SECURITY NOW!

Transcript of Episode #519

The Win10 Privacy Tradeoff

Description: While Leo and I await the revelations from the ongoing annual Black Hat and DefCon conferences, the fallout from which we will doubtless be dissecting during upcoming weeks, we keep current with other security news and events. We then examine the change of philosophy embodied by Microsoft's Windows 10 and its many controversial spying "features."

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-519.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-519-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. Lots of security news. We will cover that. And then Steve's going to run through the privacy settings on Windows 10, tell you what they all mean and why he will never use it. That's coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 519, recorded Tuesday, August 4th, 2015: The Windows 10 Privacy Tradeoff.

It's time for Security Now!, the show that protects you. And, boy, there's never been a more important time for Security Now! than right now. Steve Gibson is here. He is our security guru at GRC.com. And I could go through his credentials. He was the first person to discover spyware, right, the first antispyware tool. He's had his own lovely battles against DDoSing and others. And for the last 10 years...

Steve Gibson: Yeah.

Leo: It's going to be 10 years. It's going to be the start of our 11th year in a little bit.

Steve: Yup, exactly, yes. So this is Episode 519. And of course we've been very good about never missing a year, or never missing a week. I think we did once. So, but obviously at Episode 520, that would be 10 times 52 weeks a year. So we're definitely in the - we're in the vicinity now.

This was supposed to be a Q&A, only inasmuch as we haven't had one for a couple weeks. But the press went so bonkers over the "spying," to use the generic term, that is the default set of settings in Windows 10, that I thought, okay, let's take a look at this. Windows 10 released the day after last week's podcast, on Wednesday. And so I titled this "The Win10 Privacy Tradeoff" because, you know, this podcast we focus a lot on security and its close cousin, privacy. And I had a very sort of a much more relaxed take on this. I've studied what Windows 10 does. The good news is no one will ever make me use it, which is fine. You know...

Leo: You mean you'll never use Windows 10?

Steve: Oh, I hope I never do. The good news is that Windows 7 is supported through 2020, all the way through this next president's first term. So I figure by 2020, maybe there'll be an alternative. At that point maybe it'll be time for me to switch over to Linux or over to Mac. But Windows 10 has nothing for me. But we'll talk about that.

Leo: Wow.

Steve: So that's sort of my introduction to...

Leo: So you're not going to use Windows 10 until President Trump retires?

Steve: Or gets reelected for a second term.

Leo: Okay. Oh, good, okay.

Steve: Assuming that impeachment is off the table.

Leo: That's interesting. You know, and I've gone both ways on this one. And what I'm really curious is what capabilities we can determine that Microsoft has to spy on us. The truth is, if you're using the cloud, even with Windows 3.11, you're using the cloud.

Steve: Yeah. So, yes. So I really view this as a tradeoff. And this is something that our listeners are really, I mean, there's no better audience to discuss this with because there are people who are installing TrueCrypt on their drives, knowing that it's no longer supported, but that as far as we know, from its examinations and audits, it's secure. But they would not use the built-in BitLocker that - is it BitLocker?

Leo: Yeah.

Steve: BitLocker, that Windows makes even easier to use. They're not going to do that because they just don't trust a system that's built in. And similarly, they don't want to use IE, which comes with Windows. They want to take responsibility and use Firefox or Chrome, depending. So my take, and we'll get to this in a second, is that Windows 10 shows a new philosophy. I mean, and it's more of a catch-up than anything else. It's Microsoft catching up to sort of the iOS model with ads in apps and sort of curated. There's now a Windows Store. And also sort of the Google model of everything is cloud, and the browser is your viewer. So anyway, we'll get into that.

Right now, Black Hat and DefCon are underway. And we've already talked about a couple of the stories that are being fully illuminated during the conference - the Jeep hacking with Chrysler and the StageFright breach, the MMS problem. I want to talk about that a little bit. There's some more news about that from Android. So I imagine next week and the week after and in forthcoming weeks, I've scanned through the program, and there are some other really interesting-looking things where we just don't have enough information yet. The Jeep hacking and the StageFright issue sort of escaped and got strong press coverage. And we had enough information about them that we were able to talk about them. We're going to have to wait until most of these presentations have been given, and then we'll be able to choose the goodies. So I think we'll have no problem finding some really interesting new things to talk about.

Leo: You're going to come on The New Screen Savers on Saturday.

Steve: Yes, on Saturday.

Leo: And give us an update. So that'll be something to tune in for.

Steve: Exactly. We will just be post-conference at that point. So I want to talk about some news about StageFright. There's a worrisome DOS vulnerability affecting the Internet's DNS server, BIND. One of our sponsors, PagerDuty, suffered a database breach. OS X has a somewhat worrisome zero-day in the wild. But being a privilege elevation bug as opposed to a remote execution, it's, again, we sort of tamped down the hysteria on this one a little bit. I want to talk a little bit about NoScript versus Sandboxie because I'm experimenting with Sandboxie now, and I'll explain why. And some miscellaneous stuff, and then some discussion about Windows 10. So I think a fun podcast.

Leo: Good, good, good.

Steve: So, okay. We need to talk about StageFright because at this point, as of this morning when I looked, there is no indication that anyone has patched it. And in fact some particularly clueless providers have said, well, you know, it's not being exploited, so we're still looking at it. Well, the fact is, it is in the wild. The exploits for StageFright have appeared in some exploit kits. And so we need to talk a little bit about mitigations. What can we do in order to - until we get this thing fixed, what's the solution? And that's one thing we didn't discuss last week. And the good news is it's not super difficult.

So just to recap a bit, the problem is with some sort of pre-parsing that occurs whenever an Android phone, and that's from Android 2.2 on, receives a multimedia message, an MMS text message or media message. There are, like, six different problems that were discovered by someone looking at the code who is giving a demo right now as we speak at the Black Hat conference about how to do this. They have stated they will release proof-of-concept code after the conference. So that's really what I'm excited for because

I think that's really what we need in order to get this thing - in order for people to understand what's happening.

So the idea is that your phone receives a deliberately specially maliciously crafted MMS message, and that allows the sender to execute their own payload with strong privileges, I think it's system-level privileges, which is one step shy of root level, basically it can do everything it wants to, on the Android device. So I'm definitely on the lookout for the proof-of-concept code. I almost plowed into these exploit kits to dig around, but I'm sure we're going to get this next week. And this is a big enough problem that there's no reason for me to do this redundantly. I imagine the industry will be responding. But somehow...

Leo: I hope they do. I mean, it's...

Steve: Yes. Yeah. Okay, so essentially the problem is that the default settings, both for hangout and for messages on Android, are auto-retrieve. And so without you doing anything, your phone is retrieving and parsing MMS messages. Essentially what you need to consider is that MMS messages from someone you don't know and trust should be viewed with some caution. So, but you can't have your phone open them and process them automatically. So essentially you simply need to, first of all, I mean, number one rule is make sure you're running the latest firmware, that your phone is current and up to date, because if this gets fixed you're going to need an over-the-air update in order to have this patched, assuming that your provider starts doing that.

And again, this to me seems like a huge opportunity for hackers. Notice that, prior to the disclosure, the exploit kits already had this. Meaning that all that was necessary was for there to be any indication that there was even a problem here, and immediately this got exploited. And as we said, it's just shy of one billion total phones, on the order of 950 million phones are believed to be vulnerable. So, you know, this is a big carrot dangling in front of the bad guys.

Anyway, so bottom line, make sure you're keeping yourself updated. Then you want to disable the auto fetching, both for hangout and for messages. And I'm sure that our listeners know how to do that. For hangout you go into Options, Settings, SMS, Advanced, and then you will see "Auto retrieve MMS." Just turn that off. And then, under messages, it's under More and then Settings and then, I like this, More Settings. And then you'll see Multimedia Messages, and there it says "Disable auto retrieve." And so just turn those off.

Now, what that means is that your phone will no longer, obviously, automatically beam these down and parse them. But that's the only mitigation we have for the moment. And we'll keep an eye on this. We'll let everyone know if there's suddenly a raft of exploitation which ramps this up. At this point, there have been vulnerabilities found in the wild. So we absolutely know that it is being exploited, probably at this point in limited targeted attacks. We would sort of expect that, I mean, the one thing you need is somebody's phone number in order to send them one of these. So on the other hand, the phones tend to be allocated in blocks of phone numbers. And so in the same way that the Jeep, all of these various Chryslers could be scanned because they knew what IP range they were in, so could MMS messages be spewed to a bunch of phone numbers that are known to be offered by a vulnerable carrier.

Anyway, to me this is still very much at the front of our radar. And for listeners who want to take the appropriate measure, just telling your phone "don't pick up my MMS messages by default" is the way to do that.

Leo: CyanogenMod has fixed that in the most recent versions of CyanogenMod.

Steve: Good.

Leo: Has Google fixed it, do you know, in 5.1.1?

Steve: Yes. Yes, they instantly patched theirs. And but the problem is...

Leo: So if you're using an up-to-date Google phone, a Nexus phone, you're all right.

Steve: Right. And probably mostly, I mean, as we know, the problem is that carriers tend to abandon their older phones.

Leo: Yeah.

Steve: Yet these older phones are going to be vulnerable. So I think, I mean, I don't want anything bad to come of this. But we really do need something to get carriers to belly up to the bar and take some more responsibility. I know that there's some legislation that Congress has been talking about as a consequence of these problems to motivate carriers to do more, to take responsibility for the older property which they have sold. I mean, these are connected computers. And we know that we're finding that they have the same kind of security problems that all of our connected computers have always had. Unfortunately, despite everyone's best efforts, we keep having code that's a little bit more porous than we wish it were.

Leo: I do wish there were some place you could go to see if your phone has been upgraded.

