BIMI (Up Scotty)

Description: A great deal more about uBlock Origin which we've been underutilizing. National Public Data files for bankruptcy (is anyone surprised?). Will the .IO top-level Internet domain be disappearing? Last week was Patch Tuesday; what did we learn? Firefox fixed a bad remote exploit that was attacking Tor users. Why a Server edition of Windows won't substitute for a desktop edition. A look back at a fabulous multiplatform puzzle/game from 2015. Feedback on Saturday's surprise Security Now! Mailing. More on "What's the best router?" What in the world is BIMI for email? What it does and what it promises. And next week we dig into the just-announced Passkey "Credential Exchange Protocol" which promises to deliver passkey portability.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-996.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-996-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. He realizes, as we all have, that uBlock Origin is the greatest extension ever for your browser - he's come up with some really interesting additional uses for it - debunks the widespread story heard here and everywhere else about the .io top-level domain disappearing; and gets into this whole new thing called BIMI, a new email authentication standard. He even walks us through signing up. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 996, recorded Tuesday, October 15th, 2024: BIMI (Up Scotty).

It's time for Security Now!, the show where we cover your security, your privacy, your safety, the Internet, science fiction, and anything Steve wants to talk about - Vitamin D - with this guy right here, Steve Gibson of GRC.com. Hi, Steve.

Steve Gibson: Leo, it's great to be with you. Middle of October. Exactly...

Leo: Is there a chill in the air in beautiful Irvine?

Steve: ...three weeks from now there may be a chill in the air.

Leo: Oh, geez. Don't bring that up. Oy. You know how much anxiety I have over November 5th? I can feel it, the pit of my stomach.

Steve: Yeah, it's going to be really fun.

Leo: We will either be cheerful on Wednesday or not.

Steve: I'm a spectator. I have no control. We're both in California, so nothing will be really...

Leo: Yeah, we don't really get a choice.

Steve: And that's really - isn't that annoying?

Leo: Yes.

Steve: That, like, yeah, they're just focusing on three or four states, and those are the ones who - on the other hand, I don't miss all the ads that those poor people in those states are getting buried by.

Leo: I don't know about you, but I am buried by text messages, five or six a day now. Do you not get a lot of campaign...

Steve: Lorrie made the mistake of giving money once. And OMG.

Leo: Oh, that's why. Yeah, I donated money. So that's why I'm on the list.

Steve: They never forget you. They come back and say, well, if we got five bucks, there's got to be another five available.

Leo: And it's always an emergency.

Steve: Oh, yeah. Oh.

Leo: It's always panicking.

Steve: It's end of the world.

Leo: Yeah.

Steve: You know, do you have your snorkel, to fill your bathtub with water and...

Leo: It's kind of amazing.

Steve: ...drown yourself.

Leo: Oh, my god. It has literally made my text messaging unusable for the past month.

Steve: Yeah.

Leo: And I just...

Steve: Think about how the mailman feels, too. Suddenly, like, they had to increase the size of the trucks in order to get all of those ridiculous "he's bad, he's good, he's bad, he's good, she's bad, she's good." Oh, it's like, oh, really?

Leo: It's actually a windfall for both the postal service and your local news and TV and radio stations because all the political spending, you know, goes right into them. And the postal service, if it weren't for junk mail, would not exist.

Steve: No. And I send, you know, every month I collect my receipts and send them to Sue. It used to be 15 cents. Now it's $2.43.

Leo: Not cheap, yeah.

Steve: So, you know, yikes.

Leo: Well, I've got my ballot, and I'm ready to vote.

Steve: I remember when a candy bar...

Leo: Yup. I presume you got - everybody in California gets a mail-in ballot, which is tremendously convenient.

Steve: Yeah.

Leo: And so I've got mine. If you are watching, and you are not yet registered, or you're not sure, check, make sure you're registered, and then get out and vote, either by mail now or in person on...

Steve: The good news is that in California the ballots come with the "I Voted" sticker in them.

Leo: Yes. You can put it on right now.

Steve: So I will have mine right on my forehead in three weeks.

Leo: Yeah, yeah. If you go to Vote.org, I believe, I think that's the URL, you can check your registration. They have a little registration checker. You have 20 days in most states to - 20 days till election day. In many states you only have a few more days to register. All right. This has been the political announcement. Let's move on to the reason people are here, security. What's up this week?

Steve: So a great deal more this week about uBlock Origin, which it turns out we've pretty much all, actually there are some exceptions within our listener base, but we've pretty much been underutilizing what it can do.

Leo: I liked your emergency email midweek. I did that immediately.

Steve: Yes, yes. Everybody who has subscribed to the Security Now! email listing received an unplanned - I didn't even plan it. But Saturday morning, when I made this thing work, I thought, oh, I have to share this news. And, you know, since it's easy for me to do now, 10,442 people received a surprise email...

Leo: That's kind of amazing.

Steve: ...because of their Security Now! subscription, explaining how to easily turn off those increasingly prevalent and thus annoying when they're unwanted, which they typically are, Login With Google pop-ups. And I think it was because I went to Stack Exchange, I was doing some coding, and I thought - and I did a Google search, I clicked a link to Stack Exchange, up it came. And I looked at it, and I realized, you know, I've been getting so many of these, and they are so annoying. And then I thought, wait a minute. We have uBlock Origin. I wonder if it could help?

Anyway, we're going to start by talking about that. Also the question of will the .io top-level Internet domain be disappearing? There's some talk that it should, but I don't think it should. Also last week was Patch Tuesday. What did we learn from that? Firefox had a bad remote code exploit that was being used to attack Tor users on their Firefox-based Tor browser. I realized why the Server edition of Windows does not substitute for a desktop. We talked about this a couple weeks ago, and I've been meaning to bring it back up. Today's the day.

Also we're going to look back, thanks to a question or an observation or actually a discovery from one of our listeners at a fabulous multiplatform puzzle game that we got all hot and bothered over back in 2015. Also I do have some couple pieces of feedback from that surprise mailing on Saturday. We've got a little bit more on what's the best router. And then I titled today's podcast "BIMI (Up Scotty)," B-I-M-I. Actually, it's apparently supposed to be pronounced "bemmy." But I like BIMI.

Leo: It's BIMI.

Steve: Yeah.

Leo: What do you mean, "bemmy"?

Steve: Yeah, BIMI, I mean, that - you have B-I-M-I.

Leo: You don't wear a "bekini," you wear a bikini. What are you talking about?

Steve: We're going to answer the question, what in the world is BIMI for email.

Leo: Okay.

Steve: What it does, what it promises, and if it's going to actually happen. It's trying to. And then I just - I will end by noting that we're going - next week, because it just happened yesterday, and I didn't have a chance to get up to speed. We have the FIDO Group has just announced the credential exchange protocol, CXP, for passkeys. Which, when implemented, will give us the one thing we've really been needing, which is a means of backing up and transporting passkeys between providers. So, oh, and I didn't get it into the show notes also, I'll talk about it next week, but all of our listeners started sending me the news that RSA crypto had been broken by Chinese researchers...

Leo: I saw that, yeah.

Steve: ...who figured out how to use the D-Wave quantum computer.

Leo: Quantum, yeah.

Steve: And it's like, oh, my god. It's like, well, Leo, what was it? We left off at, was it 13 bits that they could factor?

Leo: Yeah, yeah.

Steve: The breakthrough is 22.

Leo: Oh.

Steve: Now, we are running at 2048, so...

Leo: Oh. So you're saying they broke a weak RSA password.

Steve: No. They didn't even break R. They didn't break the leading bit of font of the R. I mean, 22 bits? And you can't decompose factorization, otherwise we would have a long time ago.

Leo: Right, right, right.

Steve: So the fact that they got - they cracked, ooh, they factored a 22-bit number. Good going. Keep at it.

Leo: Yeah, keep up the good work. We'll see you in a few decades.

Steve: And meanwhile, RSA is alive and well, I mean, actual RSA. It never had a weaker key than 1024. I don't think there was a 512 bit. Maybe in the early, you know...

Leo: For a while I remember the U.S. government wanted us to use very small passcodes. I can't remember if it was 128 or 42, I think it was.

Steve: Those were the symmetric keys where it was...

Leo: It was a small...

Steve: It was disturbingly small.

Leo: Yeah.

Steve: Yeah, back in the early, well, it wasn't TLS, it was SSL back then.

Leo: Right, yeah.

Steve: And the idea was, if you didn't export it, you could have a useful strength. But if you, oh, you couldn't leave the country. Well, websites left the country. So it was necessary for them to all be neutered. But, you know, it's not like we were doing anything important back then. They were all using HTTP. So, like, not a big deal. So anyway, we have a Picture of the Week after our first announcement break. And we'll share that and get into a bunch of fun podcast stuff.

Leo: Exciting. Steve, I have the Picture of the Week queued up and ready. Shall we look at it together?

Steve: So I gave this one the caption, "When your message interferes with your message."

Leo: Hmm. All right, I get it right away. Because I like to ride my bike around town.

Steve: So for those who don't have the show notes in front of them...

Leo: Geez, Louise.

Steve: ...or are not watching the video, we have one of those large sort of mobile road signs which is lit up. They often have like a bunch of batteries on them. Sometimes they have a little generator, you know, keeping them alive. Anyway, this sign brightly says on three lines, "Give Cyclists Space."

Leo: Oh, my god.

Steve: Unfortunately, it is right smack dab in the middle of and completely blocking the cyclist lane. Which it's telling everyone you need to give more space to.

Leo: Give them space, please. Yeah.

Steve: So that's right.

Leo: That's pretty typical of our civic fathers, yes.

Steve: Yes. There're no broken bicycles and maimed bodies laying around there. But anyway, yes. When your message interferes with your message.

Leo: No kidding.

Steve: Okay. So everyone is annoyed - we know this because we've talked about it often - by the pervasive cookie permission banners which compliance with the European Union's GDPR has forced upon the world. I recently realized that I had become similarly annoyed by another increasingly pervasive website feature, which is the proactive offer to sign into whatever website I may be briefly visiting.

Leo: Here's the example that you gave on Stack Overflow.

Steve: Yup.

Leo: And there it is up in the upper right-hand corner for Stack Exchange. Sign into Stack Exchange with Google. I don't want to.

Steve: Right. And so, okay. So I'll just address this to the listeners of this podcast who for whatever reason have not yet subscribed to the weekly Security Now! mailing. You may think, oh, well, fine, you know, I'm going to hear it anyway. Well, when I realized I had a solution to this Saturday morning, I thought, oh, let's tell everybody. So...

Leo: So help me do this on this machine because I haven't done it on this machine yet.

Steve: Okay.

