The 50 Gigabyte Privacy Bomb

Description: Why is Google's AI Overview fundamentally impossible today? And what's the latest news on how to suppress it? What's LastPass's decade-late announcement? Why and when is a VPN not a VPN? Are eMMC chips really impossible to replace? Are vertical tabs finally coming to Firefox? What's one well-informed listener think about Fritz!Box network appliances? And what's just about the worst thing that could be done with four-digit PINs? Were we guilty of WinXP abuse by exposing it to today's Internet? And how can Security Now! listeners now send email directly to me? Yes! GRC's new email system is alive. After looking at all of that, we're going to examine the latest crazy idea from Microsoft which deliberately plants a 50 Gigabyte Privacy Bomb right in the middle of all Windows 11 PCs.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-976.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-976-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We have lots to talk about. He's going to give you his take on Windows 11 new Recall feature. That's the 50 Gigabyte Privacy Bomb you've heard about. Also, when is a VPN not a VPN? Can you really replace surface-mount chips? Are vertical tabs finally coming to Firefox? And a new way to contact Steve directly. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 976, recorded Tuesday, May 28th, 2024: The 50 Gigabyte Privacy Bomb.

It's time for Security Now!, yay. We wait all week for this; don't we, kids? And here he is, appearing magically like a wizard in a puffy of greasy smoke - what are you sucking your thumb for? Steve Gibson of GRC.com. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be with you again.

Leo: I called them kids, not you.

Steve: As I knew who you were talking about. We are beyond, you know, we're discussing things that happen when you're no longer a kid.

Leo: Mm-hmm.

Steve: Which they didn't really tell you about when you were kids.

Leo: No.

Steve: It's like, ah, you old people, that's never going to happen to me.

Leo: Well, we were talking on MacBreak Weekly about tinnitus, ringing in your ears. Do you have that?

Steve: No.

Leo: No. You were smart.

Steve: I have - I said "no" too quickly. Like right now, if I concentrate, I can hear probably that 9 kHz very faintly in the background.

Leo: Faint, okay. That's not bad, yeah.

Steve: Yeah, so it's not bad.

Leo: I hear it. It's very predominant, very persistent. So reason to talk about it, and I'll mention it on this show, too, I'm sure, is I'm doing this new FDA-approved process that uses electrodes on your tongue while you're listening to something, I'm not sure what, in your ears. I'm going to get fitted for that a week from Thursday. I'll let you know.

Steve: Yes, on your tongue it feels like pop rocks, kind of fizzy.

Leo: Kind of, yeah, that's what people report, little tickling. Yeah. I can take that. And they tune it. They can say, they told me, they say if it's really bothering you we can turn it down. All right. But I want all the pop rocks, personally.

Steve: Well, you want to get the full dose treatment, whatever it's going to do, that's right.

Leo: Geez, it's driving me crazy at this point. I really need to.

Steve: Be really cool to see if it helps.

Leo: Yes, I hope so. Anyway, what's on...

Steve: Eighty percent of people got helped by it.

Leo: Yeah, well, that's why I'm doing it. I mean, it's not cheap. But I thought, if 80%, if it works for 80%, maybe I should try it, yeah.

Steve: Yeah.

Leo: Watch, I'll be in the one in five it doesn't.

Steve: Okay. So we are closing in on 999.

Leo: Yay.

Steve: And the good news is, that's not bad news. So...

Leo: Bad news for you. Good news for the rest of us; right? You have to keep working.

Steve: We've got another great fun episode here. Today's episode is titled "The 50 Gigabyte Privacy Bomb," which we will be discussing at length. But we're first going to talk about why Google's AI Overview is fundamentally impossible for them to do today. And we're going to look at the latest news on how to suppress it. As you would expect, you know, lots of people are coming up with various ideas. And there are some cool solutions. Also, I just thought I would bring up the fact that LastPass has announced something that is, yeah, maybe 10 years too late. So thanks. And also, why and when is a VPN not a VPN? Are eMMC chips really impossible to replace, as I kind of offhandedly said last week? We have a listener who takes issue with that. Are vertical tabs finally coming to Firefox? Everyone wants them. No one seems to be able to get them, at least not natively.

Also, what does one well-informed listener think about the FRITZ!Box network appliance which came up last week? What is the worst thing that could be done with four-digit PINs? We have a listener who explains his firsthand experience with that. And were we guilty of Windows XP abuse by exposing it to today's Internet? Apparently someone feels we should have been a little kinder and gentler. Also, yes, how can Security Now! listeners now send email directly to me? GRC's new email system is alive. And after looking at all of that, we're going to examine the latest crazy idea from Microsoft which deliberately plants 50GB of privacy bomb right in the middle of all Windows 11 PCs.

Leo: Yeah, mm-hmm.

Steve: Where we'll be marching out our often-used, sometimes overused, "What could possible go wrong?"

Leo: So you're saying we're not talking Little Boy, we're talking Fat Man on this one.

Steve: We're talking could we have done anything that more delights Chinese attackers?

Leo: Oh, great. Oh, good. Oh, that's exciting. All right. We'll get to all that and the world-famous Picture of the Week.

Steve: Picture of the Week.

Leo: Actually, I'm glad you chose the one you chose because there are far worse ones.

Steve: Yeah, we're not doing cockroaches.

Leo: Don't do cockroaches.

Steve: I'm not doing the cockroaches one.

Leo: Okay, good, all right.

Steve: No.

Leo: All right. All right. We'll talk about that in just a little bit. First, though, oy oy oy. Picture of the Week time.

Steve: So, yes. I gave this snapshot of Google's brilliant AI Overview the caption: "Don't you just hate it when the cheese slides off the pizza?"

Leo: Apparently some people do.

Steve: That's a real problem, you know, Leo.

Leo: Yeah.

Steve: On the space station, you know. Fortunately, Google AI Overview has the obvious answer. And again, it's, you know, why, you know, of course this is what it would suggest. So the question that prompted this was "Cheese not sticking to pizza." AI Overview jumps in and says: "Cheese can slide off pizza for a number of reasons, including too much sauce, too much cheese, or thickened sauce. Here are some things you can try: Mix in sauce. Mixing cheese into the sauce helps add moisture to the cheese and dry out the sauce. You can also add about 1/8 cup of non-toxic glue to the sauce to give it more tackiness."

Leo: Mmm, yum-yum.

Steve: Oh, that's right. Yes. And it's not, like, some. It was like last week we had two quarts of urine. You were supposed - not to drink urine, but how much you should be consuming. And here, you know, you do not - Leo, you don't want to overdo the glue.

Leo: Nn-nnn, never.

Steve: So it's only 1/8 of a cup.

Leo: You actually could do this with non-toxic Elmer's Glue or something like that. You could do it.

Steve: Absolutely.

Leo: Not sure I would recommend it.

Steve: You know, kindergartners are eating that stuff, so what the heck.

Leo: Yeah, sure.

Steve: Okay. So it turns out that this latest AI hallucination is based upon an eight-year-old Reddit posting, which was posted as a joke on Reddit. And of course all of the other humans there knew that it was a joke and thought that was kind of funny. The guy wrote: "To get the cheese to stick, I recommend mixing about 1/8 cup of Elmer's glue in with the sauce. It'll give the source a little extra tackiness, and your cheese-sliding issue will go away. It'll also add a little unique flavor. I like Elmer's school glue, but any glue will work as long as it's non-toxic."

Now, of course, Google's bot came along and scraped that up and thought, hey.

Leo: Didn't know any better, yeah.

Steve: There's an idea.

Leo: Yeah.

Steve: Let's hold onto that until some asks why their cheese is not adhering to the bread. In which case we'll give them a little handy help there. Okay. So, okay. We're having some fun at Google's expense. But this seems like a large can of worms which Google's new AI Overview would probably tell you to eat. NBC News picked up on this trouble and offered some additional depth that I want to share since it's really not that funny. Their headline under "Artificial Intelligence" was: "Glue on pizza? Two-footed elephants? Google's AI faces social media mockery." And then they said, as their subhead: "A Google spokesperson said the company believes users are posting responses to uncommon questions on social media."

Okay. So NBC said: "Social media has been buzzing with examples of Google's new, 'experimental'" - and they have that in air quotes - "artificial intelligence tool going awry. The feature, which writes an AI Overview response to user queries based on sources pulled from around the web, has been placed at the top of some search results. But repeatedly, social media posts show that the tool is delivering wrong or misleading results. An NBC News review of answers provided by the tool showed that it sometimes displays false information in response to simple queries.

"NBC News was easily able to reproduce several results highlighted in viral posts online, and found other original examples in which Google's AI tool provided incorrect information. For example, an NBC News search for 'How many feet does an elephant have' resulted in a Google AI Overview answer that said 'Elephants have two feet, with five toes on the front feet and four on the back feet.'"

Leo: Oh, my god.

Steve: "Some of the false answers verged into politically incorrect territory. An NBC News search for 'How many Muslim presidents in the U.S.,' the results of which were first posted on social media, returned a Google AI Overview that said 'Barack Hussein Obama is considered the first Muslim president of the United States.'"

Leo: What?

Steve: "Obama, however, is a Christian."

Leo: Oh, yeah.

Steve: "Google said this Overview example violated its policies and that it would be 'taking action.'" I know what action they should take, Leo, and it's not the one they're going to take, apparently.