Steve: That's what we need. Someone will do it. And as I said last week, make sure that I find out about it through Twitter as soon as a service exists. If I weren't in the middle of SQRL or SpinRite, I would just drop everything and do it because - although I was thinking about it, too. It's a little tricky because you don't want to create a service that will - certainly nothing that anyone would do would be malicious. So they'd be delivering a benign demo payload. But you don't want to allow that service to be abused just to, like, harass people.

So I guess you'd need to do something like your phone - you'd need to send a text message from your phone to this particular service so that it got your phone number. And then it would echo back or maybe, like, prompt you to hit Yes if you want to receive a test message, and then it would send it to you. That's, you know, doing it right would be a little more involved.

But that's what we need. We need mostly to spread the word and get people to put pressure on their carriers. We need a demo of it. We need some way for this thing, the equivalent of how, on Windows, when you have a Flash exploit, they make the calculator app pop up on your desk, which Flash should absolutely never be able to do. It's like, whoa, there's the calculator. Now, that could have been, you know, anything we wanted it to be. But so it drives the point home.

Leo: Oh, lord.

Steve: Yeah. Anyway, I'm excited when we get a proof of concept. Maybe these guys will do this themselves. They're corporate mobile phone security. They generated a huge amount of attention for themselves. I've been keeping an eye on their website. And, I mean, this has been good for them, and I think they deserve it because they brought a potentially bad problem to light. It'd be great if they were able to bring up a demo that anyone could use to verify that, whoa, look at that. That shouldn't have happened. I need to get this fixed.

Okay. So also in the news has been a new problem with DNS. We haven't had any problems with DNS, boy, you know, for years. Of course, GRC has a spoofability page which I created after Dan Kaminsky demonstrated that the port numbers that were being allocated by DNS servers were sequential, and that that created a huge vulnerability for spoofing DNS. And so I created a system for GRC that allows people to check the DNS servers they're using, the DNS servers that are resolving their own IPs for them, for the quality of the way they're working to see how spoofable their DNS server is.

We've got a new problem, though. And what's interesting about this is that the people who have dug into this equate this in some ways to OpenSSL. The Internet's primary sort of granddaddy DNS server is BIND. And it's called BIND because what it does is it binds a domain name to an IP address. That's what it does. It creates the binding between something, www.amazon.com and whatever Amazon's IP list is.

The problem is that, exactly like OpenSSL, everything that anyone has ever thought to do with DNS, they implement in BIND. It's like the armature on which you hang all of your DNS experiments, in the same way that OpenSSL is the armature on which you hang all of your experiments about secure point-to-point TCP connections. And as a consequence, for example, this is why, whereas OpenSSL has hundreds of thousands of lines of code, Amazon has written - and this is something that we covered while you were away, Leo. Amazon has written their own little TLS implementation in 7,000 lines of code, which they're using on their AWS services. And they note that the reason for this massive, many hundreds of thousands of lines disparity is that OpenSSL, it's the Swiss Army knife for, I mean, it's got certificate stuff and communications stuff. And every little experimental feature that anyone ever wanted to implement is there.

The same is the case with BIND. And what happened is, what was discovered was that there's something known as a "transaction key record," which is part of the protocol for BIND servers to talk to each other for establishing secure keying between servers. And the discoverer revealed it responsibly, meaning that the problem was found, and it was fixed and offered and made available in BIND before it was disclosed. So we couldn't ask for anything better than that except that there's an awful lot of DNS servers on the Internet. And not everybody's keeping them up to date. And so anyone can update their version of BIND. And what they get is then somebody is unable to simply send their server, which is by definition publicly available - that's what DNS is for, it's a public DNS server - send it a deliberately malformed packet and crash it.

And so that's what this does. This crashes DNS servers. There has been no mention of this thing going any further into some sort of a deeper exploit. And it already is patched, as I said. The problem is that servers are now being crashed all over the Internet. The news of how to do this has gotten loose, and anyone who has a publicly exposed - I mean, there are internal DNS servers. In fact, GRC runs one. My DNS server, and I'm running BIND, it's the slave for the two big-iron Level 3 servers. So, and mine is not available to the Internet. There's no visibility to GRC's DNS. Instead, I use Level 3's as slaves to mine. And that is a perfect example of the fact that publicly exposed DNS servers don't need to have all these features.

What the old school DNS and Internet gurus have said of this vulnerability is the problem is BIND has gotten old and huge. It is the kitchen sink for DNS. Like I said, it's the standard repository for all experiments. And it's carrying them all. But the fact is a really scaled-down minimal feature DNS server could easily do 99.99 percent of what a DNS server has to do, be much smaller, be much faster, and not start exposing these sorts of problems which arise from the thing's age and just crazy feature set.

So one of the things I think sort of generically that we're seeing, stepping back from this particular instance, is these original tools, like BIND, like OpenSSL, they're beginning to sort of collapse under their own weight. They're getting old. The code is old. They have been and are sort of the common central store for each of their own set of functionality. But what we're beginning to see is replacements, you know, scaled down, leaner, meaner, faster rewrites that reimplement the same functionality, but because they're small, make them are more auditable. You know, you can't audit OpenSSL's, you know, 500 or - I forgot what the number was now. But it was like it was hundreds of thousands of lines of code. Only a smaller portion had to do with TLS, despite the fact that it's pulling this whole library around all the time, regardless.

So anyway, so it's sort of interesting to see that this is what's going on with the Internet is these really original big platforms are starting to have problems. And people are saying, you know, it's just not such a big deal to recreate some of this core technology and bring it current and use more modern languages that perhaps give us more control over vulnerabilities and also take this opportunity to only retain the features that we need to.

Okay. Also in the news, PagerDuty suffered a breach. And from what they said, it looked to me like they did, I mean, their architecture was as good as any we could ask for. The company acknowledged that they saw evidence that an attacker gained unauthorized access, they said, "to our users' names, email addresses, public calendar feed URLs, and hashed, salted, and peppered passwords." And in fact in my show notes I...

Leo: They said "peppered"?

Steve: Yes.

Leo: They have a good sense of humor, I have to say.

Steve: Well, I said, "PagerDuty not only salts their passwords, they pepper them, too." And that was the title of this topic in the show notes. And I said, "How do we know?" And so they wrote: "Based on the investigation, the attacker bypassed multiple layers of authentication and gained unauthorized access to an administrative panel provided by one of our infrastructure partners. With this access, they were able to log into a replica of one of PagerDuty's databases. The evidence indicates that the attacker gained access to users' names, email addresses, hashed passwords, and public calendar feed URLs."

And then they said users - oh, and they sent an email to everyone announcing that they had suffered this problem and instructing people, erring in favor of caution, change your password, which is the standard security wisdom. We went through this when LastPass saw suspicious traffic on their network and said, whoa, this looks wrong, we're going to err in favor of caution. Everybody should change your password. So PagerDuty...

Leo: So this is similar to the LastPass situation, where...

Steve: Yeah.

Leo: Yeah.

Steve: Yeah, where they have no in-the-wild, no zero-day, no reason to believe anybody has done anything, but they found evidence that somebody got in and accessed this database. So they said: "Users who do not reset their password by Monday, August 3rd" - that's yesterday - "at 12:00 p.m. Pacific Time will be automatically logged out of the website and will receive an email prompting them to reset their password."

Leo: Good. That's the right way...

Steve: So they're going a step further and saying, look, we're kicking you off. You need to do this. However, I got a kick out of this. They said: "We use robust hashing techniques to protect passwords. If you have logged into your account anytime this year, your password is hashed with Bcrypt" - and that's one of the industry standard strong PBKDF2, password-based key derivation functions, which deliberately thwarts all of the fast hash attacks - "with a work factor of 10, using a per-user randomly generated salt and a site-wide pepper." Thus the term "pepper."

Leo: So this is not a joke. There is this real thing called "pepper."

Steve: Yes. And so they said: "Older passwords were hashed with SHA-1 over multiple rounds and using the same salt-and-pepper approach." So what they did was they were always doing multiple iterations. Previously they were using an iterated SHA-1 hash, but still using per-user salt and per-enterprise or per-site pepper. And the point is that the pepper is a secret. The idea being that, if you got the database, the salt prevents you from doing a mass reverse-engineering of, like, all of their database's hashes by making it a per-user salt. The pepper is not stored with the database. So it's an additional secret which really rules out anyone's ability to do anything unless they're able to obtain the pepper. And they said: "Both the salt and pepper are 40 characters long and randomly generated." So this gives us, although they didn't want to give us in this fashion a sneak peek into the way they're protecting their users' data...

Leo: Sounds pretty good.

Steve: They're state of the art, yeah. You couldn't ask for anything better. And they've notified everybody and are forcing a password change.

Leo: You could ask for one thing better - not to get hacked in the first place.

Steve: Yes, exactly.

Leo: Minor, minor thing.

Steve: Yeah. And in fact, when I was thinking about the whole Win10 thing, I was thinking, you know, Microsoft is never in the news with major breaches of their network. And in fact the big guys typically aren't. I mean, like the really big guys, you know, Google, Microsoft, Apple and so forth. So on one hand, people are upset, there are people who are upset that there's all this cloud aggregation and cross-platform synchronization and blah blah blah, and we have to trust them and all that. But at the same time they're proving themselves responsible keepers of this material.

Leo: Well, and you have to figure that Microsoft's under attack constantly.

Steve: Yeah.

Leo: I mean, that would be the crown jewels.

Steve: Yeah. And in fact it's almost better to have a longstanding history of that because it gives you an opportunity to tune up your defenses and have them being tested all the time.

Leo: Right.

Steve: So also in the news, there was a zero-day bug which has been found. I don't know if I talked about it last week. Maybe I didn't because the news was it had not yet been exploited, and it had already been patched in the forthcoming beta. And I think that it sort of slipped under my radar because we already had plenty to talk about. But now we've moved into it being a zero-day, meaning that it has been found in the wild. What this is, though, this is not a user-does-nothing remote execution. This is a password bypass. So that's the nature of the privilege escalation is that a way has been found for bad software that does get loose on a Mac - and that is 10.10.4 and the beta of 10.10.5. Both are vulnerable. If software does manage to get onto your machine, it doesn't need - it's bypassing the standard "we must have your password to install this" isolation. And so that it's able to get past.

