

Security Now! #996 - 10-15-24

BIMI (up Scotty)

This week on Security Now!

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 multi-platform 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.

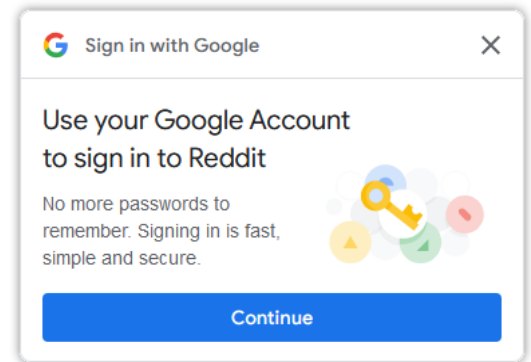
When your message interferes with ... your message.



Security News

uBlock Origin to the rescue

Everyone is annoyed 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...

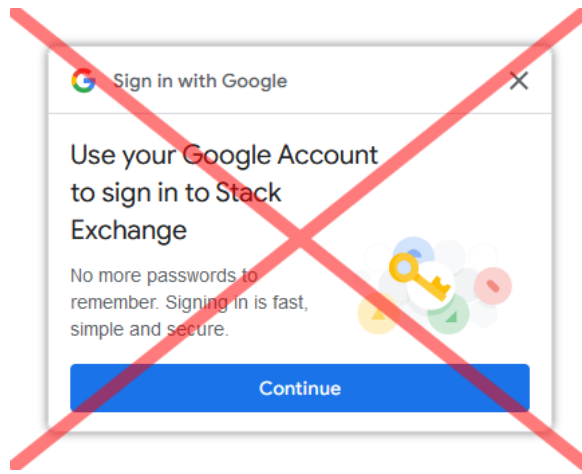


Now to be clear, I often choose to sign into websites using my Google account identity because Google provides a very secure implementation of Oauth. My primary email will be at GRC, so my Google email is my generic catchall throwaway account. So signing in with Google gives me convenient one-click login at any site that offers it. And, yes, being Oauth means that Google knows where I am, where I'm signing in and what I'm doing. But Google almost certainly knows anyway, and the truth is I don't have time to care. Sure, all other things being equal I would choose privacy – who wouldn't? And I get it that there are people 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 when I'm at a website where I **want** to have or create an account, and where signing in with Google's Oauth service is an option, it's the choice I'll usually make. So having the **option** to sign in with Google is **not** the source of my annoyance. The source of my annoyance is that a trend has been developing recently to **proactively PUSH signing in with Google on me** wherever I go and whenever I visit a participating website – even if I have absolutely zero interest in or need to "sign in" there. I don't want to sign into every website on the Internet, and I believe that's the case for most of us. 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" pushed on me, and this has become quite annoying. More and more, when surfing around the Internet we're being confronted with these "Sign in with Google" pop-up dialogs. They proactively appear in the upper righthand corner of a website and obscure whatever has been covered up by them. This reached critical mass for me this past weekend and I decided to do something about it.

I should note that today, none of this comes as news to the 10,442 subscribers to GRC's weekly Security Now! email who all received an early surprise from me Saturday when they checked their email to discover that I'd been unable to wait until today to share a solution to this growing annoyance. And based upon the overwhelmingly positive feedback I received from that extra weekend mailing, I'm glad I didn't wait since the responses confirmed that everyone else has been every bit as annoyed as I have and they universally welcomed a solution to this.

But even more than that, thanks directly to all of that feedback – I read and appreciated every one of those replies – I've learned a lot more since Saturday – and I have that to share today:



First of all, I should explain that all this occurred to me thanks to last week's discussion of uBlock Origin. My original solution, the one I shared Saturday, was very specific and has the advantage of **only doing exactly that one thing**. However it didn't work for everyone; some people needed a somewhat broader solution. And it turned out that this sort of annoyance blocking is also built into some of uBlock Origin's existing filter lists although they are not enabled by default. So it's also possible to implement much more broad annoyance suppression. But I'm getting ahead of myself. Let's examine this one step at a time.