"A Google spokesperson said in a statement" - okay, so this is Google. "The examples we've seen are generally very uncommon queries, and are not representative of most people's experience using Search. The vast majority of AI Overviews provide high-quality information, with links to dig deeper on the web. We conducted extensive testing" - you know, we spared no expense. "We conducted extensive testing before launching this new experience to ensure AI Overviews meet our high bar for quality. Where there have been violations of our policies, we've taken action; and we're also using these isolated examples as we continue to refine our systems overall."

NBC writes: "It's difficult to assess how often false answers are being served to users. The responses are constantly shifting, and on social media it's difficult to tell what is real or fake. Some Google users have created workarounds to avoid the new AI Overview feature altogether. Ernie Smith, a writer and journalist, quickly built a website that reroutes Google searches through its historical Web results function, which avoids the AI Overview or other information boxes that prioritize some results over others. Adding 'udm=14' to Google search URLs strips the new feature from results. Smith told NBC News that his new website has quickly gained traction on social media, surpassing the traffic of his entire decade-old blog in just one day. Smith said in a phone interview: 'I think people are generally frustrated with the experience of Google right now. In general, the average person doesn't feel like they have a lot of agency.'

"A Google spokesperson said the company believes users are deliberately attempting to trip up the technology with uncommon questions. Some deeper dives into why the answers have gone awry suggest that the tool is pulling from surprising sources. 404 Media reported that a Google search query for" - and here it is - "cheese not sticking to pizza pulled an 11-year-old Reddit comment that jokingly suggested mixing Elmer's Glue into the sauce. Even though Google has now removed the AI suggestion from searches for 'cheese not sticking to pizza,' according to an NBC News search, the top result is still the Reddit post, with the comment about Elmer's Glue highlighted.

"A Google spokesperson quoted that queries like 'cheese not sticking to pizza' are not searched very often, and are only being noticed because of the viral posts about wrong answers on social media platforms like X, of which there are many. The same issue with an old Reddit comment also occurred in a search for 'how to rotate text in ms paint,' referring to the Microsoft Paint application. The top Google search result, viewed by NBC News, directs the reader to a sarcastic Reddit comment that says to press the 'Flubblegorp' key on your keyboard." They note: "This key does not exist. This example was originally posted on social media.

"Despite Google's assertion that the tool is working well for many users, mistakes of the AI Overview are continuing to gain visibility and hype. Some of the answers that have been posted online seem to be fake, indicating that the trend has shifted from authentic errors to a new meme format."

Okay. So a couple of comments. First is, I think it's clear that it's wise to be extremely skeptical now about anything we see online in general these days, and not only Google AI Overview results that we receive, you know, but just as much any reports of bizarre and wonderfully wrong results. Every time I've encountered one of these reports like I've been sharing, I've immediately worked to verify its authenticity as much as I can since there's clearly some strong motivation to invent non-existent high-profile, you know, funny failures. But, you know, here's NBC News, who themselves searched for how many feet does an elephant have and was told "two."

My other observation is that I hope Google truly understands that there are two fundamental reasons why they're getting into trouble with AI Overview. The first reason is how powerful and potent this would be if it were possible. It would be truly amazing. But that's coupled with the second reason, which is that what they are attempting to do is not even remotely possible - not yet, not today, not even close.

You know, I make no claims to being an AI expert. But we've all been paying attention, and our intelligence is not artificial. We know that the current level of AI development definitely falls short of comprehension. These large language models, exactly as their name suggests, are capable of mimicking the output of an intelligent species whose actual intelligent output was used to train them. But as we're finding out, there's a world of difference between seeming and sounding intelligent, and actually being intelligent.

So here's the problem. Google is attempting to use automation to create an accurate factual summary overview of what the web contains without understanding the content that it's summarizing. It should be clear to everyone that this can never work. It is not possible to create an accurate summary of content for which there is no comprehension. AI Overview doesn't "know" that glue should not be mixed with tomato sauce because AI Overview doesn't actually "know" anything at all. Yet to do the job Google has given it, it must comprehend the content that it's accessing.

What Google appears to have completely missed here is somewhat astonishing, I think. You know, it's that the job of displaying pages of links resulting from keyword matches is entirely different from attempting to extract truth and knowledge from the content behind those links. Keyword matching and link ranking they know how to do. Truth and

knowledge extraction no one knows how to do. Not yet. Not today. But unfortunately, that has not stopped Google, and it should have.

Okay. And this brings us to the perfectly named website udm14.com, which our prolific Twitter poster, Simon Zerafa, tweeted to me. Thank you, Simon. Recall that when the string "udm=14" is included, you know, appended to a Google search query, it serves as a shorthand, asking Google to return its search results in what they term "web search mode." Among many other things, their AI Overview system is not consulted in that case. From that page at udm14.com I discovered another site named TenBlueLinks.org. And of course 10 blue links is reminiscent of what Google was, you know, decades ago, back when I first discovered it and sent that second email from GRC's first email system out back then, when no one had ever heard of Google. Ten blue links was what you got on the page.

So TenBlueLinks.org, which, with just a few clicks of the mouse, allowed me to instantly and as permanently as I want switch my default Google search to "Google Web" mode search in Firefox. For example, for Firefox on Windows or MacOS the instructions are just, you visit TenBlueLinks.org. Then you right-click in the address bar, and you get a dropdown menu which is enhanced by this site. At the bottom it says "Add Google Web." So you click on that. Then you open the hamburger menu in the top right corner, choose "Settings," and then click on "Search" on the left. And then in the "Default Search Engine" you will now have a new entry, "Google Web," which you then select, and you're done. Now Firefox will use, by default, until you change it, this Google Web mode search for all your browser searches.

You know, and when I first read the instructions I thought, what? But sure enough. You just go to this website, and it adds this cool option in the dropdown menu from right-clicking in the address bar, the URL field, and then allows you to make it your default. They've got instructions for Chrome on Android, Chrome on iOS, Chrome on Windows or Mac, and Firefox on Windows and MacOS. So anyway, again, I commend our listeners: TenBlueLinks.org. It's a very cool site.

Leo: You don't actually get the Overview on your Google search; do you?

Steve: Actually, I don't think I've ever seen one yet.

Leo: Yeah. So that's - what happened was, as part of Google's Experimental Labs, you could turn it on there. And then briefly they made it default. And that's when they got in all the trouble. It's turned off now, I believe.

Steve: Oh, no kidding.

Leo: I see it's still in Labs. Yeah, I don't think anybody's actually getting it anymore.

Steve: So they backed out.

Leo: Oh, almost immediately.

Steve: Of the full...

Leo: Yeah, yeah. They said, oh, whoops. But Google keeps doing that. It's amazing. I don't know why. It's amazing. It just keeps happening to them. But I don't think anybody's getting that now, unless you turn it on specifically.

Steve: Interesting. So...

Leo: I don't know if udm14 is different than that. I think it is. Because then I think you also don't get the knowledge graph...

Steve: Correct.

Leo: ...and the suggested links and all that stuff. So it's still worth doing that, yeah.

Steve: Correct. And all of the image search stuff and all the other junk, yeah. Yeah, well, yeah. So the udm14, which is to say invoking the Google Web mode search one way or the other, it definitely cleans that up and suppresses all that.

Leo: Yeah, yeah. I stopped using Google Search a year ago so none of this affected me. But I use Kagi. I pay for it because I don't want ads. And I think it's compromising. It's terrible.

Steve: Yup. Well, it has compromised Google Search; right?

Leo: Really.

Steve: I mean, it's completely skewed what they return.

Leo: Mm-hmm. Yeah.

Steve: Okay. So a piece in BleepingComputer caught my eye, mostly because of how pathetic the announcement seemed. BleepingComputer's headline was "LastPass is now encrypting URLs in password vaults for better security." To which I respond, gee, what a great idea.

Leo: Finally. Wow.

Steve: BleepingComputer wrote: "LastPass announced it will start encrypting" - maybe not even quite yet, but it will - "start encrypting URLs stored in user vaults for enhanced privacy and protection against data breaches and unauthorized access. The vendor of the popular password manager also notes that this new security feature is a significant step towards reinforcing its commitment to implementing zero-knowledge architecture in the product, so it's not just to protect data from external threats.

"LastPass says that due to restrictions in processing power in 2008, when that system was created, its engineers decided to leave those URLs unencrypted, lessening the strain on CPUs and minimizing the software's energy consumption footprint." That's right. It was good for the planet, everybody. What a crock of you-know-what. But let me finish just another two lines from BleepingComputer's piece. They said: "With most of the hardware performance constraints of the past now having been lifted, LastPass can now start encrypting and decrypting those URL values on the fly without the user noticing any hiccups in browser performance while enjoying ultimate data security. LastPass says this is being done to enhance user security and comply with the company's zero-knowledge architecture." So I don't know where to...

Leo: Everybody else does this; right? I mean, I know Bitwarden does. I think everybody does.

Steve: Everybody. Everybody else. So, you know, okay. It's true that the world was very different back in 2008 when Joe Siegrist designed the original LastPass architecture. And I would believe that since the URLs the user was visiting were needed for on-the-fly matching, and since their privacy - again, back in 2008 - didn't seem like a big issue, Joe would have consciously and deliberately chosen not to keep them encrypted, especially given that everything else in there was. You know, so his not encrypting the URLs at the time was obviously intentional. But that was 16 years ago.

Leo: Yeah.

Steve: Sixteen years ago. And the flow of time really does impact what we would term "best practice" today. Back then, most web sessions were only briefly encrypted during login, after which the connections dropped back to plain old HTTP. And as we know from Firesheep, the now logged-in session cookies were completely exposed to the Internet, allowing those sessions to be impersonated easily. That would no longer be considered "best practice" today, and no one does that anymore. So as times change, what's considered reasonable changes along with it.

