha release. Everything is going quite well. Thanks to a truly gratifying level of engagement - we now have exactly 500, when I looked this morning, registered users in GitLab - we've been uncovering mysteries around the edges that I've been working to solve, and also things that I didn't anticipate. And I should also mention that the people testing are also solving these mysteries, as well.

For example, in 6.1 it's possible to select a drive from the command line by its model number. But Western Digital's model numbers contain spaces, and spaces are used as a delimiter to separate command line entities. So the answer is simple; right? Allow tokens to be quoted to have their contents parsed literally. When I wrote the command line parser I forgot to add support for quoting literals. So that's an example of something that needs to get fixed. Someone booted SpinRite from a CD, and it didn't notify them that their request for logging to the CD could not be honored. So those sorts of things. They're things I want to take the time to get correct now so that I don't have to correct them later.

And we do have a couple of mysteries. One guy who has two HP All-In-One PCs, if he warm boots from Windows 10 into SpinRite, SpinRite locks up as soon as it starts running, trying to actually run on the drive. But if he cold boots the machine, everything works fine. Okay, now, we might say, okay, so don't warm boot.

Leo: Yeah, there you go.

Steve: Doctor, it hurts every time I raise my arm like this.

Leo: Well, don't raise your arm like that, you silly boy.

Steve: Exactly. So that might be all that, you know, we may end up saying, okay, you're going to have to cold boot. But it could be a symptom of something more important. So I found one of those machines on eBay for $47.

Leo: Oh, my god, I can't believe you.

Steve: And it's in my car's trunk right now.

Leo: Wow.

Steve: I'll figure out what's going on, and I'll answer the question that's best expressed using one of my favorite SpinRite development abbreviations which now comes up frequently. The abbreviation is WTF.

Leo: There's a lot of that. I've been doing a radio show for 19 years that's basically filled with that.

Steve: Wow. I have one piece of miscellany to share, and then we'll take our last break. The ZimaBoard fanless single-board computer that I stumbled upon and told everyone here about has apparently been a big hit. I keep seeing kind of casual, offhand mentions of it in the postings among those who are testing SpinRite, and also in Twitter messages. Okay. So given how long it takes to obtain one after ordering it from Hong Kong, and the fact that shipping is not free, I was surprised and delighted to learn a few hours ago that Amazon has all of them in stock and available for astonishing same-day arrival, not even next-day, today, at least in my location. So as an Prime subscriber, the cost is $10 more than ordering the ZimaBoard directly from its source. But there's no shipping cost. So $129 versus 119, and you can have it today. So anyway, I know that not everyone bothers being a Prime subscriber, but for what it's worth it's on Amazon. So I just wanted to share that bit of happy news.

Leo: All right.

Steve: I love when you talk about ExpressVPN, and you disconnect the VPN as [whisking sounds].

Leo: It's gone [whisking sounds]. It's out of RAM [whisking sounds]. Complete with sound effects. All right. I really - so this was huge news last Wednesday, after the show, when Apple announced, yes, we're going to turn on end-to-end encryption in the cloud. I just got it, iOS 16.2. Everybody did. MacOS had an update. You can turn on advanced data protection, and it includes cloud backups. But I knew I should not assume unless I listen to Steve and find out what he has to say about this.

Steve: Okay. So last Wednesday Apple posted the news, which generated the most feedback, as I said at the top of the show, of anything that's happened recently. So I knew we needed to address that today. Before that, I was planning to talk about the technology behind a clever new generic bypass of web application firewalls. Okay, nerdy, but cool. And don't worry, we're going to get to that next week. Today it's Apple time.

So Apple's headline reads: "Apple advances user security with powerful new data protections." The subhead, which introduces three new terms, reads: "iMessage Contact Key Verification, Security Keys for Apple ID, and Advanced Data Protection for iCloud provide users with important new tools to protect their most sensitive data and communications."

