One Thousand!

Description: Did Bitwarden go closed-source? The rights of German security researchers are clarified. Australia to impose age limits on social media. Free Windows Server 2025, anyone? UAC wasn't in the way enough, so they're fixing that. "From Russia with fines?" Obey or else. South Korea fines Meta over serious user privacy violations. Synology's (very) critical zero-click RCE flaw. Malicious Python packages invoked by typos. Google to enforce full MFA for all cloud service users. Mozilla Foundation lays off 30%? Is Firefox safe? Some feedback from Dave's Garage, and thought-provoking Closing the Loop feedback from our terrific listeners.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-1000.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-1000-lq.mp3

SHOW TEASE: It's time for Security Now!. Yes, our 1000th episode. We're going to look back a little bit as to how this show got started. We also have the latest news, including good news for our sponsor Bitwarden. They are still open source. How Microsoft is fixing User Access Control. And Synology's very serious zero-click RCE flaw. All that and a lot more coming up next on our 1000th episode of Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 1000, recorded Tuesday, November 12th, 2024: 1000!

It's time for Security Now! Episode - they said it would never happen - 1000, ladies and gentlemen.

Steve Gibson: Actually, some people did say it would never happen. That would be me.

Leo: That would be you.

Steve: I said it would never happen.

Leo: We've convinced Steve to go to four digits as we continue on in what is now almost our 20th year of talking about security flaws, privacy breaches, how to stay safe online and, just as important, how things actually work. Steve's a master of that. Ladies and gentlemen, I give you Steve Gibson. Nice to see you, Steve.

Steve: Coming to you from my alternative location because the roof is being changed on my normal location.

Leo: Oh.

Steve: And it felt like they were, like, walking right on top of my head this morning. And I thought, well, you know, that's not going to fly.

Leo: You could say, though, that Episode 1000 blew the roof off.

Steve: Oh, that's true.

Leo: Literally.

Steve: Fortunately, we have mild weather in Southern California.

Leo: Good time to do it, yeah.

Steve: So, yes. And I was just saying to you before we started recording, Leo, that 999 was, you know, you would have thought that would have been, like, the one that I focused on. But it was when I was putting this together, and I put in one zero zero zero, that I thought, wow, that really is cool.

Leo: Wow. Wow.

Steve: So, yes. We've got a lot to talk about. For the last several weeks I have been frustrated that there's been so much going on, so much happening, that I just wasn't able to make time to share any of the feedback that I've been receiving. So the good news is, well, okay. So there was a lot that happened this week, but there just wasn't any need to spend a lot of time, as we often do sometimes, really drilling down into anything. So we've got a bunch of listener feedback that we're going to end the show with.

But we're going to look at whether Bitwarden, a sponsor of the TWiT Network, went closed source. There were some odd rumblings about that over the last few weeks. The rights of German security researchers have been clarified, thanks to some legislation in Germany. Australia is preparing to impose lower age limits on access to social media for children, which is going to be interesting. Also, it appears that people got free copies of Windows Server 2025 without asking for it, to their chagrin, often. We're going to talk about that. Also, UAC wasn't in the way enough, so Microsoft's going to fix that.

Leo: Oh. I guess good.

Steve: Also we've got from Russia with fines, or obey or else. Also, South Korea has fined Meta over some serious user privacy violations we'll take a look at. Synology is

recovering from a very critical zero-click remote code execution flaw that affected their photo sharing stuff. A really interesting story about malicious Python packages which are being invoked by typos in an interesting supply chain typo squatting attack. Also, Google has said that they're going to enforce full multifactor authentication for cloud service users. Mozilla Foundation just laid off 30% of its workforce, so should we worry about Firefox? Also I've got some feedback from Dave's Garage, who took a look at SpinRite. Thank you, Dave Plummer. And as I said, we'll wrap up with a bunch of really thought-provoking Closing the Loop feedback from our terrific listeners. And of course we've got one of our Pictures of the Week for Episode 1000. So I think another great episode for our listeners.

Leo: I feel like I've seen this. Maybe it's because somebody sent it to me first or something. Anyway...

Steve: It's been around, but we hadn't put it on the podcast yet.

Leo: Okay. Oh, good, I like it, yeah.

Steve: And it's just - it's another one of those.

Leo: It's another one of those.

Steve: Those pesky people.

Leo: Those pesky people. Well, congratulations on Episode 1000, Steve.

Steve: Well, to us. To you.

Leo: To us.

Steve: I wrap up with a little retrospective look back at your original invitation.

Leo: I do have to say that, while I have not been here for all 1,000 episodes, you have. There is no Security Now! without Steve Gibson. So really the kudos go to you. I've only done maybe 950 of them.

Steve: Well, you do take vacations, and that keeps you fresh, so that's good.

Leo: Yes, yes. But you do not, which is odd. But okay.

Steve: I don't know why.

Leo: Anyway, we're so glad that you don't, and we really appreciate everything you do, Steve. And congratulations on 1000.

Steve: Well, so, let's see. It took us 20 years to get here. I don't think we're going to make 2000. But we'll keep going until we can't.

Leo: We'll be, like, in our late 80s, early 90s.

Steve: Yeah.

Leo: It would be interesting, let's say that.

Steve: Yeah. Toward the end Jerry Pournelle, who I think of when I think of, like, pushing the limits, you know, he was something, so...

Leo: A little crotchety. But you know what, he was perfectly sharp upstairs. There was never any question about that. Me, not so much. I'll say "What is this about honey monkeys?" And you can say, "Leo, that was 40 years ago." That's the story about...

Steve: That's right. How it would have been. Wow.

Leo: Actually, I think our first story, well, let's do the Picture of the Week first, and then we'll deal with the other Bitwarden story.

Steve: Okay. So imagine that you have a beautiful green park space, and along one side of it is sort of a paved roadway meant for pedestrians.

Leo: Right.

Steve: We can see in the distance a concrete pole sticking up in the back so, you know, cars are not able to have any throughway here. It's just people.

Leo: Plus this would stop bicycles and motorcycles and other rolling vehicles.

Steve: Well, not initially. Presumably this all was green. Everything was fine. But somebody was annoyed that bicycles or scooters or, you know, something other than pedestrians were using this, presumably at some sort of high speed. So the genius here figured, okay, we're going to slow these people down. We're going to prevent them from zooming along on their scooters or their bicycles or whatever newfangled contraption they might be using, by basically putting an obstacle course in this roadway, in what used to be an idyllic little asphalt path for people, bordering this beautiful green lawn parkway.

And so what we have here are essentially some gates that you have to weave yourself through, overlapping blockages. So somebody on foot has to go forward and then move sideways in order to get past, in order to skirt the first one and then slide over in order to get around the second one. Then they have - they can, you know, catch their breath and walk down another 20 feet, when they hit another one of these things. But, boy, is that going to stop those guys on those scooters or bicycles or whatever the hell that they're using. Well, unfortunately, I gave this the caption "What they intended was not what happened."

Leo: No.

Steve: Because the beautiful green parkway is beautiful and green not so much any longer. There is, as a consequence of the fact that they basically put an obstacle course in the middle of the road, all the people who were riding something, bicycles, scooters, whatever, just rode over on the grass.

Leo: They rode around it, kids.

Steve: That's right. That's right. They didn't slow down. They probably...

Leo: No, you can see the ruts.

Steve: Yeah, they didn't signal. They just, now, of course the first person who did that had very little effect on the grass. Probably the second person also. But after about 5,000 people did this, well, that took its toll. And so now the grass has given up. It's made its own path. And it's very clear now, you don't even have - if you are a person who hasn't yet approached this area...

Leo: Yeah, you know which way to go.

Steve: You know exactly what to do. You're not getting off your scooter and having to go through this little obstacle course. No, the path has been paved for you at this point.

Leo: That's hysterical.

Steve: Yes. Yeah. One of our listeners wrote back this morning because I got the show notes out in the late morning, and so he had time to write back. And he was speaking to a police officer, I can't remember now what the term was, but there is a term for this, like, people finding the path of least resistance sort of effect. And that's certainly what happened here.

Leo: Yeah, no kidding.

Steve: Okay. So on the topic of Bitwarden, for the past few weeks our listeners have been sending me notes regarding their concerns that Bitwarden's licensing might have

been changing to make it less open. I mean, this actually got some traction out on the Internet. It turned out that it was a good thing that I had not found the chance then to dig into whatever was going on because it has since resolved itself completely.

Now, The Register, weighing in with an explanation and, you know, their particular brand of snarkiness, I edited it a little bit for podcast clarity, they said: "Fear not, FOSS fans." You know, FOSS, Free Open Source Software. "Bitwarden is not going proprietary after all. The company has changed its license terms once again. But this time it has switched the license of its SDK from its own homegrown license to v3 of the GPL." Just as you were saying, Leo.

Leo: Yay. Yup.

Steve: They wrote: "The move comes just weeks after we reported that it wasn't strictly FOSS anymore. At the time, the company claimed this was just a mistake in how it packaged its software. Writing on Twitter, they said" - this is Bitwarden - "'It seems that a packaging bug was misunderstood as something more, and the team plans to resolve it. Bitwarden remains committed to the open source licensing model in place for years, along with retaining a fully featured free version for individual users.'"

Leo: Yay. Yay.

Steve: Yup. The Register said: "Now it's followed through on this. The GitHub commit entitled 'Improve licensing language' changes the licensing on the company's SDK from its own license to the unmodified GPL3."

Leo: That's good. That's really good.

Steve: Yup. They said: "Previously, if you removed the internal SDK, it was no longer possible to build the publicly available source code without errors. Now the publicly available SDK is GPL3, and you can get and build the whole thing." They said: "Chief Technology Officer Kyle Spearrin added a new comment to the discussion on bug #11611 on GitHub, where that bug was titled: 'Desktop version 2024.10.0 is no longer free software.'" Of course that's the comment that set off this firestorm.

So to that their CTO Kyle wrote: "We've made some adjustments to how the SDK code is organized and packaged to allow you to build and run the app with only GPL/OSI licenses included. The sdk-internal package references in the clients now come from a new sdk-internal repository, which follows the licensing model we've historically used for all of our clients." And they said: "See FAQ.md for more info. The sdk-internal reference only uses GPL licenses at this time. If the reference were to include Bitwarden License code in the future, we will provide a way to produce multiple build variants of the client, similar to what we do with web vault client builds."