On the other hand, what has been found is that, as we know, this would be part of a chain of exploitation that might begin with a browser exploit. And then this would get called into play in order to get this thing into your system without having to perform some social engineering of some sort in order to get you to believe that you're installing something that you're not, for example.

Because this is a zero-day, and 10.10.5 is vulnerable, there's some expectation that Apple may patch this in the beta of 10.10.5 rather than waiting for 10.11, which is in beta also and has this fixed. So this indicates that Apple - and it's been fixed, it was fixed, like, when the news first appeared, it was already fixed. So Apple knew about this, but was probably thinking, no, it's not a horrible problem, and there's no evidence that it's being exploited, so we can wait.

Leo: Apple knew about it because it had been revealed to them. And so what happened with this is this researcher revealed it to the public, a different researcher than the one who discovered it.

Steve: Ah, okay, good.

Leo: So he said, "I'm not going to wait anymore," or whatever.

Steve: Thumbing their nose at proper disclosure.

Leo: It's convenient. Black Hat's going on, you know.

Steve: Yeah, yeah. Okay, so I have to say that I'm experimenting with abandoning NoScript.

Leo: I'm - uh - gasp. I know you're waiting for me to gasp. Gasp. Say it ain't so, Steve.

Steve: I was waiting for that, yes.

Leo: Why? Well, why, Steve?

Steve: I've made such, I've made so much fuss and stink about scripting over, I mean, that's my number one mantra.

Leo: And I have always said, "Oh, get over it." But go ahead.

Steve: Well, what I think has happened, I mean, because I've been using NoScript for years, and I preach it, and Giorgio and I talk from time to time. There's something that NoScript does which SQRL just tripped over a couple weeks ago, and so Giorgio and I were able to exchange email, and he showed me how to allow NoScript to allow this thing that the SQRL client was starting to need it to do. And so, and he listens to the podcast, and so he knows that I'm a fan of NoScript. The problem is there has been, I mean, this is the only way I can explain it, is I've recently been covering, the last few weeks, our own listeners, who have been coming back to us and me saying, gosh, Steve, you know, this is really a pain. And what I have found is it is really a pain. But it wasn't a pain a year ago.

Leo: What?

Steve: It wasn't a pain a year ago.

Leo: I am shocked. Shocked.

Steve: You know, for example, I'm seeing unique gibberish dot CloudFront.com. So, like, CloudFront is now a big CDN providing content. Lots of sites are using it. And it's providing a random-looking DNS for themselves. I'm sure they've got some fancy DNS that is resolving that into a particular IP for that customer. Who knows? But what's happened is there has been, I mean, I've been talking about this explosion of scripting. And the problem is, it's just incredibly annoying to have to go through multiple iterations of allowing scripts to run. So I'll enable the main page. And then, in the main page's JavaScript, that's now invoking 20 more different domains. And so it's like, oh. And so it's like, okay, which ones do I have to turn on in order to get this page to go?

And my point is there has been an explosion, unfortunately, in the last year, in scripting. And so I'm experimenting now with Sandboxie. I want Firefox to be wrapped in something, but it's just not practical. I'm sorry, Giorgio, but I'm going to try going without NoScript. But I still would like some protection, some good extra belt and suspenders. And so I just wanted to mention to people, I contacted the Sandboxie people. My license, actually my version was no longer valid. And when I tried to use my old license, they said, oh. This only has five digits. You know, you've got to get a fancy shiny new one.

So anyway, I got that. And I'm in the process of sort of getting to know it. When I created my show notes for the podcast, I do that in Google Drive, and then I export it as a PDF. And I thought, ooh, what's going to happen now, because I've only been using it for a couple days. And so it showed me my normal PDF destination, which is outside the sandbox. And so when I said, yeah, I want to save this over here, I got this wonderful little prompt that said something is trying to be saved outside of Sandboxie. Do you want to allow this or not? And it's like, oh, this is a good thing. So I said yes, and it went to its normal place.

So anyway, we covered Sandboxie years ago [SN-172]. You could probably google "Security Now! Sandboxie" and find the podcast where I talked about it. We did a whole podcast on it because it is, as I mentioned when I talked about it recently, in the last couple weeks, SandboxIE, as in Sandbox Internet Explorer, was where it started. And it has then blossomed. And installation was easy. It knew that Firefox was my default browser. It put it in its sandbox all by itself and just started working. So anyway, I will report after a few more weeks on how I'm doing with it.

But I did want to just acknowledge to people who may have been suffering the same script-blocking fatigue that I have been. It's just, unfortunately, the tool that I have used for years and liked is just becoming too big a problem. Not only is there just too much scripting, but sites have become utterly depending upon it.

Leo: Yeah.

Steve: Many sites used to work with scripting disabled.

Leo: Almost universally, the people who had the most problems with our new TWiT page were people who were listeners to the show using NoScript. And, you know...

Steve: Sorry.

Leo: I don't know what to say, you know, the site's not going to work if you block JavaScript. Admittedly, there's a problem. I mean, everybody uses it. And admittedly there's a problem because a lot of sites load JavaScript from third-party sites. That's very common. And not only is that slow and big and bloated, but it's risky. I understand. The truth is, part of the problem, I just watched a great - in fact, I should give you a link to this - a great presentation from Alan Kay, one of the premier computer scientists in the world.

Steve: Alan and I are good friends.

Leo: You know Alan Kay?

Steve: Absolutely.

Leo: He's my personal hero. I have never seen a talk by him at which I wasn't deeply inspired.

Steve: He is one of the true geniuses of the early PC era.

Leo: And an Apple fellow today, and one of the guys who worked at Xerox PARC and was, I don't know, but I imagine, present at the "demo to end all demos" and all of that.

Steve: He was also - he was head of Atari's research.

Leo: Right.

Steve: And in fact he discovered the light pen. And he introduced...

Leo: Ah, that's how you know him.

Steve: He introduced me to the Atari people because he said, "Okay, we have to have this."

Leo: So he said something - this is a great talk. He gave it to the University of Illinois at Urbana, the National Supercomputer Applications Center there, which wrote Mozilla, which wrote, I mean, that's where Marc Andreessen was when he wrote Mozilla. Are you frozen on me? I think he is. He has faded away. I'll continue to talk while we get him back. And one of the things he said is we have not made forward progress, we've made backward progress with web browsers. And he challenged the grad students there to rethink - and this is in 2009 - the browser. He said, if you were going to design - what's happened, of course, is people have just built on what was done. He said Mozilla was a terrible idea to begin with. It's a shame that Tim Berners-Lee hadn't seen the work that Doug Engelbart and others at PARC had done 20 years earlier when he invented the World Wide Web. He reinvented the wheel and didn't do a good job of it. But he said, if you wanted to rethink the browser - there we go. Steve's back. You hear me now?

Steve: Yeah.

Leo: This is the important part. If you wanted to rethink the browser, how would you do it? Clean slate. And the students thought about it. I think they kind of came up with the idea. He said you'd write it like an operating system kernel. What you don't want to do is extend the local browser with all these plugins and codecs and all this crap. That's just a broken system, and that's what we do right now. But at the same time, you want to design a browser that is able to handle all sorts of new, unpredicted stuff. And then there's this security issue which is, of course, you've got to find a way to isolate the code that's running over there from your system. But he says you can do this. This is well known. This called writing a kernel. The browser should be, in effect, an operating system kernel which allows additional processes to be run remotely or locally, but totally sandboxed for security.

Steve: And that's Google. That's the Chrome model.

Leo: So the guys who did this, Google bought. He quotes a brilliant graduate student, I can't remember where he was, who wrote a paper that describes exactly this. Google hired him. He had a startup. They bought the startup. And I think it's exactly the point of Chrome OS, is how can we build - let's rethink the browser, and let's build it so that it's secure. And that's why each tab on the browser is sandboxed. And I don't know how effective it's been when you put it on a normal operating system. But certainly in Chrome OS it's very effective, I think. It's very secure.

Steve: Right.

Leo: And so that obviates the need for NoScript, if you have well-sandboxed processes running; right?

Steve: Yes, exactly. And, I mean, the expensive, in several ways of doing this, is a full VM, to create a virtual machine with its own OS, and that you use for browsing. And you could even do a state save so that nothing is kept. When you restart that VM, it reinitializes to the same state. Sandboxie, what Sandboxie does is it hooks all of the applications' means of communication. Windows apps, at the end of the executable file is a series of jumps which are dynamically patched to be entry points to the DLLs, the Dynamic Link Libraries that provide the OS functionality.

And so, for example, I take advantage of that. I have code for GRC's net engine, my web server extension. I want to make sure that I don't have any memory leaks. So I have - the net engine itself reaches down and hooks, essentially, alloc and free, and expands the allocations and puts guard bands at the beginning and ending so that I can tell if I overwrite or underwrite. Whenever I release the memory, it verifies the pattern in the guard bands, and it tracks all of my allocations so I can see whether I'm forgetting to free anything.

Anyway, the point is that it's possible to hook existing functions for various purposes. Sandboxie reaches into whatever app you have put in the sandbox and hooks all of its communication, like file reading and writing, registry reading and writing, remote procedure calls and the works, it hooks them all and essentially redirects them to a clone of the existing set of resources. So when the browser reads something, it allows that to go through and read it from the OS. But when it modifies something or writes something, that change or write is sandboxed.

Essentially, it creates a copy of the original resource that doesn't allow the modification to actually be made globally. So what you're able to do is you're able to wash those changes away or selectively say, ah, you know, these things I want to then update globally. So it's sort of a poor man's, I don't mean to denigrate it, I mean it's a less expensive in terms of resources solution for protecting against any kind of exploit.