Okay. So we have three new things. Apple explains that iMessage Contact Key Verification allows users to verify they're communicating only with whom they intend. We'll see what that means in a minute. Then there's Security Keys for Apple ID where users have the choice to require a physical security key to sign into their Apple ID account. Okay, so that's going to be very cool. And Advanced Data Protection for iCloud, which Apple explains users will be able to obtain what Apple says is end-to-end encryption to provide Apple's highest level of cloud data security where users will have the choice to enhance the protection of important iCloud data, including iCloud Backup, Photos, Notes, and more.

Okay, now, before we go any further I should note that this just became available, Leo. What was said in Apple's announcement was that it was available for beta now and would be available for non-beta by the end of the year.

Leo: Yeah, one week later. Less than a week, yeah.

Steve: Okay, right, okay. But that's only the iCloud backup. The other two are early 2023 rollout globally. And iCloud encryption also, the so-called Advanced Data Protection from iCloud, that's globally in 2023. As far as I know it's only in the U.S. for now.

Leo: I'm sure there are all sorts of issues of rolling it out globally. So I understand, yeah.

Steve: Yeah. Okay. Let's look at each of those three security improvements. The good news is that most of the information is available about the thing that people are most excited about, which is that not even Apple will be able to get in, type of true user encryption of user data stored in the cloud. But because that's where the most information is, I'm going to save that for the last. The bad news is that neither of the other two security improvements is explained anywhere that I've been able to find in much detail, but at this point maybe there's not much detail to be had.

Of their iMessage Contact Key Verification, Apple only said: "Conversations between users who have enabled iMessage Contact Key Verification receive automatic alerts if an exceptionally advanced adversary, such as a state-sponsored attacker, were ever to succeed in breaching cloud servers and inserting their own device to eavesdrop on these encrypted communications. And for even higher security, iMessage Contact Key Verification" - which I think is where it gets its name - "users can compare a Contact Verification Code in person, on FaceTime, or through another secure call."

Okay. And that's all we know presumably until it's rolled out early next year. They do provide a photo showing a little emergency triangle icon, underneath which is written:

"An unrecognized device may have been added to" - and then whatever the account's name is, you know, Steve, Jenny, whatever, account. And then they have a clearly clickable, in blue in their screenshot, "Options," dot dot dot, but we don't know what one's options might be.

Okay. So this idea of a foreign device being added to an account covers one of the two theoretical ways that we know iMessage can be subverted. Since iMessage conversations are broadcast to all of an account's registered and logged-on devices, if an adversary were to somehow get their own additional device added to a user's account, that additional device would automatically be privy to all of the attacked account's messaging. So this seems like a useful feature. Somehow Apple has arranged to be able to assure that in the event of that happening, this aspect of some sort of integrity checking won't be fooled, and that message would appear informing you that an unknown device was now sharing your account.

But since Apple handles all key management for its users, the iMessage attack we've always wondered and worried about is law enforcement serving Apple with a wiretap subpoena which would compel Apple to surreptitiously add an additional key into an iMessage conversation. Since iMessage can already handle multi-party messaging, adding a hidden key seems eminently plausible. And it's unclear under what grounds Apple could refuse a legal order for something they could probably do. But that's all speculation for which there's no evidence. The issue arises, however, any time any third-party manages keying on behalf of its users. That's the convenient way to do it, but it's less secure.

The other piece of this announcement which we'll apparently need to wait to see, is this means for somehow comparing and confirming what Apple calls this Contact Verification Code, like in person, on FaceTime, or through another secure call. So you're like reading it off of the screen to the other person. This, I'll call it the CVC, is presumably, and hopefully, a hash of the user's public key which matches their private key, which is then converted into an ASCII code. So it's not just binary gibberish or hex. And note that this is exactly what my favorite messaging agent, Threema, which you mentioned earlier, Leo, has understood was important and has always done from the start. So that's all we know for now about iMessage Contact Key Verification. I'm sure we'll talk about it again next year once it's rolled out.