The pop-up is an iframe sourced from "accounts.google.com/gsi" where "gsi" almost certainly stands for "Google Sign In". So what we want is to add a filter to uBlock Origin to prevent our browsers from loading and displaying that iframe.

With uBlock Origin installed, click on its extension's red shield icon to open its drop-down menu. In the lower right, click on the little three gears icon to open the extension's configuration and preferences browser pages. Switch to the "My filters" tab since we're going to want to add our own filter. The two lines I added are in the show notes:

```
! Block "Sign in with Google" iframe in top right corner of websites  
||accounts.google.com/gsi/iframe
```

The first line is a comment beginning with an exclamation point. The entire contents of any line beginning with an exclamation point that is not followed by a pound (#) sign is ignored by uBO. So this comment line which reads (exclamation point) "Block "Sign in with Google" iframe in top right corner of websites" is just to remind us what the next line does. And that line begins with a pair of vertical bars (||) which are used to indicate that what follows is a domain name and perhaps more, such as a path under that domain. In this case we have

```
||accounts.google.com/gsi/iframe
```

Which tells uBlock Origin to block URLs matching that much of the filter line. Under Firefox on Saturday I used the developer console and saw the page loading that. So I added that line to the "My filters" tab and clicked "Apply changes" at the upper left and the annoying sign in pop-up at StackOverflow no longer appeared.

However, after the mailing I learned that this was not effective for everyone. It seems that not everyone, perhaps using different browser or OS platforms, was able to suppress the pop-up when the filter rule ended in "iframe". But if they substituted a single wildcard asterisk (*) for the iframe phrase THEN it worked ... and they were beyond delighted to be rid of this new Internet scourge.

|| accounts.google.com/gsi/*

The downside of replacing the "iframe" phrase with a wildcard is that the filter rule will match on anything under the /gsi/ directory. But given that GSI must stand for Google Sign In, that's probably a safe tradeoff. So, if you were among those who followed the more specific filtering instructions that I provided last Saturday and found that the Google pop-ups were still not suppressed, try changing the "iframe" to an asterisk and that will likely do the trick.

Also, I didn't mention that the checkbox for "[x] Enable my custom filters" must also be checked. I didn't mention that because I'm sure I never changed that setting and my custom filters (although initially empty) were already enabled by default. So I assumed everyone's was.

But I learned something else from those who wrote back. It turns out that this particular annoyance is just one of a great many annoyances that the Internet community at large have painstakingly identified and suppressed. So there's an entirely different, far more powerful and comprehensive alternative to the "one-liner" that I first proposed:

Rather than the "My filters" tab, click the preceding "Filter lists" tab. 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". It's so easy to get one of those annoying Google sign in pop-ups – just go over to <https://reddit.com> – that it was easy to experiment with enabling and disabling these three lists. I discovered that enabling either of the first two – either "EasyList" or "AdGuard" – would suppress the gratuitous Google sign in pop-up. Drilling down a bit into some of the documentation, the "AdGuard" annoyances list says:

Annoyances filter blocks irritating elements on web pages. Includes the following AdGuard filters (all of them can be enabled separately from the Annoyances filter):

- *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.*
- *Widgets blocks third-party widgets: online assistants, live support chats, etc.*
- *Other Annoyances blocks elements that do not fall under the popular categories of annoyances.*

Okay, I'm all in! While we're on the topic of persistent annoyances, those proactive "online assistant" offers to chat with someone which have also become much more prevalent as they slide up from the bottom right of pages, asking whether we've found what we want or how they can help – are not helpful.

I've never once thought "*Oh, gee, how handy! Thanks for asking!*" So wiping them all out along with Google's coercive login pop-up, and while we're at it, suppressing all of those GDPR-driven Cookie Notices is nothing short of a total win.