He finished: "The original SDK repository will be renamed to sdk-secrets, and retains its existing Bitwarden SDK License structure for our Secrets Manager business products. The sdk-secrets repository and packages will no longer be referenced from the client apps, since that code is not used there." So, you know, they cleaned things up and fixed what was essentially just sort of a trip in this what has obviously become a rather complex build process with multiple overlapping licenses and things.

So The Register finished, saying: "This is genuinely good news for the program's more fervently FOSS-focused fans. It's all open source, and it's possible to build the whole thing, including the SDK, from freely available code. It seems to us that Bitwarden has responded to its users' unhappiness with the changes to the licensing around its password manager and has not merely undone the changes, but gone further toward making it all Free Software - even if it continues to maintain that it was all just an error. The change is commendable, and we're glad to see it. It does, however, look as if the company is leaving itself room to build more non-FOSS tools in the future." You know, fine, so what.

Anyway, so I think the whole thing here, everything that we've just seen, I mean, it's what free and open source software is about. It's a terrific example of community action which helped to bring some clarification to some initial confusion over Bitwarden's licensing terms. And to their credit, as The Register reported, Bitwarden really stepped up and did the right thing. So props.

In some good news for German security researchers, the German government has drafted legislation to protect security researchers who discover and report vulnerabilities. There was some ambiguity before. So this proposed law would eliminate the risk of criminal liability from cybersecurity research as long as the bugs are responsibly disclosed to the vendors. At the same time, the law does also introduce harsh prison sentences - ranging from three months to five years - for any researchers who abuse the process of vulnerability research for their own criminal acts. These include incidents when researchers cause substantial financial damage during their research, try to do some extortion, or acts that damage critical infrastructure. In other words, if you're a true researcher in Germany, any previous gray area has now been eliminated. So, yay.

But if you're hoping to abuse the "but I'm a security researcher" claim, your inability to get away with that has also been clarified, too. So it's good that we're seeing this because, you know, we've seen instances, and we've talked about it a lot on the podcast, where a well-meaning researcher reaches out to a company and says, you know, I was poking around at your web page, and I noticed that whatever, blah blah blah. You know, and I was able to log onto your servers. And suddenly, you know, like rather than taking this as someone trying to help them, they immediately sic their legal staff on them and start threatening them. So anyway, it's good that Germany's made this clear.

Australia. This is going to be interesting, I think. They're preparing legislation that would introduce a minimum age of 16 years for social media accounts, that is, for access to social media accounts. Under this new legislation, which is not yet law, just to be clear, but it's on its way to being law - access to social media platforms in Australia would be legally restricted to only those 16 years of age or older. And this legislation would hold online platforms accountable, only platforms would be accountable for enforcing the ban. Presumably it would also incur meaningful fines for failure to do so under this new law, or this forthcoming law.

Australia's government plans to introduce the bill in Parliament this week. So something's going to happen soon. And presumably it'll have some period before it has to take effect because you need to give the social media platforms some means of responding to this in a reasonable way. Government officials explained that they're introducing the bill due to the harm social media is causing for Australian children.

Now, we've talked a lot in the past, from the standpoint of the technological challenges associated, you know, practical challenges associated with filtering access to online services by their accessor's age. You know, how is this done, exactly? And will the legislation somehow put parents in charge? Can parents, you know, for example, choose to opt their children out of such filtering? You know, and there's a slippery slope there because, if that's possible, that creates the problem of one's kids saying, "Hey, but Mom

and Dad, all the other kids' parents let them watch TikTok," you know, regardless of the degree of the truth of that.

But regardless of the legal and social side of this, it seems to me that if we're going to start legislating age-based filtering for Internet services of any kind, the underlying platform itself should be robustly providing this information to any application through some sort of platform-specific API. For example, at this time, iOS, for all of Apple's devices, I think it was since the iPhone 13, allows granular restrictions of age four and above, nine and above, 12 and above, or 17 and above. But there's no 16 and above. So that's kind of a mess.

And none of this is automatic. You know, it's up to Mom and Dad to lock down their children's phones. Nor does this locked-down setting change automatically, like on their birthday. So from that point, the point of like setting the 12 and above or 17 or above or whatever, the device's apps that have previously declared their own minimum age usage will then be restricted by the phone. Which none of this is the way it should work. And I'm not sure how we got to where we are now. But it just doesn't seem like it was well thought out. It seems to me that a superior solution would be to allow the parent to set and lock in the date of birth of the phone's user. Based upon their feelings, the parental feelings about the maturity of their child and/or their feelings about the perceived dangers of unrestricted access to social media, they could choose to fudge their child's declared birth year in either direction, as they see fit.

But the advantage of this is that, you know, this could be a set-and-forget feature where services would become available on successive birthdays, based on the legislation that restricts what age they can be used in which locale in the world. You know, and at some point it will become accepted that on such-and-such a birthday, access to this-or-that social media service becomes available. So, you know, this is certainly another interesting aspect of today's Internet, the ubiquity of smartphones among minors, and of the platform's willingness to treat them like everyone else. So I don't know, Leo. We're tightening down access based on birthday, but we really don't have the mechanisms in place yet.

Leo: That's the problem is how do you do age verification without impeding on the...

Steve: Privacy.

Leo: ...privacy of adults, let alone kids.

Steve: Yup. Yup.

Leo: And, you know, they have all these companies that say, oh, we just look at them, and we can tell by their faces we use AI and blah blah blah. That seems ripe for misuse and failure.

Steve: Yeah.

Leo: So, yeah, you know, it's one of the - I can understand the desire to do it. But it's one of those things where, if you don't have the means to do it in a safe way, you've not improved things.

Steve: And here's the legislators in Australia saying, you know, thou shalt this.

Leo: Figure it out.

Steve: And it's like, uh, how, exactly?

Leo: Right.

Steve: Oh, well, that's not our problem. You're techie people. You'll work it out.

Leo: I mean, I think your solution is the only way to do it. I think that the mistake is government says, oh, we don't - we'll do it for parents. No. Parents, give parents the capability and let them decide. Only they know what their kids should and shouldn't do.

Steve: Yup, exactly. And if the parent puts in their birthday, and again, they could fudge it, you know, plus or minus a year or two depending upon their own perceptions of the risks and so forth, then once that's there, an API in the platform can be queried by any social media application or anything else, for that matter, to determine the age of the person watching. Now, okay, maybe the reason Apple did this is that having a birth date is considered itself a loss of privacy. So they're like, well, we're just going to create these big brackets of four, 12, and 17, and nine. And, you know, that way we're not divulging much. But I don't think you can have it both ways. You're saying that the platform must enforce an age-based restriction. Well, then you have to know the person's age. So, yeah.

Okay. Last Wednesday, The Register posted another interesting piece that I don't recall seeing anywhere else, although I did hear about it from a number of our listeners. The Register's headline was "Sysadmin shock as Windows Server 2025 installs itself after update labeling error." And then, of course, being The Register, their tagline on the article was "Screens sprayed with coffee after techies find Microsoft's latest OS in unexpected places." So with that tease, we need to find out what happened. So The Register writes: "Administrators are reporting unexpected appearances of Windows Server 2025 after what was published as a security update turned out to be a complete operating system upgrade." Whoopsie!

Okay. So "The problem was flagged by a customer," they wrote, "of the web app security company Heimdal. Arriving at the office on the morning of November 5th, they found to their horror that every Windows Server 2022 system had either upgraded itself to Windows Server 2025 or was getting ready to. Sysadmins are cautious by nature," they wrote, "so an unplanned operating system upgrade could easily result in morning coffee being sprayed over a keyboard. Heimdal's services include patch management, and it relies on Microsoft to label patches accurately to ensure the correct update is applied to the correct software at the correct time. In this instance, what should have been a security update turned out to be Windows Server 2025.

"It took Heimdal a while to trace the problem. According to a post on Reddit: 'Due to the limited initial footprint, identifying the root cause took some time. By 18:05 UTC, we traced the issue to the Windows Update API, where Microsoft had mistakenly labeled the Windows Server 2025 upgrade as KB5044284. Our team discovered this discrepancy in

our patching repository, as the GUID for the Windows Server 2025 upgrade does not match the usual entries for KB5044284 associated with Windows 11. This appears to be an error on Microsoft's side, affecting both the speed of release and the classification of the update. After cross-checking with Microsoft's Knowledge Base repository, we confirmed that the Knowledge Base number indeed references Windows 11, not Windows Server 2025.'" Okay, so whatever.

They said: "The Register has contacted Heimdal for more information and will update this piece should the security organization respond. We also asked Microsoft to comment almost a day ago. Since then, crickets. As of last night, Heimdal estimated that the unexpected upgrade had affected around 7% of their customers. It said it had blocked KB5044284 across all server group policies. However, this is of little comfort to administrators finding themselves receiving an unexpected upgrade." They finished: "Since rolling back to the previous configuration will present a challenge, affected users will be faced with finding out just how effective their backup strategy is..."

Leo: Oh, dear.

Steve: Uh-huh, "...or paying for the required license and dealing with all the changes that come with Windows Server 2025." Wow. What a mess. So I cannot speak for other admins, but I would be desperately checking that everything was still working after such a jump, if it were my servers. You know, and if it were, I'd probably choose to remain on that platform if it hadn't, like...

Leo: Broken everything.

Steve: ...irrevocably broken things, which, you know, it could easily do, you know, after such a jump like that had been made, since Microsoft would eventually be forcing the move anyway; right? I mean, anybody who is on 2022, well, they've got 2025 in their future. So, wow. I can definitely empathize with the panic that would ensue.

Leo: To be more clear on this, did this happen to anybody who wasn't a Heimdal customer?

Steve: It's a good question.

Leo: Because if it didn't, then it's Heimdal's fault, not Microsoft's fault.

Steve: Yes. I did hear from some of our listeners already who experienced this themselves, but they didn't specify whether they were a Heimdal customer or not. There was some - I believe it was third-party upgrade management...