Next up is "Security Keys for Apple ID." Apple explains it by writing: "Apple introduced two-factor authentication for Apple ID in 2015. Today," they say, "with more than 95% of active iCloud accounts using this protection" - that's nice to know, and that's a big number - "it is the most widely used two-factor account security system in the world that we're aware of." And they broke their arm patting themselves on the back. I should clarify that what we're talking about here is just the use of some other device to receive a six-digit code to authenticate a user. So, yeah, everybody has that. Okay. Then they said...

> **Leo:** Although Apple, I don't know if you've experienced it, does it nicely by showing you the location of the person asking for the code on a map, and then you say "Allow," and then it shows you the code, I mean, they've done a nice job of that, I think.

Steve: Right, right.

> **Leo:** They're not texting you a six-digit code on your SMS number.

Steve: Right. So they said: "Now with Security Keys, users will have the choice to make use of third-party hardware security keys to enhance this protection."

Leo: Woohoo.

Steve: Yeah. "This feature is designed for users who, often due to their public profile, face concerted threats to their online accounts, such as celebrities, journalists, and members of government. For users who opt in, Security Keys strengthens Apple's two-factor authentication by requiring a hardware security key as one of the two factors. This takes our two-factor authentication even further, preventing even an advanced attacker from obtaining a user's second factor in a phishing scam.

Leo: Woohoo. That's the key; right? Because you can phish that six-digit number.

Steve: Yes.

Leo: But you can't phish a YubiKey because it's mine.

Steve: Nope.

Leo: Yeah.

Steve: So we're getting hardware authentication dongles. That's good. And I imagine that Stina and the team over at Yubico is happy to see third-party hardware dongles becoming far more mainstream.

Leo: They've offered YubiKeys with Lightning for a long time. I have the one that has Lightning on one end and Type C on the other. They also have NFC YubiKeys that work. So, yeah.

Steve: So what I'm wondering, Leo, is what stage of authentication. Is this unlocking your device? Or is this like when you need to like put in your passcode, like after the first time you turn it back on, I would imagine.

Leo: I would guess it's that second, you know, you're not going to do it every time you unlock your device. I mean, maybe you could set that. But it's whenever the two-factor pops up anyway; right?

Steve: Right.

Leo: But I do wonder, and you taught me this, what's the fallback method? Because the weakest link is always the fallback method; you know? So they might be great and say, well, you could use a YubiKey, or we'll text you a message. And that wouldn't be quite as useful.

Steve: That's a very good point.

Leo: Yeah, yeah.

Steve: Okay. Now...

Leo: I'll have to learn about that.

Steve: Encrypting the cloud. Most of the content of that first announcement page is glitz and self-congratulatory hype. The good news is that there's a second page available containing much more detail. But since it leaves out some of the broad strokes, we'll cover them here first.

Okay. Ivan Krstic, is that how you pronounce his name? Krstic? He needs some more vowels, just like ExpressVPN. Ivan Krstic, who's Apple's head of Security Engineering and Architecture, is quoted in this first broad overview, saying: "Advanced Data Protection is Apple's highest level of cloud data security, giving users the choice to protect the vast majority of their most sensitive iCloud data with end-to-end encryption so that it can only be decrypted on their trusted devices." For users who opt in, Advanced Data Protection, which you'll hear me just abbreviating to ADP because they keep saying it over and over and over, keeps most iCloud data protected, even in the case of a data breach in the cloud.

Now, this is what's interesting. For users who opt in, Advanced Data Protection keeps most iCloud data protected, even in the case of a data breach in the cloud. They're big on this data breach in the cloud here. I have some comments about that later. So they're naturally not saying that this keeps their hands off any of their users' data, which is of course the main reason everyone wants this, but rather they're saying it's to protect their users in the event of an iCloud security breach. Okay, fine, whatever, you know, as long as we can have it.