So I went back and removed the two lines from the "My Filters" page and enabled all three of the filters in the "filters list" Annoyances section. As you enable them you may find that you get little orange "caution" triangles. This just means that the latest lists need to be loaded into your machine. So after you've enabled them – again, I went for all three – you may see that the "Apply changes" or "Update now" buttons are highlighted at the top of the page. If both are enabled, click "Update now" to handle both.

Also, while we're here, I'll mention that the section above "Annoyances" is "Social widgets" where we find "EasyList", "AdGuard" and "Fanboy". AdGuard says:

***Social media filter** removes numerous "Like" and "Tweet" buttons and other social media integrations on popular websites.*

All three of those are now also enabled for my instances of uBlock Origin. I won't miss the ability to Tweet or Like from web pages I'm visiting. So for any of us who take these steps, uBlock Origin will now be doing **far** more than it ever was for us, silently and thanklessly working to sanitize our experiences of the web. And the other thing to note is that there are teams of volunteers who are working to maintain these lists on our behalf. So as new tricks are found to get around the filters in these lists, the lists are updated to keep up... all without us having to do anything.

Some of our Chrome-using listeners wrote after last week's exploration of Manifest V2 and V3 to ask what **they** would do once we reached June, Chrome's V2 extension support was deliberately terminated, and they lost access to the full power of uBlock Origin? We're nearly 9 months away from that and as we've seen – for example with Google's changing 3rd-party cookie plans – anything could change before then. So there's no clear answer yet and my advice would be to not worry about it until we get much closer. Last week's registry hack to enact a 9 month extension buys a lot of time during which anything could change. Also, the V3-compatible Lite version of uBlock Origin may not be useless. Gorhill has 37 million users on Chrome vs 7 million on Firefox. So once uBOL is the only solution under Chrome I imagine he'll work to do everything he can to keep it relevant. And that may be sufficient.

What I will say is that after enabling these six additional filter lists for uBO I'm more happy than ever that I'm using Firefox. And also remember that the Chromium-based Brave browser has formally said that it has no plans to drop support for V2. So it might be possible for those who want or need to remain on a Chromium-based browser to switch from Chrome to Brave.

I'll close by noting that I felt a bit self conscious sending that unscheduled mailing to the Security Now! list subscribers, since everyone explicitly signed up to that list to receive weekly podcast summaries, show notes and pictures of the week. But many people said that this was exactly the sort of power user tip they would welcome receiving anytime as a subscriber to that list.

Since the system I've built makes it so effortless to send these sorts of announcement mails to our 10,000+ subscribers, I would like to formally expand the mission of that list 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 would probably be of interest to everyone. This one certainly appeared to be.

Let's take a break, then more news!

National Public Data files for bankruptcy

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

The Register writes:

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.

[To recap] Last June, the hacking group USDoD put a 277.1 GB 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 - a data 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, such as "name, email address, phone number, social security number, and mailing address(es)." 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."

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 US states. Any plaintiffs will have a hard time getting any money out of Jerico since the documents state the business has 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 \$33,105 in a corporate checking account in New York as its assets, although the business pulled in \$1,152,726 in the last fiscal year, and estimates its total assets are between \$25,000 and \$75,000 in total. It also lists 27 Internet domains with a value of \$25 each. These include the corporate website - now defunct - as well as a host of other URLs including criminalscreen.com, RecordsCheck.net, and asseeninporn.com.

So 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 presents an inherent danger. But today there is no regulation over this. Anyone who wishes to can amass such data to create a latent data bomb. On the one hand it's free enterprise and capitalism which no one wants to stifle. But allowing a fly-by-night operation 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 be on the hook for losses, would be motivated to assure that the enterprise's IT staff, procedures and security are adequate to protect their investment.

Will the .IO top level domain be disappearing?

Many of the top level domains are associated with countries. The BIT.LY service is "BIT<dot>LY" where "LY" is the country code for Libya. GRC's shortcut domain of "GRC<dot>SC" uses .SC which is for the country Seychelles. Other top level domains are created independently such as .COM, .ORG, .NET and .EDU... but when a top level domain belongs to a country it is tied to that country.