Leo: Right.

Steve: ...that was the source.

Leo: Right. So Microsoft's getting all the blame for this, but it's not Microsoft's fault.

Steve: No. I believe it was somebody who - so systems that were under patch management by a third party were updated, not by Microsoft, but by their patch manager. Yes. And so I'm glad you brought that up, Leo, because that is the case. And the other thing that is the case is that it's time for me to take a sip of coffee.

Leo: Oh. I just took a bite of sandwich. So, okay. You take that sip, and I'll try to chew fast.

Steve: Doot ta doo. I have my eye on the clock, and we're 34 minutes in, so a good time before we talk about what it is that Microsoft has decided they're going to do to Windows 11 to further protect people from User Account Control. Turns out it's not in your face enough. So they're going to fix that.

Leo: Yeah, well, that's true. Everybody just - you get the prompt to elevate, and you go, okay, yeah, fine.

Steve: I have mine turned off.

Leo: You don't use UAC?

Steve: No. The first thing I do.

Leo: Oh. And I understand completely why.

Steve: I bring it down to minimum, and then I go into the registry, and I disable it completely because it's just, you know, I'm a mother hen over my machine.

Leo: Yeah. You don't need two mother hens. One's enough.

Steve: No. And the fact is, I mean, the problem is people are saying, oh, there's that annoyance again, and they just click yes.

Leo: Yeah.

Steve: And so it's like, okay, what protection is that? Well, Microsoft's going to fix that.

Leo: Let's not make this easy.

Steve: Ah, right.

Leo: Now I want a cup of coffee. It's my turn for...

Steve: Your time. Your turn.

Leo: For a cup of coffee.

Steve: Okay. So we all know UAC, User Account Control. This is Windows' clever and workable solution to the age-old dilemma of users running root privileges on a system just so they're not constantly being told that they can't do what they want to do with their own system. The problem with doing this, with running as root, is that it's their logon that has the root privileges. This means that anything they might do inadvertently, like innocently run some malicious software, you know, by mistake, inherits their account's root privileges and allows their system to be easily and potentially irreversibly compromised.

So the solution Microsoft evolved, and we talked about this when it first appeared in Windows, and I said then I think this was very clever, I mean, I think it's, like, the best solution we've had so far. What they did was they split credentials where an administrative user, even though they're an administrative as opposed to a standard Windows user, an administrative user effectively logs on with both standard user and elevated credentials, or tokens, as Microsoft calls them, while always running as a standard user with reduced privileges. This way they're protected from anything that might inadvertently happen when they're not intending to have anything happen, when they're not looking.

Then, when they try to do something that their lesser privileges doesn't permit, such as installing a new application into the system or disabling some system protections, Windows will pop up the User Account Control, the UAC prompt, which essentially serves as an "Are you sure you want to do this?" required confirmation. And when the user sighs and clicks "Yes, I'm sure I want to do what I just asked for," Windows briefly switches over to their elevated permission token credentials to allow that requested action to be performed.

Okay. So that's the way it's been now for many years. But we learned last week that it will be possible to optionally add another layer of security to this existing mechanism. Microsoft wrote: "Administrator protection," which is what they're calling it, admin protection, "is an upcoming platform security feature in Windows 11, which aims to protect free floating admin rights for administrator users, allowing them to still perform all admin functions with just-in-time admin privileges. This feature is off by default," meaning, okay, just for clarity, when this is part of Windows 11, it will not be enabled by default. So UAC will continue working the way it has. But it can be enabled via group policy. So systems that are being administrated remotely over the network in enterprises can cause this to be on for all of their Windows client machines. Microsoft said: "We plan to share more details about this feature at Microsoft Ignite."

Now, The Hacker News dug into this a bit and did some reporting. They said: "Microsoft will add a new security system to Windows 11 that will protect admin accounts when they perform highly privileged and sensitive actions. Named 'Admin Protection,' the system is currently being tested in Windows 11 canary builds. The new feature works by taking all the elevated privileges an admin needs and putting them into a separate super admin account that's most of the time disabled and locked away inside the core of the operating system."

Okay, now, I'll just note, we don't know how they're implementing this yet. I mean, this sounds like more than UAC with more protection. So maybe it is. I don't know. Like maybe their intention is to make this super-duper bulletproof. Anyway, The Hacker News says: "When users select the 'Run as Administrator' option, they will receive a prompt from the Admin Protection feature. The difference from a classic UAC prompt that features 'Yes' and 'No' buttons is that the Admin Protection features will ask the user to authenticate with a password, a PIN, or some other form of authentication before they're able to go forward."

They said: "But a change in prompting authentication is not the only major change. According to technical and non-technical write-ups from Microsoft MVP Rudy Ooms, who first spotted this feature, Admin Protection is a lot more powerful and innovative than you might expect. It changes how the entire Windows OS assigns admin privileges." Okay, so that answered my question. This is not just adding additional authentication to UAC, you know, this bury it down somewhere in the bowels of Windows, so whatever that means. That's, you know, that's apparently what's going on. Changes the way the entire Windows OS assigns admin privileges.

"In past versions," they wrote, "Windows created two tokens for an admin account," right, "one to use for normal operations and one for when the admin needed to do admin things, with the user switching between the two." They finished, saying: "Unfortunately, this allows threat actors to develop UAC bypass techniques and abuse admin accounts for malicious purposes." Okay. So stated in another way, UAC, even as intrusive and potentially annoying as it was, was still too easy to use. So it was being abused, also. So Microsoft is going to give it another go, and even more robustly lock up these privileges which are too powerful to allow bad guys and bad ware to get their hands on.

The Hacker News said: "The new Admin Protection basically locks away all those highly privileged actions into a separate, system-managed account. The threat actor would not be able to switch to that super admin account unless they could now bypass all the extra authentication options. The way this will exactly work in detail," they said, "is unknown. Microsoft is set to provide more details about the new Admin Protection feature at its Ignite developer conference later this month. And we hope," writes The Hacker News, "that these extra authentication prompts will be able to support some form of MFA. If they do, threat actors that compromise admin accounts will have a much harder time exploiting those accounts for high-privileged actions."

So, you know, I suspect that the operational profile of a developer such as myself is probably very different from the typical office worker. Even having UAC constantly popping up drives me nuts, as I said earlier, since I'm extremely careful with what I do with my system, and I maintain somewhat obsessive management over my machines. So I've never felt that I really needed Microsoft to protect me from myself.

Now, at the other end of the Windows user spectrum, you know, we have someone sitting behind a desk at a large enterprise. They are probably running a fixed set of pre-approved software and logging into a "standard" rather than an "admin" account. So they would already need to provide complete administrative credentials if they wanted to change anything in the system. This still sounds like the admin privileges that the system will have somewhere, you know, because there is an account defined on a system that has admin privileges, even when the user who's currently logged in is a standard user. So Microsoft is going to, you know, much more deeply lock this down.

So all this suggests that the forthcoming Windows 11 "Admin Protection" feature, you know, is intended to better protect everyone else, you know, all of those who have been logging in with admin accounts, but for whom the "Are you sure? Yes/No" UAC pop-up has not been providing sufficient protection. So again, I can't fault Microsoft for providing options and for also, first of all, making it optional, thank goodness, although I don't

intend to be under Windows 11 control anytime soon, but also providing an option to more thoroughly lock down this security. And I was just going to say, and given that, like, a biometric multifactor authentication might be available, then that would make it tolerable. You wouldn't have to...

Leo: Yeah. Windows Hello is very secure, I think, yeah.

Steve: Yes. You wouldn't have to constantly be going over, you know, to your smartphone and getting a one-time password in order to continue doing things you want to do.

Leo: Do you run as administrator?

Steve: Yeah.

Leo: Yeah, of course you do.

Steve: Yeah.

Leo: But, I mean, that was always the advice, so don't run as an administrator, and UAC solved that by kind of having these different levels.

Steve: Right, right. I mean, I'm - Windows has become such a nanny OS that I have to turn, I mean, I'm creating brand new code; right? That's what I do.

Leo: Right. So that's inherently dangerous.

Steve: Every time, you know, yeah, and I hit - well, it's not dangerous.

Leo: No, but it looks that way to the operating system.

Steve: Yes. So I have to completely shut down Windows Defender, or it deletes my EXE the moment it gets created.

Leo: That's terrible.

Steve: Like, what's this? Boom, it's gone.

Leo: Get rid of that. Quarantine it. Get it out of here.

Steve: We never saw this before.

Leo: Get the elements.

Steve: Bang, it's gone. No, it's - so, you know, being a developer really requires you to just say, "Calm down, Windows. It's all right. It's me sitting here." So, yeah. But again, I'm glad that they're able to allow enterprise admins to really crank the security up. And clearly they're not doing this because they don't have anything better to do. They're doing it because they've seen problems with not having, you know, enough of the ability to lock things down as much as they are.

Okay. So under the category of "Who cares?" last week we noted that fine-happy Russian courts had levied such insanely large fines against Google, for refusing to allow YouTube to spew Russian media anti-Ukraine propaganda, that not only did their own spokespeople have no idea how to pronounce the number of Russian rubles levied, but the fine far exceeds the total amount of money in the known universe. Moreover, you know, the Google branch of Russia, you know, the local Google entity Russia has fined went belly-up and bankrupt about a year and a half ago. So there's no assets there, either. So good luck squeezing some rubles out of Google. I don't think that's going to happen. But it seems that Russia has not been deterred in the fining department. They apparently decided that levying a reasonable fine against a going concern might actually produce some cash, if not any change in that entity's behavior.

So to that end, a Moscow court has fined Apple, Mozilla, and TikTok for failing to remove content the Russian government deems as being "illegal." Apple was fined for not removing two podcasts, Mozilla for failing to remove some add-ons from its store, and TikTok for failing to remove videos related to the war in Ukraine. The fines range from $35,000 USD to $40,000 USD equivalents in Russian rubles. Now, since fines on that scale probably fall into the "petty cash" category for those three companies, at least there's something for them to discuss about, you know, going forward. It's not some ridiculous number with 30 zeroes that no one knows how to pronounce that, you know, Google's been hit with.