They explain, and here's the interesting bit. They said: "iCloud already protects 14 sensitive data categories using end-to-end encryption by default, including passwords in iCloud Keychain and Health data. Meaning that Apple does not have access to that stuff, unlike most famously the iCloud backup. For users who enable Advanced Data Protection, the total number of data categories protected using this end-to-end encryption rises from that 14 to 23, which then includes iCloud Backup, Notes, and Photos, and more. The only major iCloud data categories that are not covered are iCloud Mail, Contacts, and Calendar because of the need to interoperate with the global email, contacts, and calendar systems.

But iCloud Backup, that's the biggie; right? Remember that back in 2016 after the San Bernardino shootings, it was Syed Farook's phone whose iCloud Backups, had they been available, and had the FBI not changed the password on the account, could have been decrypted by Apple to provide the FBI with the vital evidence that they say they needed at the time. So this was the big deal about iCloud backup; you know? We learned that under some situations it could be made available.

Leo: Yeah, Apple even said, yes, see, we cooperated. All they had to do was go back to his house.

Steve: Right. Okay. So just to wrap up the overview, Apple is expending some significant effort, in my opinion, to spin this additional encryption as user protection in the event of a breach, presumably to deflect some of the government's and law enforcement's annoyance over more stuff being encrypted. Apple went out of their way to write.

They said: "Enhanced security for users' data in the cloud is more urgently needed than ever before, as demonstrated in a new summary of data breach research, 'The Rising Threat to Consumer Data in the Cloud,' published today. Experts say the total number of data breaches more than tripled between 2013 and 2021, exposing 1.1 billion personal records across the globe in 2021 alone. Increasingly, companies across the technology industry are addressing this growing threat by implementing end-to-end encryption in their offerings." So again, this is Apple saying we're doing this to protect our users from data breaches because that's a big problem. And of course the users want it because Apple has the keys.

Okay. So that's the broad strokes. There is more good stuff in a secondary document. "Advanced Data Protection for iCloud," they write, "is an optional setting that offers Apple's highest level of iCloud data security. When a user turns on Advanced Data Protection" - I'm going to now call it ADP - "their trusted devices retain sole access to the encryption keys for the majority of their iCloud data, thereby protecting it with end-to-end encryption. For users who turn on ADP, the total number of data categories protected using end-to-end encryption rises from 14 to 23 and includes iCloud Backup, Photos, Notes and more." But that stuff all seriously encrypted.

"Conceptually," they said, "ADP is simple. All CloudKit Service keys that were generated on device and later uploaded to the" - what's called the "available-after-authentication," you'll hear that phrase a couple times more - "to the available-after-authentication iCloud Hardware Security Modules (HSMs) in Apple data centers" - get this. Okay. I'm going to back up again because this is important.

"All CloudKit security keys that were generated on device and later uploaded to the available-after-authentication iCloud Hardware Security Modules in Apple data centers are deleted from those HSMs and instead kept entirely within the account's iCloud Keychain protection domain." Which again, Apple has no access to. Apple does have access to that available-after-authentication iCloud hardware security modules where the keys have up until now or up until the user turns that on, that's where they've resided. So they were in hardware. They were protected as well as Apple could. But available after authentication. Now, not. They are deleted. When the user turns that on, those keys are deleted from the HSMs that Apple had. They're handled, and they're moved into the iCloud Keychain protection domain, meaning Apple can't get there. That stuff is sent down to the user for them to decrypt locally. They are not decrypted at Apple's end. They're handled like the existing end-to-end encrypted service keys, which means Apple can no longer read or access them.

Okay. They wrote: "ADP also automatically protects CloudKit fields that third-party developers choose to mark as encrypted, and all CloudKit assets. When the user turns on Advanced Data Protection, their trusted device performs two actions: First, it communicates the user's intent to turn on ADP to their other devices that participate in end-to-end-encryption. It does so by writing a new value, signed by device-local keys, into its iCloud Keychain device metadata. Apple servers cannot remove or modify this attestation while it gets synchronized with the user's other devices.