But computers have been plenty powerful for the past decade at least to handle on-the-fly URL decryption without introducing any discernible pause or overhead. Back when we were talking about this, I noted that it would have been possible to keep the user's vault encrypted on disk and only decrypt it in RAM. That was the decryption event that would have been one time only during browser launch, when the extension was coming to life. It would have decrypted the on-disk storage into RAM, where it could then access it easily on the fly. But what was actually stored in the computer and was available potentially to be stolen would have been kept fully encrypted. So there have been ways to offer vault encryption at rest, without any problem, for a long time.

I suspect that the real problem is - and we talked about this at the time. LastPass's parent, LogMeIn, was purchased by a purely financial private equity firm back in 2019 for, what, four point some billion dollars. I mean, a ton of money. And that new parent did not love it for anything more than the cash flow it could produce. In any event, for anyone who may still be lingering with LastPass, I just wanted to note that, for what it's worth, your vault-stored URLs on your machine will now finally be encrypted at rest. So good on you. And Leo, let's take a break.

Leo: Good on you, yes.

Steve: I'm going to share a piece of feedback that will lead on to our next bit of news.

Leo: All right. I don't think we're ever going to get any data brokers advertising on this show. I'm just guessing. I'm just guessing. All right.

Steve: Yeah, that would be a difficult...

Leo: I wouldn't do it. I wouldn't do it.

Steve: So I'm going to take one piece of listener feedback out of sequence, ahead of the pack, because of the P.S. that Andrew included, which I'll get to in a second. So this is from Andrew Gottschling, who said: "Hey, Steve. I wanted to provide some feedback to Hakku's comment on VPNs and Firewalls. It's probably not an option for many, if not most, corporate users. This is because many corporations these days, and all of the ones I've worked for thus far, utilize 'split tunneling' on their VPNs to reduce bandwidth usage for high bitrate communications that are common, for example, voice and video calling on Teams or Slack. Therefore, simply blocking all traffic from leaving on anything other than the VPN interface, unless it's to the VPN concentrator, would not be feasible in these cases, especially in the case of something like Slack, which runs in AWS, and their IP range is very dynamic. Love the show. Thanks for all you do. Andrew."

So Andrew's exactly right, and this could be a problem with any VPN that insists upon forcing all of the system's traffic through its tunnel, and its tunnel alone. The problem we're running into sort of more broadly is that we're tending to use the term "VPN" generically. Like there's only one sort of VPN, you know, a VPN only does one thing, as if they're all created equal. But that's not the case.

For example, the VPN that a typical roaming consumer in an Internet-equipped caf, airport, or hotel might want installed on their laptop would be a VPN that proactively refuses to allow any packet traffic in or out of that machine that does not travel through its tunnel. What such a consumer will want is full protection. This is contrasted against, for example, an IT-managed enterprise setting where a great deal of attention has been paid to exactly which traffic flows where.

For example, headquarters might have several satellite offices located elsewhere in the world which need to participate on the same corporate network, as if they were, you know, attached. And since that traffic cannot safely be exposed to the Internet, static VPN tunnels would be established to securely interlink the satellite offices no matter where they were. In this case, only the traffic that's bound for network addresses at the other end of a VPN tunnel would be routed there, with all the other local traffic allowed to have contact with the Internet directly.

So, you know, these are all just differing applications for private virtual networks where, you know, that's sort of a generic umbrella term. The common factor is that traffic is being encrypted and decrypted as it flows between one or more local and remote IP addresses. And part of what's so cool about VPNs is that they are, you know, V stands for Virtual. They really are a virtualizing technology that is very flexible and very powerful.

Now, as I said, I chose Andrew's note because it arrived, Leo, via email, addressed to "securitynow@grc.com." And Andrew ended his note with a P.S., which read: "P.S.: This new email system is REAL [all caps] slick. Glad to get rid of Twitter."

Leo: You have set something up, haven't you.

Steve: What email system, you ask? Well, since you asked, it's GRC's new email system.

Leo: Ah, excellent.

Steve: I finally have the long-awaited email announcement for GRC which features for this podcast a simple means for our listeners to send feedback and thoughts to me through spam-proofed email. As I mentioned last week, GRC's been without any form of subscription email news system since I shut down the first system, which I wrote 25 years ago, back in 1999.

The completion of SpinRite v6.1 created my need to announce it to 20 years' worth of SpinRite 6 owners, and it would be nice to be able to send news of new things I create to those who would like to know of them. For example, I do have plans to revisit ValiDrive, which has turned out to be extremely popular. I've got a list of things I want to do for ValiDrive 2.0 that'll just be a little quickie update, but very useful. And of course GRC's DNS Benchmark, which continues to be the most popular download we have, could use a bit of attention as DNS servers come and go. So that's on the side of sending email out. What about receiving feedback from our listeners?

Just yesterday, I received a very useful DM tweet from someone who said he created a Twitter account just so he could send me that tweet. And as we know, many of our listeners have had to do so. On the one hand, I'm deeply honored that our listeners are as interested in engaging as so many are. I'm blown away by that. But on the other hand, I'm horrified that the bar has been set so high by the need to join any social media service just to send me some thoughts, or a link to something that might be of interest to our listeners, especially when everyone already has email. Email is the obvious common denominator.

Now, before I go on, just for the record, allow me to reiterate one last time, because I know there are still some people who need to hear this: This has absolutely nothing whatsoever to do with Elon Musk's ownership of Twitter. Really. Nothing. I could care less. For one thing, I am barely a Twitter user. When I start working on each week's podcast, I check in with Twitter to collect all of the tweets I've received since my previous check-in the week before. I don't even look at it during the week. I scan through those, replying when I can, and that's been where our listener feedback has mostly come from every week. As everyone knows, I've never followed anyone on Twitter. So I've never used it the way it was intended to be used. As a consequence, I'm not directly aware, you know, of what may have changed after Elon's reluctant purchase of Twitter, other than things I've heard secondhand. So I could care less. I just want to lower the bar for all of our listeners. And everyone has email. The normal downside of asking people to share their email addresses is that the implied trust might be abused. I think everyone knows that will never happen with me.

Until this past weekend I've not had a workable means for receiving incoming email from our listeners. Now I do. GRC now has the subscription management front-end of its new email system up and running. It's what I've been developing for the past few weeks, and of course it's all written in assembler because that's just where I'm most comfortable. It's now possible for anyone who wishes to, to optionally subscribe to any one or more of our three mailing lists. One is aimed at our commercial product owners; one is aimed at general GRC news of products, freeware, services, et cetera; and one is intended for this Security Now! podcast, which has become a significant part of my life through these past 20 years.

But, and this is crucial: You do not need to be subscribed to any of these lists to be able to send email to securitynow@grc.com. There's no requirement for anyone to subscribe, although of course everyone's welcome to if they wish. Here's the requirement: The email address from which you are sending email to me does need to be known to the system. So here's how you register: At the top of every GRC page, in the page's header, is a little white envelope with an "Email Subscriptions" link. There's also a link under the Home menu. And, as you might expect, it's also just grc.com/mail.

So you go to grc.com/mail and enter the email address you wish to register with GRC. GRC will send an email to that address containing a link back to your own subscriptions page here. And as you'd expect, everything defaults to "unsubscribed." I don't ever want to send anyone any email they don't want to receive. But if you wish, you can optionally provide your name and join any of the three lists shown there. Then, either way, click the "Update Subscriptions" button, and your confirmed email will then be known to GRC.

From that point forward you can simply address anything you wish to the email address securitynow@grc.com. No exclamation point or hyphen or anything, just securitynow@grc.com. When that email arrives at GRC's server, the sender's address will be looked up; and if it's known to the system, the email will be accepted and will appear in my SecurityNow account inbox. If email you send to securitynow@grc.com is rejected and bounces back to you as undeliverable, you'll know that something went wrong somewhere.

So that's the front end system. The back end is the part that contains the subscriber database and actually sends email to the lists. I should mention that at this exact moment, due to a limitation that the back end had, this new system is unable to accept email addresses containing plus signs, which I'm sure our listeners would like to use. The back end has been fixed, but I haven't updated my code yet because it just happened yesterday, and I haven't, you know, I've been working on the podcast. So that'll be the first thing I do later today.

And as for the back end, all I have running and tested at this point is the subscription management. So please do not be surprised when you don't immediately start receiving email from me. It's not you, it's me. Since the industry has become so spam-sensitive, I plan to proceed with caution to be very sure that any bulk email I send meets all of today's anti-spam technical and legal requirements, and there are many. So it will likely be another week or two before email begins to flow. While I hope to be able to send weekly podcast summaries and links, the other two lists will always be very, very low volume. I think over the eight-year life of the previous email system, I sent a total of 11 pieces of email. So, you know, no one's going to get spammed. You'll be wondering what's going on. If you weren't listening to the podcast, you would wonder where I went.

But today, the new incoming email system filter is in place. And frankly, I have no idea what will become of my use of Twitter. It's trivial for me to tweet the weekly summary of the podcast, you know, a link to the show notes and the Picture of the Week. My ambition is to deliver the same thing via email, but I'll be doing that somewhat cautiously as we see how it goes. And I should note that I have recently noticed a significant uptick in spam to my, Leo, as you always mention, my Open DM channel. You know, I got one this morning: "Hello. My sister saw your profile while browsing X on my phone, and she's interested in you." And then I have a link: e.yqyh571.xyz.