And while we're on the topic of fines, South Korea has fined Meta 21.62 billion won. Now, although it takes around 1,400 won to equal one U.S. dollar, when the fine is 21.62 billion won, that still equals around $15.67 million USD for a fine. So that's an attention-getting amount. Unlike Russia's fine for Google, South Korea actually expects Meta to pay.

Okay. So what did Meta do to upset South Korea's privacy watchdog? The fine is for illegally collecting sensitive personal information from South Korea's Facebook users, including data about their political views and their sexual orientation and - wait for it - sharing that data with Meta's advertisers without their users' consent.

The organization is called the Personal Information Protection Commission (PIPC). So the PIPC in South Korea says that Meta gathered information such as religious affiliations, political views, and same-sex marital status of about 980,000 domestic South Korean Facebook users - so just shy of a million - and then shared it with 4,000 advertisers on Meta. The PIPC said in a press statement: "Specifically, it was found that behavioral information, such as the pages that users 'liked' on Facebook and the ads they clicked on, was analyzed to create and operate advertising topics related to sensitive information."

Okay, now, actually that sort of sounds like a level or two removed, but still a breach of privacy because, you know, Facebook is analyzing their users' behavior and then drawing conclusions about who they are based on what they do, and then making the "who they are" information available to their advertisers. The PIPC added that these topics

categorized users as following a certain religion, identifying them as gay or a transgender person, or being a defector from North Korea.

The agency accused Meta of processing such sensitive information without a proper legal basis, and that it did not seek users' consent before doing so. It also called out the tech giant for failing to enact safety measures to secure inactive accounts, thereby allowing malicious actors to request password resets for those accounts by submitting fake identification information. Meta approved such requests without sufficient verification of the fake IDs, resulting in the leak of the personal information of 10 South Korean users. So just sloppy and not caring on Meta's part.

PIPC said: "Going forward, the Personal Information Protection Commission will continue to monitor whether Meta is complying with its corrective order, and will do its best to protect the personal information of our citizens by applying the protection law without discrimination to global companies that provide services to domestic users."

So for their part, in a statement shared with the Associated Press, Meta said that it will "carefully review" the commission's decision, after which it will probably get out its checkbook to pay the fine, I would imagine. So, you know, the good news is everywhere we turn it appears that the early freewheeling behavior of unaccountable Internet services is being increasingly brought to heel. If user profiling has been as valuable as advertisers claim it to be, and if this profiling is gradually being squeezed and reduced out of the population of services, that suggests that the economics of online advertising will eventually be changing, too. The advertisers don't want anything to change. They want all the information they can get about everybody all the time. And governments are beginning to say, not so fast there. We don't want you to have that. And of course governments are able to make the laws that they want to.

Our favorite NAS supplier, Leo, Synology, just patched a critical zero-click, zero-authentication flaw that would have created chaos had it been discovered first by bad guys. The flaw affected Synology DiskStation and BeePhotos and could be used for full remote code execution.

Leo: Ugh.

Steve: Yeah. It's being tracked as CVE-2024-10443 and has been dubbed "RISK:STATION" by security researcher Rick de Jager of Midnight Blue. He successfully demonstrated and exploited the vulnerability at the recent Pwn2Own Ireland 2024 hacking contest. And this one is as bad as they get. "RISK:STATION" is an "unauthenticated zero-click vulnerability allowing attackers to obtain root-level code execution on the Synology DiskStation and BeeStation NAS devices which would affect millions of devices." Now, as we know, "zero-click" means full remote takeover without any action required on the part of the owner of the device. We also know that the only way this could be possible would be if Synology Photos for DiskStation or BeePhotos for BeeStation have open and exposed ports to the Internet.

So I'll say it again: It doesn't matter how tempting and cool it might be to have roaming access to your photos and other features, available to one and all on the Internet. It doesn't matter that it's necessary to login and authenticate to use such a service. Everything we see reinforces the truism that there is no safe way to do that using today's technology, no matter how much we wish it were otherwise.

Now, the good news here is that this was disclosed during a Pwn2Own competition, so the bad guys have no idea how this was done. And in keeping with the responsible disclosure that's inherent in Pwn2Own, no technical details about the vulnerability have

been released, nor will they be soon. They're currently being withheld to give Synology's customers sufficient time to apply patches. Midnight Blue said there are between one and two million Synology devices that are currently simultaneously affected and exposed to the Internet. So, you know, easy to do; right? You just ask Censys or any of the online scanning services like Shodan, give me a list of all the IPs that are listening on this particular port. And bang, you get the list.

So as it happens I just updated my two Synology NASes. They notified me that there was new firmware available, and that presumably fixes this and other lesser problems. But I would never expose my NAS to the Internet. It's sitting behind the NAT services of a pfSense firewall that has UPnP disabled. My NASes were never in danger, and I hope and trust that that's true for all of our listeners. But certainly it's not true for those one to two million Synology NAS users who said, oh, hey, cool, I can publish photos for my friends. And, you know, what could possibly go wrong?

Leo: Somehow I doubt you use Synology's photos app.

Steve: No.

Leo: You don't seem the type.

Steve: I don't do that, either.

Leo: Neither do I, yeah, no.

Steve: So, you know, it is definitely more of a hassle not to simply be able to open ports and expose services to the Internet. I get it. You know? But that's exactly what between one and two million Synology NAS users have apparently done. There are ways to safely obtain remote access. For example, I'm a huge fan of port knocking, which has never taken off the way it could. But there are truly secure mechanisms that exist which are still not being built into our devices due to, I don't know what, programmer hubris which continues to imagine, despite all evidence to the contrary, that the last horrific bug that was just found and fixed will be the last one ever. So we don't need more security. This is what needs to change.

Okay. This is really interesting. Over on the supply side of attacks, we learn that cybersecurity researchers have discovered a nefarious malicious package in the Python Package Index (PyPI) code repository. And get this. This particular Python package is called "Fabrice." It's been downloaded tens of thousands of times over the past three years of its availability while going undetected for those three years as it stealthily exfiltrated developers' Amazon Web Services (AWS) credentials.

Now, the package's name is "Fabrice," which sounds like some sort of air freshener or something.

Leo: Yeah.

Steve: And it would be a believable package name on its own. It's actually derived from a typo of a very popular Python library called "Fabric."

Leo: Oh.

Steve: So with an "e" added to the end of Fabric. The legitimate Python "Fabric" library is used to execute shell commands remotely over SSH. But any developer who too hastily types "Fabric" into their code might instead wind up with "Fabrice," and that's where things begin to go very wrong for them. Whereas the legitimate "Fabric" package has over 202 million downloads, its malicious typo-squatting counterpart has been downloaded more than 37,100 times. Since developers trust the well-deserved reputation of the "Fabric" library, that's what they assume they're getting, even when they mistype the name and enter "Fabrice." Unfortunately, "Fabrice" is then able to exploit the trust that's associated with "Fabric" to incorporate payloads that steal credentials, create backdoors, and execute platform-specific scripts.

"Fabrice" carries out various malicious actions depending upon which operating system it finds itself running in. If it's executed on a Linux machine, it will download, decode, and execute four different shell scripts from an external server located at the IP address 89.44.9.227. When the same script runs on Windows, two different payloads - a Visual Basic Script named "p.vbs" and a Python script named "d.py" - will be extracted and executed. The p.vbs script runs the hidden Python script "d.py" which resides in the Downloads folder. This d.py script downloads another malicious executable which it saves as "chrome.exe," then sets up a scheduled task to run that "chrome.exe" every 15 minutes. Once that's been done, the d.py file is deleted.

In any case, regardless of the operating system and the path taken, the common goal is credential theft. AWS access and secrets keys are gathered and exfiltrated to that server at that address. By collecting these AWS access keys, the opportunistic attacker gains access to potentially sensitive cloud resources. Now, who knows what developer will run this, and what resources might be obtained? Since 2021, when this malicious "Fabrice" library was first dropped into the PyPI repository, 37,100 developers have downloaded it by mistake, thinking they were getting "Fabric." The first time they ran it, their machines were compromised. When they later corrected their typo, it was too late. Their development systems were already infected with a trojan designed to seek out and send any AWS credentials they might have.

So at this point, from time to time, the attacker's server at 89.44.9.227 simply receives unsolicited AWS credentials. Every time someone new shows up, the attackers probably head over to AWS to see what their trap might have snared. So we have a sophisticated typosquatting attack, crafted to impersonate a trusted library which exploits unsuspecting developers who enter the wrong library name just once. This thing sat undetected for three years, collecting more than, well, we don't know how many AWS credentials were collected, but it was installed in more than 37,000 systems and then began looking for AWS credentials before it was finally spotted and removed from the library.

Of course this begs the question, what other similar typo traps are still sitting out there, salted out among the thousands of legitimate repository packages? This is why we've got researchers scouring the repositories looking for these kinds of nefarious baddies.

Leo: And this is a continual problem in these repositories. I wish there was some easy way to fix this.

Steve: Yeah. You know, [crosstalk]...

Leo: PyPI's been particularly notorious; right?

Steve: Yup. And NPM, of course, also.

Leo: Yeah, the Node Package Manager, yeah.

Steve: It's a problem because we want public software; right? I mean, the whole idea is to create a community of people working together, publishing software packages and libraries like this, intending to share it. Well, how do you keep the bad guys out? You really can't. And Leo, speaking of good guys...

Leo: I bet you I have a product that can get the bad guys out. Let me check.

Steve: Yay.

Leo: We continue on with Episode 1000.

Steve: Thousand.

Leo: Steve Gibson's cup. I already had my mug. I'm wishing now that I had the quad venti latte that you always order. I only made a double, and it went quick. On we go.

Steve: Okay. So we've seen this one coming for a while, and we're nearing the year 2025, which is the year during which Google has said they're going to be requiring, with no excuses, all of their cloud services users, which includes all Gmail users, to be authenticating with some form of multifactor authentication.

Leo: Good, good.

Steve: Yup. It's like it's time.

Leo: Yeah.

Steve: So more than just their username and password, which will no longer cut it. Google still hasn't provided explicit deadlines, but anyone who doesn't already have MFA set up can expect to start being pushed to do so near the beginning of next year. So there's not much more amnesty for people who haven't done that yet.