"Second, the device initiates the removal of the available-after-authentication service keys from Apple data centers." So that's what I was just talking about before. Now we're getting more into the detail. "The device initiates the removal of the available-after-authentication service keys from Apple data centers. As these keys are protected by iCloud HSMs, this deletion is immediate, permanent, and irrevocable. After the keys are

deleted, Apple can no longer access any of the data protected by the user's service keys. At this time, the device begins an asynchronous key rotation operation, which creates a new service key for each service whose key was previously available to Apple servers. If the key rotation fails, due to network interruption or any other error, the device retries the key rotation until it succeeds."

Okay. This is very cool and very serious. Apple is saying, since we once had those keys, we want all of those keys, not only to be deleted, but then rotated out of service so that even though we've already deleted the keys, you're now using new keys that we have never seen and never had anywhere in our possession...

Leo: Excellent.

Steve: ...in an unencrypted form.

Leo: Excellent.

Steve: Yes. Yes. It is really serious. So they said: "After the service key rotation is successful, new data written to the service cannot be decrypted with the old service key." Right, because key rotation means replacement. "It's protected with the new key, which is controlled solely by the user's trusted devices, and was never available to Apple," they wrote. So notice what's been quietly acknowledged here. This is has nothing to do with breach protection anymore. This is all about Apple strongly selling the truth that they no longer have access to their users' iCloud device backups, photos and notes.

Leo: Wow.

Steve: Okay. Then they say: "When a user first turns on ADP" - now, here's some interesting caveats because, you know, they've got some things that they needed, they offer some things that they have to have the keys for at their end if you want those things.

Leo: Yeah. We've talked about that. There is a limitation on what you can do if you don't have access to the data.

Steve: Right. They said: "When a user first turns on ADP, web access to their data at iCloud.com is automatically turned off."

Leo: Oh, that's a big one.

Steve: "This is because iCloud web servers no longer have access to the keys required to decrypt and display the user's data."

Leo: Wow.

Steve: "The user can choose to turn on web access again, and use the participation of their trusted device to access their encrypted iCloud data on the web."

Leo: Ah.

Steve: "After turning on web access, the user must authorize the web sign-in on one of their trusted devices each time they visit iCloud.com."

Leo: Good.

Steve: "The authorization 'arms' the device for web access. For the next hour, this device accepts requests from specific Apple servers to upload individual service keys, but only those corresponding to an allow list of services normally accessible on iCloud.com. In other words, even after the user authorizes a web sign-in, a server request is unable to induce the user's device to upload service keys for data that isn't intended to be viewed on iCloud.com, such as health data or passwords in iCloud Keychain. Apple servers request only the service keys needed to decrypt the specific data that the user is requesting to access on the web. Every time a service key is uploaded, it is encrypted using an ephemeral key bound to the web session that the user authorized, and a notification is displayed on the user's device showing the iCloud service whose data is temporarily being made available to Apple servers."

Now, what this really means is, if you really don't want Apple ever to have access, you have to stop using iCloud.com. iCloud.com is a backdoor. I mean, they've done everything they can, all the due diligence possible. They've proscribed their access. They've limited it. But if you're saying you want your data to be shown on a web page, that's got to come from our server.

Leo: Right.

Steve: So you have to give us transient access to that.

Leo: And presumably, if they wanted to, they could cache that key.

Steve: Right.

Leo: So you're giving them a key again, and suddenly, yeah. So if you really want to be private, you wouldn't use the web.

Steve: And given that turning ADP on forces a key rotation, maybe turning it off and back on again would reinitialize those keys.

Leo: Ah, rotate that. Yeah, yeah.