Leo: If you can help me get Alan Kay on a Triangulation, I'd be thrilled. And if you want to, folks, view this video, which I highly recommend, search - it's on YouTube. Just search for YouTube "Normal Considered Harmful." That's the title of his talk that he gave at a university.

Steve: Great talk. And how long ago was that?

Leo: 2009.

Steve: Okay. I have a good friend who will no doubt have stayed in touch with him. I haven't talked to Alan for years, but we spent a lot of time together. So I'll see if I can track him down.

Leo: Man. If, folks, you want to be inspired, he gave talks that were like TED talks before TED talks. They were a little longer and a little less polished. But, boy, the ideas in them are incredible. And I always just feel like it was a kick in the head when I watch his talks.

Steve: Yeah. He's one of the true pioneers of, like, deep computer science.

Leo: Yeah, yeah, really good.

Steve: Yeah, I mean, he's the father of Smalltalk, one of the first languages where everything is an object.

Leo: It's really good. He starts the talk. He's talking now, remember, to - these are high-level graduate students at one of the best computer science schools in the world. And he starts the talk. He says, "Can you name these three scientists?" And it's Newton, Darwin, and Einstein. Of course everybody can. Then he shows five computer scientists, some of the most important, the guys who've changed this business. And can you name any of them? And these are computer scientists.

Steve: Nope. Right?

Leo: None. Including Doug Engelbart. I think some people knew Doug Engelbart, but they thought that his key contribution was inventing the mouse. It's a good talk. Anyway, sorry, didn't mean to interrupt, but I watched it this morning, and I was so excited by it.

Steve: It's great. No kidding, just this morning?

Leo: Well, you know, I don't know if you ever look at Hacker News. This is YCombinator's kind of Slashdot or Digg. It's people submit stories and vote them up or down. One of the things I like about it, I check it all the time, like more than once a day, is sometimes old stuff gets posted and surfaced. And this is obviously a six-year-old talk. But then people look at it, and they go, yeah, thumbs up, thumbs up, thumbs up, and it rises up to the top. And it's a really good resource, if anybody wants to kind of geek out. It's geek news. It's very geeky news. Lot of programming language stuff and so forth. It's, I think, let me just check real quickly, I think it's news, yeah, news.ycombinator.com.

Steve: Yeah, actually I think I have some links from them later on in the notes.

Leo: Hacker News is it.

Steve: Hacker News.

Leo: I love it, yeah.

Steve: So I did run across an interesting new podcast distribution system. Somehow Security Now! I think is being pitched to them. Anyway, it's PodCall.io, which is an interesting concept. They're wanting to use a telephone. And so you would call a phone number, and then I think you run through a little keypad switch, you know, it says press 1 for this podcast, press 2 for that podcast, and so forth. But the idea being that, rather than subscribing to podcasts, or as an alternative, if you're away from whatever your podcast source is, you're able to - they don't support very much. I think they're just getting themselves launched. But the people who told me about it said they're pushing to get Security Now! picked up by these guys. I don't know what that means, but I just thought I'd put it on everyone's radar.

Leo: An issue I have with it, this comes up every few years, we don't get counted. I don't care because so few people use it, it doesn't matter. But to do a service like this, they have to download the podcast, store it on their own network, and then serve it to the public. So it counts as one download.

Steve: Oh, oh, okay. So they would cover the ads, but it wouldn't be...

Leo: Well, I think the ads would get heard, but we wouldn't know how many people used the service.

Steve: Ah, okay. Then in that case...

Leo: If it's convenient, do it.

Steve: ...forget what I said.

Leo: If it's convenient, do it, that's fine. This comes up a lot.

[Crosstalk]

Steve: ...don't have any...

Leo: Go ahead?

Steve: Sort of alternative podcast aggregators.

Leo: No, phone. Calling a number and listening to a podcast.

Steve: Oh, no kidding. Oh, I've never heard it done.

Leo: Every couple of years somebody writes me.

Steve: Ah, okay.

Leo: Yeah, I don't know why this - I guess if you didn't have any bandwidth. Seems like bandwidth is more plentiful than minutes.

Steve: Yeah.

Leo: But anyway.

Steve: Yeah. And I did get a nice note, middle of last month, from Jeff Lunt in Evanston, Illinois. He said: "Hey, Steve. Huge fan of the Security Now! Podcast. Listener since Episode 1." And then our standard "blah, blah, blah." He said: "I've been a fan of regularly backing up my data since my first major data loss at the age of 19." Now, we don't know how old he is today, so we don't know how long ago that was. But major data loss when he was 19. He says: "And while I've lost a drive or two in my time, I can't offer one of those 'really saved my bacon' kinds of testimonials because, since that first data loss, I've always had a backup for my truly important data. That said, I've also always been frustrated with disk utility tools built into OSes when something like SpinRite is the only thing that really does the complete maintenance and recovery job.

"I recently bought a copy of SpinRite to fix some of the drives in my media server, and just wanted to drop you a line and say thanks for the awesome tool. While storage is cheap, and it's easy to replace a dead drive," he says, parens, "(assuming you have a good backup) and go about your day, I just like the idea that I don't have to throw out a drive just because CHKDSK in Windows, or fsck in Unix/Linux, or Disk Utility on Mac can't do anything useful with it. SpinRite is a great piece of work, and the stuff you're doing with Security Now!, I think, qualifies you as a great human being on the whole. Keep up the great work." So I think that qualifies you as a huge fan, Jeff. Thanks very much for the testimonial.

Leo: That's awesome. That's great.

Steve: Okay. So I'm sure this comes as no surprise, no huge surprise to our listeners. I'm still, I mean, right now, the machine in front of me, I'm looking at five big screens, and I'm running Windows XP. Because for me, an operating system is a tool. It's my working device. I mean, it's what I use to, like, it's where I spend my day. And so I sort of see this distinction as, you know, are these tools or toys? And Windows as an operating system, I load applications into it. It provides the applications with a place to live. It allows me to manage my files and lets me run apps. I mean, that's what it is. It is not itself - it sort of is not an end in itself.

And Microsoft has done really nothing since, like, what, Windows 98, to change that. You load apps, and you manage your files, and you run applications. You know, that's it. But again, I recognize that's not everybody. I was running, until a year and a half ago, GRC's website was Server 2000, Windows Server 2000, because it was fine. It ran for years, literally three years, I think, at one point, without rebooting it, because I had dialed it in. I had shut down everything unnecessary. It's wrapped in layers of additional security so its own security wasn't a problem. But I started getting these really bad marks at SSL Labs because it didn't support the latest TLS protocols.

And so I jumped to Windows Server 2008R2 in order to step up and be able to support the latest protocols. Which I acknowledge is important. But I'm happy that I got 14 years of use out of that operating system before I had to make the move. And I sort of feel the same way about my own operating system. That is, XP's not supported, of course. Gee, still works fine. Firefox is being maintained; Chrome is being maintained. I've got Firefox in a sandbox, as I mentioned. I'm not downloading crazy apps all the time and running them. That isn't my mode. This is a working operating system for me.

And nothing Microsoft has done since this has given me any reason to move except it's now getting a little old. You know, 64 bits is becoming important. This is 32 bits, and so the 4GB of memory, and of course Windows famously only really is able to use three out of that four due to architectural limitations. So I'm sort of thinking, hey, you know, Chrome would be more feasible if I had a 16GB machine rather than 4 because it takes up a chunk of my memory when I start Chrome.

So I got into Windows 10 early and had it, I was set for the fast cycle update. And over the last couple months I was staying current with it and looking at it. And when it all settled down, I then spent some time. And I came away feeling very glad that Windows 7 is being supported through 2020. I expect that probably after I get SpinRite 6.1 launched will be a good time for me to finally move from XP to Windows 7. But I won't be going to Windows 10. Not because - well, okay. I was going to say, not because there's anything wrong with it. Except it...

Leo: Well, wait a minute. There is, obviously; right?

Steve: Well, yeah. It doesn't offer me anything I want.

Leo: Right. But you would be happy with a command line operating system; right?

Steve: Yes, yes. I'm...

Leo: Okay, let's be very clear here.

Steve: Yes.

Leo: The Start Menu does you no good.

Steve: No. In fact, it's in my way.

Leo: Yeah.

Steve: I look at that, and I think, okay, you made the things I want to do harder for me to do. It's less accessible. And what I want is not the OS to be an end in itself. I just want it to give me access to my programs. And I don't see that Windows 10 - and this is my point. They didn't write it for me.

Leo: You should have written your own, Steve. Come on.

Steve: Well, maybe somebody will skin it. Because I'd like to have, if there's better innards, then that would be a good thing. If they could skin it so that it didn't get in my way. It just, to me, poking around in there, it's just like, wow. I don't want to use this. Like I tried to turn on, I did turn on file extensions. And looking at the browser, well, I get this ribbon full of Sesame Street icons rather than menu options. It's like, what? Okay. You know, this is for Jenny. This is not for me.

Leo: It's for normal users.

Steve: Yeah, well, it's for - yes, I think you're right.

Leo: You're a developer.

Steve: I would agree. I'm a developer.

Leo: And you primarily use it as a server; right?

Steve: Well, I use it as an operating system.

Leo: Oh, oh, okay.

Steve: See, the operating system used to be something that ran applications. Now it's a Disneyland fairy park with flipping tiles and stuff coming in and out. I mean, it's just ridiculous. You know, sort of...

Leo: It is kind of a Disneyland. You kind of have a good point there, yeah.

Steve: Yeah, I mean, it's - and again, the Internet has happened, and we're connected. And I got very unnerved when it wanted me to log in with my Microsoft account.

Leo: Yes, yes.

Steve: And it's like, whoa, wait a minute. I have a really secure password. Now it's disappeared, and now I log in with my Microsoft account. And I took it, I removed that and went back and it worked okay. And then I thought, well, you know, Steve, come on. You have to have the experience, so go ahead and do this. And of course what that does is that's the glue that allows your different instances of Windows 10 to synchronize themselves in the cloud so that things like the new browser, the Edge browser, tabs and open pages and things, follow you around. And when you go to a different machine and log in with yourself there, it sort of is able to - that stuff follows you, thanks to its connectivity.