Okay. So I don't know how to read between the lines of some recent worrying news from the Mozilla Foundation. Just to be clear, that's not the same as Mozilla. The Mozilla Foundation is the nonprofit arm of Mozilla. But the Foundation has just laid off 30% of its employees. Even though it's not Mozilla, it still makes me nervous since I depend upon Firefox for the web and Thunderbird for email.

The official statements from the Foundation, well, to me they sound like gobbledygook. Get a load of this: "The Mozilla Foundation is reorganizing teams to" - oh, and while I'm reading this, think about the turbo encabulator and the reverse trunions that it uses because similar language. "The Mozilla Foundation is reorganizing teams to increase agility and impact as we accelerate our work to ensure a more open and equitable technical future for us all. That unfortunately means ending some of the work we've historically pursued and eliminating associated roles to bring more focus going forward.

"Our mission at Mozilla is more high-stakes than ever. We find ourselves in a relentless onslaught of change in the technology and broader world, and the idea of putting people before profit feels increasingly radical. Navigating this topsy-turvy, distracting time requires laser focus, and sometimes saying goodbye to the excellent work that has gotten us this far because it won't get us to the next peak. Lofty goals demand hard choices."

Leo: Oh, geez.

Steve: What the hell does that mean?

Leo: Obviously they fired whoever it was on their PR team who spoke sense. Yeah.

Steve: Wow.

Leo: That's just bad PR.

Steve: What a bunch of utter nonsense.

Leo: Here's the good news. The Mozilla Foundation had more than doubled its staffing in the last two years.

Steve: Ah, okay.

Leo: So 30% cut still puts them ahead of where they were. It's also not the browser, it's their, as you said...

Steve: Right, it's their nonprofit arm.

Leo: Right, right.

Steve: Okay, good. Good, good, good. I mean...

Leo: So don't worry. You use Mozilla. Or no, you use a Chrome browser.

Steve: No, I'm a Firefox, 100%.

Leo: Oh, good. Yeah, yeah, yeah.

Steve: Yeah, yeah, yeah.

Leo: Me, too, yeah.

Steve: Yeah, yeah. I'm...

Leo: We need diversity. It's the last man standing. That and Safari are the only two mainstream browsers that don't use Chromium.

Steve: I know. And for me, my computers run cooler and quieter when I'm not running Chrome.

Leo: Yeah, Chrome is a pig.

Steve: The reason I left Chrome was that, like my fans were spinning up. It's like, what the heck, it's just sitting here.

Leo: To be fair, Mozilla has had its problems in the past with resources. But I think right now it's a pretty darn good browser.

Steve: Well, and it is getting heavy donation from Google.

Leo: Oh, yeah, 200 million a year, I think, from Google. Not donation. It's the same reason Google has 20 billion to Apple. It's to...

Steve: Right.

Leo: Yeah.

Steve: Oh, right, in order to feature the...

Leo: Default search engine.

Steve: Yes, yes. And I do use Firefox's whatever that - the home page that comes up with sponsored stuff.

Leo: Yeah?

Steve: Yeah, I do. I want to...

Leo: Support them, yeah, good for you, yeah.

Steve: Yeah, I have no problem seeing that. And every so often there's something kind of interesting. It's like, oh, what's that about?

Leo: Yeah.

Steve: Okay. So that covers the most interesting news of the week. Today is Patch Tuesday, so we don't have any results from that yet.

Leo: But count on it next week.

Steve: Absolutely. We're not sure that the number of things fixed will be two digits or three digits, but it'll be one of those two.

Leo: Yeah, it'll be in there, yeah.

Steve: So I was glad that there was not a torrent of news for today's ONE THOUSANDTH episode of Security Now! since there's been so much news recently that I've been unable to share, as I said at the top, some of the truly great listener feedback we've been receiving. So we're going to do that today. But I've got a couple things first.

Dave Plummer was an early Microsoft engineer. Among other things, Dave is credited with creating the original Task Manager for Windows. He wrote it, and also the Space Cadet Pinball ports for Windows NT. He was also the developer who added native ZIP file support to Windows. Thank you, Dave.

Leo: Hard to pick just one of those as his most important - I liked the pinball a lot.

Steve: Yes, yes, Space Cadet Pinball. So today Dave is best known for his two very popular YouTube channels. He has "Dave's Garage" and "Dave's Attic." I'm mentioning this today, first because Dave puts a lot of effort and energy into the videos he posts to his channel, and our listeners might find a lot there to enjoy. So I created one of GRC's shortcut links to make finding Dave's Garage easy. It's just grc.sc/dave. So, you know, "sc" as in shortcut, grc.sc/dave.

But the main reason I'm mentioning this is that one week ago today, Dave posted his look at SpinRite 6.1. His sub-head was "Optimize Your Hard Drive and Extend Data Life - Including SSDs - with SpinRite!" And his review of SpinRite was so positive that in the metadata info about this video he made his motivation clear by explicitly stating: "By the way, this is NOT [all caps] a sponsored episode. I'm just a 30-plus-year customer and fan of the app!"

So anyway, everyone who's been following this podcast already knows everything Dave talks about. We all know that SSDs are prone to slowing down over time when their data is only ever being read and never written, such as the file system's metadata and most of the operating system files and drivers and so forth. And early in the work on SpinRite 6.1 we discovered that running a SpinRite Level 3 pass over SSDs that had slowed down over time would restore their original factory performance. So I'm mentioning this due to two viewer comments that were posted to Dave's SpinRite video last week.

Brent Smithline said: "Have used SpinRite since the early '80s after talking with the head of support at Compaq. He stated that they used SpinRite to test hard drives before they were installed in Compaq devices. The bad ones were weeded out and sent back to the manufacturer so they did not become a support issue at the very start for Compaq."

Now, I've mentioned this anecdotally several times through the years, but it was fun to see it independently restated. And it brought to mind a useful strategy that may still be useful today. One of the things I've noticed while running drives on SpinRite is that the drive's self-reported SMART health parameters will often be pushed downward while SpinRite is running. This is one of the biggest mistakes made by all of the various - although they really don't have a choice - SMART drive health reporting tools. A drive that's just sitting there idle and doing nothing is always going to be relatively happy because it's not being asked to do any work. And it's not the drive's fault for not reporting anything since it has nothing to report. It's only when the drive is under load - by being asked to read or write data - that it's able to gauge its own ability to actually do that.

For the past 35 years this has been one of the fundamental tenets of SpinRite's value: A drive can only determine that it has a problem when it's asked to go out into its media and attempt to read or write those regions. The fact that in a sense it "owns" that media doesn't automatically mean that it knows everything about what's going on out there. It needs to be asked to go take a look. And it turns out, today's SpinRite can still be used the same way that Compaq once used it, to help qualify the relative integrity of spinning hard drives and SSDs.

Another interesting comment that was posted there, among 756 others since last Tuesday, was by Seagate's ex-Chief Technologist, Robert Thibadeau.

Leo: Thibadeau, yeah.

Steve: Thibadeau. In addition to being Chief Technologist at Seagate for years, Robert is also one of the six founding directors of Carnegie Mellon University's Robotics Institute from which he resigned in order to guide Seagate's development of, among other things, self-encrypting drives.

In response to Dave's SpinRite video last Tuesday, Robert posted. He said: "As a Chief Technologist for Seagate for years, SpinRite is generally done right. There are some errors in Dave's presentation, but they are minor. The biggest thing that needs to be said is that if you wish to retain digital data" - and Leo, you're going to love this - "plan to keep essential data on multiple drives that do not depend on each other."

Leo: Very good, yeah.

Steve: He said: "RAID is not a solution except for transactional data management or in disk duplication mode." I think he means full mirroring.

Leo: Mirroring, yeah, yeah.

Steve: He says: "And always keep a full dated copy or two air gapped, meaning not connected to anything electrical." He said: "Safe deposit boxes are useful for this. And plan to make new copies on new drives every few years." He said: "Digital storage devices can fail in more ways than you can count, and the ones that can preserve data for decades are really not commercially available and often give a false sense of security leading to catastrophic data loss. The design life of storage devices is generally five years, although it's not unexpected that a given device will preserve storage for 10 plus a few years.

"Knowing what I know, I buy new drives every year or so and make new full copies, as well as keeping at least a couple of copies air gapped all the time. Lightning can, and does, strike. Fire," he says, "(heat) demagnetizes. And it is not true that solid state drives are non-magnetic and susceptible to failures associated with magnetic field losses." So anyway, I wanted to share those two...

Leo: Is that true?

Steve: Well, I mean, you'd have - you'd stick it in an MRI machine, and that would hurt it.

Leo: Yeah. I mean, you can't, like, degauss an SSD with a magnet or anything like that.

Steve: No, no. They are electrostatic as opposed to electromagnetic.

Leo: Yeah. But they're still sensitive to changes in the electrical field.

Steve: You'd have to hit them with a serious pulse. But I appreciated Robert's reminder about the inherent volatility of mass storage. Back when I first designed and wrote SpinRite, you, Leo, and I had 10, 20, or 30 megabytes of spinning hard drive storage.

Leo: Oh, and we thought we were fat. We thought...

Steve: Oh, we were fat. Well, because nothing was big back then. So 30MB, that was, you know, I'm never going to fill that up.

Leo: I take single photos that are bigger than that now.

Steve: Right, exactly. So, you know, and those drives cost us thousands of dollars.

Leo: That's right, yeah.

Steve: That price dropped rapidly, but it was still uncommon for anyone to own more than their system's primary mass storage drive. That's why SpinRite's data recovery was designed to work "in place," because back then there was nowhere else for recovered data to go. That's one of the many things I am very excited to be changing as SpinRite continues to evolve in the future. And thanks to the ongoing support from this podcast's listeners, and the greater SpinRite community, as well as independent influencers and reviewers like Dave Plummer, it appears that SpinRite will have a bright future. Nothing, truly nothing could make me happier because there's nothing I will enjoy more than continuing to work on SpinRite to move its code forward.

Leo: Yay. Yay.