Steve: Yeah. So they said: "ADP and iCloud.com web access settings can be modified only by the user. These values are stored in the user's iCloud Keychain device metadata and can only be changed from one of the user's trusted devices. Apple servers cannot modify these settings on behalf of the user, nor can they roll them back to a previous configuration." Again, not about protection from data breaches. It's all obviously about Apple going well out of their way to demonstrate exactly how they no longer have access.

Then they said: "In most cases, when users share content to collaborate with each other - for example, with shared Notes, shared Reminders, shared folders in iCloud Drive, or iCloud Shared Photo Library - and all the users have ADP turned on, Apple servers are used only to establish sharing, but don't have access to the encryption keys for the shared data." Again, they've really done everything they could.

Leo: So an encrypted blob would go through Apple, but never be unencrypted at Apple.

Steve: Right.

Leo: And then presumably I'd have to share a key. That's part of the sharing. I'd have to share a key with the recipient.

Steve: Right. So it would actually be - it wouldn't be the encrypted blob. It would be the key would get shared to the other device, and then the device would do the decryption of the blob.

Leo: So the data is device-to-device shared? It's peer-to-peer?

Steve: No, no. The keys.

Leo: Right. But the data - so I have some data on my phone I want to share with somebody else. It's still going to go through Apple. It has to go through Apple.

Steve: Exactly, because it comes from your iCloud Keychain that they don't have access to, to the other account's iCloud Keychain.

Leo: So I have - my photos are on Apple's iCloud. I want to share an album with Lisa. I would send her the key, and then she could get the data from Apple, encrypted as it is with Apple, download it, and unencrypt it locally. Yeah.

Steve: Right.

Leo: That makes sense.

Steve: Right. So they said: "The content remains end-to-end encrypted and accessible only to participants' trusted devices. For each sharing operation, a title and representative thumbnail may be stored by Apple with standard data protection to show a preview to the receiving users."

Okay. Also, other little gotchas here. Like this is why they had to work to do this. "Selecting the 'anyone with a link' option when enabling collaboration will make the content available to Apple servers under standard data protection, as the servers need to be able to provide access to anyone who opens the URL. iWork collaboration and the Shared Albums feature in Photos don't support Advanced Data Protection. When users collaborate on an iWork document, or open an iWork document from a shared folder in iCloud Drive, the encryption keys for the document are securely uploaded to iWork servers in Apple data centers. This is because real-time collaboration in iWork requires server-side mediation to coordinate document changes between participants. Photos added to Shared Albums are stored with standard data protection, as the feature permits albums to be publicly shared on the web."

Okay. So they also said - so those are the caveats. Basically they've done everything possible. The typical user who isn't using iCloud.com and doesn't want to do like dynamic document and photo sharing, they're locked down tight when they turn this on. They said: "The user can turn off ADP at any time. If they decide to do so, two things. First, the user's device first records their new choice in iCloud Keychain participation metadata, and this setting is securely synchronized to all their devices.

Second, the user's device securely uploads the service keys for all available-after-authentication services to the iCloud HSMs in Apple data centers." In other words, you turn off ADP, here are the keys, Apple, that you're going to need to return us to previous, this is the way we've always encrypted your stuff before, mode. And they said: "This never includes keys for services that are end-to-end encrypted under standard data protection, such as the iCloud Keychain and Health."

They said: "The device uploads both the original service keys, generated before ADP had been turned on, and the new service keys that were generated after the user turned on the feature. This makes all data in these services accessible after authentication and returns the account to standard data protection, where Apple can once again help the user recover most of their data should they lose access to their account."

And now this is really interesting. "The requirements to turn on Advanced Data Protection for iCloud include the following." In other words, what you have to do to get this on in the first place. And Leo, your mentioning of what happens if you lose your YubiKey is what put me in mind of this because again, Apple can't help you. So they said: "The user's account must support end-to-end encryption. End-to-end encryption requires two-factor authentication for their Apple ID, and a passcode or password set on their trusted devices." In other words, that 5% globally who don't have what they consider two-factor authentication, they can't turn on ADP. They've got to first set better security on their device. So that has to be there.