So first of all, I completely get it that Windows 10 is not for me. I'm not the target audience. They lost me back when I had all I needed, which was just get out of my way and let me run apps quickly, without having to navigate through, I mean, and I started to pull things down onto the tray so that I could get to them more easily. And, I mean, so, yeah, you know, if I had to use it, then maybe. But the good news is I've got five years before the OS that I will probably move to, which is Windows 7, in order to go 64 bits, and I'll probably - god knows how many gigabytes of RAM I'll load it with because, if I'm doing it, I'm doing it. And I'm sure I'll use Windows 7 well past its expiration date, just as I have used XP, probably very happily. And then, who knows. That'll have given Windows 10 some seasoning time, and maybe they'll have skinned it.

But, okay. So we're dealing with an audience which is probably more sympathetic to that point of view, my point of view, than the typical Microsoft customer. And Leo, you are probably more aware of this than I am. I do remember seeing that in the first 24 hours Microsoft reported 14 million installs or downloads or whatever, however you would call it, upgrades.

Leo: Yeah, 67 million after three days.

Steve: Okay. And do we know where they are now? I mean, is it still just probably cranking along.

Leo: What do mean? No, they're all in a toxic hell stew. A certain number of them may well have rolled back. You have 30 days to roll back to your previous version, if you took advantage of the free upgrade. But I think most of us, and I'll include myself here, think this is a really nice version of Windows. But I kind of agree with you, I don't care about the flipping tiles. But I also think you, if you weren't writing software for Windows, you would probably be using BSD.

Steve: Yes. Well, in fact, I heard you say on MacBreak Weekly that what you like about the Mac is that it's got BSD under it. And I've said here, once I am no longer developing Windows code, I'm Mac. That'll be a happy day for me.

Leo: But the good news is, for those who are not, like Steve, developers of software for Windows, go ahead and use a UNIX version. Don't install a window manager, just use - you can make it as plain and as simple as you want. And you know what, UNIX is still the best operating system ever written, period. And going along with what you're saying here, the whole point of UNIX, and in fact Alan Kay mentioned this, was to do as little as possible.

Steve: Right.

Leo: And if you want more, you add an app.

Steve: Right. Well, and that actually follows from the original philosophy of C. C, the language, was a minimal, just a scaffolding of syntax. And it was all the libraries that you brought in that gave it the functions and made it a richer environment. So that's always been that approach.

Leo: C was designed for the purpose of writing UNIX.

Steve: Right.

Leo: Basically.

Steve: Yeah, exactly, yeah. Yeah, it was. And UNIX was rewritten from PDP-11 assembly language in C as its first task.

Leo: To your point, the less the operating system does, the easier it is to secure it.

Steve: I think that's correct. Now, what we have, my take on Windows 10 is that this represents sort of a philosophical change from, now, maybe 8 already had this, and I never really looked at 8 closely because it was so clearly...

Leo: Oh, it was horrible.

Steve: ...the wrong thing.

Leo: Yeah, it was a horrific UI.

Steve: So we sort of, we have a relationship with Microsoft, with the new Windows, much like users of Apple ecosystem and Google ecosystem have, where there's a set of services which are now becoming desired, I mean, they're available. They are a function of the connectivity we have, the bandwidth that we have, the incredible amount of inexpensive cloud-based storage that we have, the crypto security technology, which everyone who does these things brings to bear, where it's now about being connected and being mobile and being multiple device and having things synchronizing among themselves. And of course we know that one of Windows' claims to fame is that it is a single OS which is multiplatform in terms of scaling platform. The same thing runs on your laptop. It's touch-enabled, and it can also run on a Windows phone, if anyone ever buys one of those.

Leo: It's getting harder and harder.

Steve: All connected. So with that connectivity comes consequences on privacy. And we've spent lots of time talking about Apple's privacy agreement and how they support, you know, can they actually not decrypt iMessage and those sorts of things. We've talked lots about Google privacy and what Google is doing and the ways in which they're monetizing us. We know that, when we're using Gmail, Google is looking at the plaintext of the mail and using that in order to produce email context-aware ads. I mean, that's part of the deal with Gmail.

And so, again, not knowing anything about 8, what I see as the big change, and this is a sea change, certainly from XP, and even from everything I've seen of 7 - because all my new machines are 7. I'm not in front of one now. But like, you know, Skype is running on Windows 7. I was playing with Media Center for a while on Win7. And Windows 7 is what I would use now, setting up any new machine. And I'm just in front of XP because I don't want to set up a new XP machine right now because that takes a lot of time to get it working.

But so this to me represents Microsoft doing the same as Google has done and as Apple has done. That is, wanting to play in the same ballpark. Which means with that comes a whole bunch of features which have never been in Windows before at this level. That is, like in the OS, without any applications installed, just the operating system itself is - it's cloud aware. It's connectivity aware. It's an account with Microsoft. We never had an account with Microsoft. I had a username and password on my operating system. Now Microsoft magically logs me in when I log into them, into the cloud.

So this is, to me, this is a huge change. I think it is future looking. I mean, this is, I think, what most people look for. It's like, oh, look, now I have in Windows these sorts of things, social networking and connectivity and all that. And so I don't think that's evil. I mean, I don't think any of this is evil. And in fact what Microsoft has done has been to be very transparent. But the other thing they've done is enable it all. And that's, if there's any controversy, it's that if you choose the Express Install - and you don't have to. And my advice to anyone who's concerned is not to use Express Install.

So my number one recommendation when installing Windows 10 for your first time - and it's not like these settings can't be changed later. But don't use Express Install. Express Install doesn't ask you any questions and just turns everything on. I mean, with the exception of location services. And I was impressed that that was off by default. That's the one thing that isn't on. The rest is. And we'll run through that, like what "the rest" means here in a second.

Leo: And if you did Express Settings, which I did because I wanted to get going as fast as you can, you can go back and step through these. I mean, it's hard...

Steve: Absolutely.

Leo: It's hard to find them all. But you can totally do that.

Steve: Yes. They're all there. And, okay. So I think what Microsoft has also done is, yeah, they're under Privacy. There's 13 pages of settings.

Leo: Oh, hi-yo. Hey, hey.

Steve: Under Privacy.

Leo: Okay.

Steve: Yup. But so what Microsoft has done, I would argue, they may have leapfrogged, well, first of all, Microsoft is in a slightly different position than Google, although to the degree that our experience is now the browser, and Chrome is Google's browser, and Google has all these browser-based services, people have already said, you know, the browser is the operating system. I mean, it's like that's - they're in the browser. You can now do whatever you want. You can do word processing. You can do spreadsheets. You can do social networking and mail and messaging and everything.

So what Microsoft has done is to integrate all of this stuff deeply into the OS so that, for example, traditionally, when we've been talking about tracking, we've been talking about cookies or Panopticlick-style browser fingerprinting, or using the browser's cache in different ways, or ETags, you know that was sort of the focus was, okay, here's a user on this browser. And the things they do are, as they move around the Internet, thanks to third-party content which websites are putting in, sometimes for their analytics, sometimes in order to offer ads or whatever, are identifying these people to different degrees. Microsoft has been absolutely upfront with the fact that they have something new called an advertising ID, which is uniquely assigned to each user on a device. And, yep...

Leo: That's right there, the very first privacy setting.

Steve: Yup. The number one thing that you see is it explains that this is what it is, and you can turn it off, if you don't want that. And they also explain that there will be some features which no longer function if the advertising ID is turned off. Now, as is always the case, it's going to take us a while to deeply understand this new thing. So when they say that that ID can be used by third parties, such as app developers and advertising networks, for profiling purposes, I'm not sure what that means. Again, I'm not using Windows 10, so no one's going to make me do this.

And so the reason I want to explain it is that, from what we're being told, and again Microsoft is upfront about it, this is a single ID, which to me seems very powerful. Apparently apps that you run can query for it, and advertising networks, and Microsoft's own advertising network I know for sure is able to use it. It does give a different ID for each user on the device. So that's sort of a good thing. There was always this concern about, well, what if multiple people use the same browser? Then you're not actually tracking individuals, you're tracking the browser, and that's not the same as the person.

I guess if you are logging off and logging into different sessions on the same machine, certainly then you would have per-user browser experiences. And so then you get this. But Microsoft is clear, this advertising ID is for each user on a device.

Okay. So there's that. And you can turn it off. It is on by default if you use Express Settings. The other concern is, again, part of convenience and helping people not hurt themselves, I think, and that is that the BitLocker whole drive encryption recovery keys are backed up into your Microsoft OneDrive account.

Leo: Now, by the way, this is not available on Windows 10 Home.

Steve: Okay, not in the Home version.

Leo: Only in the Pro and Enterprise versions is that true.

Steve: So BitLocker itself is not available?

Leo: Yeah, that's correct.

Steve: Okay. Right. And so there have been, you know, people have written whole columns about how horrible this is that your whole drive encryption keys are being sent to Microsoft. I read one account that said "in the clear." And it's like, well, they have to be because they need to be usable. And presumably you forgot what the password was or lost your keys or something. So, yeah. But, again, I think for what it is, BitLocker protects you if your laptop is stolen at the airport, so that nobody else is able to access the contents of your local hard drive.

It doesn't provide the same class of TNO protection that using a third-party whole drive encryption would, where you are a hundred percent responsible, and you'd better not lose your keys, or you're completely out of luck. Here, Microsoft is saying, we're going to encrypt your drive, and we're going to make sure you don't lose the contents of your drive by losing your keys. So we're going to back them up to OneDrive. I haven't dug into this to see whether that uniquely can be turned off. But that was one of the other things that I saw. And it's like, yeah, well, this is the sort of tradeoff that to me makes sense.