Leo: There I am in the upper right-hand corner. I've gone into the uBlock Origin settings, and I'm going to click the gears.

Steve: Actually, what we should probably do is wait until I update you and everyone with the better solution.

Leo: Oh. Oh, you've got a better one.

Steve: I've got a better one.

Leo: Okay. Because I did the manually entering in the filter thing.

Steve: Yes. And that works for most people. There were some people for whom it didn't work. Okay. So I'm getting ahead of myself. So, okay. So just to be clear, I don't want to have people misunderstand my annoyance here. I often choose to sign into websites using my Google account identity because Google provides a very secure implementation of OAuth. My primary email, you know, everyone knows, my main email is going to be a GRC mailbox, so my Google email is my generic catchall throwaway account that most of us have one or two or more of these days. So signing in with Google gives me convenient one-click login at any site that offers it.

And, yes, we know, being OAuth means that Google knows where I am, where I'm signing in, and what I'm doing. But Google almost certainly knows that anyway, and the truth is, you know, I don't really have time to care. You know, all other things being equal, yeah, I would choose privacy. Who wouldn't? And I get it that there are people, many of them are our listeners, who make a hobby out of the rigorous enforcement of their online privacy. I respect that, but that's not me. I'm in a hurry. And since I have no way of gauging my actual success at privacy enforcement due to the myriad sneaky ways in which it can and is being violated, it's not something I'm willing to invest in heavily.

So, okay. For the sake of convenience, I use Login With Google when I'm at some site where I do want to log in for some purpose. And that's not a problem. I like having the option to sign in with Google. And at that point it's not the source of my annoyance. The source of my annoyance is that what we are seeing, and I can now speak for our listeners because I heard, by mid-afternoon on Saturday I had 135 pieces of email from our listeners saying, "Oh, my god, thank you, thank you, thank you." Some said it was life-changing. I mean, clearly I was not alone in this really bugging me.

So the source of the annoyance is that this trend has been developing to proactively PUSH signing in with Google on us wherever we go and whenever we visit a participating website, even if we have absolutely zero interest in or need to sign in there. You know, I don't want to sign into every website on the Internet, and I believe that's the case for most of us. You know, if I want to sign into a website, I'll click the site's Sign-In or Login link and be taken to a page to do that; thank you very much. I don't need to have "signing in" suggested to me or pushed on me. And what happened Saturday morning was it finally - it was like the straw that I finally realized, okay, I'm really being annoyed by these.

Okay. So I'm skipping over a little bit in my notes here that I've already covered. So this occurred to me thanks to last week's discussion of uBlock Origin. My original solution, the one that I came up with Saturday morning and shared, was very specific, and it has the advantage of only doing exactly that one thing. However, it did not work for everyone. Some people needed a somewhat broader solution, which turns out is easy. And it also turned out that this sort of annoyance blocking is also built into some of uBlock Origin's already existing filter lists.

Leo: That's what I was wondering, if there's a checkbox.

Steve: Yes, there is, and we're going to be there in a minute. So they're not turned on by default. Well, for our listeners probably. They are for me, and I'm happier even than I was Saturday afternoon.

Leo: Yeah.

Steve: Okay. So the way we got into this is, as you were going to do, Leo, if you open the uBlock Origin dropdown, and then click on the little gears, you get taken to a series of web pages that have tabs across the top. The My Filters tab is initially empty. Mine was empty. I didn't have any, you know, custom filters there. And then the instructions that I gave were to first put in a comment line so that when you come back to this in a year...

Leo: You know what you did.

Steve: You're not going to be, what? What the heck is that? You know, anyone who's done any coding, by the time you're our age, Leo, we've become humbled. We've realized that...

Leo: We forget.

Steve: ...no matter how sure we are that we will never forget this wonderful code that we've just created, a week could go by, and we look at it and go, what the heck is that? You know, who wrote that? You're looking around for anybody else. It's like, did I do that? Anyway, so any line that begins with an exclamation point is a comment. So I said, "! Block 'Sign in with Google' iframe in top right corner of websites." And then the filter phrase to do that is two vertical bars, which is sort of - it sort of stands in for the normal //. Anyway, the vertical bars tell the easy filter list syntax, which is what Gorhill has adopted, that what follows is a domain name. So "||accounts.google.com/gsi/iframe."

Okay. So that says when the browser attempts to load something from a URL that begins with this, just skip over it. Just say, eh, these are not the droids you're interested in. So nothing happens. Now, it turns out that a couple people wrote back and said, well, that did not work. But if I put "client" instead of "iframe," then it worked. Or even broader, if you do an asterisk. Asterisk is sort of the generally accepted wildcard character. So if you did //gsi/*, then that generally works for more cases. Now, you might think, oh, wait a minute, maybe a wildcard is more than I want. Well, okay. You could put one line with

"iframe," and then another line below it with "client," and block those two. But gsi, you know, so we're accounts.google.com/gsi, that certainly stands for Google Sign-In. So it seems like safe...

Leo: That's fair to block that.

Steve: ...to follow that with an asterisk and just know that you're going to nuke anything that tries to put up on your screen to do that. Okay. But after the email went out, I started getting some feedback from people. One of them said, well, I'm not getting those, and I think I know why. So rather than the "My Filters" tab, we click the preceding tab, which is "Filter Lists." Down near the bottom you'll find a group of three filter lists under the heading "Annoyances." Couldn't have phrased it better myself. Open up the list of three and you'll see "EasyList," "AdGuard," and "uBlock."

Now, it's so easy to get one of those annoying Google Sign-In pop-ups - just go over to Reddit.com, for example, that it was easy to experiment with enabling and disabling these three lists. I discovered that enabling either of the first two, EasyList or AdGuard, would suppress - yes, and look at how comprehensive that is, Leo.

Leo: This is the "uBlock" one, yeah.

Steve: Oh, okay. And EasyList and AdGuard are similar. Either of those two suppresses that gratuitous Google Sign-In popup. In other words, people have been here before us.

Leo: Oh, yeah.

Steve: And they've already fixed this for us. We just didn't tell them, "fix this."

Leo: I think one of these also blocks the cookie banner, if I remember.

Steve: Ah, that's the one. Actually, yes. Okay. So we have some documentation for the AdGuard list. And so under AdGuard's list, under the Annoyances filter, they said: "Annoyances filter blocks irritating elements on web pages, including the following AdGuard filters. All of them can be enabled separately from the Annoyances filter." In this case, Cookie Notices blocks cookie notices on web pages. Popups blocks all kinds of pop-ups that are not necessary for websites' operation. Mobile App Banners blocks banners that promote mobile apps of websites. You know, thank you anyway. Widgets blocks third-party widgets: online assistants, live support chats, all that nonsense. Other Annoyances blocks elements that do not fall under the popular categories of annoyances. At that point I thought, okay, I am all in.

Leo: Turn them all on.

Steve: Yes. And mine are.

Leo: In fact, I'm going to turn on all the uBlock Filters. But I have to point out, occasionally you'll be on a website where they do things in a pop-up that this could break. So you have to be aware you've done that.

Steve: Yes.

Leo: And whenever I have trouble on sites I just disable uBlock on that site.

Steve: Turn it off briefly, and then it'll work. Yes, that is exactly the correct strategy.

Leo: And don't forget to click "Apply Changes" when you do this.

Steve: Correct. So actually you want the "Update Now," which does both.

Leo: Oh, okay.

Steve: So, okay. So I also did want to mention the other thing that I'm sure people are seeing and being annoyed by are those "Would you like some help" sliding up from the upper right.

Leo: Hate that guy. I hate that guy.

Steve: No, I don't want any help. I want you to stop distracting me and leave me alone. So that's gone now, too. And while we're here, I'll just mention that the section above Annoyances is Social Widgets. So we have the EasyList, the AdGuard, and the Fanboy social widgets. And it's described as "Social media filter removes numerous 'Like' and 'Tweet' buttons and other social media integrations on popular websites." That may not be something everybody wants, but I bet you that there are a lot of people...

Leo: Anybody who listens to this show wants it.

Steve: Exactly.

Leo: The thing is, this is why we're really sad about Google disabling what is easily the most important tool on the web, I think.

Steve: Yes, yes. So those are turned on on mine. And as I said, after you've done that, you'll want to click the Update button, which will refresh, download the latest instance of those lists, and then bring them current. And life has been sweet ever since this happened. It's like, oh, whew.

Leo: Whew.

Steve: Thank you, thank you, thank you.

Leo: What a relief. No longer do I see on Reddit the pop-up saying, "You want to use Google? Yeah, come on, I know you do." That's nice.

Steve: I know. I know. So anyway, so I wanted to thank everybody who did take the time to say, hey, Steve, take a look over here, because that allowed me to get this into today's podcast and update everyone with what I think is a superior solution. And, you know the cool thing about this is that these lists are being constantly curated by people who do really enjoy this. They're chasing these things down. Some of the expressions on these things, I mean, they're also professional filter list builders because these things are hair-curling. But so they're going in with a scalpel and saying, okay, exactly THAT I don't want. And we don't want to break anything else. Just stop doing THAT to me.

Leo: Yeah.

Steve: And so this does that. Now, the other thing that is different about this from the uBlock Origin Lite is that - and Gorhill mentioned this, and we talked about it last week. The V2 Manifest is able to independently update its lists. That's not something that Chrome wants to promote going forward. It's not available in Manifest V3. So you'll need like a new version of the entire add-on extension, rather than the extension being able to reach out and update the lists on its own behalf. So that's another, as you said, Leo, it's why we're annoyed with Google.

Now, I'm sure, since Chrome has 37 million users of uBlock Origin, compared to Firefox's seven, that Gorhill will be incentivized to do everything he can to make the Lite version as powerful as possible. And as we know from last week, we do have nine months more until Chrome users lose access to the V2 Manifest, thanks to the policy tweak that we found and shared last week. So a lot can happen in nine months. You know, we've seen Chrome back off on terminating third-party cookies when it turns out they couldn't. So maybe there will be sufficient pressure on them to reconsider saying no to V2. Or maybe they'll just turn it off for most people, but they'll give us a little backdoor where, if we really must have it, we'll be able to, like, maybe have a policy that says I'll make a registry tweak if I can keep my V2 Manifest.

Leo: They're going to do something about it because, as you point out, Brave, and many of the people in our chatroom, has all these lists built in.

Steve: Yes.

Leo: By the way, you know, I use Arc from The Browser Company, which I love. It's also a Chromium-based browser. And what Arc has, what The Browser Company has already said is, yeah, if once V3 is in our browser, because it's going to be, as it will be in any Chromium browser, we're going to have to write our own blocker and put it in the browser that way, as Brave has done. So that's - I think Chrome's at great risk of losing a huge number of people by forcing this. So we'll see what happens. You're right, it may not happen. I wouldn't be surprised.