This has recently created some concern when, a couple of weeks ago on October 3rd, the British government announced that it would be releasing its 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 1100 miles off the southeast coast of Africa. 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 <dot> IO domain, this 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. The Internet Assigned Numbers Authority (IANA), which creates and delegates top-level domains, uses this specification to determine which top-level country domains should exist. Once IO is removed, the IANA will refuse to allow any new registrations with a .io domain. It will also automatically begin the process of retiring existing ones.

What's not known at this point is whether this will be allowed to happen. Humans make the rules and humans can change the rules if the rules are causing too much trouble. Since we certainly have no lack of non-country TLDs. We have .XYZ, .LOL, .ONLINE, .ME and .MY ... so I, for one, see no reason why .IO cannot simply be repurposed into a non-country rooted top level domain. But then again, I'm not the IANA who ultimately decides these things.

Patch Tuesday

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 are rated Critical, 113 are rated Important, and two are rated Moderate. And, as usual, that count does not include the 25 additional flaws that Microsoft previously addressed in its Chromium-based Edge browser over the past month.

Firefox under attack

Also, Firefox and the Firefox-based Tor Browser have been warning everyone of the discovery of a serious attack against Tor users. The flaw carries an attention-getting CVSS of 9.8 and affects both Firefox and the Firefox Extended Support Release (ESR) products. It's a use-after-free bug in the Animation timeline component. Mozilla reported in a post last Friday, October 11, that it had received from ESET an exploit sample containing a <quote> "full exploit chain that allowed remote code execution on a user's computer." Mozilla also noted that the fix was shipped within 25 hours of responsible disclosure. Two days before that, last 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 the added "We have had reports of this vulnerability being exploited in the wild." The issue has been addressed in Firefox 131.0.2, ESR 128.3.1, and ESR 115.16.1. The Tor project has also released an emergency update to version 13.5.7 of their Tor Browser.

Next Week: Credential Exchange Protocol (CXP)

We have so much more to talk about this week that I'm going to switch to some miscellany, a Sci-Fi update and some listener feedback. But several of our listeners asked if I could talk about the new Passkeys **Credential Exchange Protocol (CXP)** which was just unveiled yesterday during the FIDO Alliance's "Authenticate" Conference which was held in nearby Carlsbad, California. And that's a definite yes! So unless something even more important comes up between now and then everyone can look forward to full coverage and a deep dive into the promise we have all been waiting for, which is full secure portability for our passkeys between providers.

Miscellany

Several weeks ago I mentioned that a listener of ours had suggested that when I move my Windows 7 workstation to Windows 10, I choose a Windows Server version. At the time I thought that 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 long ago. It may have been back in the Windows XP era that I did try running a server edition of Windows, probably because I wanted to be using exactly the same build of Windows that GRC's servers were running. 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 I was running on a Server release of Windows. I fought against that and put up with it for a while, but it ultimately forced me to return to a desktop release.

Sci-Fi

I'm 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. 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 Salina, our JammerB, who is already well into his second read through. He noted that the second pass is more fun because by then you know who all the players are – and the players are somewhat dizzying. The book begins with a chronology that's stunning in its sweep and scope of humanity's near and far future. Next, it runs through and introduces a vast array of characters. The historical summary was engaging and I then forced myself to sit still and at least take the time to read through all of the names of entities whose roles were described mostly in relation to others in the same 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 start and go again.

If I imagine rereading what I've read so far I doubt I'd find it boring. I'll give Peter this, he has a gift for spinning a yarn. He knows how to tell a story. I'm not in the position to recommend this to anyone yet since I have no idea what's going to happen. It might be another of Peter's slow burn novels which is interesting while not leaving you gasping for breath. I'll know more in a few weeks. John, of course, already knows.