Now, there's been a bunch of confusion about WiFi Sense. Really, some over-the-top writing about this. And my complaint is only that you don't have to-the-individual granularity because it turns out that what we first thought, when this first appeared, it looked like it was enabled by default in a way such that people in your, what is it, three, it's Skype, Outlook, and Facebook, your friends, your contacts that you have there would automatically be connected to your network or any network that your computer knows about, your Microsoft account knows about, just when they approach that network. What people missed was that it needs to be enabled per network, and it is not enabled per network by default. So while WiFi Sense itself, that is, sort of the umbrella service is enabled, and the sharing is enabled, you need to deliberately say, I want to share my home network or my work network or whatever network that my machine knows about. You need to explicitly enable that.

Now, again, the problem we still have is that when you do that, you can't control to whom. That is, it's all of your Facebook friends. It's all of your Skype contacts and so forth. And I'm hoping that we'll see that change. I imagine, you know, this is v1, and one of the appealing things about Windows 10 is that they're promising not to strand people, like I am stranded now on XP, unwilling to invest in completely setting up a brand new system from scratch. They're saying that maybe they'll stop calling it 10 after a few years because that'll just be, well, there's not going to be any 11 or 12 or 13. We're just going to roll features forward because we're not longer charging and making this a profit center. Well, it is a profit center in a different manner, probably. We're not charging people to upgrade from one operating system to the next, so might as well just give them features as they're ready, in rolling service packs. Which, again, I think is an appealing idea because I wish they were doing that for my operating system. But anyway.

So for what it's worth, I'm hoping that what we'll see is the ability to select from your contacts the people who you wish to share your WiFi password with, rather than it just being everyone on a given network or no one, because I think that would be a nice enhancement.

Okay. So number one recommendation for people who are interested in getting control or having control is, if you install or when you install Windows 10, don't use Express Settings. In which case you will be taken through all of the things that you can later look at separately. But this sort of, you know, for the purists among us, you know, there are people, for example, who put whole drive encryption on a blank drive before they start using it because they feel better never having written in plaintext to that drive. It's always been encrypted. So when they blast the password off of their whole drive encryption volume, there's never been any sector relocated that had some plaintext in it, for example. So for someone who wants to, like, start off with Windows 10 locked down the way they want it locked down, the secret is don't use Express Install.

So if you use Express Install, or if you've already got it installed, everything you need is either in the 13 different pages of the Privacy section under the Settings menu, or Settings dialogue, or in links that shoot off of that. So, as I mentioned, this first page, the so-called "general privacy settings," allows you to disable, completely disable the advertising ID. So it's on by default, presumably; and I also, I wanted to get the experience most users have, so I deliberately did an Express Install, and so I have not yet taken Windows myself through the step-by-step non-express. But I imagine one of the things that they ask you is do you want to enable the advertising ID which will be made available to other apps on the platform and advertising partners and Microsoft themselves. That you can turn off, and it will erase it from existence if you turn it off.

Also under Privacy General, one of the things that has sort of annoyed people is the option, the second option reads "Send Microsoft info about how I write, to help us improve typing and writing in the future." So this has been billed as, you know, keystroke logging.

Leo: It's a really weird setting. I don't even know what that means. To improve typing and writing in the future?

Steve: Yeah, I know. And in fact, some of these are worrisome. Not that I want to be paranoid. It's just it would be nice to know what they were actually doing.

Leo: Yeah. They haven't documented them very well, that's the problem.

Steve: Right. And so this is what I meant when I said it's going to take us time to learn this big new thing. What exactly do they mean? Now, one of the things that they've done is this is Windows for the first time has Cortana, which is a system very much like Siri or Help Me Google or maybe Alexa over on the Amazon side. It's the assistant which wants to be as prescient as it's able to. And it wants to do the best job it can. So much of what the scarier stuff of, like, that we'll get to here in a second is arguably all of the sensors which Cortana is aggregating from so that when you ask her to call somebody, you've given her access to your contacts, and maybe you were recently in Contacts and looking at that person, and so you've made her...

Leo: Maybe that's it. But we don't know.

Steve: Yeah, you've made her job a lot easier because we know that she is watching what you do as you use Windows. And there's more detail about that in a minute. But so this, yeah, the second setting, send Microsoft info, we don't know what info, about how I write to help us improve typing and writing in the future. Okay. I don't use semicolons enough. I don't know. So...

Leo: Well, it could be an autocorrect thing. I mean, we're used to that with keyboards, for instance.

Steve: Yes, yes.

Leo: SwiftKey does that, for instance, for predictions.

Steve: Right.

Leo: But as far as I know, I don't see any predictions in Windows, unless they're talking about Edge. Maybe - part of the problem with this is this could be specifically for Edge's autocomplete. But it doesn't say. And I wish it would say.

Steve: Right. So...

Leo: By the way, I leave all this stuff on. So I'm just the - I'm the anti-Steve. I'm the opposite.

Steve: Yeah, yeah. And again, I'm not, first of all, like I said, no one's making me use this.

Leo: Right.

Steve: So mine is offer than off because I'm not getting near this thing.

Leo: I read that, and I thought, that is a strange sentence. And, you know, I can see why people would be a little nervous about that.

Steve: So let websites provide locally relevant content by accessing my language list. It's like, okay. So browsers have a query header which tells them what the language is of the operating system. So maybe, I don't know, if you have more languages listed, I mean, let websites provide.

Leo: That's already happening with Google. When I was in Germany, Google decided that I should read things in German.

Steve: Okay.

Leo: So that's a feature a lot of browsers do. By the way, I think we've figured out what that writing thing, at least one potential use. The touch keyboard, the onscreen keyboard does do autocorrect, does do predictions.

Steve: Ah, nice.

Leo: So in order to do that, Microsoft would in fact have to learn about what you're typing. It would also need to know where you are to appropriately recommend in the language that you use. I mean, it could be as benign as that. But because they don't tell you, we don't know.

Steve: So, well, okay. And again, yes. And all of these services, like Siri and Cortana and Help Me Google, they're all about the cloud. So once upon a time, autocorrect could have been done locally. You'd have a dictionary, and it could learn. But then that wouldn't necessarily automatically translate to you typing the same thing on your laptop. And so this is all glued together through the cloud.

Leo: Incidentally, there is, in the Microsoft EULA, an explanation, thanks to CLTSteve in the chatroom. Microsoft says: "We collect your typed and handwritten words to improve character recognition and provide you with a personalized user dictionary and text completion suggestions. Some of this data is stored on your device; some is sent to Microsoft to help improve the services. You could turn it off in the settings."

Steve: Yeah, yeah.

Leo: So, yeah.

Steve: Yeah, I mean, so again, I don't think any of this...

Leo: It's not a keystroke logger.

Steve: No, exactly. Well, it is.

Leo: It is, but it's not a nefarious...

Steve: But they're saying, "Look, this is what we're going to do." And this is my point. There's nothing being hidden here. And I think Microsoft has been the victim of, like, all kinds of lawsuits over the years. They know they want to do this. And so what they're saying is, okay, don't use Express Install, and we'll walk you through making these decisions. Do you want this or not? So what they're doing is completely open. Nothing underhanded. And so that allows people to decide do I want that feature or not. Am I creeped out by having Microsoft monitoring what I'm typing? It's like, probably not. I think most people would rather have Microsoft fix their typos for them.

Leo: Yeah. At least, you know what, I have to say, at least they surfaced this.

Steve: Yes, yes, exactly. And here they're not bogging us down in details. I think that the license agreement is 12,000 words, I read somewhere.

Leo: Yes, that's correct, yep.

Steve: So, you know, if you really want to know what these things mean, you'll have to sit down and read. But it's there. I mean, I'm sure Microsoft is telling us what they're doing.

The fourth item there is manage my Microsoft advertising and other personalization info. This has gotten a lot of concern, only because it takes you - it's not local. It takes you to Microsoft, to choice.microsoft.com/ in my case en-gb/opt-out.

Leo: Wait a minute, wait a minute. Yours is en-gb?

Steve: Yeah.

Leo: It should be en-us. You're in Great Britain. See, you turned that feature off, didn't you. That's why it wants to know where you are. It's going to spell everything with a "U" now. Don't you care?

Steve: Actually, I think I pulled this off of one of the...

Leo: Oh, a British site, okay.

Steve: Off the British site.

Leo: Mine says "us."

Steve: Okay.

Leo: By the way, some of this is mandated by - we got bit by this - the Ad Bureau, and a consent decree they had with the Federal Trade Commission. We got a certified email and some serious threats about our website because we didn't have the AdChoices verbiage on there. And you've seen this around. And this is the advertising, online advertising industry's attempt to self-regulate so, heaven forfend, the government doesn't regulate us. And we actually, they threatened to turn us in to the FTC if we didn't actually put the verbiage that they specified on our web page. So we did.

Steve: Yeah.

Leo: Even though we collect no tracking information about you at all. But that doesn't matter.

Steve: Okay. So, yeah. So on this page, this web page...

Leo: This is what that is.

Steve: Yes.

Leo: Because you see that logo with the green triangle? That's the AdChoices logo.

Steve: Yeah, sort of the sideways pointing green triangle.

Leo: Yup, yup, yup.

Steve: So the first thing is "Personalized ads in this browser." You're able to say, no, I don't want those. And then "Personalized ads whenever I use my Microsoft account." And they mention that also includes Windows, Windows Phone, Xbox, and other devices. However, I will say to people, if you turn this off, check back in a day because there have been reports for it not being sticky, that it sort of - people have reported that they've gone back, and it's turned itself back on again. And these were prerelease reviewers, so this may have been a bug that has since been fixed. But just a little tip for our interested users.

Leo: Just so you know, we do it here. See that? Privacy Policy and AdChoices.

Steve: Nice.

Leo: And they were going to report us to the FTC if we didn't have that right on the front page that tells you...

Steve: Who is "they"? They, the advertising people?