Steve: So I'll just say that, after enabling the six additional filter lists for uBlock Origin, I'm more happy than I've ever been that I'm using Firefox, which shows no sign of getting rid of V2 compatibility and uBlock Origin. And we have a bit of feedback that I'll share down in our feedback section. But this has sort of brought me to the awareness that we've been underutilizing this marvelous tool.

Leo: Yeah.

Steve: Because, you know, I could have had these turned on a long time ago and saved myself a lot of clicks of, you know - the other thing, Leo, this thing, this unsolicited sign-in prompt for a site I don't want to sign into covers up regions of the screen that, like, I have to see sometimes. So it's like it's annoying. You can't move it. You have to close it.

Leo: I find it most annoying like on Reddit, where I already have a login. I don't want to use the Google login because I already have a login. And it covers up the part of the screen where you click to log in. It's incredibly frustrating. It's terrible. Terrible design.

Steve: Okay. So anyway, I want to just...

Leo: Good on your mailing list, though. I'm glad that you sent that out as a burst. And nobody complained about that; right?

Steve: I did not get a single complaint. In fact, I said at the end, I said, I hope you don't mind me interfering, you know, interrupting your weekend for this. I was a little - I did feel a bit self-conscious because it was, you know, it was unscheduled. And, you know, Security Now! list subscribers did explicitly sign up to that list to receive weekly podcast summaries, the show notes and the Pictures of the Week. Everyone said they loved it; okay?

And since the system that I built makes it so effortless to send these sorts of announcement mails to what we now - I think we're now at 10,500-plus subscribers - I would like to formally expand the mission of that list, I am announcing it here, to include things like this in the future. I don't know what they might be, but I'll make sure that whatever it is will be, you know, have a high probability of being of interest to everyone, just like this one certainly appeared to be. So thank you for our subscribers, and I'm glad that I was able to brighten everyone's weekend because it certainly did that.

Leo: Yeah. You're right, we underutilize one of the greatest things in the world. And now that we're about to lose it...

Steve: Yeah, now we're appreciating it.

Leo: We're appreciating it.

Steve: Wait, wait, I'm sorry, honey, I didn't mean it.

Leo: Come back.

Steve: So under the heading "It couldn't happen to a nicer guy," last Wednesday The Register reported that everyone's favorite massive data leaker, National Public Data...

Leo: Boo, hiss.

Steve: ...a.k.a. NPD, the organization which first collected the personal data on pretty much everyone, then had their collected data stolen, sold first on the dark web and finally released publicly, has, not surprisingly, filed for bankruptcy.

The Register wrote: "The Florida business behind the data brokerage National Public Data has filed for bankruptcy, admitting 'hundreds of millions' of people were potentially affected in one of the largest information leaks of the year."

Now, just to recap a bit: "Last June," as we know, "the hacking group USDoD put a 277GB file of data online that contained information on about 2.9 billion individuals, and asked $3.5 million for it. The data came from National Public Data," they wrote, "a brokerage owned by Jerico Pictures, which offered background checks to corporate clients via its API.

"NPD confirmed it had been hacked in an attack on December 2023 and initially said just 1.3 million people had lost personal details," you know, "such as name, email address, phone number, social security number, and mailing addresses. But in the court documents filed for bankruptcy, the business concedes the total is much higher.

"The bankruptcy petition from Jerico Pictures states: 'The debtor is likely liable through the application of various state laws to notify and pay for credit monitoring for hundreds of millions of potentially impacted individuals. As the debtor's schedules indicate, the enterprise cannot generate sufficient revenue to address the extensive potential liabilities, not to mention defend the lawsuits and support the investigations. The debtor's insurance has declined coverage." Oh, you bet they have.

"According to the filing, the organization is facing more than a dozen class-action lawsuits over the data loss and potential 'regulatory challenges' from the FTC and more than 20 U.S. states. Any plaintiffs will have a hard time getting paid any money out of Jerico since the documents state the business has," shall we say, "very limited physical assets.

"In the accounting document, the sole owner and operator, Salvatore Verini, Jr., operated the business out of his home using two HP Pavilion desktop computers valued at $200 each, a ThinkPad laptop estimated to be worth $100, and five Dell servers worth an estimated $2,000. It lists, the company lists $33,105 in its corporate checking account in New York as its assets, although the business pulled in $1,152,726 in its last fiscal year, and estimates its total assets are between $25,000 and $75,000 all told. It also lists 27 Internet domains with a value of $25 each. These include the corporate website, which is now defunct, as well as a host of other URLs including CriminalScreen.com, RecordsCheck.net, and asseeninporn.com."

So yes, we have another example of legislation running far behind the consequences of technology. At some point it's going to become clear that the aggregation of large quantities of personal data, along with its merging into comprehensive profiles, itself, that is, just the aggregation and consolidation present an inherent danger. But today there's no regulation over this. Anyone who wishes to can amass such data to create

essentially a latent data bomb. On the one hand, it's free enterprise and capitalism, which no one wants to stifle. But allowing fly-by-night operations of this sort to do this is clearly a problem. The solution may be to require any such information aggregator to have a substantial bond posted, plus a verifiably effective insurance policy in place to cover the losses and lawsuits that would follow any egregious breach of responsibility.

This would nicely serve to "privatize" the risk so that the investors who would be required to create and post the bond, and the insurance company who would be collecting insurance premiums and would be on the hook for their losses, would both be motivated to assure that the enterprise's IT staff, its procedures, and security are adequate to protect their investment. It's the only way I could see that this makes sense moving forward.

We're going to have to have some legislation which says anybody who does and, you know, aggregate data and, you know, the attorneys can figure out what exact language to use, but the idea being anyone who is warehousing quantities of data affecting over some number, some minimum number of individuals, must have the ability to pay for the consequences of the loss of that data. Otherwise, sorry, you know, you can't collect it. Maybe we'll get there someday. It's just going to take legislation.

Okay. Many of the top-level domains that we have today we have because they're associated with countries. You know, the bit.ly service that I used to use, "bit.ly," you know, that "ly" is the country code for Libya. That's why .ly existed and why it was possible for bit.ly to get the domain "bit" in Libya's country code, .ly. And when I left there, of course, I created grc.sc. Well, .sc is the country of Seychelles. So I got GRC.sc because Seychelles has its own top-level domain, .sc. And as we know, there are lots of top-level domains that are created independently, you know, .com, .org, .net, .edu, the original big four. But when a top-level domain belongs to a country, it's tied to that country.

This has recently created some concern because a couple of weeks ago, on October 3rd, the British government announced that it would be releasing its claim of sovereignty over a small tropical atoll in the Indian Ocean, and that these islands would be handed over to the neighboring island country of Mauritius, which lies about 1,100 miles off the southeast coast of Africa. Now, remember that I said the island nation being dissolved was in the Indian Ocean? Well, that country's top-level domain is .io, as in Indian Ocean. And the presumption is that, as has happened a few times in the past, when the country controlling its top-level domain is dissolved for any reason, so too is its top-level domain. And given the strong interest in and use of the .io domain, that presents a problem.

What's supposed to happen is that once Britain signs the new treaty with Mauritius, the British Indian Ocean Territory will formally cease to exist, so various international bodies will update their records. In particular, the International Standard for Organization (ISO) will remove country code "IO" from its specification list. The IANA, the Internet Assigned Numbers Authority, which creates and delegates the top-level domains, uses the ISO's specification to determine which top-level country domains should exist. Once IO is removed, the IANA is supposed to refuse to allow any new registrations with a .io domain. And it's supposed to automatically begin the process of retiring existing domains within the .io top level.

What's not known at this point is whether this will actually be allowed to happen. You know, humans make the rules, and humans can change the rules that we've made. And so, you know, if the rules are causing too much trouble, that may be what happens. You know, we certainly have no lack of non-country TLDs. You know, in addition to those original big four, there's for example .xyz, and .lol, and .online, which are not country domains. So I, for one, see no reason why .io cannot similarly be repurposed, you know, just adopted as a valid non-country TLD. People who are writing online are saying .io is

going to go away. But I find that hard to believe. But again, I'm not the IANA, who ultimately decides these things. So we'll see what happens.

I should note in passing that last Tuesday, October 8th, was the second Tuesday of the month, which meant that Microsoft and many others used the occasion to release their monthly patches. Nothing was particularly notable this month. Microsoft released updates to fix a total of 118 vulnerabilities across its software offerings, two of which were being actively exploited in the wild. So of the 118 flaws, three were rated Critical, 113 are rated Important, and two were rated Moderate. And, as is the case these days, that count does not include the 25 additional flaws that Microsoft previously updated in its Chromium-based Edge browser over the past month. So, you know, good to update, as usual. After the second Tuesday. And restart your machines if you tend to leave them running all the time.

Also, Firefox, as I mentioned at the top, and the Firefox-based Tor Browser, have been warning everyone of the discovery of a serious attack which was levied against Tor users. The flaw carries an attention-getting CVSS of 9.8, and it affects both Firefox and the Firefox Extended Support Release products. It's a use-after-free bug that has been found in the Animation timeline component. Mozilla reported in a post last Friday, October 11th, that it had received from ESET an exploit sample containing a "full exploit chain that allowed remote code execution on a user's computer," just by causing their browser to go to a web page. So, yeah, that'll quality as a 9.8, you know, under anyone's scoring system.

Mozilla also noted that the fix was shipped within 25 hours of its responsible disclosure, so one day and one hour. Two days previous to that, on Wednesday, Mozilla said: "An attacker was able to achieve code execution in the content process by exploiting a use-after-free in Animation timelines," and then added: "We have had reports of this vulnerability being exploited in the wild." So the issue has been addressed in Firefox 131.0.2, ESR - that's the extended support release - ESR 128.3.1, and ESR 115.16.1. The Tor project has also released an emergency update to what they're calling version 13.5.7 of their Tor Browser. So certainly, if you are a Tor user, you'll want to make sure that your Tor Browser is updated to 13.5.7, since those were the targets of this attack. But the vulnerability did affect everyone.

And as I mentioned at the top, next week - this just happened - we will be talking about the Credential Exchange Protocol. So I have not had a chance, because I've been working on this podcast, to dig into it. But I will have. And unless something really very significant happens, I have a feeling that that will be the title of next week's podcast because that's something we're going to want to take a close look at and understand exactly what it is, what it does, and how it works.

Leo: Yeah. This is big news because this was something you could not do.

Steve: Yes. Yes.

Leo: And that's what's kept, frankly, kept people kind of frozen in place, I think, with passkeys, a little bit.