Closing the Loop

Brian Hendricks

*Hey Steve, I was looking for a new puzzle game to play on my tablet and 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 did not enjoy it as much. Hopefully this new game lives up to the original. Happy Security Now-ing to 4 digits and beyond!*

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' too) that 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 and I went looking. It is nowhere I could find 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: <https://play.google.com/store/apps/details?id=com.onemanband.thesequenceplus>

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, an outfit by the name "One Man Band", authors these apps with the Unity framework, it would also be available for iOS and I'm hoping that it's just delayed while Apple vets it because a new edition of that original "The Sequence" puzzle would be well worth playing.

I should note that when Brian said "a few years ago", he meant nine years ago, back in 2015. So there's 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, each having a single very simple 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 and ready to do it again.

And one final comment for those who may have heard of things like this before, only to be 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 this and I've been quite 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: <http://ombgames.com/> (not https, only http) and I also have a link to the author's official YouTube video: <https://www.youtube.com/watch?v=bq3Q0OR1NeU> And it earned this week's GRC shortcut of the week. So it's: <https://grc.sc/996> It's available for a few dollars **without any ads or 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!

As I was preparing these show notes, I spent some some 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 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" that this podcast and I came to his attention and he decided to follow me.

He hadn't posted anything recently there, so I shot him a note asking about the status of "The Sequence Plus" and not long after I received a reply. His first name is Maxim, and he wrote:

Hi Steve, I'm glad to hear that everything is going well with you. I am 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. For now, it is only available on Google Play as an experiment. 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." Best regards, Maxim

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 doesn't sound like "The Sequence Plus" would be anything I want even if it were available on iOS. As Maxim said, it's largely just "The Sequence" renamed and made free, but with ads. If you're someone who enjoys puzzles, my advice would be to follow GRC's shortcut of the week at <https://grc.sc/996>. That will show you a 50-second sample of the original "Sequence" – and if it

looks appealing, send a couple of dollars Maxim's way to show him that paid puzzles are not dead, at least not here. And then get ready to really enjoy yourself under Windows, Steam, iOS or Android.

Parker Stacy

Dear Steve, Thank you for this EXTREMELY helpful tip. 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 am 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

I chose Parker's note as a placeholder for the 135 replies I've received and read (so far) following Saturday's special mailing. 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. I was glad to learn that it wasn't just me being a cranky old curmudgeon.

Frank from the Netherlands

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

I wanted to share Frank's note to point out that most of us, certainly I, have been grossly underutilizing the power of uBlock Origin. It is an extremely capable general purpose web experience filter.

The reason it's been underutilized is probably a case of cooking the frog in the pot of water whose temperature is slowly increased as that the frog never thinks to jump out. For us, the incursion into our browsers has been very gradual and incremental. For example, at first only a few sites were pushing us to login with Google. So we put up with those few 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 are just one symptom. What's happening is that little by little our online experiences have been increasingly leveraged and we're being increasingly coerced. No one likes being coerced.

So it clearly occurred to “Frank from the Netherlands” that he could employ his copy of uBlock Origin to more completely take back control of his online experience by using it to edit many of the pages he sees throughout his days.

Two pieces of feedback about routers

Justin Long

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. 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. 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, etc. If you have multiple networks on the same account, one eero plus subscription covers them all for the same price. (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 in 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.

Joking aside, it’s a great solution. Hopefully this is helpful to someone- Justin

And another listener took Michael Horowitz’ advice about the Pep Link router:


Phil wrote:

Hi Steven, I’m glad you pointed out Michael’s router security website yet again. I’ve recently replaced my Verizon FiOS router with his recommended Pep Link 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). 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 pretty straightforward. Thanks, Phil

The Pep Link router is what the 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 Phillips’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.

Let’s take a break, then we’ll plow into our main topic!

BIMI (up Scotty)



Temporarily Offline

Internet Archive services are temporarily offline.

Please check our official accounts, including [Twitter/X](#), [Bluesky](#) or [Mastodon](#) for the latest information.

We apologize for the inconvenience.

BIMI – Brand Indicators for Message Identification

For this week's main topic I want to share an adventure from late 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 has been a paused until the Internet archive is back up.