Leo: Oh, I know them. They're great, yeah.

Steve: Yeah, that's right. "Open the link to complete the registration, and she will take the initiative to call you." And I've got four different emojis. And by the way, the emojis

differ every time I receive this, although the text is always the same. And it says: "Remember to say hello to her. She's very shy." Right. And she's also going to be very lonely in this case. So anyway, if the spam becomes a lot worse, I'll likely be forced to abandon open DMs. So the establishment of this alternative channel is coming at an opportune time. The bottom line is I'm very excited to finally be adding this long-missing piece of GRC's infrastructure. It's been crazy that we've had no means of announcing new stuff. And once the dust settles from that, I'll begin sending out the news of SpinRite 6.1 to all 6.0 owners. So, very pleased.

Okay. So some closing-the-loop feedback. A listener, Hatcher Blair, said: "Hi, Steve and Leo." He described himself as a "medium-time listener" and huge fan of the work we do.

Leo: Medium is good. I'll take medium. I'm happy with medium. That's fine.

Steve: A medium-time listener, exactly. So that's what, he came around maybe 10 years ago, something like that?

Leo: Yeah, something like that.

Steve: Jumped in about halfway along, yeah. So he said: "I hope this is still the appropriate place to contact you as I made a Twitter account just for this." So bless you, Hatcher, in the future you can send email to securitynow@grc.com. Anyway, he said: "I just listened to SN-975, and I wanted to thank you for alerting me to the Web Search option in Google." So again, and I'm glad you pointed this out, Leo, not just to remove AI Overview, but to clean up the pages significantly.

He said: "I wanted to make it my default search option, but you cannot add the search engine to Chrome or edit the Google Search engine in Chrome's settings. However, you can create an extension which adds a Web Search engine and make it the default. I made a simple Chrome extension that makes Web Search the default option when searching from the address bar. This extension is not and cannot be published on the Chrome web store because I use the domain https://google.com and would need to have ownership of that domain to publish the extension. Although it's not on the web store, it is on my GitHub for anyone that wants to clone the repo and install it for themselves.

"A warning to anyone who wants to install the extension." He said: "It is bad." I don't know what he means. He says: "All the extension does is make the default search," you know, and then he shows a search query with the &udm=14. He said: "There is no localization support or option to enable or disable the extension in the UI. If you end up sharing this on the show" - here I am, doing that - "feel free to share the repo, and anyone who wants to contribute is welcome to. Anyone is also welcome to use anything on the repo for their own purposes if wanted.

"I did a little bit of googling, and making a similar extension should be possible in Firefox. It might even be easier as Mozilla seems to have much better documentation than Google. Keep up the great work and looking forward to episodes 999 through infinity," says Hatcher Blair. So I've got a link to his GitHub repo in the show notes. And just another piece of work along the lines of the TenBlueLinks.org that we talked about earlier, you know, this one from one of our listeners. And as I said, I'm sure this will be very popular moving forward.

Defensive Computing's Michael Horowitz wrote to say: "Steve, a fun story. I recently got a fairly standard scam email message claiming my computer had been hacked and asking

for Bitcoin. As proof of the hack, the bad guy told me my password. But I use a different password everywhere. Have for years and years. So the revealed password told me the service that had been hacked, and I logged onto it and changed that one password. It had a stored credit card, but fortunately that had expired." He says: "It's rare to actually experience, firsthand, up close and personal, the benefit of never re-using a password."

So thanks for sharing, Michael. I think that's very cool. As I've been perusing the email domains of our listeners who have been subscribing to GRC's new service since I announced the email system on Twitter yesterday, I've seen many gmail.com email domains; but also, as indicative of the listeners we have, many personal domains. As we've discussed, unfortunately, there's no good way to hide from tracking when websites are willing to trade their visitors' privacy for cash by colluding with advertisers and other data aggregators. Not even a personal domain will help with that. But it can be very useful for tracking down personal information leakage.

I established a unique email address for the dealership that services my car. So when I started receiving unwanted spam from some auto-related source, from that one email address that I had never shared with anybody else, I knew who had leaked it. So, yeah. Even though it won't help for tracking, it is a little bit satisfying just to be able to say, uh-huh, I got you. And of course I'm then able to retire that email address if the spam becomes annoying. And when they wonder why they're unable, when the dealership can't send me email, I say, oh, yeah, I changed that because you guys sold my address to a third-party commercial entity. So here's the new one. And I imagine, Leo, that you at Leoville.com...

Leo: Oh, it's unusable, yeah.

Steve: Oh, yeah, Leo is unusable. So imagine...

Leo: Well, also, oh, no, I don't even use that. I mean, I do, but I don't. I have lots of solutions around this.

Steve: Right.

Leo: Similar to yours, but not.

Steve: Right.

Leo: You have to. I have many addresses. I can't use laporte@gmail anymore. That really went downhill fast. But no, what I do now when I sign up for something is I use - I actually don't use those unique passwords, unique email addresses that Bitwarden and Fastmail do. I just make it the name of the company at a particular address that I haven't used before, you know, that I use exclusively for that.

Steve: And you have a catchall so that everything comes in?

Leo: Yeah, right. I don't have to worry about that in Fastmail. I have about 10 domains or 15 domains that get email at Fastmail. It all goes in the same inbox. And

then I can do sorting based on the address it thinks it's going to and stuff like that. It's, look, spam is a mess. It's just a mess out there.

Steve: Oh, Leo.

Leo: It's terrible.

Steve: Yeah. Well, and as somebody facing the task of sending subscription email, you know, I mean, I'm...

Leo: Well, yeah, yeah. That's the biggest issue. It's not that we're getting a lot of spam. It's just really hard to send email out now. Google will not accept email if it doesn't have DKIM, SPF, and DMARC authentication. They just won't even accept it. So it's gotten really - that's where it's really, it's much harder. Deliverability has gone downhill.

Steve: Yes, yes. And in fact in my instructions, as does everyone, I say, if you don't receive the confirmation email, you know, look around for it. You know, check your spam folder or wherever it might have gone.

Leo: Yeah, that's a must also, yeah.

Steve: Yeah.

Leo: I think Google loves this because it means that eventually they hope everyone in the world will use Gmail. And that'll solve it. Sort of.

Steve: Oh, you mean from Gmail to Gmail.

Leo: Yes.

Steve: Wonderful.

Leo: That solves it. You know, as long as everybody's using Gmail, we can get rid of spam. We can authenticate. It's just it's our fault for not using Gmail. That's Google's attitude.

Steve: Right. That's right.

Leo: That's Google's attitude.

Steve: So Elliot.Alderson tweeted: "Hey, Steve. One extra way to avoid Google's AI Search." He says: "Don't sign in." He says: "I've never seen any of that AI nonsense. I have a different browser profile for signing into Google, and I clear it whenever I'm done with whatever Google account management I need to do."

Huh. Okay. So I can't speak to that myself. I don't do Google account management. And like you, Leo, I've never run across that. And now we learn from you that it's gone.

Leo: You won't. Yeah, it's gone. You won't anymore. It's still crappy search, but at least you won't see an AI Overview.

Steve: Yes, exactly, telling you to eat glue. Steve Murray said: "Steve, just FYI, you can replace soldered motherboard components like eMMC/RAM." He says: "A ton of YouTube videos cover it." He says: "The hard part is doing it in an economically viable way if not doing it DIY." Okay. Now, I would argue...

Leo: Just because it's on YouTube doesn't mean it's possible.

Steve: I would argue that, right, that the hard part is doing it at all. I've been soldering electronics, literally, I'm not kidding, since I was four years old. I still recall my dad's big honking soldering iron. It was about 3/4 of an inch in diameter and 18 inches long, with a wooden handle. It was nothing like what we have today. This thing took about 30 minutes to come up to temperature, at which point you could push its tip through a solid steel plate. And while growing up, my standard Christmas present was a Heathkit, which I would receive every Christmas Eve.

Leo: Aww. That's so cool. Aww.

Steve: I would open it on Christmas Eve, and it would be fully assembled by Christmas morning...

Leo: That's so cool.

Steve: Since I had no interest in sleeping with an unfinished kit in front of me.

Leo: No wonder you're a geek. Now I get it.

Steve: Oh, and I remember, Leo, the VTVM, the Vacuum Tube Volt Meter that I built, I must have, let's see, I was still living on Overhill in Orinda, and I left Sleepy Hollow Elementary in the middle of the fifth grade. So I was, what, eight, I guess?

Leo: Wow. Wow.

Steve: And Dad - one Christmas was a shortwave radio receiver.

Leo: Holy cow.

Steve: One Christmas was, you know, all Heathkits.

Leo: Was he an engineer? Is that why he really encouraged this?

Steve: Yeah, he was - he had his masters in engineering from Berkeley. But mechanical engineering, not electrical engineering. But there's a lot of overlap.

Leo: Right. Sure.

Steve: And, you know, he set me up with a battery and knife switches and light bulbs because I just had to understand how all this stuff worked.

Leo: That's so great.

Steve: Anyway, so, while, yes, technically I agree that it's possible to remove and replace today's modern high-density surface mount components, doing so - because I have - is neither fun nor easy.

Leo: And it's really easy to screw up the substrate, the motherboard; right?

Steve: Oh, so easy.

Leo: Yeah.

Steve: Especially when they're surrounded on all four sides with a forest of tiny pins on half-mil centers, or when it's a BGA, which is a ball grid array chip, with its myriad connections underneath the chip itself. I'm sure anybody who's looked at a modern motherboard or circuit board, you see this chip sitting there with no obvious connections to it.