Steve: Many of - I took a quick look at it, Leo. Many of the password manager people were participating in the development, as was Google. I did not see Apple there.

Leo: Not Apple. See, this is a perfect example. They don't have any incentive to let you move your passkeys off your iPhone because they want you to be stuck there forever. Wow.

Steve: Yeah. That was annoying. It doesn't mean they're not going to adopt it.

Leo: Right. But they might have to if FIDO does. I mean, don't they kind of want to keep full compatibility with a standard? I would think so.

Steve: We'll see.

Leo: Depends what FIDO Alliance says. Is it required, or just optional?

Steve: Well, it will be optional, unfortunately.

Leo: It has to be; right?

Steve: But then maybe at some point to get the next level of certification you'll need it, and then Apple will like, aghhhh. I mean, it's really - it would be very short-sighted, I think.

Leo: I agree.

Steve: For them to, I mean, almost punitive for them to say, no, if you use ours, you can't take them anywhere else.

Leo: Right, right.

Steve: Okay. Several weeks ago I mentioned that a listener of ours had suggested that when I move my Windows 7 workstation over to Windows 10, I choose a Windows Server version in order to have a simplified experience. At the time, that sort of caught me by surprise, and I thought it was a great idea since Microsoft will presumably have exercised far greater restraint against including all of the unwanted Xbox, Candy Crush Jewels, Android phone integration, and all that other crap that they force on regular desktop Windows users. But then I remembered that I had that idea a long time ago. It may have been back in the Windows XP era that I did try running, and I did run for a while, a server edition of Windows as my desktop machine, probably because I wanted to be using exactly the same build of Windows that my servers were using back then.

But I hit a big problem. The installers for many of the desktop applications I wanted to run would complain and refuse to proceed when they saw that I was running on a Server release of Windows. I fought against that, and put up with it for a while. I remember looking around, seeing if there was like some way I could create my own hack to make the Server edition look like the desktop version. I didn't end up doing that. I just ended up learning my lesson and deciding to go to a desktop.

And in fact, for example, the Windows 7 workstation version is essentially server, you know, Windows Server 2008 R2. So it's essentially the same code anyway. But I just wanted to close the loop on that in case anyone else was thinking, hey, that sounds like a great idea. I'm going to run server. I'll just caution you that in some cases apps just would not install. In other cases, they said, well, if you're a server version, you're going to have to - it's going to cost you this much money, you know, like way more than it was for the equivalent desktop version. So I just said no, thank you.

Okay. Touching on sci-fi briefly, I am 15% into the book I said I would not read until its companion novel was also ready, though as I recall, my position on that was noticeably softening recently. Anyway, yes, I now know a lot about Peter F. Hamilton's "Exodus: The Archimedes Engine." However, I don't know nearly as much as John Slanina, our JammerB, who is already well into his second read-through. He noted that the second pass is more fun for him because by then you know who all the players are. And, boy, the players are somewhat dizzying. The book begins with a chronology which is stunning in its sweep and scope of humanity's near and far future. And knowing Peter, I knew not to skip over that. I figured this was important. So I read all of that.

Then it runs through and introduces a vast array of characters. And as I said, the historical summary was engaging, and I did force myself to sit still and at least take the time to read through all of the names of the entities whose roles were described mostly in relation to each other in that vast list. And then the book began. So I can well understand why John, upon finishing it once, would immediately reset his eBook to the beginning and go again.

So anyway, I don't know if I'll read it a second time immediately. Maybe I'll wait for who knows how long for its second half of the whole story to be finished. Anyway, I just did want to mention that, yeah, I'm in. I was rereading the Frontiers Saga, like for the fourth time, and that was getting a little boring, actually. So I thought, okay, let's try something new. So I'm there.

Okay. A bit of closing the loop with our listeners. Brian Hendricks wrote. He said: "Hey, Steve. I was looking for a new puzzle game to play on my tablet, and I saw that The Sequence Plus was released a couple of weeks ago. I haven't tried it yet, but thoroughly enjoyed The Sequence at your recommendation a few years ago. I tried The Sequence 2 when that came out, but I did not enjoy it as much." He says: "Hopefully this new game lives up to the original. Happy Security Now!-ing to four digits and beyond."

Okay. So I agree with Brian completely. Whereas I loved The Sequence, I was disappointed by The Sequence 2, and I never bothered to spend much time with it once I saw that, in my opinion - and I guess his and others' - it missed the mark. It turns out that it's not a simple matter to create a truly terrific puzzle game, which the original was.

So I agree that more of the original would be welcome, so I went looking for it. It is nowhere that I was able to find it in Apple's notoriously horribly indexed App Store. So I dropped back to searching the 'Net, and I found something called "The Sequence 2" in the Google Play store. I have a link to it in the show notes for anyone who's interested.

I replied to Brian, asking whether he might be an Android person playing The Sequence 2 on an Android tablet, and he confirmed that he was. So I'm hoping that it just hasn't yet surfaced in Apple's App store. Since the author, who is an outfit by the name One Man Band, uses the Unity framework, it could also be available for iOS. I'm hoping it's just delayed. So anyway, I should note that also, when Brian said "a few years ago," he actually meant nine years ago, back in 2015. So I wanted to tell all of our listeners there is a big treat awaiting any of our listeners who have joined us since then, who enjoy extremely well-crafted puzzle recreation and who are not yet familiar with what we've been talking about.

The Sequence, created as I said by One Man Band, is a sort of graphical sequential programming environment. It's that perfect blend of progressively, increasingly difficult challenges where you're required to discover new tricks and problem-solving techniques as you progress forward through the game's levels. You build machines composed of individual functional blocks, with each block having a single, very simple and very clear function. And then you turn it loose to loop through its operation four or five times, since another requirement is that each iteration leaves the machine you've built in a stable state, ready to do it again.

And one final comment for those who may have heard of things like this before, only to be then disappointed. I have, too. We haven't talked about my affection for puzzles for years. But I've often tried other things that sound exactly like what I just described, and I have been disappointed. So I would never recommend them. This one I recommend without reservation. I have a link in the show notes to its author's website. It's OMB, as in One Man Band, OMBGames.com. And note that it's http only, not https. So if your browser assumes "s," it'll complain one way or the other. You want http://ombgames.com. I also have a link to the author's official YouTube video in the show notes, and it earned this week's GRC Shortcut of the Week.

So you can get a quick sense for what I'm talking about by opening any browser and going to grc.sc/996, which is this week's episode number, grc.sc/996. It is available for a few dollars without any ads or any in-app purchases, thank god, from the Windows Store, Steam, Apple's App Store, and Google Play. If anyone discovers The Sequence Plus in Apple's App Store, please let me know. I'll be all over that one.

And as I was preparing these show notes, I spent some time poking around the author's One Man Band site. On his Contacts page he had both a Gmail and a Twitter handle. So I first went over to Twitter, and I was surprised when Twitter said that he was following me. The only way that was possible was that back in the day I had made such a fuss over The Sequence...

Leo: Well, of course. I'd be following you, too, my biggest fan.

Steve: Yeah. You know. So I figured that this podcast must have come to his attention, and he decided to follow me. He had not posted anything recently over on his Twitter feed, so I shot him a note asking about the status of The Sequence Plus. And not long after, I received a reply from him. His first name is Maxim, and he wrote: "Hi, Steve. I'm glad to hear that everything is going well for you. I'm grateful to you and your podcast for giving my little-known game a loving audience back in 2015. As for The Sequence Plus, I can say that it is a slightly improved version of The Sequence, with some tweaks in the controls and fixes in certain levels. It is free and contains ads, so it might not be suitable for everyone. Let's just say this is my attempt to bring the game to a larger audience, as it is currently very difficult to promote paid games."

Leo: Yeah. Apple doesn't let you do demos or anything. And that's a big problem, frankly.

Steve: Yeah, yeah. He said: "For now, it's only available on Google Play as an experiment." He said: "I can't say for sure if I will release it on iOS, but for all lovers of logic puzzles on iOS, my three games are still available: The Sequence, The Sequence 2, and Unit 404." He said: "Best regards, Maxim."

Okay. So now we know. And apparently he understands me, since I would gladly pay to not have any sort of advertisements in a good puzzle game. I mean, we're only talking a couple of dollars for many hours of engaging mystery. I've been driven nuts by the prevalence of advertising in iOS puzzles where, again, I would gladly pay for their removal and to have a quiet and puzzling experience. I hate ads.

So it does not sound like The Sequence Plus would be anything I want, even if it were available for iOS. You know, as Maxim said, it's largely just The Sequence as it used to be, but renamed and made free, but with ads. So anyway, if you're someone who enjoys puzzles, my advice would be to follow GRC's shortcut of the week - as Leo, you did, and you played his little 50-second sample to give you a sense for what this is. And if it looks appealing, lay down a couple of bucks on Maxim, either on iOS or Android, to purchase, or actually Windows or Steam, to purchase The Sequence, and get ready to have some fun. I really think you will.

Parker Stacy wrote: "Dear Steve. Thank you for this EXTREMELY helpful tip." He's referring to Saturday's email. He said: "You have saved me time. You have saved me frustration. You have saved me from the repetitive irritation felt on so many sites these days. These annoyances on websites around the globe are more than just little gnats to be swatted away. They divert our attention; and, more importantly, they divert our focus.

"When I'm researching something online, I'm usually trying to follow a train of thought a thread, a path, a stack of ideas. Something so seemingly mild as a cookie policy or sign-in-with-me box can interrupt my flow and completely unwind the stack, and it can take an unreasonable amount of time to rebuild it. I know you know this, and I am grateful that you take the time to share these types of countermeasures with us. This type of 'special' notification email is greatly welcomed, and I look forward to more in the future. With gratitude and kind regards, Parker."

And I'll just note that his is a placeholder for the 135 replies I've received and read (so far) following Saturday's special mailing. So I wanted to say thank you to everyone who took the time to mostly express their utter joy over the knowledge that it would be possible to suppress these unsolicited and unwanted login push pop-ups from appearing. It turns out they're quite unpopular, and I was glad to learn that it wasn't just me being cranky that this was all about. And as we know now, by turning on those pre-curated lists, we are getting rid of a whole host of other stuff. But Leo, your point is very important. If you go to a site where something seems broken, something doesn't work, it could be that uBlock Origin has been overprotective, in which case it's a matter just of opening it up and disabling it for the site, or briefly turning it off. And then, you know, you'll get the full site in all of its glory, and you can wade through...

Leo: And you may be sorry.