It all began when I checked my email after last Tuesday's podcast and found a new feature notification from DigiCert. It said:

We're writing to let you know that Common Mark Certificates are now available. Common Mark Certificates allow organizations to place a brand logo in the Sender field of outbound emails, confirming the organization's DMARC status and authenticated identity, and helping protect against phishing and spoofing attacks.

***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.*

To qualify for a Common Mark Certificate:

- *The corresponding email domain must be configured to enforce DMARC.*
- *The corresponding brand logo must either.*
 - *have at least year of previous public usage on a domain controlled by the applicant, or*
 - *be an acceptable modification of a registered mark. (See Section 3.2.16 of the BIMI Group's Minimum Security Requirements for Issuance of Mark Certificates for more details.)*
- *The logo file used for the Certified Mark Certificate must be an SVG file that adheres to the SVG-P/S profile.*

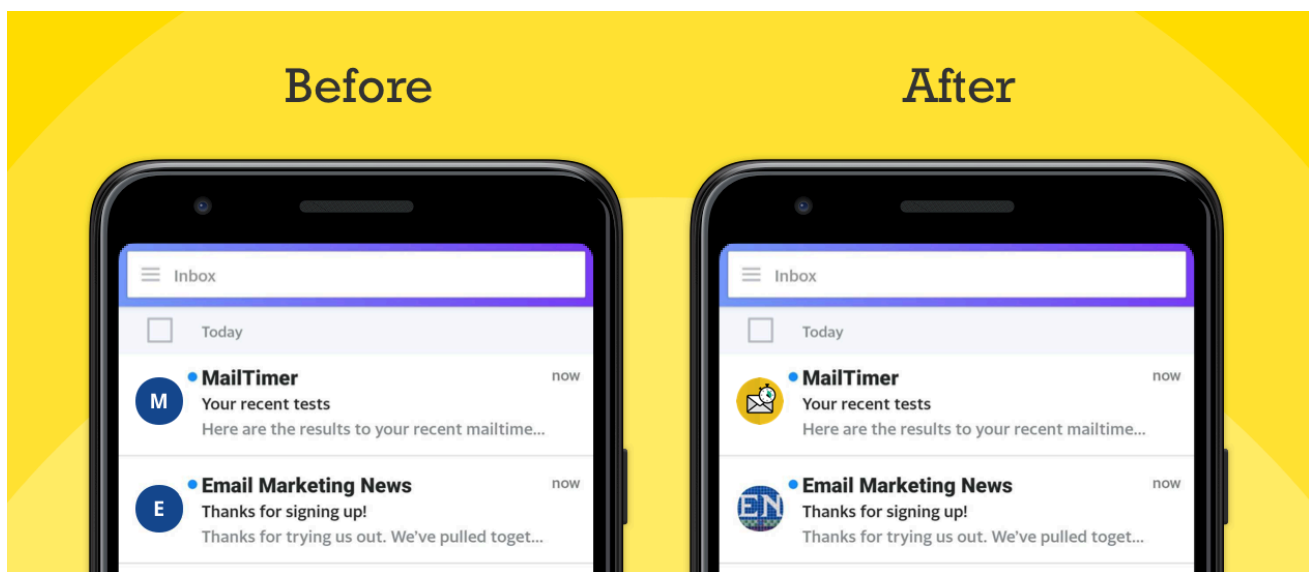
Note: Currently, most image editing tools do not support the SVG-P/S profile and will require using a specific conversion tool or manually editing an SVG file. See our guide for properly formatting the logo.

First I should confess that BIMI is officially pronounced “Bih-mee” not “Bee-mee” – but I was unable to resist “BIMI up, Scotty.” BIMI is the abbreviation for “Brand Indicators for Message Identification.” It’s a new and slowly emerging email standard that creates a secure means for incoming email to carry and display its sender’s unspoofable logo icon. Email clients and online services that 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 (<https://bimigroup.org/>). The members of this group are Fastmail, Google, MailChimp, Proofpoint, SendGrid, Validity, ValiMail and Yahoo! The project began a full ten years ago, back in 2014 and today the display of BIMI logo icons is supported by Apple, Cloudmark, Fastmail, Google, Yahoo! And Zoho.