Leo: Right, right.

Steve: It's because they're little dimples on the underside of the chip. You've got to heat the whole thing up in order to melt the solder of them all at once in order to pull this thing off the circuit board. Anyway, the reason there are a ton of YouTube videos is that it's actually not possible to do.

Leo: It makes for an excellent YouTube video.

Steve: It'll hold you on the edge of your chair. Is it going to come off? Is it going to come off?

Leo: You know, just because you see somebody doing it on YouTube does not mean you can do it, or anyone normal or even that they...

Steve: Yes. Hank is able to show me how to create a recipe which I am unable to reproduce.

Leo: Yeah, exactly, yeah.

Steve: So the fact that Hank is able to do it does not mean that I can.

Leo: My son, yes. No, I watch with wonder myself.

Steve: Sylvester said: "Replying to @firefox," he said, "@SGgrc Vertical tabs are coming!" So his tweet sent me off looking, and I found a posting by Martin Brinkmann over at gHacks.net. Martin wrote: "Mozilla released a Firefox Nightly test build recently that includes support natively for vertical tabs. This new functionality is not available in regular Firefox Nightly builds, but there is a way to get that build and test it for yourself. Native vertical tabs support is a highly requested feature. It is placed third currently on Mozilla's Connect website, just behind native tab grouping, and the restoration of Progressive Web App support in Firefox.

"Vertical tabs," he says, "move tabs from a horizontal bar at the top of the browser to the side. It enables better drag and drop support, sorting, hierarchical views, and better use of space on widescreen monitors or sites that limit their width. Firefox would not be the first browser to support vertical tabs. Several browsers, including Microsoft Edge, Brave, or Vivaldi, support vertical tabs already," and he says, "with Vivaldi taking the cake when it comes to customization options. There has always been talk of introducing vertical tabs in Firefox. The last time was in February of 2022, when Mozilla looked into the matter."

Okay. So I don't understand this. Vertical tabs are such an obvious improvement for modern web browsing that it is difficult for me to understand what's taken so long. Fortunately, I've had vertical tabs in Firefox thanks to the browser's sidebar that can be used to contain browser tabs. I use the add-on Tree Style Tabs, which works wonderfully. And then I tweaked the browser's UI, the CSS style sheet, to hide the tabs across the top, which are still there. So although I've found a solution to place tabs to the side, where they should have been immediately moved once our screens moved away from their original 4:3 aspect ratio, it will be wonderful for Firefox to offer them natively. So let's hope that happens because, like, what's the problem? It's just so obvious.

Leo: You raise an excellent point. We have wide, wide screens. There's lots of room.

Steve: Yes.

Leo: On the left. I hadn't really thought about it that way. Yeah.

Steve: Yes, exactly. And many sites, in fact, my site looks weird because it sets the width to 85% of the browser window, which on today's browsers is wrong. So as I'm rewriting pages, I'm changing the way that works. As a consequence, there's a lot of empty space on the sides. So anyway.

Leo: Yeah, yeah. I put my dock on the left for that reason on my Mac, yeah.

Steve: Right. And we're an hour in, Leo. Let's take our third break.

Leo: Let's go to work. Let me do some work while you relax. It's my turn.

Steve: I've got coffee.

Leo: The world's largest mug of coffee. Hey, you're going to like - whoa. Steve?

Steve: So Tal in Israel, he said: "Back at Episode 970 you read a listener's feedback about a SOHO router that requires you to press a button on the router in order for configuration changes to be applied." We've talked about this is now recommended behavior for future routers, in order to minimize the ability of attackers to do a purely electronic, non-present change of configurations. Anyway, he said, speaking of the listener feedback, said that "A well-known router manufacturer named FRITZ!Box has been creating such routers, where configuration changes require the press of a button on the router.

"I've been looking for a new router, as my old Xiaomi router stopped receiving updates in 2021. Xiaomi is notoriously known for not providing many updates to devices after they've been sold. Also, that router was always underpowered, dropping WiFi connections and being generally unable to handle my needs. I remembered the name FRITZ!Box, looking around a little, and it seems the company who manufactures them is very security-aware, and the performance of them is very good. I was happy to discover an Israeli seller, and bought the FRITZ!Box 5530, which seems to be what is most suitable for me.

"After I've been using it, I think it's the best router I've ever had. It does not even break a sweat with multiple video streaming and downloading and anything else I do. And I think it can serve as an example of how SoHo routers should be. First, it comes with automatic updates turned on by default. Second, both wireless key and router admin passwords are randomized when you get one. And if you reset it to factory default, those passwords will be reverted back. There's a very durable sticker on the bottom of the router with them so you should not worry about losing them.

"Changing some configurations like DNS will require you to go and press a button on the router. But since it can also serve as a telephony hub, if you have a phone directly connected to it you can pick it up and dial some number it tells you to dial in order to apply the configurations. Or you can define an authenticator app and then use the six-digit token to apply changes. Other nice things it supports" - oh, by the way, that's a cool feature, right, because now you've got a way where you don't have to physically be present, but you do have another authentication token that is changing dynamically to prevent someone from making changes electronically. That's something we hadn't talked about. That's brilliant.

And he says: "Fourth, other nice things it supports is DNS over TLS so your ISP will know nothing of your DNS queries." And he says: "I use both Google and Cloudflare OpenDNS resolvers, which I trust way more than my ISP provider. And finally, fifth, FRITZ!Box is well known for supporting their devices for a long time." He finishes: "It has many other features where you can definitely see that security awareness went into the design. So whoever mentions FRITZ!Box in Episode 970, thank you. Unfortunately," he said, "I could not find your name in the transcripts."

Well, okay. Since this is all about listener feedback, I wanted to keep this thread alive by sharing this listener's very positive experience with FRITZ!Box. I brought up a site web search of GRC some time ago, so I went to GRC and put "FRITZ!Box" into the search field at the upper right of every page. That brought up all of our many mentions of FRITZ!Box through the years, as well as some comments over in GRC's forums. The listener who tweeted the news to us in Episode 970 used the Twitter handle "ndom91." So we still don't know his name or who he or she is, but thank you again for the mention. And thank you, Tal, for sharing your impressions.

I went over and looked at their lineup. It's a German company. They've got, fortunately, an English language website. And it is very impressive, I have to say. I especially liked the integrated DOCSIS 3.1 cable modems and routers.

Leo: Oh, nice.

Steve: They have several devices. Yes. And I've been sort of unhappy with domestic cable modem suppliers. They, you know, they really don't seem to be doing a great job. This German firm, you know, really does seem to have their act together. So if we ever get fiber in our area, they also have an integrated fiber modem router. I might take a look at that. And they're all WiFi 6 and even 7. So they're keeping up to date with the standards, yeah. Look at that thing. That's just beautiful.

Leo: Yeah, it really is.

Steve: And somehow they're doing a good job without lots of antennas sticking out everywhere.

Leo: Well, I think that's - the antennas are a marketing thing, I think, yeah.

Steve: Uh-huh, exactly.

Leo: Oh, this is cool.

Steve: Yup. And there's a WiFi 7-enabled cable modem router that I'm seeing there.

Leo: Yeah. And with Zigbee onboard so you can control your smart home.

Steve: Yup.

Leo: Oh, these are nice. This is really nice. This is for LTE, so you use mobile broadband.

Steve: They are solid-looking devices.

Leo: Of course, you've got to make sure that your cable company will support their...

Steve: Yes, that's the thought I had was that the Cox does, you know, they make a point of saying, well, these are the ones we support.

Leo: Yeah. This is the one I would get, though, if I - interesting. 3.1, WiFi 7.

Steve: And apparently really strong.

Leo: Yeah.

Steve: As he said, you know, they're not, like, they didn't cheap out the processor and RAM.

Leo: I like that, yeah. Look at that. Okay. FRITZ!Box.

Steve: And a telephone system. It does telephony built-in, too.

Leo: Oh, yeah, with DECT Base Station for cordless telephony. Wow. Wow. They put everything in here but the kitchen sink. Oh, wait a minute, here's a kitchen sink.

Steve: Oh.

Leo: No. At least use a kitchen. And their operating system is called FRITZ!OS. No. FRITZ!OS.

Steve: Too bad it's not Fritos.

Leo: It's so close to Fritos, I want to get it, yeah. So it's not - you can't put WRT or something else on there. This is their...

Steve: No, I don't think you - but I would bet that they've got a beautiful-looking built-in router.

Leo: Well, it's made in Germany, so it's got to be good; right?

Steve: Jawohl.

Leo: Look at that, yeah. Wow. Okay.

Steve: Okay. So Richard Green in Lethbridge, Alberta, Canada, his subject was "Four-digit PINs in a corporate environment." Okay. Get a load of this, Leo. He said: "Hi, Steve. Absolutely love the show. Thanks for doing it. I thought you might enjoy this story. I'm a physical security installer, as in physical alarm systems, and I was asked to do a system audit and upgrade on a major chain grocery store. So we came out and gave everything a physical check up and upgraded their equipment. We then asked for their list of current users so we could verify and remove any old and unused alarm-disarming PINs. At first, they didn't want to do this, and I figured it was a corporate policy. But then they relented and started printing off pages of names and PINs. Pages and pages of PINs.