Steve: ...all the pop-ups and ads and nonsense, yes. And finally, Frank from the Netherlands wrote: "Dear Steve. I wanted to report a feature of uBlock Origin that I don't see other people using, but that significantly improves my productivity. In addition to blocking ads, I use uBlock Origin to clean up cluttered user interfaces. Many web applications today include more features than I need, or aggressively promote new ones. For example, ClickUp is now filled with AI buttons and banners. I hide all these distractions to restore a clean interface that helps me focus on my work. Hope it helps other listeners. Best regards, Frank from the Netherlands."

So that's interesting. There are still features of uBlock Origin that we're not using. Frank is. I just haven't spent any time with it. And I'm beginning to feel like I'm missing a bet

here. uBlock Origin has like a dropper, and I think you're able to use it to go, like, click on something which allows you to identify the something on the page to it, and maybe you're able to say I don't want this anymore. Anyway, I haven't looked. But I wanted to share Frank's note to note that, again, most of us, certainly myself, have been grossly underutilizing the power of uBlock Origin. It is an extremely capable general-purpose web experience filter.

And, you know, I think the reason that it's been underutilized is probably a case of, you know, that old story about cooking the frog in the pot of water where you slowly increase the temperature so the frog never thinks to jump out, it just gets cooked. For us, this incursion into our browsers has been very gradual and incremental. You know, at first only a few sites were pushing that login popup for Google. So we put up with a few of those unwanted appearances. But over time, that number grew and grew until it was something some of us were seeing and tolerating throughout our day. And those Google pop-ups were just one symptom. What's happening is that little by little our online experiences have been increasingly leveraged, and we're being increasingly coerced. Nobody likes being coerced.

So anyway, thank you, Frank from the Netherlands, who is using uBlock Origin more fully, and I will invite others to consider doing the same. And Leo, we're at an hour in. Let's take a break now.

Leo: Okay.

Steve: And then I will finish up with two final pieces of feedback.

Leo: Good thinking. I almost stopped you, then I thought, well, no, he's put in these breaks. He knows what he wants. But okay, good.

Steve: I thought I did.

Leo: Now back to Mr. G. and a little router discussion here.

Steve: Yes, two pieces of feedback from our listeners about routers. Justin Long wrote: "Steve, had to throw in my two cents about routers for parents: Eero. Full stop. Do not pass go. Do not collect $200. Leo mentioned its great mesh networking capabilities, but there's one thing that makes it a perfect router for parents: the ability to configure it without having to be at their house."

Leo: I do that with my mom. I can actually look at her setup.

Steve: Exactly. He said: "All Eero devices are configured via a smartphone app. This means when you get 'the Internet stopped working' call, you can pick up your phone, which you're probably already holding, and see what's going on without having to drive to their house."

Leo: Which is good because her house is in Rhode Island, and I'm in California.

Steve: She's across the country.

Leo: Yeah.

Steve: "You can add multiple Eero networks to one account, so you can switch between your own network and theirs for administration. Another benefit is Eero Plus, which is their monitoring software that blocks access to sites that host malicious content, botnets, phishing sites, et cetera. If you have multiple networks on the same account, one Eero Plus subscription covers them all for the same price." He said: "Currently I have ours, my parents, and my in-laws. Another added bonus: There's no way for Dad to attempt to 'fix' something by blindly clicking around the router's UI. They don't have access to it at all. As far as they're concerned, it's just the magic box that allows them to complain about things on Facebook."

Leo: I will add one more thing. I don't know if you've ever used Waveform's Bufferbloat test, which is a really useful speed test I've done on all of my routers from time to time because it is really much better than a regular speed test. It shows whether latency goes up when you're doing other things like uploading and downloading. And but one of the things you'll find there is their recommendation for routers that don't have buffer bloat, and among others, the Netgear Nighthawk and the IQ Router and Ubiquiti EdgeRouter you've recommended so many times, the Eero Pro 6.

I think all the Eero routers are well designed, and they're also very - I think they pay a lot of attention to the latest thinking in terms of configurations and so forth. And I think that's one of the reasons they do such a good job with buffer bloat. So another good reason. I think they're - we've recommended them ever since they started coming out. And as far as I can tell, Amazon's ownership has not made them worse, it's made them better.

Steve: Oh, Amazon bought them. I was wondering why you said Amazon Eero.

Leo: Yeah. Yeah, they bought them.

Steve: Oh, okay.

Leo: Yeah, some years ago.

Steve: And another listener took Michael Horowitz's advice about the Peplink router. Phil wrote: "Hi, Steven. I'm glad you pointed out Michael's router security website again." Remember that was RouterSecurity.org. He said: "I've recently replaced my Verizon FiOS router with his recommended Peplink router, P-E-P-L-I-N-K, Peplink router, and was able to go over his shortlist, as well, and I could not be more happy. He's even been very responsive in answering my questions that I may have had in configuring the router and anything relating to what to expect when you ditch your ISP's router.

"Not only that, but Peplink themselves have been responsive in replying to email inquiries about any issues, for which there have been none." He said: "When I do my monthly Tech Talk at the library where I work, one of the topics is router setup and

security, and I recommend the Peplink. Patrons will come back saying how it was pretty simple to set up, and Michael's instructions were very straightforward." So he says: "Thanks, Phil."

And I'll just mention that the Peplink router is what RouterSecurity site's author, Michael Horowitz, recommends. I have no experience with it, so I can't weigh in either way, but I wanted to share Philip's positive experience and invite our listeners to consider these alternatives. As I said on this topic earlier, unless someone deliberately chooses an insecure configuration, and with just a few tweaks, any modern consumer router should be safe, though I won't argue that security is relative. And you can certainly spend a lot of time securing a router. But generally what you get, unless you turn on lots of remote serving features, you're probably okay.

Okay. So BIMI (Up Scotty), B-I-M-I. That stands for Brand Indicators for Message Identification. For this week's main topic, I want to share an adventure of mine from last week. It will introduce some new email authentication technology while touching on the challenge of thwarting North Korean and AI identity spoofing and ending with the fact that several recent DDoS and network penetration attacks have left the world's Internet Archive offline; and that, as a consequence, something I was trying and hoping to do last week has been paused until the Internet Archive is back up. And last night it seemed to be better. This morning it was slow and sluggish. Then later this morning it was better.

Leo: It's been DDoSed by an ass-something.

Steve: Yup.

Leo: And it is, it was supposed to be up read-only this morning, but maybe it's still having trouble. I don't know.

Steve: Yeah. And I did see that. And in fact only the Wayback Machine portion was up in read-only. Apparently it's able, you're able to, like, manually submit pages to it for archiving, and that feature is not currently operating.

Leo: What kind of lowlife would attack the Internet Archive is beyond me. It was apparently - was it Iranian hackers? I can't - or North Korean, somebody.

Steve: I saw the same thing, that there was, you know, some attribution given to some, you know, something about some of the mess going on in the Middle East was supposedly behind it. But, okay. So this adventure began when I checked my email after last Tuesday's podcast and found a new feature notification from my favorite certificate authority, DigiCert. It said: "We're writing to let you know that Common Mark Certificates are now available. Common Mark Certificates allow an organization to place a brand logo in the Sender field of outbound emails, confirming the organization's DMARC status and their authenticated identity..."

Leo: Ah.

Steve: Uh-huh, "...and helping protect against phishing and spoofing attacks." They said: "Common Mark Certificates are similar to Verified Mark Certificates, but do not

require a registered trademark for usage. This allows a broader range of senders to add an additional layer of security to emails and help their recipients feel comfortable that the emails come from a legitimate source."

They said: "To qualify for a Common Mark Certificate," and we've got a few bullet points. First, "The corresponding email domain must be configured to enforce DMARC. The corresponding brand logo must either have at least a year of previous public usage on a domain controlled by the applicant, or be an acceptable modification of a registered trademark." And they say: "(See Section 3.2.16 of the BIMI Group's Minimum Security Requirements for Issuance of Mark Certificates for more details.)" And finally: "The logo file used for the Certified Mark Certificate must be an SVG file that adheres to the SVG-P/S profile." Then they finished, saying: "Note: Currently, most image editing tools do not support the SVG-P/S profile..."

Leo: Oh, that's handy.

Steve: Oh, yeah, like I said, I had an adventure - "...and will require using a specific conversion tool or manually editing an SVG file." They said: "See our guide for properly formatting the logo."

Okay. So first I should reiterate that BIMI is officially pronounced "Bih-mee."

Leo: Oh, like Bimini or bikini, okay.

Steve: Yeah, BIMI.

Leo: Yeah, BIMI.

Steve: Not "Bee-mee." But I was unable to resist the "BIMI Up, Scotty."

Leo: I think "BIMI Up, Scotty" is just as good.

Steve: It's Kirk in a hurry. BIMI Up, Scotty.

Leo: BIMI Up, Scotty.

Steve: You know? Because we've lost a bunch of red shirts, and we're about to go, too.

Leo: Whoa, boy. Get me out of here.

Steve: So you know how that goes. Okay. So BIMI, as I said, is the abbreviation for Brand Indicators for Message Identification. It is a new - relatively, we'll see it's been around for, they've been working on it for 10 years - and slowly, as in very slowly, emerging email standard that creates - what's interesting here is a secure means for incoming email to carry and display its sender's unspoofable logo icon. Email clients and

online services that choose to support BIMI will be able to display these logos, and will only display these logos, if and when the email's senders have jumped through quite a large number of hoops to make that possible.

This is all being managed by an industry BIMI working group at BIMIGroup.org, B-I-M-I-G-R-O-U-P dot org. The members of this group are Fastmail, Google, Mailchimp, Proofpoint, SendGrid, Validity, Valimail and Yahoo!. The project began, as I said, a full 10 years ago, back in 2014. And today the display of BIMI logo icons is supported by Apple, Cloudmark, Fastmail, Google, Yahoo!, and Zoho.

Leo: I want to do this. We have a trademark.

Steve: Yes, you do.

Leo: On our TWiT logo.

Steve: Yes, you do.

Leo: Yeah.

Steve: So what this group has managed to design and achieve, finally, wide consensus on is the rough equivalent of the web server TLS certificates we rely heavily on to prevent interception and spoofing of the domains our web browsers visit. This BIMI system provides a means for senders who care to, to strongly authenticate that they are the sender of their email.

I don't have to tell anyone that email is a mess. Whether one is on the sending or the receiving end, everyone knows this. Yet everyone needs email. It is, as we know, the Internet's lowest common denominator for communication. As we've observed here, we could not have usernames and passwords without email because no other authentication system is viable without some reliable backup lowest common denominator fallback means for ultimately authenticating users when they forget their password or don't have their second factor authenticator handy or whatever. It always comes down to email.