What this group has managed to design and achieve wide consensus on, is the rough equivalent of the web server TLS certificates we rely heavily upon 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 it. Yet everyone needs it. It is 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 means for ultimately authenticating users when they forget their password or don’t have their 2nd factor authenticator handy. It all 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 recipient’s inboxes.



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 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 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 email 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. That will likely be worth something to them, and in time it may serve as a useful indicator to those on the receiving end.

Okay. 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. Let’s briefly review these three email validation standards, SPF, DKIM and DMARC:

SPF (Sender Policy Framework) 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, of 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 cost 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 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.

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. stands for “DomainKeys Identified Mail”. DKIM allows sending email servers to digitally sign the email envelope headers their outgoing email 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 may 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 of DMARC – Domain-based Message Authentication, Reporting and Conformance. 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 fail. Do they reject the message or quarantine it or what? And the DMARC policy can also specify how an email receiver can report back to the sender’s domain about messages that pass and/or fail.

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 passes, which in turn requires SPF and DKIM to be present and to 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? To answer that question let's see what the BIMI group themselves have to say. In their FAQ for this, they write:

Verifying that 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 7 years to develop the specification. [And I should note that since this was written three years ago in 2021, it's now been 10 years.] 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 – 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.*
- *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.*

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 (VMC).

In order to obtain a VMC, 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.

*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 (e.g. relying on their own reputation data about the domain), a VMC moves the trust model from the domain to the VMC issuer.*

In other words, we introduce the classic concept of a certificate authority. We trust the certificate authority so we trust that CA's identify assertions by extension. The FAQ continues:

*At this time, there are two Certificate Authorities (CAs) that are accepted as Mark Verifying Authorities (MVAs) who can issue VMCs for use with BIMI: **DigiCert** and **Entrust**.*

And, yes, it's that Entrust, the Entrust from whom Chrome will no longer trust certificates signed after the end of this month. (And Mozilla, by the way, has made the same decision, ending their new certificate trust of Entrust one month later, after November.) 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, it's essentially the job of the MVA (the 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! Wow!)

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:
https://bimigroup.org/resources/VMC_Guidelines_latest.pdf

If you've gone through the entire 94 pages (congratulations... it's pretty dense [and actually it's now 129 pages]), 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 from that CA (which would essentially neutralize the CA's VMC business).

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. 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 not to be routed to spam or junk folders, then I would regard that as time well invested.

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 for the logo itself to be uploaded. But 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 out we needed to do that with 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??]

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.

That's all entirely reasonable, but it introduces another hurdle. After searching around the Internet the only tool I could find that would export an SVG file in "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 7-day trial, so I installed it, converted my simple GRC "Ruby G" from raster and vector and used an illustrator script I found on DigiCert's BIMI help page to export in fully compliant SVG Tiny-PS format. I then uploaded that to DigiCert, who inspected the file and approved it for BIMI use.

So now what? It turned out that was the easy part. I'll explain that happened next when we come back from our final break...

The last break for the week!

Before a would-be BIMI user even begins the process, it's necessary for the organization to be certified at the EV level. Remember EV's? 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? And also since nothing prevented typo-squatting sites from obtaining their own EV certificates to create the presumption of trustworthiness. Well, 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.

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. What might have once seemed intrusive is now longer any big deal after the National Public Data breach. 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. 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. He had told me that I would need to show the same ID during the video conference, so 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 so that both my face and my ID were on camera side-by-side at the same time. I did that. 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. 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.

And, since this created an unbroken trust chain from GRC's public corporate records, to our offices, to me and my identity, this was able to satisfy their need to confirm the authenticity of our submission. I forgot to mention that earlier in the process, after I had successfully created and uploaded and verified the Tiny v1.2-PS SVG logo file, DigiCert's website had required me to post a specific TXT string in GRC's DNS and click "Okay" once I had so that I could prove ownership of 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 since, I figured this final step would be a slam dunk.