"Apparently, some higher-up decided it would be a great idea to have every manager, assistant manager, or anyone else of importance nationwide, programmed into every store's alarm system just in case they might travel. We started out, of course, with 10,000 possible PINs, but their list was nearly 7,000 PINs long. This meant that any random guess would have a 70% chance of disarming their alarm system at any facility." He said: "I flat-out refused to be the guy to set up a system that was so insecure. Luckily for me they finally relented, and we only added about 60" - six zero - "user PINs, local to our region. I wouldn't have believed it had I not seen it for myself."

Amazing. So Richard, thank you for sharing that horror story from the field. It's helpful, I think, to see, like, the way things are actually being done out there in the real world, you know, way far from the ivory tower.

Manuel Schmerber, sorry for messing up your last name, Manuel, in St. Louis. He said: "Hi, Steve. I noticed that the UDM value just selects from the menu of search options: 15 is attractions, 12 is news, 14 is web, and so on. I also noticed that an easier way for me to get to the simpler Web results is to just select from the menu of offerings below my search phrase. I select the More dropdown and then Web." And he says: "Thanks for the lowdown on search."

So I just wanted to thank Manuel for demystifying the "magic 14" of the UDM value. I didn't spend any time digging around, and I'd been wondering where the 14 came from, you know, why was it UDM=14. And yes, it is certainly possible to select the Web menu item from Google's already displayed results. But the various hacks that are emerging allow us to get those same "web only" results right from the start with our browser's default search.

Vern Mastel in Mandan, North Dakota. Oh, I got a kick out of this. The subject was "SN-975 Windows XP Test." He said: "The Windows XP report is misleading. The test was not fair. What Parker did was test a 1935 Chevrolet sedan on a modern eight-lane superhighway at rush hour. He should repeat the test with a new out-of-the-box configuration Windows 10 or 11 machine on the same, no router, open Internet connection. That would be very interesting."

Vern said: "Windows always has come out of the box with EVERYTHING" - that's all caps - "turned on. I claim that the biggest holes in that test XP machine were Windows File and Print Sharing and Windows Remote Desktop. Both are wide open in a fresh Windows XP install. Such a machine should be dead meat on today's Internet. So that begs the question, what ISP was used for the test?

"When XP was new in 2001, ISPs did not do any active protocol blocking. Windows NetBEUI/NetBIOS ports 137, 138, 139, and 445, along with many others, were open to the world. For example, with File and Printer Sharing turned on, the default, you could see and easily access other Windows XP machines in the vicinity. For many years, when I set up a new Windows XP machine on the networks I administrated, I spent an extra hour changing network and system settings to close security holes, and shut down or remove the many unneeded features.

"Now things are pretty well locked down at the ISP level. Old LAN protocols are blocked by default, you cannot run your own mail server out of your house, and other server protocols like FTP are monitored or blocked outright. Properly configured, XP is/was a stable, reliable, and reasonably safe version of Windows."

Okay. I agree with everything Vern said, except for his thesis that this was in some way not a fair test. I have a problem with that characterization only because it wasn't meant to be a test of fairness. It was a test of reality, or perhaps a test of yesterday's reality versus today's reality. And of course everything Vern noted about the way he would first spend his first hour with any new Windows XP machine was the reason I created the ShieldsUP! port probing facility. It was precisely because these early machines from Microsoft were such a disaster on the Internet.

That said, I also agree with him that it would indeed be interesting to place a currently fully patched Windows 10 or 11 machine directly on the 'Net to see how it would fare. You know, direct exposure to the Internet. Given that all Windows machines have a very competent application-driven firewall that is up and running before the rest of the vulnerable networking behind it comes to life, I would expect it to do well.

But in any event, Parker's whole point was to get some sense for the malicious crap that is circulating out on the Internet right this moment. We're all so well insulated and so well shielded behind our NAT routers and firewalls that it's possible to sort of forget just what's out there constantly pounding away at those defenses. These defenses that we have today are absolutely not optional.

Okay. And lastly, Jeff Smock says as his subject: "I offer you my very own First Law of Cloud Data Security." He said: "Forget about all the bluster and jazz hands the cloud service providers give us regarding the security of our data." He says: "Here is the simple truth: 'The security of cloud data is inversely proportional to its potential value as perceived by a hacker or rogue staff member." So, yes, the more they want it, the bigger problem we're going to have keeping them from it. So I completely agree with that characterization. And Leo, let's take our final break, and then we're going to talk about the 50 Gigabyte Privacy Bomb.

Leo: Can't wait.

Steve: Which Microsoft plans to drop into everyone's lap.

Leo: Can't wait. Hey, I just wanted to mention, because that FRITZ! thing got me really excited, and I went to the website, it's a German company. As far as I could tell they do not sell in the United States. Your correspondent was in Israel.

Steve: Ah.

Leo: If somebody who's listening tells me where I can get FRITZ! stuff in the U.S., and if it's U.S. compliant, I'd be very interested. But right now it looks like, I mean, it's Germany.

Steve: I wonder why.

Leo: Well, we have an FCC. I mean, they'd have to get approval in the U.S.

Steve: But they're Germans.

Leo: How hard can that be?

Steve: I mean, I'm driving - we're each driving one of their cars, Leo.

Leo: I know. I like...

Steve: They work just great.

Leo: German engineering, okay. But as far as I can tell I couldn't find anywhere I could buy it in the U.S.

Steve: Wow.

Leo: And I checked, and your correspondent was in Israel, which might explain how they could get it.

Steve: Yes, he was.

Leo: Yeah. Okay, 50 gigabyte pile of nonsense.

Steve: Uh-huh. So since we began the podcast with a general theme of how AI, which is not even close to being intelligent, is being misapplied during these early days, I feel as though a security and privacy-focused podcast like this one ought to take note of the new "Recall" feature that will be part of the next-generation ARM-based Windows 11, what's known as Copilot+ laptop PCs.

First of all, yes, it does appear that ARM processors have finally come far enough along to be able to carry the weight of Windows on their processors. And while having Windows on ARM will certainly create a new array of challenges, like for example the lack of specific hardware drivers that only exist for Intel kernels, in the more self-contained applications, you know, where drivers are much less used, such as laptops, where power consumption and battery life trumps pretty much any other consideration, it's foreseeable that Windows may finally be able to find a home on ARM. Today, laptop and tablet form-factor machines containing Qualcomm Snapdragon ARM processors, running

Windows 11, have been announced and are in some cases available for pre-order from Acer, Asus, Dell, HP, Lenovo, Microsoft, and Samsung.

It's also worth noting that Intel PCs will also be getting Copilot+ at some time in the future. But they will need to have a neural processing engine. Answering the question "What makes Copilot+ PCs unique," Microsoft writes: "Copilot+ PCs are a new class of Windows 11 PCs that are powered by a turbocharged neural processing unit (NPU), a specialized computer chip for AI-intensive processes like real-time translations and image generation, that can perform more than 40 trillion operations per second." So we have TOPS, trillion operations per second. So more than 40 TOPS. And later, Microsoft writes: "We are partnering with Intel and AMD to bring Copilot+ PC experiences to PCs with their processors in the future." So potentially everybody's going to be able to get this.

Okay. So what is Recall? Microsoft explains. They said: "You can use Recall on Copilot+ PCs to find the content you have viewed on your device. Recall is currently in preview status. During this phase we will collect customer feedback, develop more controls for enterprise customers to manage and govern Recall data, and improve the overall experience for users. On devices that are not powered by a Snapdragon X Series processor, installation of a Windows update will be required to run Recall.

"Recall is currently optimized for select languages, including English, simplified Chinese, French, German, Japanese, and Spanish. This means Recall is able to retrieve snapshots from your PC's timeline based on more sophisticated searches in these languages. During the preview phase, we will enhance optimization for additional languages. Recall can also retrieve snapshots from your PC's timeline based on text-to-text searches in more than 160 languages."

Okay. Fortunately, they then ask themselves "How does Recall work?" To which they reply: "Recall uses Copilot+ PC advanced processing capabilities to take images of your active screen every few seconds. The snapshots are encrypted and saved on your PC's hard drive. You can use Recall to locate the content you have viewed on your PC using search, or on a timeline bar that allows you to scroll through your snapshots. Once you find the snapshot that you were looking for in Recall, it will be analyzed and offer you options to interact with the content.

"Recall will also enable you to open the snapshot in the original application in which it was created." Whoa. Really? Okay. "And, as Recall is refined over time, it will open the actual source document, website, or email in a screenshot." Which, okay, is mindboggling. But they said: "This functionality will be improved during Recall's preview phase." So before they let it loose.

They said: "Copilot+ PC storage size determines the number of snapshots that Recall can take and store. The minimum hard drive space needed to run Recall is 250GB, and 50GB of space must be available. The default allocation for Recall on a device with 256GB will be 25GB, which can store approximately three months of snapshots. You can increase the storage allocation for Recall in your PC Settings. Old snapshots will be deleted once you use up your allocated storage, allowing new ones to be stored." Okay, so it's sort of a rolling 90-day window, the most recent 90 days of screen snapshots taken every few seconds.

Okay. Then they ask: "What privacy controls does Recall offer?" They respond: "Recall is a key part of what makes Copilot+ PCs special, and Microsoft built privacy into Recall's design from the ground up." Which of course we all recognize as standard boilerplate, which we all hope is true. They said: "On Copilot+ PCs powered by a Snapdragon X Series processor, you will see the Recall taskbar icon after you first activate your device. You can use that icon to open Recall's settings and make choices about what snapshots Recall collects and stores on your device. You can limit which snapshots Recall collects;

for example, you can select specific apps or websites visited in a supported browser to filter out of your snapshots. In addition, you can pause snapshots on demand from the Recall icon in the system tray, clear some or all snapshots that have been stored, or delete all the snapshots from your device."