So for the past decade an effort has been underway to allow email senders who choose to, and email services who choose to, to display strongly authenticated visual graphic logos in email recipients' inboxes. And I have a picture in the show notes showing what you normally see. It shows MailTimer, and so there's just a generic M in a circle, and Email Marketing News, an E in a circle, as opposed to their actual logos, which the email client is able to show. And I confirm that my iOS devices are showing those where they're in use.

Leo: Now, if I - okay. So I have my picture as a Gravatar. And most email clients will pick that up as the icon and put it next to the email. How can I distinguish a BIMI official trademark from a Gravatar, which anybody could do?

Steve: Yup, that's a good - that is a good point. A Gravatar, if it is available, or if you have a photo associated with a person's contact name.

Leo: Right. On Apple, if it's in the contacts; that's right.

Steve: Right. Yeah. So we are seeing, you know, some collision here.

Leo: It's kind of a flimsy authentication method. Is that all there is, the icon on the email?

Steve: Yes. That's what this is for.

Leo: Okay. All right.

Steve: Yeah.

Leo: I mean, I use PGP authentication that not only verifies that I am the sender, but that the message is unmodified.

Steve: But nobody knows how to receive that.

Leo: Nobody knows what to do with it. But it's there.

Steve: Right.

Leo: You could use S/MIME certificates to do that. Nobody knows how to use that, either.

Steve: Yeah. So what I want is when GRC's email comes, people will see that Ruby G logo that I've been using for 40 years, since before the Internet existed.

Leo: Right.

Steve: And, you know, and make no mistake, this has been slow to catch on. For one thing, as I'll explain in a minute, it's a serious pain in the butt, it's almost comical, for the sender to get it working. And it's not for end users, it's intended specifically for use by bulk email senders. It's also not free, since it requires the use of an annually expiring certificate behind which is some truly world-class authentication.

But I would argue that, for this purpose, "not being free" is a benefit, since the entire reason the world is being buried in unwanted email is that it costs nothing to send. And even in a world with high BIMI adoption, email will still cost nothing to send. But only those senders who are willing to spend some money and take the time and trouble will be able to embellish their incoming email with their company's unspoofable brand logo. And Leo, for what it's worth, if this becomes adopted and becomes valuable, then Apple could, for example, could certainly choose to further enhance...

Leo: Sure, somehow put a key on it or something that says "This is not a Gravatar," right.

Steve: Right. Exactly. This is an authenticated piece of email. Okay. So for bulk mail senders, and even for me, I want that G to show up, it'll likely be worth something. So how does all this new stuff work? The first gating requirement for any possible display of a BIMI logo is that the sender's email passes "DMARC" validation. Okay. So let's briefly review these three email standards, which are all part of this: SPF, DKIM, and DMARC.

SPF, which stands for Sender Policy Framework. It uses additional records in the apparent sending domain's DNS to indicate which IP addresses are valid originators of that domain's email. Since email is sent using the SMTP protocol over TCP, the IP addresses of the endpoints cannot be spoofed. So when a remote sending email server connects to a receiving server, the receiving server obtains the unspoofable IP address of the sending server. Then, when the recipient receives an email claiming to be from a specific domain, the receiving server can issue a DNS query on the spot to request that originating domain's SPF records, if any.

Those SPF records will specify which IP addresses are authentic senders for that domain. So if the IP of the sender of the incoming email for that domain is not authorized by the domain's SPF records, the connection will be dropped, and the email will not be accepted. This costs nothing to do, and it very nicely prevents spammers from spoofing the domains of valid senders.

For example, I have an SPF record for GRC. It uses GRC's DNS to publish the IP address of GRC's email server. So when a random spammer generates email claiming to be from the GRC.com domain, any receiver of that email is able to check the sender's IP, see that it's not coming from the one IP allowed by GRC, and to then ignore the email. Note that SPF has no way of preventing the attempt to spoof an email's origin, but it does provide a zero-cost means for a recipient to confirm the validity of the originator. And you can believe that Apple and Outlook and Google and Yahoo! and everybody, they're using this because they want to block all of this that they can.

While SPF identifies the authorized sender by IP address, it does not protect the integrity of the email itself. It offers no protection against anything that might alter the email's contents in transit. For that we have DKIM, D-K-I-M, which stands for DomainKeys Identified Mail. DKIM allows sending email servers to digitally sign the email envelope headers their outgoing email has so that the receiving server is able to verify that signature. And once again we have another use for DNS where additional DKIM records in the server's DNS domain are used to publish the public key with which its DKIM-signed email envelope headers can be verified. The receiving server sees the claimed FROM domain, queries that domain's DNS for its DKIM public key, then uses that key to verify the signature contained within the incoming email.

The final piece of this triumvirate is DMARC, Domain-based Message Authentication, Reporting, and Conformance, D-M-A-R-C. DMARC is a policy which is also published in the sending domain's DNS. It allows the sender's domain to indicate whether their email messages ARE protected by SPF and/or DKIM, and this DMARC policy instructs a recipient what to do if either of those authentication methods, which the site says must be enforced, fails. Do they reject the message, or quarantine it, or send back a report, or what?

So a crucial thing to appreciate is that, even today, all of these layers of email integrity and anti-domain-spoofing are completely optional. There is no need for any of them to be present or applied. They benefit the sender by preventing the sending domain's reputation from being abused, and they benefit the receiver by providing a means by

which the true sender of any DMARC-protected email can be verified. But all of this only works if both ends play. If the sender doesn't take advantage of these tools, or if the recipient doesn't bother to check against them, then neither end gets any benefit.

The other factor here is that all of this happens down in the plumbing of the Internet's SMTP protocol. None of this is ever seen by any of the eventual recipients of the email. There's never been any obvious visual indication of whether or not any of these various tests pass or fail, until now. One of the key requirements for any display of a BIMI logo is that the sender's DMARC policy must pass, which in turn requires SPF and DKIM to be present and to both succeed. So the first thing BIMI's display will mean in the real world is that the email actually originated from the claimed sender.

And this brings us to the logo itself and the question of how BIMI avoids the unauthorized or fraudulent use of organization logos. What, for example, prevents somebody else from copying GRC's Ruby G logo and using it for themselves? To answer that question, let's see what the BIMI group themselves have to say.

In their FAQ for this, they write: "Verifying a logo is authorized for use by a specific domain has been at the center of the debate since the idea for BIMI was first discussed. In fact, that very issue is why it has taken the past seven years to develop the specification."

Leo: I should point out, by the way, that DKIM, SPF, and DMARC are often now supported. For instance, Gmail will reject mail that isn't properly signed.

Steve: Right.

Leo: So that's the good news, right, that the things are getting better, at least in that regard.

Steve: Maybe. Google's policy is that, if you send more than 5,000 pieces of email a day, then you have to have DMARC.

Leo: Ah, okay. But I'm talking about inbound. I think that you have a good chance of getting blackholed if you are not - Google said they were going to require DMARC. But I might be mistaken on that.

Steve: The problem is there are still too many servers out there that do not support it.

Leo: Right, right.

Steve: And they want to be able to send email to Gmail people because that's about half of the world. So, yeah. But bulk mail senders sending more than 5,000 pieces of mail a day, Google will say...

Leo: Ah, you're right, it says bulk. Google and Yahoo! announced requirements that bulk senders must have DMARC in place. Yeah, yeah.

Steve: Yeah.

Leo: Oh, I misread that. I thought it was everybody. But you're right. So few people have that.

Steve: Right. So one of the cool things about this, and again, anyone who - any email supplier like Apple or Google or whomever who chose to could use BIMI to create a stronger indication that authentication was in place because that would be nice to know. So anyway, they said this issue has taken seven years to develop, and this thing I'm reading was written in 2021. So it's been 10 years.

Leo: Oh, my god.

Steve: They said: "Since this was such a difficult problem to solve, we developed two different types of BIMI records to get where we are today. Self-Asserted Records," they said, "In the first case, there is no verification of the logo at all. It was left up to the mailbox providers to decide whether or not to display the logo." And I should just mention nobody does because it doesn't provide what BIMI wants to provide. The second is: "Records with Evidence Documents. As many pointed out, there needed to be some form of evaluation such that a logo could be verified as being authorized for use by a domain."

So they said: "Up until recently, the most broadly deployed BIMI records were 'self-asserted.' Only a couple of mailbox providers accepted them, and those that did (for example Yahoo!) carefully considered which domains they allowed to display logos. Then on July 12th Gmail announced support for BIMI which required an evidence document in the form of a Verified Mark Certificate. In order to obtain a Verified Mark Certificate, a company must provide evidence that their logo is a registered trademark, i.e., that a government agency recognizes its legitimate use. The VMC also attests to the use of that logo in relation to identified domains. Mailbox providers can now retrieve and verify the VMC to ensure that the logo is authorized for use by that domain." And I'll note that they've actually softened this a bit for that Common Mark. The Common Mark Certificate just requires that you can demonstrate at least a year's worth of use of that logo on your domain.

So they finish: "Regardless of which BIMI record is used, the situation collapses into a single requirement: reputational trust. While a self-asserted record requires that the mailbox provider trusts the domain, for example, relying on their own reputation about the domain, a VMC moves the trust model from the domain to the VMC issuer." And so now we're talking certificates, and now we're talking certificate authorities, which is why DigiCert got into the game. In other words, we introduce the classic concept of a certificate authority. We trust the certificate authority, so we trust the CA's identify assertions by extension.

Now they have an FAQ. They said: "At this time, there are two Certificate Authorities that are accepted as Mark Verifying Authorities (MVAs) who can issue VMCs for use with BIMI." And get this, Leo, DigiCert and Entrust. And, yes, it's that Entrust.

Leo: How did that happen?

Steve: The Entrust from whom Chrome will no longer trust certificates...

Leo: That's crazy.

Steve: ...signed after the end of this month. And, by the way, Mozilla has made the same decision, ending their new certificate trust of Entrust one month later, at the end of November. Now, I don't know whether Entrust's hack to become a certificate intermediary would work here, and I don't care, because GRC's BIMI certificate, if I'm ever able to get one, will certainly be signed by DigiCert. More on that in a minute.

The BIMI FAQ continues: "So," they said, "it's essentially the job of the MVA (Mark Verifying Authority) to verify that the logos are authorized for use with BIMI. Then it's up to the mailbox providers to decide what MVAs they trust to issue VMCs (Verified Mark Certificates)." And believe me, if everyone does what DigiCert does, it'll be a cold day in Arizona before any spammer is using GRC's logo. Okay. I'll explain in a second.

They said: "And if you're curious about the steps the MVAs perform when evaluating a request for a VMC, here's the current process the CAs are following." And then they provide the VMC_Guidelines_latest.pdf. Now, they said: "If you've gone through the entire 94 pages, congratulations, it's pretty dense." And actually today it's 129 pages.