Steve: But I just wanted to mention that I'm always made a bit nervous when I get the sense that people are carrying around single copies of important data on today's thumb drives or external drives, you know, in their laptops or desktops, wherever, where there may not be any other copy of that data. Drives are certainly becoming more reliable as time goes on. But there's also a danger in that since, as Robert reminds us, lightning does still strike. So the fact that drives are generally not dying left and right can lull us into a false sense of security of believing they never will. With today's data storage being so economical, it might pay off to take some time to make backups automatic and transparent.

And that's really where I'm headed here. Automatic is the key. It's the main point I wanted to make. Everybody's busy. We get distracted. We naturally forget to do things that don't call for our attention. That's why it really makes sense to find some time, if you haven't already, to arrange to have the data you care about kept safe for you without you needing to remember to do anything at all. These days, with storage being so inexpensive, that doesn't have to be expensive. I mean, almost free, in fact. The best case is that nothing bad will ever happen, and that your backup system will never be needed. But even then, the peace of mind that buys, of knowing that the system you put in place will have your back, I think is worth the time and trouble. So I just sort of wanted to take a moment to say, really, don't have a catastrophe. There's just no reason.

Leo: Yeah, good advice.

Steve: There's no reason to have a catastrophe any longer.

Leo: I think some things have changed since Dave was working at Seagate. For instance, cloud storage is very, very common. Almost everybody I would imagine listening has at least one copy of their data in a cloud somewhere. It's so cheap. It's so ubiquitous.

Steve: Oh, my god. And now Microsoft is like dunning you in...

Leo: Yeah, OneDrive just comes with - yeah, yeah. And so that's a little annoying, to be honest. But Apple does the same thing with iCloud. I think that most people probably have their most important stuff in the cloud. And, you know, you mentioned the Syncthing, which I think is a great solution.

Steve: Yes.

Leo: I just have everything synchronized everywhere.

Steve: Yes. Yup. Okay. One last bit before we get to our listener feedback. I mentioned last week that my mailing system's "instant unsubscribe" feature had turned out to be a bit too "instant," since many of our listeners were being repeatedly silently unsubscribed from the Security Now! mailing list. The trouble was caused by some email providers. And this is a known issue I had never encountered, but I had heard of it. They attempt to protect their listeners from malicious links in email by following those links, pulling up the content they point to, and then checking it for any sort of malice.

So it's not a bad idea, though it certainly does make email a lot more trackable, since many savvy users will deliberately not click anything in spam they receive as a means of remaining invisible because they don't want to give any indication that, oh, you know, they've got a live one here on the end. So the issue of trackability must have been a trade-off that these providers decided was worthwhile.

In any event, the system I had in place until a few hours ago last week, a few hours after last week's podcast, when I said I was going to fix it, the system I had in place would assume that requesting the content behind the "instant unsubscribe" link was the user clicking it, so it would do as requested and instantly unsubscribe them. So I wanted to affirm that I did, in fact, change the way the system functions so that links now display an unsubscribe confirmation page that's actually very pretty. And you can click on it, and then just to see what it looks like, if you're curious, and then just don't proceed to give it the additional click of "yes, I'm sure," because that's now what's required. So henceforth, everyone should now remain properly subscribed.

If you were not among the 12,656 listeners who received today's podcast topic summary, you know, the Picture of the Week, the show notes link and everything, in an early morning email, you may now resubscribe to GRC's Security Now! mailing list, you know, GRC.com/mail, and subscribe. From now on, if you do that, all subscriptions should be "sticky" and remain in place until and unless you choose to later unsubscribe. So I'm done with the email system. As I mentioned last week, it's now very easy to change your email address anytime you want. Users can do that. This last glitch is gone. This mailing to 12,656 of our subscribers went out beautifully this morning. So I am now, I actually already have turned my attention to my next project, which is to create this next DNS Benchmark. So I'm very excited to get going on it deeply and get it done as quickly as I can.

And Leo, let's take our last break, and then we're going to look at some listener feedback for the final half-hour of our podcast.

Leo: Excellent. Excellent. One thousand episodes, kids. It's amazing.

Steve: Wow.

Leo: And by the way, I wish you had a list of all of the sponsors we've had over the years. It all started with Astaro, you remember, way back.

Steve: Yup, and Alex is still listening.

Leo: Alex Neihaus is still a listener. Thank you, Alex. I get regular emails from him. Probably it's not a thousand sponsors, but it's been quite a few. We're very grateful to all of them because it makes the show possible. We are, like the Mozilla Foundation, dependent on your support with Club TWiT and of course on our advertiser support.

Steve: Yes. They think, wow, this really makes sense to advertise on this podcast.

Leo: It does. It does. I mean, who else, what better place to tell the world about your security product?

Steve: Okay. So Paul Walker asked: "Hey, Steve. Just listening to Episode 999 and your piece about AI to find/fix/prevent security vulnerabilities. I'm sure you're right. It'll be a great tool for developers. But I wonder if it'll just become the next arms race in the field? Couldn't bad actors deploy AI similarly to find vulnerabilities, and all we're going to end up with doing is raising the bar of complexity, picking off more of the lower hanging fruit as the vulnerabilities just become more obscure and harder to find by humans? Is there even a danger that a bad actor wielding AI might have an advantage for a while as they turn this new generation of powerful bug hunting tools loose on all the old (current) software that's already out there?

"Don't get me wrong, it should be a good thing, assuming the overall balance of power between good and bad doesn't shift too far the wrong way. But I fear your hope for a world of 'no vulnerabilities' still isn't much closer. Congratulations on reaching 999, and thank you for going past it. Here's to the next thousand episodes. Thanks, Paul."

So yes, Paul. I've had the same thought. I agree that AI could just as easily be used to design exploits for the vulnerabilities that already exist or that will exist. And I also agree that the inertia lag and upgrade friction we keep seeing throughout our industry is likely to mean that malicious AI will initially find itself in a target-rich environment.

So, yes, I agree 100% that things may get rough during the phase where AI is still newly being deployed by both sides. But there is an important lack of symmetry here. The good guys will have an advantage in the long run because no malicious AI, no matter how good it is, will be able to create vulnerabilities out of thin air. All a malicious AI can do is find problems that exist. It cannot create new ones. So once the good guys have their AIs working to starve the bad AIs of any new vulnerabilities to discover and exploit, the game will no longer be an arms race. There will be a winner, and that winner will be the good guys. So, but certainly an interesting point, and we are in for some interesting times.

And also speaking of AIs, Mathieu from Montreal, Canada, he said: "Hi, Steve. I might not be the first person to share this snippet of code with you, but I thought you'd find it useful. I asked ChatGPT how to remove YouTube Shorts. Initially, it suggested plugins. But since I have security concerns about plugins, I asked it again, this time specifying that I wanted a solution using only uBlock Origin. Here's the solution it provided, and it works great."

Okay. So now I've got it in the show notes. Basically ChatGPT, to its credit, created a three-rule filter which, you know, you go to uBlock Origin, open the dashboard, click the "My filters" tab, and then paste - its actually six lines because it's got comments for each

of the lines. Paste those in, click apply changes. Anyway, he said it worked. He said: "This approach has worked perfectly for me," he said, "and I thought you might find it handy, too. Let me know if you try it out. Best regards, Mathieu from Montreal."

Okay. So as I said, and as he wrote, Mathieu from Montreal found that this worked for him. But a listener named Darrell, a man of few words, sent just a link to a GitHub page. And it's GitHub dot and then I have the link in the show notes. It looks like gijsdev/ublock-hide-yt-shorts. So I followed that link and was taken to a page that said: "A uBlock Origin filter list to hide all traces of YouTube Shorts videos." He said: "This filter list might work with other content blockers, but I haven't looked into that yet." He says: "Copy the link below, go to uBlock Origin > Dashboard > Filters and paste the link underneath the 'Import...' heading." So that's very cool. Under uBlock Origin there is an Import dot dot dot. You can give it a link, and it will suck the list in for you.

So anyway, I used WGET to grab the LIST.TXT file referred to in that link. It's an extremely comprehensive, well-commented, 71-line filter. Although that includes blank spaces and comments, lots of comments. I would be quite surprised if anything resembling a YouTube Short was able to squeak though that gauntlet. Then I discovered where Darrell found his GitHub link. He sent me another piece of email with a link to a piece on Medium where a software developer explains.

He said: "As a software engineer, I typically spend eight to 10 hours daily on my laptop. Following that, I frequently indulge in YouTube Shorts, which, combined with my extensive screen time, has started to negatively impact my eyesight. Despite recognizing this, I found myself too addicted to simply stop. Hence I decided it would be better not to see any Shorts on YouTube at all. That's when I discovered my savior, uBlock Origin. uBlock Origin is a Chrome extension that not only blocks ads on YouTube, but can also stop YouTube Shorts, which I hope, in turn, will save me more time. Here are the steps to follow." Okay. And then he provides a link.

Actually, he copies a bunch of stuff into his Medium posting. At the bottom he provides a reference. It turns out that this software engineer is also not the originator of this filter list. As I said, at the end of his Medium posting he links to the YouTube video where he presumably learned about uBlock Origin and found this filter.

So first of all, we've confirmed my suspicion from last week that uBlock Origin all by itself, which can obviously function as a Swiss Army knife for web content filtering, could probably nip this YouTube Shorts problem in the bud without the need for any sort of possibly sketchy additional web browser add-on, which is what brought this whole topic to the podcast; right? Remember that somebody had a YouTube Short blocker, and it became owned by somebody who started using it to track all of its users around the Internet. So we were saying, hey, do you even need an add-on? Why not just uBlock Origin? So sure enough.

But I was still unclear about what all the hullabaloo was over this so-called "YouTube Shorts problem." What's the problem exactly? Why are people creating web browser extensions to hide these? So I followed this software engineer's link to the YouTube video where "Chris Titus Tech" tells us how to do this. I did not watch Chris's video, but some of the - and I kid you not - 8,423 comments that have been posted to his explainer over the past 10 months since he posted this video, which has been viewed 1.6 million times, were quite illuminating. So here's a sampling.

For example, people said "The fact that people want to disable Shorts, and there are developers that create these amazing tools, really goes to show how crap Shorts really are."