Leo: We call that "I'm going to watch porn button now."

Steve: Yeah.

Leo: Press the porn button.

Steve: Yeah.

Leo: Yeah.

Steve: And it occurs to me that I'd later talk about how snapshots of the Windows-based Signal app would be a problem.

Leo: Oh. Because that's in the clear; right?

Steve: Right, right. I mean, it's what the user sees. Maybe this allows you to say "Don't take snapshots of that window." And we should also remember that what we see is a graphic user interface. But Windows knows the text behind the actual controls that it's displaying. So it doesn't actually have to be, I mean, I guess it's - who knows what it's doing in detail. But my point is that, while we see graphics, there's actual text which is being mapped into bitmapped fonts which is then being displayed on the screen. So behind the screens, so to speak, Microsoft actually has the raw text which was used to generate the screen.

Leo: Yeah, yeah. That makes sense.

Steve: Okay. So they said: "Recall also does not take snapshots of certain kinds of content, including InPrivate web browsing sessions in Microsoft Edge." And by the way, they only said Edge, but I saw elsewhere that it's any of the browsers that have a well-defined private browsing mode. You know, they do not record that. And they said: "It also treats material protected under digital rights management," you know, DRM stuff, "similarly. Like other Windows apps such as the Snipping Tool, Recall will not store DRM content."

And they said: "Note that Recall does not perform content moderation. It will not hide information such as passwords or financial account numbers. That data may be in snapshots that are stored on your device, especially when sites do not follow standard Internet protocols like cloaking password entry."

Okay. So we're rolling toward an entirely new capability for Windows PCs, where we'll be able to store data which I presume is somehow indexed first, then encrypted for storage and later access. And unless otherwise instructed and proscribed, this system is

indiscriminately taking snapshots of our PC screen content every few seconds and is, by Microsoft's own admission, potentially capturing and saving, for later retrieval, financial account numbers, monetary balances, contract language, proprietary corporate memos and communications, and who knows what private things we'd really rather never have recorded, or whatever else the user might assume will never go any further. This is where our much beloved and overworked phrase "What could possibly go wrong?" comes to mind.

Does anyone not imagine for an instant that having searchable access to the previous 90 or more days of a PC's screen might be hugely interesting to all manner of both legal and illegal investigators? Corporate espionage is a very real thing. China is moving their enterprises away from Windows as rapidly as they can. But you have to know that cyberattackers, many of the most skillful and persistent who seem to be persistently based in China, must be beside themselves with delight over this new prospect that we decadent capitalists in the West are going to start having our PCs recording everything that's displayed on their screens. What a great idea. If history teaches us anything, it's that we still have not figured out how to keep a secret, and especially not Microsoft. So what Microsoft is proposing to plant inside all next-generation PCs is tantamount to a 50 Gigabyte Privacy Bomb. Maybe it will never go off, but it will certainly be sitting there trying to.

And just ask yourself whether law enforcement and intelligence agencies don't also think this sounds like a terrific idea? Oh, you betcha. With great power comes great responsibility. And here, clearly, there's much to go wrong. Microsoft understands this perception, and so they ask: "How is your data protected when using Recall?" They explain: "Recall snapshots are kept on Copilot+ PCs themselves, on the local hard disk, and are protected using data encryption on your device and, if you have Windows 11 Pro or an enterprise Windows 11 SKU, BitLocker. Recall screenshots are only linked to a specific user profile, and Recall does not share them with other users, make them available for Microsoft to view, or use them for targeting advertisements.

"Screenshots are only available to the person whose profile was used to sign into the device. If two people share a device with different profiles, they'll not be able to access each other's screenshots. If they use the same profile to sign into the device, then they will share a screenshot history." And thus, you know, be able to scroll back to see what the other person has been doing. "Otherwise, Recall screenshots are not available to other users or accessed by other applications or services."

Okay. So all that really means there is they've done the obvious thing; right? Is that they've, you know, they've divided the machine in the same way they do currently now, you know, with things like apps that you install for only one profile. So, okay. That's what Microsoft had to say.

The guys from Ars Technica watched Microsoft's presentation of this last Monday and gave their write up an impressively factual and neutral headline. They said: "New Windows AI feature records everything you've done on your PC." And then they said: "Recall uses AI features" - okay - "to 'take images of your active screen every few seconds.'" So Ars wrote: "At a Build conference event on Monday, Microsoft revealed a new AI-powered feature called Recall for Copilot+ PCs that will allow Windows 11 users to search and retrieve their past activities on their PC. To make it work, Recall records everything users do on their PC, including activities in apps, communications in live meetings, and websites visited for research. Despite encryption and local storage, the new feature raises privacy concerns for certain Windows users.

"Microsoft says on its website: 'Recall uses Copilot+ PC advanced processing capabilities to take images of your active screen every few seconds. The snapshots are encrypted and saved on your PC's hard drive. You can use Recall to locate the contents you have

viewed on your PC using search or on a timeline bar that allows you to scroll through your snapshots,'" quotes Ars Technica.

Ars wrote: "By performing a Recall action, users can access a snapshot from a specific time period, providing context for the event or moment they're searching for. It also allows users to search through teleconference meetings they've participated in and videos watched using an AI-powered feature that transcribes and translates speech. At first glance, the Recall feature seems like it may set the stage for potential gross violations of user privacy. Despite reassurances from Microsoft, that impression persists for second and third glances, as well." They said: "For example, someone with access to your Windows account could potentially use Recall to see everything you've been doing recently on your PC, which might extend beyond the embarrassing implications of pornography viewing and actually threaten the lives of journalists or perceived enemies of the state." And I'll interject to say, in other words, this puts examining someone's web browser history to shame. How quaint that becomes.

Ars continues: "Despite the privacy concerns, Microsoft says that the Recall index remains local and private on device, encrypted in a way that is linked to a particular user's account. Microsoft says: 'Recall screenshots are only linked to specific user profile, and Recall does not share them with other users, make them available for Microsoft to view,'" anyway, blah blah blah, what I just wrote about that.

So they said: "Users can pause, stop, or delete captured content, and can exclude specific apps or websites. Recall won't take snapshots of InPrivate web browsing sessions in Microsoft Edge or DRM-protected content. However, Recall won't actively hide sensitive information like passwords and financial account numbers that appear onscreen. Microsoft previously explored a somewhat similar functionality with the Timeline feature in Windows 10, which the company discontinued in 2021, but it didn't take continuous snapshots. Recall also shares some obvious similarities to Rewind, a third-party app for Mac we covered in 2022 that logs user activities for later playback."

They said: "As you might imagine, all this snapshot recording comes at a hardware penalty. To use Recall, users will need to purchase one of the new 'Copilot Plus PCs' powered by Qualcomm's Snapdragon X Elite chips, which include the necessary neural processing unit. There are also minimum storage requirements for running Recall, with a minimum of 256GB of hard drive space and 50GB of available space. The default allocation for Recall on a 256GB device is 25GB, which can store approximately three months of snapshots. Users can adjust the allocation in their PC settings.

"As far as availability goes," they conclude, "Microsoft says that Recall is still undergoing testing. Microsoft says on its website: 'Recall is currently in preview status. During this phase we'll collect customer feedback, develop more controls for enterprise customers to manage and govern Recall data, and improve the overall experience for users.'"

Okay. I just should note that the amount of storage Recall uses does scales upward with the size of the system's mass storage. And presumably the duration of the scroll back increases similarly. It'll take 25GB when 256 is available, 75GB on a 512GB drive, and 150GB from a system with a 1TB drive of primary mass storage. So presumably, the more storage the system is able to commandeer, the further it's possible to scroll back through the system's display history.

Okay, now, while trying to be objective about this, the first question that leaps into the foreground for me is whether anyone actually needs or wants this? Is this a big, previously unappreciated problem that everyone has? Okay. But trying to be objective. First of all, compared to the static contents of a hard drive, Recall would be objectively a goldmine of additional new information about the past 90-plus days of someone's life, as viewed through their computer activities. And more than ever before, people's entire

lives, and their private lives, are reflected in what's shown on the screens of their computers. Maybe that makes scrolling back through their recorded lives compelling. I don't know.

But we know from Microsoft that it will be snapping video conference content on the fly. And as I mentioned, the Windows Signal app that goes to extremes to protect the contents of its chats would presumably be captured, unless you're able, as I mentioned before, and they sort of suggest, you can tell Recall don't record specific applications. So you probably want to turn that off, or maybe you trust Microsoft, and it'll be part of your scroll back.

But, you know, email screens and nearly everything that happens on a PC would be captured. And of course that's the point; right? But the vast majority of that content will not have been stored on the machine's hard drive ever, until now. So objectively, the presence of Recall clearly introduces a new, never before existing liability. And that's what everyone who talks about this sees as a potential for creating havoc where none existed before.

So the question, it seems to me, is whether the new value that's created and is returned by Recall's scrolling usage history justifies whatever new risk might also be created by its retention of that data. How useful will having all that actually be? I've tried to imagine an instance where I wish I could look back in time at my computer screen. I suppose I don't feel the need since I've never had the option.

So if I knew I could scroll my computer's screens back in time, I suppose it might be an interesting curiosity. But it really doesn't feel like a feature I've been needing and missing until now. I suppose an analogy would be that the world had no idea what it was missing before the creation of social media. And hasn't that been a big boon to mankind? Now, unfortunately, we seem unable to live without it. Perhaps this will be the same.