Leo: Oh, wow.

Steve: So they said: "You'll see that the evaluation process is reasonably thorough. The CAs are trying very hard to ensure that their VMCs can be trusted. As a checksum, if the email security community finds the CA has improperly issued a VMC, mailbox providers will no longer accept VMCs provided from that CA, which would essentially neutralize the CA's VMC business." So maybe Entrust shouldn't even bother.

Okay. So I know that listeners to this podcast would find it interesting to see GRC's "Ruby G" logo appear in the sender field of their email client when, for example, they open email from me in Gmail or Yahoo! or Apple. And if the presence of a BIMI logo, and everything that went into obtaining one, lent more credibility to GRC's email and helped them to be routed not to spam or junk folders, then I would regard that as time well invested. And in fact, that's the other thing that is expected is that BIMI-signed email will have a stronger reputation out of the gate.

So last week, after seeing that email from DigiCert, I headed over to their site to see what I needed to do. On the "Request Verified Mark Certificate" page, the first thing that's needed is to create the logo. You've got to create it and upload it for them to approve. But as I mentioned before, the uploaded format is quite specific and not readily created. In this day and age of widely varying device resolution, it makes sense for anything being newly defined to finally drop "pixels" and "resolution" in favor of "vectors." Vectors are the only way to go for the future, and the world figured that out in the case of fonts a long time ago.

So the BIMI specification nominally uses the SVG (Scalable Vector Graphics) standard. But they really wanted to get this right, which creates a few roadblocks since pretty much nothing currently supports the new deliberately constrained standard that they defined. On their "Solving SVG Issues" page, they wrote: "There are many reasons why your SVG might fail one of the online BIMI validators, and many of these issues stem from the requirement that all SVG images conform to the Tiny Portable Secure (Tiny-PS) standard." Huh?

They said: "The SVG Tiny-PS (where PS stands for Portable/Secure) is a streamlined profile of the SVG (Scalable Vector Graphics) specification, designed to provide a lightweight, secure, and portable solution for displaying vector graphics, particularly in environments with resource constraints. It retains the core functionality necessary for rendering scalable images while eliminating more complex features that may pose security risks or require extensive processing power. Its simplicity and focus on security ensure that graphics are rendered consistently and safely across diverse platforms. When updating an SVG file to comply with the SVG Tiny-PS standard, additional considerations include ensuring device compatibility, maintaining performance efficiency, and adhering to the standard's limitations. SVG Tiny-PS supports a limited subset of SVG elements and attributes."

And I can attest to that. Basically the SVG standard grew over time, as all standards of this sort do, to include all kinds of superfluous crap. In fact, you can even put a bitmap in an SVG, even though that's contrary to the SVG concept. But of course. So what they've done is they've stripped it back to the things you really need. You know, curves and rectangles and circles and filled patterns and gradients and things. So you could do what you need. You just can't dump anything in. So it ends up being constrained.

I think it's entirely reasonable, but it does introduce a hurdle. After searching around the Internet, the only tool I could find that would export an SVG file in what's known as the "Tiny v1.2" format was Adobe Illustrator. And having been an early fan of PaintShop Pro and Corel Draw, I've never been over in Adobe's camp. But I discovered that Illustrator is available with a seven-day free trial, you don't need a credit card or anything, it'll stop working after seven days, so I installed it. I converted my simple "Ruby G" bitmap from raster to vector and then used an Illustrator script which I found over on DigiCert's BIMI help page to export a fully compliant SVG Tiny-PS format. I then uploaded that to DigiCert, who inspected the file and approved it for BIMI's use. So now what? It turned out that was the easy part. I'll explain what happened next.

Leo: Oh, boy.

Steve: That was the easy part. Then we start having to prove things.

Leo: Oh, boy.

Steve: So let's take our last break, Leo, and then the fun begins.

Leo: Wow. What fun this is down the BIMI trail. Okay.

Steve: Yeah. BIMI up, Scotty.

Leo: BIMI up, Scotty. All right. And you know that no normal human is going to know anything about this, or whether it exists or anything. So, well, our audience will, so that's good.

Steve: Before a would-be BIMI user even begins the process, it's necessary for the organization to be certified at the EV level. Remember EVs? Those Extended Validation certificates that fell out of favor when web browsers decided to stop showing extra fields

of green for EV certificate sites because end-users didn't ever really understand what was going on, to your point, Leo, about the BIMI logos. Maybe we won't ever understand. Or maybe they'll be given special treatment once they, you know, achieve critical mass. Who knows?

And also, since nothing prevented typo-squatting sites from obtaining their own EV certificates, that was really the death knell because typo-squatters were able to get EV certs on their mistyped domain names, so users saw that and said, oh, look, it's all green. It must be safe. No. So even though EV certificates are not coming back, the level of organizational validation they once required is still going strong.

What this essentially means is that any organization displaying a BIMI mark in their email will have been validated at the same level as is required for EV certification. In this case, it means that I had to have Sue standing by at our corporate landline when someone from DigiCert called the phone number that an organization such as Dun & Bradstreet has listed in their corporate records for Gibson Research Corporation. Sue answered DigiCert's call and verified a bunch of information about our company and our website. She also confirmed that I, Steve Gibson, would be serving as DigiCert's "Verified Contact" for this "Verified Mark Certificate" order, and that I was authorized to request and have a Verified Mark Certificate generated.

Leo: Do you get a special hat?

Steve: No. But I got a special phone call. Once that was done, I received an email explaining what my role would be. I first needed to take photos of the front and back of an officially issued U.S. government photo ID and securely upload them to DigiCert through their SharePoint 365 account. Now, what might once have seemed intrusive is no longer any big deal since, after all, National Public Data has already posted all of that stuff publicly.

Leo: Everybody's got that.

Steve: It's all out there already, so who cares? On the other hand, couldn't all of that public data now be used to convincingly spoof an uploaded identity? Maybe, but DigiCert thought of that, too. The next step was to use an online scheduling app to arrange an interview, first by phone and then by online Zoom video conference.

Leo: Oh, my god.

Steve: Using the scheduling app, I booked the first available 30-minute slot. And at the appointed time I received a phone call from a DigiCert person. He identified himself as the person I'd been corresponding with, and he instructed me to please upload photos of my ID to their SharePoint 365 account. I told him that I had already followed the link in the earlier email and done so. He thanked me and asked if I was ready to switch to Zoom. I told him I was, so he sent me a Zoom link.

Clicking the link brought me into a two-way audio conference with a one-way video. His camera was never enabled, so I only saw his name, but he had a clear view of me, just like our listeners do right now because I used our same system.

Leo: Yes.

Steve: He had told me that I would need to show the same ID during the video conference. So I went back, got it out of my wallet, and I had it handy. He first asked me to pose on camera so he could capture that. Then he asked me to hold the ID up next to my head...

Leo: Oh, my god.

Steve: ...so that both my face and my ID were on camera side-by-side at the same time. I did that.

Leo: This is more than you had to do for an EV cert.

Steve: Oh, yeah. EV, we left off on Sue telling the guy to have a nice day.

Leo: Yeah. Wow.

Steve: So then he asked me, while still holding the ID up next to my head, to pass my other free hand across my face and then both in front of and behind my ID, while still holding it relatively motionless.

Leo: Oh, my god.

Steve: It took a bit of finagling to satisfy him. But since I was neither an AI-generated spoof nor a North Korean posing as some old white guy, I was able to follow his instructions and satisfy him that I was indeed me.

Leo: Wow.

Steve: And, since this created an unbroken trust chain from GRC's public corporate records, through our offices, to me and my identity, this was able to satisfy their need to confirm the authenticity of our logo submission. I forgot to mention that earlier in the process, after I had successfully created and uploaded and verified the Tiny v1.2-P/S SVG logo file, DigiCert's website had required me to post a specific text string in GRC's DNS and then click "OK" once I had so that I could prove ownership over the GRC.com domain.

And this brings us to the final step where they verify that I've been using that logo on GRC's website for at least a year. Since I've been using it for the past 40 years, since before the web came into existence, from the moment it came into existence and every day thereafter, I figured this final step would be a slam dunk. So how do you imagine they verify my longstanding use of this logo?

Leo: Oh, no.

Steve: Oh, yes. They use the famous "Wayback Machine"...

Leo: Oh, no.

Steve: ...at The Internet Archive over at Archive.org.

Leo: I was wondering what the connection was.

Steve: However, there was a slight glitch last week, since for most of last week and all of the weekend and apparently until sometime yesterday, all of The Internet Archive was under attack and offline.

Leo: They were trying to keep you from getting your BIMI. Now we know why.

Steve: And as a consequence of that, after everything I had gone through, the final step in the long process of obtaining a BIMI certificate has been placed on hold.

Leo: Oh, my god. The weakest link. Oh, my god.

Steve: Now, that's fine with me since GRC obtaining this certification is certainly not an emergency. So whenever it manages to happen will be fine with me. Probably, you know, later this week. All of the required steps have been taken on my end. So once DigiCert is able to look back in time at GRC's historic use of that logo, which they will see on every single page that the Wayback Machine has ever indexed...

Leo: Wait a minute. What if you weren't on the Internet Wayback Machine? Not everything is; right?

Steve: That's true.

Leo: The heck? That seems very...

Steve: In that case you could, if your logo was registered, then you would be in the U.S. Patent and Trademark Register.

Leo: Our logo's - your logo's not registered?

Steve: I never bothered to register the logo. Yes.

Leo: So that's why. Because ours is - this logo is in the trademark.

Steve: Yup. And if you've got that trademarked, then no problem.

Leo: It's a service mark or whatever it is, yeah.

Steve: Right. Okay. So what happened was that a series of DDoS attacks began last Tuesday, October 8th. And somehow mixed in with that was a JavaScript library-based site defacement which affected the Internet Archive, and a breach which leaked usernames and email addresses and salted hashed passwords for 31 million past Internet Archive users. The Archive's greatest concern was the preservation of the integrity of their archive, so they took everything offline while they worked to figure out exactly what had happened.

Wikipedia informs us that Brewster Kahle is an American digital librarian, computer engineer, Internet entrepreneur, and advocate of universal access to all knowledge. In 1982 he graduated with a bachelor's degree in computer science and engineering from MIT, and in 1996 Kahle founded the Internet Archive. In 2012, he was inducted into the Internet Hall of Fame.

Leo: And a year later he was on Triangulation, if you ever want to see an interview with him. Quite - I love Brewster Kahle. Amazing fellow.

Steve: Yup. He seems like 100% good, you know, he's like what we wish we had more of.

Leo: I agree, yeah.