Somebody else said: "What's wrong is YouTube themselves keep pushing Shorts on people. It's a form of spam and should be something you can opt out of. Unfortunately, opting out doesn't work within the YouTube platform. I hate Shorts, and I hate the way YouTube is going."

Someone else said: "Thank you for the tip. It's a lifesaver. YouTube Shorts are cancer."

Somebody else said: "Alternate title: 'How to cure YouTube's cancer.'"

Somebody else wrote: "My child can't stop himself once he starts watching them. I have to step in. He even tells me he wants to stop watching Shorts but 'can't,' which is terrifying. Knowing this will make a huge difference in our lives. Thank you."

Finally someone said: "Dude, I literally cannot thank you enough for this. I'm currently trying to really focus on my studies, but Shorts have been my DOWNFALL [all caps] literally." He said: "I just get so addicted to it, and I feel like I physically can't stop. Once I realize how much I wasted doing nothing, I feel empty and dumb inside. So glad this is a thing, and it works great. You're a lifesaver. Thank you so much."

And the last comment: "Could you please make a shorter version of your video?" Okay, I confess that I made that last one up. But, wow! Whatever this is, it really appears to have people in its grasp. It's somewhat astonishing. But these reactions to the posting of Chris's extremely comprehensive YouTube Shorts content and how to block it using uBlock Origin answers the question of why anyone would want to remove these from their browser. So also apparently from their life, in addition to from their browser. So anyway, we know you can use uBlock Origin. The show notes have lots of links, and one to a very comprehensive filter list for anyone who feels like a lot of these, you know, 8,000-plus people who discovered Chris's list do.

Tom Damon said: "Steve, I ran into this on LinkedIn about last week's Photo of the Week. Just thought I would let you know. 'Here's How a Bunch of Firemen Created a Viral Image That Fooled the Internet.' That was the title from Business Insider." He said: "Thanks. Been listening since Episode 1. Tom Damon."

Okay, now, Tom is actually referring to the week before last's photo for Episode 998.

Leo: Oh, this is the one where the train tracks...

Steve: Yup. The insane one showing the fire truck's hose crossing the train tracks while being protected by tire protectors, as if that would do what was intended for the wheels of a train. Right?

So Tom linked to an article in Business Insider. Unfortunately, it was behind a paywall which placed a firm pop-up covering the page in my face and refused to allow me to proceed. But I was quite curious to see what Tom had seen. So once again, uBlock Origin to the rescue. I simply disabled JavaScript for the site.

Leo: Yeah, that site is really hard to get to. I'm glad to know I can do that. Okay.

Steve: Yup. Refreshed the page, and no more popup blocking the page's content. So I can tell you that Business Insider wrote: "If you spent any time on the Internet over the past few months, there is a chance you saw a photo of firemen who had found a foolproof way to lay a hose over train tracks. The photo went viral, being shared all over

Twitter and Facebook. Insane; right? Not quite. The photo was actually a joke. Firefighter Tom Bongaerts from Belgium took the photo at the beginning of April, posting it to Facebook. The caption says something like: 'Fire early this morning. Our hoses are still protected from the train!'"

But that track was down that week for repairs. Those in town presumably Tom's Facebook friends knew that the photo was created and posted for laughs. There was no chance a train would be coming. But soon, hundreds of people were sharing the photo on Facebook, adding their own commentary. People who didn't know Tom, or about the defunct train track, began to see the photo and, in disbelief, share the photo themselves. After his picture was shared hundreds of times, it eventually became separated from its original source and from its sarcastic caption. People believed it was real. Stories like the one about how a train was derailed began going viral, as well. Several days later, after tons of tweets, shares, and email forwards in lots of languages, Tom wrote a follow-up post explaining what happened.

It says: "Hey, this past week our funny photo went viral throughout the whole world. Thousands of shares and likes in many different countries! Once and for all: The picture was taken in Belgium, in a small village called Bornem. After a minor intervention, we had some" - meaning a minor intervention meaning some firemen-related activity - "we had some time left near the railway to make this picture."

Leo: Oh, boy.

Steve: "Since there were no trains running at all for a week due to maintenance works, we can state that our joke was a real success."

Leo: Oh. And now, many years later, still fooling people on the Internet.

Steve: So a big "thank you" to our own Tom, our listener Tom Damon, for resolving this mystery for us. It's good to know that those firefighters were aware that either their scheme would not actually survive a train, or that any passing train might not survive their scheme. Opinions among our listeners who sent feedback about the photo differed widely about what might transpire if the integrity of that crossing hose solution were ever to be tested.

Paul Northrup wrote: "Dear Steve. In regards to the new DNS Benchmark offering, will there be versions for other operating systems - Apple, Linux, BSD? Thanks." Okay. Fifteen years ago, when I first wrote the DNS Benchmark, I took great pains to make sure it would run perfectly under WINE, and it does, beautifully. So I'll definitely be preserving that functionality anywhere WINE can be used with the DNS Benchmark. And as it turns out, all three of those non-Windows OSes that Paul mentioned - Apple, Linux and BSD - are POSIX-compliant and can and do run WINE. So while it won't run natively, it will be possible to run it on any of those platforms in addition to Windows. So got that covered.

Jim Riley poses an interesting question. He writes: "Hi, Steve. Thank you for being here for Security Now! every week. You and Leo make a great podcast. I have a question about AI which is a bit philosophical. A comparison of answers between Gemini, ChatGPT, and Copilot shows the systems can disagree on basic facts such as who won the 2020 presidential election."

Leo: Well, there is disagreement in general on that one. I don't know why.

Steve: Uh-huh. And that is exactly to my point, Leo. He says: "Gemini refuses to answer the question. This sounds like Big Brother, and Google has anointed itself the Ministry of Truth, deciding what facts it will suppress or reveal. Having our access to knowledge regulated by corporate overseers is disturbing. How can AI be trusted if it withholds facts? Do you think a control system should be installed in AI that will prohibit AI from withholding the truth? Regards, Jim."

Okay. This is an aspect of AI that I suspect is going to be a real issue. My wife and I have grown to know the neighboring couples within our little community enclave quite well. Lorrie enjoys socializing, and since she lets me work every other minute of the day, I'm happy to join in. What I know, because I've grown to know our neighbors, is that I could ask each couple the same question and obtain a different answer from each, sometimes radically different answers. And their intelligence is not artificial, though in some cases it may be questionable.

So I suspect we may be asking a lot of AI for it to be some sort of absolute oracle and truth teller. And moreover, the truest answer may not be a simple binary yes or no, true or false. I believe in the fundamental rationality of the universe, so I believe there is an absolute truth. But I've also observed that such absolute truth is often extremely complex and colored by subtlety. Many people just want a simple answer, even when no simple answer can also be completely true. In other words, they will choose simplicity over truth.

Having come to know our neighbors, I have also come to understand their various perspectives. So when they share what they believe, I'm able to filter that through who I know them to be. I know we would like things to be easier and more straightforward with AI, but I see no reason why it might be so. Whether we like it or not, what we've going to get from AI will just be another opinion.

Leo: Hmm. Couple of things I would add to that.

Steve: Good.

Leo: First of all, the AI didn't give him or refuse to give him the answer. The coding did because everybody - Google, Meta, everybody except Elon Musk on Grok, has a bunch of bumpers put in to keep it from answering controversial questions. That's just a human saying, no, no, no, if it says this, don't answer it. The AI would give you an answer. I don't know what the answer would be, but it would give you an answer. The other thing I would say is this is exactly what Timnit Gebru, Margaret Mitchell, and others who were working in Google's ethics department at the time, until they were fired for this, said in a paper called Stochastic Parrots, where they talked about the problem with AI is, because it's coming from a computer, people give it more weight. They assume, oh, it's a computer, so it's smart, so it's going to be right. And that's of course a mistake.

Steve: Right.

Leo: And really, if you ask the same AI the same question several times, it will give you different answers each time. It's designed to do that. So, yeah, it's more a

question of us understanding, and I think the term "artificial intelligence" is part of the problem, understanding what it is we're playing with. And it's not intelligent at all.

Steve: Well, and we've been using the term forever. You know, when I was in high school I was at the AI lab at Stanford University. Well, [crosstalk], you know, yeah. And so, like, okay, that's nothing like what we have today.

Leo: Although, you know, it's really interesting, I just read an article, a really good article about Fei-Fei Li, who was one of the early researchers, who believed in neural networks. And this was 20 years ago. And the entire AI community had said, nah, you know what, we've tried. They don't work. And she persisted, spent two years inputting something like 20 or 30,000 images into it, and created an image recognition program that worked.

I remember we interviewed the people at the University of Toronto when I was up at Call for Help in Toronto about this image recognizer. This was what inspired Geoffrey Hinton and others later to continue on with the AI, in fact using neural networks and other techniques that we see today. So even as AI weathered, there were people out there who had ideas that made sense and worked, but for a variety of reasons didn't get a chance to try it out. It's been an up-and-down thing. There are people who say today, a lot of people seem to know what they're talking about, AGI is close, like within a few years.

Steve: Yeah, actually I think that's our topic for next week.

Leo: Is it?

Steve: Yeah.

Leo: Oh, good.

Steve: Yeah, because Sam Altman has just gone on record.

Leo: He's a hype master.

Steve: I know, but there was enough meat in the discussion that I thought it would be interesting to share that.

Leo: Good. I've been dying to hear what you have to say about this. Oh, I can't wait. I'll look forward to that.

Steve: So John Torrisi, or, wait, John Torrisi...

Leo: Torrisi.

Steve: He said: "Hi, Steve. As someone who's been in security for over 20 years, I have found myself constantly overthinking anything that would result in lowering security which could lead to a breach or intrusion. As a keen home automation tinkerer I have numerous devices" - he sounds like you, Leo - "probably over 100..."

Leo: Yup.

Steve: "...at home for controlling everything from lights to fans to monitoring solar, et cetera, et cetera." He says: "All partitioned off, of course, with VLANS, multiple firewalls, separate SSIDs, et cetera. One of my biggest conundrums, though, is how do I expose the controller - for example, Home Assistant - to the Internet so I can access it when traveling around. I have a fixed IP, so that's fine. But I really don't like exposing this type of software directly to the Internet. At the moment I connect using OpenVPN. That's fine, but this means I need to turn it on and off every time I want to do something, which is a pain. I have also thought about an overlay network but need to research a bit more on data usage as it will be used primarily from a mobile device and hence limited data.