So how do you imagine they verify my long standing use of this logo? They use the famous "Wayback Machine" at The Internet Archive over at Archive.org. 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. And as a

consequence of that, the final step in the long process of obtaining a BIMBI certificate has been placed on hold. 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. All of the required steps have been taken at my end, so once DigiCert is able to look back in time at GRC's historic use of that logo we should be in business.

But this attack on the Internet's Archive is a concern. While I was assembling these show notes Monday evening I checked-in with the Internet Archive and found that the The Wayback Machine portion was provisionally back online in a read-only mode but that their other services were still temporarily down. But then this morning when I checked again connections were timing out, which is the symptom of an ongoing DDoS attack or a resource shortage for some reason. It could also be administrative. But in any event, the world still doesn't have access to the Internet's history.

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 and a breach which leaked usernames, email addresses and salted-hashed passwords. 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 that Brewster Kahle (/keɪl/ KAYL) 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. Archive.org has a mastodon instance and Brewster has posted two updates there:



Brewster Kahle @brewster_kahle

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.

73 595 3.4K 378K



Brewster Kahle @brewster_kahle

Sorry, but DDOS folks are back and knocked archive.org and openlibrary.org offline.

[@internetarchive](https://twitter.com/internetarchive) is being cautious and prioritizing keeping data safe at the expense of service availability.

Will share more as we know it.

13 73 285 10K

Checking in this Tuesday morning, I see a raft of articles about this event. Headlines read:

BleepingComputer: *"Internet Archive hacked, data breach impacts 31 million users"*

Forbes: *"Internet History Hacked, Wayback Machine Down—31 Million Passwords Stolen"*

The Verge: *"The Internet Archive is still down but will return in 'days, not weeks'"*

CyberNews: *"Internet Archive down after two day DDoS attack, user info compromised."*

Fast Company: *"The Internet Archive is back online after a cyberattack"*

I've observed some of the Internet dialog surrounding this event and this interruption in the availability of the Internet's Archive 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" 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 the 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 made possible because the Wayback Machine had been quietly, dutifully and continuously taking and storing snapshots of the polyfill.io site – along with every other site on the Internet – throughout its entire life.

The Verge's most recent reporting on this 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 also 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."

While you can access the Wayback Machine to search 916 billion web pages that have been archived over time, you can't 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 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 pages 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.

I don't know if an organization like Cloudflare might be interested in being a benefactor here, nor what Brewster's requirements would be, or if it's even feasible. But the Internet Archive is a vital tool for many researchers, academics and others and I suspect that its value and importance will only increase with time.

In any event, it now appears that the Wayback Machine is limping back online and that before much longer 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, and I'm fine with that. So they'll provide the URLs for each and I add a TXT record to GRC's DNS which contains those two URLs.

Then whenever a BIMI-supporting email provider receives email from GRC, in addition to verifying its authenticity by pulling GRC's SPF, DKIM and DMARC DNS records, they'll proactively check for and pull GRC's BIMI record. That will tell them where to obtain the "Ruby G" logo and also where to find its validation 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 must contain 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-embellished mailboxes could lookup 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.

For GRC, that didn't happen for this week's podcast mailing to Security Now! subscribers. But having jumped 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.

Upon learning that Gmail had adopted BIMI support some time ago, I went poking around in my own Gmail inbox. Though I didn't dig too deeply, I saw that PayPal and Disney+ both had BIMI logos for their email. So BIMI logo usage is around but they're certainly not yet common. Will they become more common over time? It's too soon to tell.

Since email providers have total freedom to decide which CA's Verified Mark Certificates they wish to support, and having seen the costly rigor DigiCert applies 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 identification for the email – if anyone notices or understands. At this point I'm pretty certain that most users have no idea what's going on – I certainly didn't until I dug into it. But if this catches on it might begin to chip away at some of the catastrophe that completely free email creation and delivery has created.