Steve: So Archive.org has a Mastodon instance, and Brewster has posted two updates there. His first one said: "What we know: DDoS attack fended off for now; defacement of our website via JS library; breach of usernames/email/salted-encrypted passwords. What we've done: Disabled the JS library, scrubbing systems, upgrading security. Will share more as we know it."

And then he said a little bit later: "Sorry, but DDoS folks are back and knocked Archive.org and OpenLibrary.org offline. @InternetArchive is being cautious and prioritizing keeping data safe at the expense of service availability. Will share more as we know it."

So as I said, I checked this morning, and I saw - I checked this morning online and saw a raft of articles about this. You know, headlines read, from BleepingComputer: "Internet Archive hacked, data breach impacts 31 million users." Forbes wrote: "Internet History Hacked, Wayback Machine Down, 31 Million Passwords Stolen." The Verge wrote: "The Internet Archive is still down, but will return in days, not weeks." That's something that Brewster posted elsewhere. CyberNews said: "Internet Archive down after two-day DDoS attack, user info compromised." And Fast Company more recently said: "The Internet Archive is back online after a cyberattack."

So I've observed some of the Internet dialogue surrounding this event, and this interruption in the availability of the Internet's Archive has served a useful purpose, I think. It has served to remind people just how important this service has become. It's one of those things that's easily taken for granted until it's not available, at which point

you realize just how important it can be to have a "Wayback Machine" that allows us to view earlier states of the Internet.

Our listeners may recall that I put the Archive's Wayback Machine to extensive use back when we were examining the effects of that Polyfill.io trouble, where we looked at the danger of a publisher of a widely used and publicly hosted JavaScript library turning control over to another entity. I needed to look back in time to see how the Polyfill.io site had grown and evolved since its earliest days, and this research was only possible because the Wayback Machine had been quietly, dutifully, and continuously taking and storing snapshots of the Polyfill.io site - along with all the other sites that it crawls on the Internet - throughout its entire life.

The Verge's most recent reporting said this. They said: "The Internet Archive is back online in a read-only state after a cyberattack brought down the digital library and Wayback Machine last week. A data breach and DDoS attack kicked the site offline on October 9th, with a user authentication database containing 31 million unique records stolen in recent weeks. The Internet Archive is now back online in a 'provisional, read-only manner,' according to founder Brewster Kahle, 'safe to resume, but might need further maintenance, in which case it will be suspended again.'"

And they wrote: "While you can access the Wayback Machine to search 916 billion web pages that have been archived over time, you cannot currently capture an existing web page into the archive. Kahle and team have gradually been restoring Archive.org services in recent days, including bringing back the team's email accounts and its crawlers for National Libraries. Services have been offline so that Internet Archive staff can examine and strengthen them against future attacks.

"A pop-up from a purported hacker claimed the archive had suffered a 'catastrophic security breach' last week, before Have I Been Pwned confirmed the data was stolen. The theft included email addresses, screen names, hashed passwords, and other internal data for 31 million unique email accounts.

"The Internet Archive outage came just weeks after Google started adding links to archived websites in the Wayback Machine. Google removed its own cached page links earlier this year, so having the Wayback Machine linked in Google search results is a useful way to access older versions of websites or archived pages." Okay. So...

Leo: This would be a good opportunity, by the way, for people to donate to the Internet Archive. I'm a longtime supporter. I give them money every month.

Steve: As am I, yup.

Leo: Yeah. This is such an important - more than a service, this is an important way to back up our history.

Steve: Yes, yes.

Leo: And it's got to be supported.

Steve: And I don't know if an organization like Cloudflare might be interested in being a benefactor here, nor what Brewster's requirements would be. They might be in collision.

Or even if it's, you know, even feasible. But the Internet Archive, Leo, as you said, it's a vital tool for researchers, academics, and others. And I suspect that its value and importance will only increase over time.

In any event, it now appears that the Wayback Machine is limping back online, and that before long DigiCert will say that they have been able to use the Wayback machine to verify my decades-long use of that "G" logo. At that point they will approve and issue a BIMI certificate that will be valid for any newly minted certificate's maximum life of 398 days. They seem eager to host the logo and the certificate from their servers. You can do it yourself, but they're volunteering. So I'm fine with that. It seems to me that they'll provide the URLs, and it might add a little more credibility to it that it's coming from DigiCert.com.

So whenever a BIMI-supporting email provider receives email from GRC - as Apple will, Gmail will, Yahoo! will and so forth - in addition to verifying that email's authenticity by pulling our SPF, DKIM, and DMARC DNS records, they'll proactively check for and pull GRC's BIMI record. That will provide two URLs. It will tell them where to obtain the "Ruby G" SVG logo itself, and where to find its validating certificate. I haven't looked into how the logo and the certificate are related, but since it's possible for me to host those files myself, they must be protected from tampering. Assuming that the SVG file itself is not altered, the certificate probably contains a hash of the approved SVG logo file and an indication of the domain for which the logo is valid.

So anyone wishing to support BIMI logo-embellishment on their mailboxes could look up the information, hash the SVG logo they retrieve, and check for the matching hash inside its matching BIMI certificate. Since the certificate would be signed by DigiCert's trusted root, this would establish a chain of trust sufficient to authenticate the logo's use for the indicated email domain. And the email provider could then confidently show that logo to its email users, but only if the email also passes DMARC validation. So it's the first visible indication we've had on the Internet of email authenticity in the guise of a logo provided by the email sender.

Now, for GRC, as I've said, that did not happen in time for this week's podcast mailing to the Security Now! subscribers, which went out this morning. But having jumped through, as I said, through all those hoops to get this far, and with us now only waiting for the Wayback Machine to be available to allow GRC's historical logo usage to be confirmed, I'm hopeful that everyone may see it in their mail next week. So that'll be an interesting change.

Upon learning that Gmail had adopted BIMI support some time ago, I went poking around in my own Gmail inbox. Though I did not dig too deeply - and again, I don't get lots of valid email there, it is my throwaway email account - I did see that PayPal and Disney+ both had BIMI logos for their email. So BIMI logo usage is around; but we're certainly, you know, not seeing it in common use. Will it become more common over time? It's too soon to tell.

Since email providers have total freedom to decide which Certificate Authority's Verified Mark Certificates they wish to support, and having seen the costly rigor DigiCert just applied to me to prevent any form of spoofing, it's clear that if the BIMI group could be accused of anything, it would be setting the bar for this too high. But in an industry that has repeatedly been in such a hurry that the bar is usually set too low, I consider this to be a change in the right direction. Though obtaining this level of identity proof is difficult and costly, any organization that does this gets a year of extra strong identity for their email, if anyone notices or understands.

At this point I'm pretty certain that most users have no idea that any of this is going on. I certainly didn't until I dug into this. But if it catches on, it might begin to chip away at

some of the catastrophe that completely free email creation and delivery has created. And it only costs something to the sender who's decided that they care enough to super-authenticate the sending of their email to its recipients. So that's BIMI.

Leo: Couple of questions. One, doesn't an EV cert cost quite a bit of money?

Steve: Yeah. They are not cheap.

Leo: Okay. Like thousands of dollars a year.

Steve: I don't think it's that much.

Leo: It's not that much. Okay.

Steve: I think that's a multiyear with an annual renewal.

Leo: But you can't get multiyear renewal anymore. So, yeah, okay, maybe it's not that expensive. But it's expensive. It's not trivial to get it. It's interesting that it's required. Is that just a DigiCert requirement? Or is that a BIMI requirement?

Steve: That's a good question. And as I said, I did not look through that 127-page document...

Leo: I don't blame you.

Steve: ...on its requirements. But what is required is that is EV level certification.

Leo: Right. That makes sense.

Steve: So I didn't actually get an EV cert. I didn't mean to imply that I got an EV cert.

Leo: Oh.

Steve: But EV-level certification...

Leo: Oh, you don't have to have an EV cert. You just...

Steve: No.

Leo: Oh, oh, oh. You were just saying it's the same level. I misunderstood.

Steve: Right. It's EV-style certification where, I mean, so...

Leo: They call and all that.

Steve: Yeah. Back when we were doing EV certs, Sue had to do the same thing. She had to be standing by when the phone rang and answer it, you know, and say...

Leo: Yeah, we did the same thing, yeah.

Steve: Yeah. Yeah.

Leo: And any company would be able to, you know, jump through these hoops.

Steve: Oh, yeah, PayPal's got, you know, they pay people to stand around.

Leo: Yeah. All right. Okay. That'll be interesting, to see if this catches on. I feel like it doesn't really go the full distance. And of course you've got to get all the email clients to display it.

Steve: True. True.

Leo: I was just looking at Fastmail. I don't see any provision in Fastmail to display BIMI logos. Obviously Gmail does.

Steve: Fastmail, I named them. Either they're...

Leo: They're on the group. They're in the group. That's why I was surprised.

Steve: So are they in the group that were supporting it or were displaying it?

Leo: They were in the initial team putting it together.

Steve: Ah, okay. So...

Leo: But whether they, I mean, maybe they do. Just was a cursory search.

Steve: So you should, if you have PayPal or Disney+, those are the only two that I know of.

Leo: I have a PayPal, dedicated PayPal folder. Let me...

Steve: And maybe, if this works by next week, you'll be able to look at my mail.

Leo: That would be so cool.

Steve: Yeah.

Leo: Yeah. I would like that. Oh, well. Yeah, I don't see any...

Steve: I'm going to do it, and our listeners who receive email from me will, I mean, like anytime you get email from GRC it'll then have - it'll be embellished with that Ruby G logo.

Leo: Yeah. I'm looking at PayPal emails, and I don't see any logos. The other question was...

Steve: It's got their little double P leaning is the logo.

Leo: Yeah. And that's presumably stored, not by PayPal; right?

Steve: It is, well, PayPal could source it, or DigiCert could source it.

Leo: See, I don't like it if PayPal sources it because then that's a tracking pixel.

Steve: Oh, if it's not embedded, you're right. No, well, no. Because Google, for example, would download one copy of it and then would cache it locally.

Leo: It would use it everywhere, cache it, okay.

Steve: Right.

Leo: That's fine. I would just - I could see PayPal going, oh, good, one more way to...

Steve: Yeah. So it's not the email client that reaches out and fetches it. It is the email provider...

Leo: It's a server.

Steve: ...that is only if the email passes DMARC and you have matching certificate for the logo. Then the email provider adds that to your inbox.

Leo: I don't mind the idea. We'll see what happens. I'll look forward to seeing a Ruby G in my email from that. Make it a lot easier to find you.

Steve: Yay.

Leo: In that pile of trash I call "my email." Steve Gibson is at GRC.com. You know what that stands for? Gibson Research Corporation. That's where he does his work.