Leo: Yeah. Ironically, it's a group funded by Google and Yahoo! and all the ad people. And it's because of an FTC, I'm convinced it's probably an FTC consent decree. No, no, no, we'll regulate, we'll self-regulate. And, but, you know, threatening letters. And believe me, if you go to our site compared to a hundred other sites, we're not exactly swamping you with tracking material.

Steve: No, no.

Leo: Anyway, but you know what, I was glad to do it because we do want people to know. It's the digital, just so you know, Digital Advertising Alliance Self-Regulatory Principles. And if you go to AboutAds.info, you can read all about it.

Steve: Very good. So that's...

Leo: And I think that's what Microsoft's doing. It's got an opt-out for the whole thing.

Steve: Yes. So that's the first tab.

Leo: We've only just begun.

Steve: Okay. I'm keeping my eye on the clock. But the second one is location. Now, the way these are organized is also nice. There's generally, on most of these things, where there are sort of like app-level granularity, they provide a global enable/disable, and then a per-app setting, so that you're able to - and we've seen this on our mobile devices, for example, when we're able to specifically allow and disallow things. So for me, it defaults to on. So location services is globally for all users on the machine. But I was impressed that the individual apps were all off on mine. I hadn't turned any of them on. So I thought, okay, that's nice. I'm not quite sure why that's the case, but it was. It was the only area where there were, like, things Microsoft was denying itself preemptively. And it looks like yours is the same way, Leo.

Leo: Yeah, and I did Express Settings.

Steve: Yeah, as did I.

Leo: They default, I guess, to off.

Steve: Yup. So that's one thing you've got to explicitly say "I want to turn on location services."

Leo: My guess is it's per app. This is how most mobile devices do it, where when an app wants it, it asks you.

Steve: Yup.

Leo: And then, if you say yes, it'll turn it on.

Steve: Right.

Leo: That would be my guess. All of these are Microsoft apps, as far as I can tell.

Steve: Yeah. And mine, too, because I haven't put any third-party stuff in yet.

Leo: In Cortana you can't turn it off. You can't turn it off.

Steve: Yeah, we're going to know where you are, suckers.

Leo: It says, "Location history must be on for Cortana to work." You'd have to turn Cortana off.

Steve: I have to know where you are, Leo.

Leo: I can't help you, Leo, if I don't know exactly where you are.

Steve: Now, the next tab is Camera, which defaults to on. And I had four apps, and they're all defaulted to on, too. You've got a lot more than I do.

Leo: Yeah, probably because I've given them permission at some point; right?

Steve: I don't know what MSN Food & Drink is, and why it needs to look at me or have the camera on.

Leo: Well, I don't know either. Let's find - there it is. Food and drink, hmm. Oh, god.

Steve: I am going to [crosstalk] my operating system.

Leo: Maybe it wants to take a picture of how fat I am or something. I don't know. That's interesting.

Steve: But what is that?

Leo: Oh, it's one of - they have a whole bunch of Hubapps that they created for Windows Phone, I think initially. And then later...

Steve: No, I mean, what was that thing? It looked like a weird pizza puff kind of thing.

Leo: It's sure to be wholesome.

Steve: I had four things. I had App Connector.

Leo: Yeah.

Steve: And App Connector shows up a lot, and I've never had a...

Leo: I have that, too.

Steve: I didn't have a chance to figure out what the heck that is. But, you know...

Leo: Turned that off. I'm sure it'll ask me if it needs it ever again. Same thing with all of these. Oh, Steve's frozen. So while we're calling Steve back, I'll just take advantage of this moment to turn off the camera. Yeah. Twitter, you know, might say, oh, do you want to put a picture of you. But I don't, especially on this computer. This Dell, the camera's down here in the lower left of the screen. It's always a picture of my nose. So, in fact, why don't I just turn the whole thing off. I bet if you turn the whole thing off, apps don't ask you. If you leave it on, then apps will ask you.

Steve: So Microphone is of course on, and everybody can listen to you. Then we get to Speech, Inking, and Typing. And the interestingly labeled button is "Getting to know you."

Leo: Stop getting to know me.

Steve: And you can say no.

Leo: It's a button, it says "Stop getting to know me."

Steve: It does. And so under "Getting to know you" title, it says: "Windows and Cortana can get to know your voice and writing to make better suggestions for you."

Leo: That's good.

Steve: "We'll collect info like contacts, recent calendar events, speech and handwriting patterns, and typing history."

Leo: Why not?

Steve: Yeah. And if you don't want Windows and Cortana to get to know you, you can press that button, and it will stop. Then there's Manage Cloud Info, which has "Go to Bing and manage personal info for all your devices." So they make it easy for you to go and deal with that, sort of giving you an easy-to-find portal into whatever Microsoft has. If you want to know what this is, this Speech, Inking, and Typing setting, there's a "learn more" about that, so you can do that, and a privacy statement. So this is sort of the we're watching you do stuff on your computer unless you tell us not to. And apparently there's a nice video that talks about, you know, shows you all the benefits of having Windows know you.

Leo: One point that one of our chatters made, which is a very good point, is these are all, like the food app, universal apps. They're designed to work on mobile as well as on desktop, and on your phone as well as your tablet as well as your desktop. So these are kind of settings that are universal to Windows 10. Windows 10 now is Xbox, Windows Phone, tablets, desktops, laptops. So it makes sense that they're going to have a broader range of settings, some of which make more sense on mobile.

Steve: Correct.

Leo: Location of my desktop is pretty much fixed. Right?

Steve: Well, no, unless you've got that lever that raises and lowers it.

Leo: Well, I can go up and down. But it's not moving to Denver anytime soon.

Steve: So under Account Info, we have "Let apps access my name, picture, and other account info." Defaults to on. And then there is app-level granularity. I didn't have any.

Leo: Me, neither.

Steve: But it says choose the apps that can access your account info. So as you install apps, exactly as you say, Leo, where the app says, we'd like, you know, permission to access your account info, your name, your picture, and other stuff, you'll probably say yes or no, and that list will get populated. Unless you globally say no, I don't want any of that for any apps. In which case it's globally disabled. So I like the fact that they've got this global permit, and then per-app granular management. I think that's the right thing to do this.

And then management of contact information: Choose apps that can access contacts. I had the App Connector again, Mail & Calendar - makes sense that it could access my contacts - and the Windows Shell Experience, which is flippy tiles, I guess, who knows. It wants to access my contacts, too, for some reason. Maybe so they can show me whose birthday is coming up. Calendar is the next tab. And so basically this controls whether apps are able to access your calendar. Defaults to on. And then App Connector is there again, and Mail & Calendar, not surprisingly. We need to access your calendar. So that provides that granularity.

Messaging: Let apps read or send messages, text or MMS, defaults to on. And once again, app-level granularity over which ones you can do. And I had none, but I see you've got two there.

Leo: App Connector. Wait a minute. You've gone on to Messaging.

Steve: On Messaging.

Leo: Yeah, I don't have any, either.

Steve: Yeah. Okay, you don't have any yet. So apparently apps have access to - and this is, again, exactly as you were saying, Leo, this is a perfect example of something that makes much more sense in a mobile environment than on a desktop.

Leo: Well, here's an example. On Android and iOS, if you install WhatsApp, I presume on Windows Phone, too, WhatsApp sends itself a message to verify your phone number. And in order to automate that process, it needs a permission to read incoming text messages. That's the kind of thing. So if I installed WhatsApp, I'm betting this suddenly would have a checkbox here.

Steve: Yup. Control over your radios is next. Some apps use radios like Bluetooth in your device to send and receive data. Sometimes apps need to turn these radios on and off to work their magic. This has been a sore point with a number of people who follow me in Twitter, and we've talked about it, how iOS always tends to turn Bluetooth back on whenever you upgrade.

Leo: That's for the beacons, I'm sure, yeah.

Steve: It's like, no, darn it. So again, this defaults to on. You can globally turn it off or control individual, give individual apps permission to turn on and off your device's radio settings.

Leo: And we should also be clear, when we say "default," we mean if you choose Express Settings.

Steve: Correct.

Leo: We're looking at mine, which is Express Settings.

Steve: And mine, which was same thing.

Leo: If you don't choose Express Settings, you're walked through each one of these settings; right?

Steve: Right, right, right. And, you know, and get to decide what you want to do.

Leo: Right. Which, you know, I have to - I think that's good. Personally, I leave all this stuff on. It doesn't bother me. But I think it's good they give you the choice.

Steve: Yes. And again, Microsoft is being, I would say, transparent and deep.

Leo: Yes.

Steve: Deep and transparent. Sync with devices is on, on the Other Devices tab, which is described as "Let your apps automatically share and sync info with wireless devices that don't explicitly pair with your PC...

Leo: Oh, that's - hmm.

Steve: Yeah, with your PC, tablet, or phone. And the example they give is beacons.

Leo: Ah.

Steve: So, you know, something that's there that, like, wants to ping you, and you'd like beacon functionality. So it's like, yeah, okay, fine. And then again, app-level granularity. Once there are some apps that can do that, you're able to enable, presumably, permit them over time and then also manage them on this 13-page privacy settings dialogue. Finally we get to - we're almost done - Feedback & Diagnostics, which is - and this is weird, too. Feedback & Diagnostics. So under Feedback Frequency is "Windows should ask for my feedback," dot dot dot. And the default I had was "automatically." That's what's recommended. But you can also say "always." So I want Windows to always ask for my feedback?

Leo: No.

Steve: Or once a day, once a week, or never. And so maybe Cortana - this reminds me of the little Clippy, jiffy clip, you know, filling out...

Leo: How you doing? Is it good? Do you like it? What do you think? What do you think?

Steve: Oh, my lord. So I don't know what, I mean, I'm tempted to turn it off.

Leo: I'm setting that to never. I don't - yeah. But what's not clear is does that mean that no feedback will be sent, or it won't ask me?

Steve: Yeah, it's "Windows should ask for my feedback," dot dot dot. And so you could say I don't ever want Windows asking for my feedback. I mean, I don't know what it, I mean, I'm tempted to say "always," just so that I can see...