The bottom line is this I think we're just going to need to live with this thing for a while. We're going to need to see whether this is a capability desperately searching for a need; or whether, once people get used to having this new thing, they start thinking, how did I ever live without this? However, one thing that is also absolutely objectively true is that everyone will be carrying around a 50GB privacy bomb that they never had before. Maybe it'll be worth the risk. Only time will tell.

Oh, and Simon Zerafa posted a tweet from someone who has been poking into Recall's storage. He's detective@mastodon.social, who wrote: "Can confirm that Recall data is indeed stored in a SQLite3 database. The folder it's in is fully accessible only by system and the administrators group. Attempting to access it as a normal user yields the usual 'You don't currently have permission' error." And he said: "Here's how the database is laid out for those curious." And he said: "Figured you might appreciate a few screenshots."

So I've put one in the show notes. And sure enough, it's got a DB browser for SQLite and shows the layout of the table with all of the various components, you know, window capture text index content, window capture text index data, window capture text doc size and relations and all kinds of stuff. So anyway, I guess what this means is that, if nothing else, if that data should ever escape from anyone's PC, it will not be difficult for anybody who gets it to open it up and browse around in it because it's just a SQLite3 database.

And Leo, you know, I guess, you know, if search really worked, and you were able to search on something that you remember, but you didn't write down or didn't record, didn't save, but it was just like right there at your fingertips, and bang, it popped up and showed it to you, I guess I could see that that could be compelling.

Leo: Yeah. I mean, I want to have - the late Gordon Bell passed away last week. He used to wear around a camera. His wife Gwen, I knew them both, wonderful people, had severe Alzheimer's, so he became very aware of the idea of remembering things. And I can't remember what he called it, the "mem-it," the "meme-it" or something. But this was '96. This was way before there really was the technology to do this. But it would take a picture every 20 seconds. And his theory was I would like to have, I mean, it's not just recall of your Windows desktop, but of everything, that you could then search and query.

And now there are, you know, I just bought something called the Limitless Pin that should come in August, it's a little lapel pin that records all your audio and then feeds it to an AI. So you can query it of things like that. You know, Steve and I were talking, and he mentioned a router from a German company, I can't remember the name of it. What was the name of that? "The name was Fritz." You could see that that kind of might be useful. There are absolutely privacy issues with this. In fact, that Limitless Pin won't record somebody's voice unless you get explicit spoken approval to do so, which is very interesting. It uses voice printing.

Steve: So it's doing voice recognition.

Leo: Yeah, yeah.

Steve: Instead of just being a generic audio recorder.

Leo: Right. But then, once they say yes, then it will say, "Steve said," "Leo said," that kind of thing. I don't - you know what? This is very early days. But you nailed it. There is potentially some use for this, but there's also a downside, many downsides.

Steve: Yeah. And so I think it's a tradeoff, like anything else. Is this so useful that it's worth carrying around the last 90 days plus of everything that your computer screen showed? And that's the other thing, Leo. You're not going to want to not record, like, chunks of your screen, like you would probably not want to not record - I'm sorry. You would want to record Signal because you'd want to be able to...

Leo: You want to be able to query it, yeah.

Steve: Exactly. Exactly. So the tendency will be to, you know, record everything and trust the Force. Unfortunately, that's Microsoft.

Leo: It's a challenge, I mean, this is really a challenge. I would not turn on Recall, partly because of the burden, the strain it puts on the system seems like a bad idea.

Steve: Well, yeah. I have a feeling that our audience will not be among the first adopters.

Leo: Right.

Steve: I mean, some will. I'm curious. And as I was thinking about this, I thought, I will be interested in hearing. Like, you know, to hear Paul - lord knows he's not a pushover. So if Paul Thurrott says, hey, this is the greatest thing since, you know, bananas, sliced bread, you know, whatever, then wow.

Leo: Yeah, we'll watch what Paul - exactly. I mean, you've searched through your - I have - searched through your browser history; right? I can't remember, what was that site? And you go through your browser history. That's what browser history does, except it's just recording websites you visit, just the URLs. Might be more useful if it recorded the content. And then maybe if all your apps did the same, and you can see how you can slide into this.

Steve: Yeah. Content, there was an app back in the DOS days, and I've tried to remember what it was. It would take little notes. And so you could easily create a little text window and type some text in, and it just went into a big pile.

Leo: Was it Sidekick?

Steve: Well, as you typed, I think it was a TSR, and you would bring it up full screen, and it would be this blizzard of little overlapping, like, Post-its.

Leo: Yeah, that sounds familiar, yeah.

Steve: But then, as you type a few characters, all the ones that did not contain that substring would - they disappeared. And it was compelling to be able, like anything you thought you remembered, you could just type a few characters, and it would, like, whittle it right down.

Leo: There was "Ex." Do you remember "Ex"? That was the idea of "Ex" was a superfast - but that wasn't like what you just described. But the idea was it indexes your - just like Windows does, but it faster and better indexes everything on your drive. And then you type one letter, it finds everything that matches that, two letters, three letters, it's that progressive search. So you could very quickly - "Ex" was very, very fast. It was very cool.

Steve: What happened to it?

Leo: It's still around. I think they went - they became an enterprise tool.

Steve: Okay. Well, and it's built into Windows now. So, you know...

Leo: Yeah. Yeah, but Windows doesn't do it as well as "Ex" did. It was [crosstalk] even when "Ex" did it. It was a smart search tool. What was the name of that DOS program? I know exactly what you're talking about.

Steve: Yeah. It was, and I've tried to remember it, and like Instant Recall or something like that.

Leo: Oh, that sounds familiar, yeah. Oh, this is "Ex." That's the wrong "Ex." This is the problem with the word "Ex." It's not a good search term. It's not easy.

Steve: No, it was a dumb thing for Twitter to get renamed to.

Leo: Not the only dumb thing Elon's ever done. That's interesting. I want to know this Instant Recall thing.

Steve: I want to think - I think it was written by Phil Katz.

Leo: Oh, well, there you go. Yeah, he was a genius.

Steve: The PKZIP guy.

Leo: The PKZIP guy.

Steve: Yeah.

Leo: Yeah, Recall 11. It was called Recall.

Steve: Just Recall.

Leo: I think so.

Steve: Wow.

Leo: I think so. Memory resident, no, it's command line editor and history utility. That might be it. It's TSR.

Steve: No. This thing was definitely - it was little notes. It was not a command line history.

Leo: Okay.

Steve: That does sound like a DOS command line history.

Leo: Yeah. Huh. Somebody will remember, and they'll message you on your new email platform.

Steve: Yay.

Leo: How do they do that again? They go to GRC.com.

Steve: /mail.

Leo: /mail.

Steve: Or just GRC.com, and there's a little white envelope up at the top of the screen.

Leo: They have to get whitelisted, though.

Steve: Yes. Exactly. So GRC.com/mail. Okay. And there it is.

Leo: I put in my email.

Steve: Yup. And I just sent you a link.

Leo: And then you're going to send me an email. Okay. And then I confirm that that's my email, which no spammer would ever do.

Steve: Correct.

Leo: So right there you've eliminated spammers.

Steve: Correct. And so you click on - the email that comes is very attractive. And you click on the little button that you get, and it takes you to your subscriptions page. And you can put your name in if you want so that I address email to you by name.

Leo: Well, there it is.

Steve: There it is.

Leo: Very attractive. Nice choice of colors, Steve. Confirm.

Steve: Well, I need to think about that, though, the black on white. It looks much better on a white background.

Leo: Ah, yes. I'm dark mode, man. Okay. So now I'm - you know better than clicking a button in email. So what I'm going to do is the smart thing, which is copy it.

Steve: That's right, I gave you a link.

Leo: And paste it in.

Steve: I gave you a link because I know who our...

Leo: Yeah, GRC.com/manage, yeah, that looks good, okay. And now I can choose, if I wish, to subscribe, but I don't need to. Oh, look, you can subscribe to Security Now!. Oh, I definitely want product news. Oh, and GRC news. Okay. And my name, Leo.

Steve: Is Leo.

Leo: Yes. And I'm going to update my subscriptions. So now I can email you from this address.

Steve: Correct. And now, if you get the mail again, you'll see the confirmation that was sent, which is also very pretty.

Leo: Okay. Look at that. Also, you know, let me get out of dark mode so I can enjoy the fresh...

Steve: Yeah, it's very pretty.

Leo: ...beauty of what you're doing here. Of course I've been in dark mode so long I have no idea how to get out of it.

Steve: How to turn it off.

Leo: How do you turn this off here? I don't know. I think I have to go to system settings. And I go, let's be light. Light mail. Oh, look how pretty that is, Steve.

Steve: Yup. So I show - I address it by name, show you your email address, and which list that you're subscribed to.

Leo: Nice. Very nice.

Steve: Yup, that's all there is to it. And so now you are whitelisted, and you can send email to securitynow@grc.com.

Leo: And that's where you should do your feedback. Go through those steps, and you can have a nice conversation, a nice chat with Steve.

Steve: Yeah, and I don't know what's going to happen with Twitter. As I said, it's easy for me to post the weekly notes there.

Leo: Oh, you should keep doing that.

Steve: I'm beginning to get a lot of spam. So I guess I don't see any reason for it any longer.

Leo: I've been gone more than a year, and I don't miss it. Good. Good. Very nice. Now, while you're at GRC.com, don't stop there. Do that, GRC.com/mail. But you can also find Security Now! there.