"Second, devices where the user is signed in with their Apple ID must be updated to iOS 16.2, iPadOS 16.2, macOS 13.1, tvOS 16.2, watchOS 9.2, and the latest version of iCloud for Windows. This requirement prevents a previous version of iOS, iPadOS, macOS, tvOS, or watchOS from mishandling the newly created service keys by re-uploading them to the available-after-authentication HSMs in a misguided attempt to repair the account state." Right? You wouldn't want, I mean, it used to be that all of these previous iOS versions were using, you know, if they couldn't access something in the iCloud, they'd go, uh-oh, Apple must have lost the keys, and it would send them again. Well, that's exactly what we don't want now. So you've got to have the latest version of everything.

"Finally, the user must set up at least one alternative recovery method, one or more recovery contacts or a recovery key, which they can use to recover their iCloud data if they lose access to their account." And Leo, I have not had a chance to play with this. I didn't realize it was already there. So we'll find out as we turn on ADP what this alternative recovery method, one or more contacts, recovery key and so forth, is all about.

Leo: Yeah. I think somebody said you should store the recovery keys in your password vault. So somebody's turned it on in our chatroom, and they said that's what they could see. So you might get, you know, you usually do get with these things five "use once" recovery keys, that kind of thing.

Steve: Yeah, yeah, yeah. I mean, you know, you'll want that when you've got a no-way-out scenario.

Leo: Yeah, print it out and put it in your safe or something, yeah.

Steve: And they said: "If the recovery methods fail" - here it is. "If the recovery methods fail, such as if the recovery contact's information is out of date, or the user forgets them, Apple cannot help recover the user's end-to-end encrypted iCloud data." Period.

Leo: Wow. Good. Good.

Steve: They finished - yup.

Leo: If they said anything else, it wouldn't be good.

Steve: Right. "Advanced Data Protection for iCloud can be turned on only for Apple IDs. Managed Apple IDs and child accounts, which varies by country or region, are not supported."

So I am officially 100% impressed. We heard what you need to hear, which was that if you lose your device or forget your password and are unable to authenticate, and none of the emergency recovery methods we made you set up when you turned on Advanced Data Protection available after we made you jump through all those hoops and acknowledge that your first born might be up for sacrifice, there is truly nothing we can do to help. You turned it on. We made you jump through hoops. You acknowledged the risks. And now it's on you. So, yay.

Leo: Good.

Steve: You know, it sure took us a long time to get here, but we are here at last. Everything that Apple is storing for us is encrypted in our devices before it ever leaves them. They're storing keys in keychains, but they cannot decrypt those keychains because that's the one ultimate key that's being held by the user's device. So Apple has

finally been willing to move the rest of the keys that they were holding into the Keychain to which only its users have access.

Leo: Very good. Very, very good. Right? Can you see any holes in that?

Steve: No. No. The only thing might be that Apple could say to the FBI, well, if the user logs into their iCloud.com, then we could get a snapshot. But so in that sense, you know, they're having to, in order not to lose the feature entirely, they're saying, okay, well, if you still want iCloud.com, we'll give it to you, and we double pinky swear that we're not going to do anything with the data that we shouldn't.

Leo: We've talked about this before. It's why Dropbox and OneDrive and Google Drive, none of them do this end-to-end encryption because you lose capabilities when you do it. And I think what Apple's done is actually kind of interesting.

Steve: It's why I like Sync. Sync.com does have true end-to-end encryption.

Leo: Fully encrypted. But then it's hard for them to de-dupe. I can't remember what all the features were, but there were features that you lose if they can't see the data; right?

Steve: Yup.

Leo: Chiefly de-duping, which is only for their benefit so you don't waste their storage.

Steve: Needlessly.