"Anyway, going back to the main thread, I know security by obscurity can be somewhat effective in a layered approach, so what are your thoughts on using an IPv6 address rather than IPv4 for inbound traffic in these scenarios as it's much harder to do full network scans across IPv6 address space compared to IPv4. Long-time listener and SpinRite owner from Australia. Keep up all the great work you, Leo, and all the team do over there at TWiT. Thanks, John."

Leo: Thank you, John.

Steve: So the problem John has is, as we were talking about earlier with Synology, is a problem many people are having. This is why those one to two million Synology Photo sharing services were exposed, are currently exposed and vulnerable. Hopefully they're getting patched. No one appears to have created a solid solution for this because developers keep believing, as I noted before, that they've just found and fixed the last problem that they're ever going to encounter. So, you know, right, sure, go for that. What we still need is a clean and efficient means for remotely accessing the devices within our networks at home when we're out roaming.

So John's wondering about the security of hiding his devices within the larger 128-bit address space afforded by IPv6. He clearly understands that such a solution is only offering obscurity at best. So I suppose I'd say that doing that would be better than doing nothing. But that also requires IPv6 addressing support at both ends. And the trouble is that it's not as if he gets to pick any 128-bit address at random from all possible 128-bit addresses. ISPs are allocated well-known blocks of IPv6 address space, and they generously hand out smaller blocks of 64K (16 bits) of IPv6 addresses per subscriber. So it would still be possible for bad guys to target any ISP's range of known addresses and scan across that space. Given the massive scanning power of today's botnets, discovering open ports located within an ISP's assigned IPv6 space would not be prohibitively difficult.

John mentioned the use of an overlay network such as Tailscale, ZeroTier, or Nebula. I think those solutions are about as close to the perfect user-friendly solution as exists today. They all support all major desktop and mobile platforms, as well as popular open-source routing software such as pfSense, OPNsense, and others. So an instance could be installed in an edge router to provide extremely secure connectivity to any roaming

devices. Or if you prefer, Docker can be used to install, for example, ZeroTier on a Synology NAS. Once you have an instance of one of these terrific solutions running on something at home, you can have secure connectivity to that network from any roaming laptop or smartphone. And there's no indication of excess network bandwidth consumption since all of these solutions are economical in their overhead.

And the way they work is exactly what you want. You simply have that client running on your smartphone. And when an app you have wants to connect to, for example, Home Assistant, presumably you use a web browser, and you give it your home IP, or maybe you have DynDNS set up so that your home IP has a public DNS, you go to that DNS: and the port number, and the traffic that is routed to your home only goes over the overlay network. I mean, it is, like, it is the perfect solution. It's, you know, not everybody's going to use it because, you know, it's the kind of thing that our listeners will use. It's not as simple as, you know, Synology saying, oh, look, now all your friends are able to browse your photos, you know, that you stick in a public photo sharing folder or whatever, using your home NAS. That'll never be safe. But it is definitely possible to use an overlay network like Tailscale, ZeroTier, or Nebula to successfully get what John wants.

Alan, our last bit of feedback, said: "Steve. Congratulations on 1000 episodes of Security Now!." He said: "I listened to the first episode during my first year of college for Computer Science, while donating blood plasma for money to buy a second monitor."

Leo: Wow. That's dedication.

Steve: "Now, I am a Senior Software Engineer at Google, where I have been for nine years."

Leo: Nice.

Steve: "I've listened to every episode within the week it came out. Your podcast was at least as useful to my understanding as my bachelor's degree, and in many cases your early podcasts helped me understand that material in my classes much more deeply. Thank you for all your years making Security Now!. Alan."

Leo: That is so beautiful.

Steve: And so to Alan and to all of our many listeners who have recently written something similar - and I actually have something else that just came in this morning I'll share next week that was really, really wonderful - I wanted to say, as we conclude this 1000th episode of Security Now!, that providing this weekly podcast with Leo has been, and I'm sure shall continue to be, my sincere pleasure. As I've said before, I'm both humbled by and proud of the incredible listenership this podcast has developed over the years. It has been one of the major features of my life, and I'm so glad that you, Leo, thought to ask me, 20 years ago, whether I might be interested in spending around 20 minutes a week to discuss various topics of Internet security. Just look what happened!

Leo: Oh, my goodness.

Steve: So thank you, Leo, for making this possible.

Leo: Oh, thank you, Steve.

Steve: We'll see where the next thousand will take us.

Leo: I just provided you with the platform, and you took it from there. It's been really amazing. Our web engineer, Patrick Delahanty, posted some statistics about the show. He said the shortest show we ever did - do you remember this? We did like an extra thing that was three minutes, I think. It was like an update of some kind. I can't remember why, but we had to do an update for some reason. So I guess that will always be the shortest show, or that there wasn't a whole lot in it. I'm looking, trying to scroll back, see if I can find his post. And then he said the longest one we did I think was close to three hours, was two hours and 57 minutes.

Steve: Wow. I didn't know that we actually - I thought that week or two ago was - that was two and a half hours, and I thought that one was the...

Leo: Well, there's always the outliers. You keep it to two hours pretty nice. I think that's good.

Steve: I think that's a target. I think that's a reasonable time. We've got a couple listeners who complain, "I don't have two hours to spend." It's like, well, okay, so...

Leo: Don't listen to the whole thing, then.

Steve: Yeah.

Leo: Nobody's making you. It's not like you have to. My attitude's always been give people - usually, you know, you're supposed to give them less than they want. And my attitude towards podcasting is, as long as it's longer than your commute, that's - you don't want it to end halfway to work.

Steve: And we know how people feel about those YouTube Shorts. We don't want to be accused.

Leo: There you go. We don't want to be Shorts.

Steve: Unh-unh.

Leo: No. We're Longs. Yeah. In the early days of TWiT I tried to keep everything under 70 minutes because people were burning the shows to CDS, and that was the maximum length of a CD; right?

Steve: Yup.

Leo: I don't worry about that anymore, as you probably know. I think we are now, on almost all of our shows, two hours is the shortest that I do. Almost all of them are 2.5 to three hours. So you actually have the honor of hosting our shortest show. Congratulations.

Steve: And dare I say most focused.

Leo: Yeah, very focused, and we love that. It is easily the geekiest show we do. And I say that proudly. I think that we, you know, we try to serve a broadish audience because I don't want people to say, oh, I don't understand anything he ever talks about. But at the same time we also want to serve the hardcore person who really gets this and really wants to know deeply what's going on.

Steve: Well, and we do have listeners who write and say, well, I think that I understand about 15% of what you guys talk about, but I like it. I'm not sure what it is, but it makes me feel good, and I always get a little something. It's like, okay, great.

Leo: Yeah. That's okay, too. I mean, I've often thought of what we do as aspirational. There's a good documentary about Martha Stewart on Netflix right now. It's actually fascinating. I would watch it even if you're not interested in Martha Stewart. But people said about her and her magazine, nobody can live that way. Nobody can be that perfect. You're setting too high a bar. She says, "It's aspirational." Everybody might want beauty in their life and want to be able to have that. Everybody wants to understand what's going on in the world of technology. And if you don't understand it all, you will. Just keep listening; right?

Steve: Yup.

Leo: Steve, it has been my great honor to know you and work with you for more than 30 years. I can't believe it's been 30 years. It doesn't...

Steve: I know.

Leo: Doesn't feel like that at all.

Steve: And that's the good news. Because, you know, we're only at a thousand.

Leo: Yeah. Look, we're going to keep doing this as long as we can. But I am so honored and thrilled that you were willing to do this way back then and continue to do it. I know it's a lot of work. I'm very aware how much work you put in.

Steve: It's a lot of work, but I'm happy to do it.

Leo: Yeah. Here's Patrick Delahanty's note. I found it. The shortest episode of Security Now! was four minutes and 12 seconds. That's this one, Security Now! 103-SE. Vote for Steve. Do you remember that? That was you were trying to win the podcast awards.

Steve: Oh, right, right, the podcast awards.

Leo: And I think you did; didn't you?

Steve: We won the first several years of podcast awards.

Leo: Yeah, yeah. Well, and rightly so. And then the longest episode, and I have the receipts to prove it, three hours and 57 seconds, but it was a Best Of. So you don't have to take credit for that one.

Steve: Ah. Thank goodness. I can't imagine I would have participated in that. I would have been on the floor.

Leo: Yeah. Well, the reason was there were so many good sections, segments in 2018, we couldn't do less than three hours.

Steve: That's neat.

Leo: Yeah. So that's good. That's fair. I think that's okay. Steve, thank you from the bottom of my heart for continuing on. I would have been bereft sitting here on this Tuesday afternoon without a Security Now!, and I know I'm not alone on that. So thank you for all the work, so much work every week.

Steve: There's no end in sight. They used to be saying, our listeners were saying "To 999 and beyond." Now I think it's going to be "To 1999 and beyond."

Leo: Oh, how about 9999? How long would that take? 200 years?

Steve: Yeah. I'm feeling great, but as I said, I do believe in a rational universe.

Leo: Well, but wait. Maybe, we're laughing now, but somebody in the future will be listening to AI Steve.

Steve: That's true.

Leo: And Episode 10,000.

Steve: I'm sure you could dump all the transcripts into an AI and say, "Okay, give me the last week's news as Steve would present it."

Leo: Exactly. Totally. You could probably do that now.

Steve: Probably could do that now.

Leo: But certainly before we're done with the second 20 years. Steve, bless you, thank you.

Steve: Thank you, my friend.

Leo: We are all eternally grateful, and we will see you next week.

Steve: On to 1001. Next week. Bye.

Copyright (c) 2014 by Steve Gibson and Leo Laporte. SOME RIGHTS RESERVED

This work is licensed for the good of the Internet Community under the Creative Commons License v2.5. See the following Web page for details: http://creativecommons.org/licenses/by-nc-sa/2.5/