Leo: Well, let's see what happens. Yeah. All right. Then we'll at least get some idea of what it's asking for.

Steve: Yeah. Next tab is Background Apps. And so this is let apps run in the background. Microsoft explains: "Choose which apps can receive information, send notifications, and stay up to date, even when you're not using them. Turning background apps off can help conserve power." Once again, this is more something a battery-running user might be concerned about. But my list, they were all on by default, as are yours, Leo. And so the list is alarms and clock, would make sense to have that running in the background, certainly. I don't know why food and drink wants to run in the background.

Leo: It wants everything. It's very demanding, yeah.

Steve: Maybe it's worried about getting thirsty. Groove music; health and fitness; mail.

Makes sense to run mail in the background. Maps, for tracking you or knowing where you're located. The browser, Microsoft Edge, wants to run in the background. One Note. People, there's a people app. I don't know what that does, but that wants to run in the background. The phone companion, that sounds good, if you have a phone. Photos, store, weather, and Xbox. Which I'm sure is the Xbox remoting streaming thing that you and Paul have talked about.

Leo: Right.

Steve: Last tab is - that is the last tab. Oh, I had separate notes about Cortana because, again, that's stirred up people, I think, needlessly. Again, in order for Cortana to work as well as Siri does, I mean, Siri is also looking at all your stuff in order to get context, in order to know, like, when you say "Call somebody," she needs access to your contacts list and to look through the names in order to figure out who you're referring to.

Leo: This is good because, I'll tell you what, in the example they say, "When is the next Seahawks game?" I don't ever want to know when the next Seahawks game is. So fortunately, she at least knows enough not to tell me there's a Seahawks game coming up. She would tell me when the Giants and the Niners games are coming up.

Steve: However, now that we've turned "Ask me always," Windows may ask you how you like seeing Seahawks games.

Leo: How do you like the Seahawks? How are you liking them? You like those uniforms?

Steve: Yeah. So in some of the boilerplate I found, they've explained. Under Cortana, it says configure what you need. Or, no, I think that's my advice, configure what you need. By default, Cortana has visibility into pretty much everything in order to improve performance.

Leo: You want a long list of things? Look at the Cortana interface and its notebook, what things it knows about me.

Steve: Yes.

Leo: Wow.

Steve: So location, location history, contacts, search history. Again, Cortana has your search history. Calendar details, content and communication history from messages and apps, and any other information on your device.

Leo: Knows when my packages are coming.

Steve: So basically you're saying, in order to get this functionality in the watch-everything-I-do version, just leave this all on. And also Microsoft explains that, in Edge, their browser replacement of IE, Cortana collects and uses your browsing history. And I was talking about search history before. So from the Privacy Agreement, Microsoft says: "To enable Cortana to provide personalized experiences and relevant suggestions, Microsoft collects and uses various types of data, such as your device location, data from your calendar, the apps you use, data from your emails and text messages, whom you call, your contacts and how often you interact with them on your device.

"Cortana also learns about you by collecting data about how you use your device and other Microsoft services, such as your music, alarm settings, whether the lock screen is on, what you view and purchase, your browser and Bing search history, and more." Meaning, you know, everything. Now, I have survived until now quite happily without any of this. And I'm going to continue to do so.

Leo: Your loss, Steve. That's all I'm saying. Your loss.

Steve: And the last thing I had in my notes was the issue of whether you choose to tie your local Windows account into your Microsoft account.

Leo: Right.

Steve: And so some of the advice I've seen online suggests, and this is done by default, that is, it says, oh, log into your Microsoft account, and I did, because I've been a developer for decades. And then when you log into your computer, suddenly it was asking for my Microsoft account login at my login screen, rather than the password that I had just assigned to that machine. Which was like, whoa, what?

So again, you may wish to remove your Microsoft account from Windows 10 and use a local account instead. If you do, then you're not logging into Microsoft at the same time as you log into your machine. And so you lose the synchronization features which you would otherwise have. But under Settings/Accounts, we just went through Settings/Privacy and all the subtabs. Under Settings/Accounts, you have complete control over this. You can easily go back and forth to experiment with it. So again, it's not like you're locked in forever. You get to choose.

So that's it. As I said, I think this is - it's deep penetration into, essentially, your entire experience of using Windows, but it is also transparent. Microsoft wants the depth to provide you services, to provide the set of features that are now becoming expected, the sort of things you get when you're in the Googleverse, or when you're in the Apple ecosystem. This is now put into the base OS platform, and the user has control of it. I'm just going to stay with Windows 7, as far away from this as I can.

Leo: But like I said, if you had your druthers, you'd just have a command line, little C prompt and a blinking cursor.

Steve: And in fact, I heard someone tell you, I think it was maybe one of your Mac guys, maybe it was somebody on - I don't remember where. But they launch apps just by being in the search and typing the first few characters.

Leo: I do, too.

Steve: Yeah. I mean, like that's better than browsing through a big growing tree of applications.

Leo: You can do that on Mac and Windows.

Steve: Yes.

Leo: Which is nice. You just type the first few letters and hit return, and boom. Boom.

Steve: Yeah, I have a simple - the first layer of my Start Menu. A Start button, and then there's everything right above it that I typically use. And for the things I use less, I have a nice hierarchy I drill down into. And so, you know...

Leo: You're going to like Windows 7 in about five years, when Donald Trump leaves office, because it has that feature built in. All you have to do - and Windows 8 and 9, 10 as well.

Steve: Oh, in fact you have to have a keyboard with a Windows key, though, don't you.

Leo: Yeah, you hit the Windows key, and you start typing, W-O-R-D, and then you hit return, and you've got WordPad.

Steve: Nice. Nice.

Leo: So, yeah, yeah.

Steve: So there we have it. Again, we needed to do a podcast to talk about this because privacy is of big interest to our listeners. And I would just say, when you're setting up Windows 10, now you know what's there. Don't use Express Settings. Walk yourself through this, and tune this the way you want. Or just say no to Windows 10. And you can use Windows 7 until 2020 with me.

Leo: Join the Unabomber in his cabin. Well, that's why this show is so great. We've got you, and we've got me. And between the two of us somewhere, you know, you could take your pick.

Steve: Yeah.

Leo: Steve always - because, see, I never saw technology I didn't like and turn on and say yes to. And I always want to use the newest, latest version of everything.

Steve: Yeah, and that just sort of seems unnecessary to me. It's like, eh.

Leo: Eh.

Steve: I mean, when I build this new machine, it's going to scream on Windows 7.

Leo: It is.

Steve: Because there won't be any of this nonsense with tiles flipping around.

Leo: Absolutely. Yeah. Steve is - you can find him at his lovely modern website, GRC.com. Minimal JavaScript; right, Steve?

Steve: None.

Leo: None. Zero. Don't even worry. No trackers, nothing. You can examine it with Ghostery till the cows come home, you'll never find anything on there. But you will find SpinRite, the world's best hard drive and maintenance utility. You will find lots of free stuff, including SQRL and Perfect Paper Passwords and all sorts of great stuff. You will find this show, 16Kb audio, too - no one else has that - as well as the transcripts from Elaine - no one else has that - the full show notes, and all of the stuff you need at GRC.com. Maybe questions next week.

Steve: Yes. Well, that's post-Black Hat.

Leo: Oh, maybe not.

Steve: So...

Leo: No questions. Hold your questions. If you have a question, GRC.com/feedback is the feedback form. You can also tweet Steve. He's @SGgrc. And he definitely is now engaged in the Twitter.

Steve: I am.

Leo: Next we're going to get him on the Facebook, and he's going to be soaring with the eagles.

Steve: No. Facebook and Windows 10 go together.

Leo: I think he's probably not going to use either of those, yeah. We have audio and video of the show at our site, TWiT.tv/sn. Can't promise you a JavaScript-free environment, however. You can also use your favorite podcatcher. This show is everywhere. You can even dial, what was it, 407? You can phone us in.

Steve: Don't bother.

Leo: You can also watch live, if you want. We do the show every Wednesday, 1:30 Pacific, 4:30 East - I'm sorry, Tuesday, 1:30 Pacific, 4:30 Eastern, 20:30 UTC on TWiT.tv. And we love it when you're in live, and I've been interacting with the chatroom, and we've been having fun, too.

Steve: Yup.

Leo: Thank you, Steve.

Steve: I will see you on Saturday for The New Screen Savers.

Leo: Oh, yes. Tune in, everybody.

Steve: That'll be our first post-Black Hat and DefCon confab. And then I have no doubt there were some really interesting, spooky, scary things.

Leo: Mm-hmm.

Steve: That are just - they're teasers in the Black Hat program. And it's funny, too, because I was on TWiET with Father Robert and Mark Smith and a couple others, and they were saying they love to go. And I said the problem with going is that all the good things are happening at the same time.

Leo: Yeah, yeah.

Steve: And I actually saw people tweeting, like in fact Matthew Green is there, our Johns Hopkins cryptographer. And he tweeted that four different topics, all of which he wanted to see, were at the same time. So I rest my case. I can do a better job staying here getting work done, and then sweeping up the debris after we see what these things actually are.

Leo: Actually, Robert agrees with you. He says he just goes for the social. He doesn't even attend any of the tracks. He sits in the lobby, talks to people. Because everything's on video. At Black Hat, anyway, everything's on video after. Or is it DefCon? At DefCon everything's on video after the fact, so you can always - you're not going to miss anything. You can always watch it later.

Steve: Right.

Leo: Ah, Steve. Thank you so much. We'll see you next week. Actually, we'll see you Saturday for The New Screen Savers.

Steve: Saturday, and then next week for our post-DefCon/Black Hat. And then we'll probably do a whole bunch of Q&As in order to catch up with those because we haven't been doing enough.

Leo: I'm sure there are a few.

Steve: Thanks, Leo.

Leo: Thanks, Steve.