Leo: Yeah. But I think the ability to give them a temporary one-hour key so that you can look at the stuff, you just have to trust that they'll delete that key.

Steve: Yeah.

Leo: Or as you said, you could rotate the keys. We should play with that and see how long it takes, for instance, to rotate the keys.

Steve: Yeah. Yeah, yeah.

Leo: You know, if it takes an hour, well, that's no good. If it's instant, then you could do that all the time.

Steve: I think it'll be instant.

Leo: It should be; right? Yeah.

Steve: Yup. Yup, absolutely.

Leo: Yeah. This is why you listen to this show. I don't need to say this, but I say it every week, this is the best stuff. And when I see stories like Apple is adding end-to-end encryption, all I can think is, oh, I can't wait to hear what Steve has to say about this. Well, now we know. Now we know. That's why we count on him, Mr. Gibson. You'll find him at GRC.com, the Gibson Research Corporation. Somebody was - you mentioned this Apple Light Pen video that was going around.

Steve: Uh-huh.

Leo: Somebody posted it, I can't remember where, probably in Mastodon, and said: "That's not Steve Gibson, is it?" Yeah, yeah, it is, it's Steve Gibson, a long time ago. It's great. That's I guess where GRC came from, the Gibson Research Corporation. These days the research is mostly around SpinRite, getting your solid-state or hard drive back to normal, working fine. It is the world's finest mass storage recovery and maintenance utility. It's a good thing for maintenance, as well. And he is working hard on 6.1, as you've probably heard. 6.0 is the current version. Don't be put off by the fact that it's been there since 2004. Bug free since 2004. How about that? Bug free.

Steve: And that's what we're trying to do on 6.1.

Leo: Yeah. You will get a copy of 6.1 if you buy 6.0 right now. You'll also participate in the development. It's just a matter of, well, I won't make any promises for Steve. But it's just around the corner. How shall we put that? By the end of next year for sure, 6.1. No, no, I didn't mean to say that. Poor Steve. He's, you know what, god bless you, you're just putting in the effort to make sure it's absolutely robust. You've got a $40 all-in-one in the trunk of your car just so you can check it.

Steve: Actually, while Lorrie was down last week with the 'flu, I worked 18 hours a day on SpinRite.

Leo: Oh, man.

Steve: Because I couldn't get near her, and we couldn't have any fun doing anything.

Leo: Didn't have anything else to do, yeah.

Steve: So, and she was really worried. By like the end of the fifth day she said, "Are you okay?"

Leo: You're self-sufficient. She should know that.

Steve: Yeah, she does.

Leo: You've spent most of your life self-sufficient.

Steve: That's true.

Leo: It's the same thing. You have to balance, a life-work balance. And it's not easy for us geeks because we get tunnel vision, and that's all we can think about. I'm looking at some code right now thinking, I could probably simplify that. But all you have to do is go to GRC.com, pick up a copy of SpinRite. That's Steve's bread and butter. While you're there, take a look at all the other free things he offers like ShieldsUP! and on and on and on.

Plus of course the podcast. He's got 16Kb audio versions. That's for people who really want a small download. He made that for Elaine Farris who is in a bandwidth-constrained environment. She downloads it and makes a human, beautifully written, crafted transcription. Somebody said the 900's not up yet, but it takes a few days. Takes a few days. So as soon as it's done it'll be up on the website there. He also offers 64Kb versions for those who have ample bandwidth. Go to the GRC site to get that and lots of other great stuff. You can also leave feedback there at GRC.com/feedback.

He's also a Twitterer. He's still on the Twitters, @SGgrc. And his DMs are open. Talk about brave. So you can leave him a message there, @SGgrc. And he posts a link to the show notes there every week, so that's another place you can get those. Those are good. If you listen to the show, get the show notes. They're either on his website, or you can get them from Twitter. Because that, you could read along, but it's got links, it's got pictures. The show notes are a really great resource that Steve puts a lot of effort into.